NIFTeTRUST Trust Network (NTN)

Certification Practice Statement

Version 5.3.0

April 14, 2023

NIFTeTRUST
Business with Trust

NIFT (Pvt.) Ltd.
5th Floor, AWT Plaza, I.
I. Chundrigar Road,
Karachi, Pakistan.
009221-111-112-222
www.niftetrust.com

Published date: April 14, 2023

Trademark Notices

Contents

1 INTRODUCTION

This document is the NIFTeTRUST Trust Network (NTN) Certification Practice Statement ("CPS"). It states the practices that NIFTeTRUST certification authorities ("CAs") employ in providing certification services that include, but are not limited to, issuing, managing, revoking, and renewing certificates in accordance with the specific requirements of the NIFTeTRUST Trust Network Certificate Policies ("CP").

The CP is the principal statement of policy governing the NTN. It establishes the business, legal, and technical requirements for approving, issuing, managing, using, revoking, and renewing, digital Certificates within the NTN and providing associated trust services. These requirements, called the "NTN Standards," protect the security and integrity of the NTN, apply to all NTN Participants, and thereby provide assurances of uniform trust throughout the NTN. More information concerning the NTN and NTN Standards is available in the CP.

NIFTeTRUST has authority over a portion of the NTN called its "Sub-domain" of the NTN. NIFTeTRUST Sub-domain includes entities subordinate to it such as its Customers, Subscribers, and Relying Parties.

While the CP sets forth requirements that NTN Participants must meet, this CPS describes how NIFTeTRUST meets these requirements within NIFTeTRUST Sub-domain of the NTN. More specifically, this CPS describes the practices that NIFTeTRUST employs for:

- securely managing the core infrastructure that supports the NTN, and
- issuing, managing, revoking, and renewing NTN Certificates

within NIFTeTRUST Sub-domain of the NTN, in accordance with the requirements of the CP and its NTN Standards.

This CPS conforms to the Internet Engineering Task Force (IETF) RFC 3647 for Certificate Policy and Certification Practice Statement construction. CAs within the NIFTeTRUST Trust Network hierarchy conforms to the current version of the CA/Browser Forum (CABF) requirements including:

- Guidelines for the Issuance and Management of Certificates, and,
- Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates,

In the event of any inconsistency between this document and those Requirement, those Requirements take precedence over this document.

1.1 Overview

This CPS is specifically applicable to:

- NIFTeTRUST Public Primary Certification Authorities (PCAs),
- NIFTeTRUST Infrastructure CAs, and NIFTeTRUST Administrative CAs supporting the NIFTeTRUST Trust Network
- NIFTeTRUST Public CAs and the CAs of Enterprise Customers, who issue Certificates within NIFTeTRUST sub-domain of the NTN.

More generally, the CPS also governs the use of NTN services within NIFTeTRUST sub-domain of the NTN by all individuals and entities within NIFTeTRUST Sub-domain (collectively, NIFTeTRUST Subdomain Participants") including NTN CAs managed by NIFTeTRUST. Unless specifically noted within this CPS, Private CAs and hierarchies managed by NIFTeTRUST are outside the scope of this CPS.[3]

The NTN includes two classes of Certificates, Classes 1-2. The CP is a single document that defines these certificate policies, one for each of the Classes, and sets NTN Standards for each Class.

NIFTeTRUST currently offers two Classes of Certificates within its Sub-domain of the NTN. This CPS describes how NIFTeTRUST meets the CP requirements for each Class within its Sub-domain. Thus, the CPS, as a single document, covers practices and procedures concerning the issuance and management of all three Certificate Classes.

NIFTeTRUST may publish Certificate Practices Statements that are supplemental to this CPS in order to conform to the specific policy requirements of Government, or other industry standards and requirements.

These supplemental certificate policies shall be made available to subscribers for the certificates issued under the supplemental policies and their relying parties.

The CPS is only one of a set of documents relevant to NIFTeTRUST Sub-domain of the NTN. These other documents include:

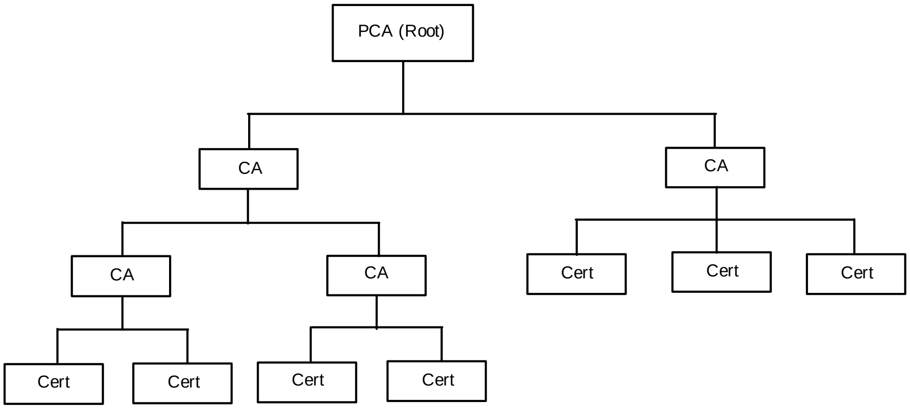
- Ancillary confidential security and operational documents that supplement the CP and CPS by providing more detailed requirements, such as:
    - The *NIFTeTRUST Physical Security Policy*, which sets forth security principles governing the NTN infrastructure,
    - The *NIFTeTRUST Security and Audit Requirements (SAR) Guide*, which describes detailed requirements for NIFTeTRUST concerning personnel, physical, telecommunications, logical, and cryptographic key management security, and
    - *Key Ceremony Reference Guide*, which presents detailed key management operational requirements.
- Ancillary agreements imposed by NIFTeTRUST. These agreements bind Customers, Subscribers, and Relying Parties of NIFTeTRUST. Among other things, the agreements flow down NTN Standards to these NTN Participants and, in some cases, state specific practices for how they must meet NTN Standards.

In many instances, the CPS refers to these ancillary documents for specific, detailed practices implementing NTN Standards where including the specifics in the CPS could compromise the security of NIFTeTRUST Sub-domain of the NTN.

1.1.1 Trust Model

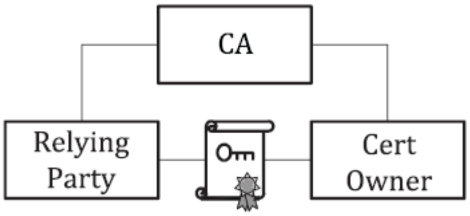
The model used by a NIFTeTRUST PKI is a strict hierarchical model or tree model. The hierarchical model or tree model is the most common model to implement the PKI. NIFTeTRUST Public Primary Certification Authorities (PCAs) at the top provides all the information and the intermediate CAs are next in the hierarchy, and they only trust the information provided by the NIFTeTRUST Public Primary Certification Authorities (PCAs)

Digital certificates are arranged in a hierarchy. Every digital certificate can be traced back to its origin—known as the root or the Primary CA (PCA). This hierarchy is called the public key infrastructure (PKI). The root of a digital certificate is traced through the hierarchy of CAs that have generated and signed them. Figure 2-2 depicts an example PKI hierarchy.



PKI hierarchies consist of CAs linked through a chain of certificates to a NIFTeTRUST PCA, a customer's private root, or a third party root (such as a government root CA). When a PCA or root issues a CA, the CA is signed by the private key associated with the PCA or root. When a CA issues an end-entity certificate, it also signs the certificate with its private key. Because these entities are signed, they can be validated with the public key. This unbroken chain of certificates—linking a given certificate to its issuing CA and ultimately to the PCA or root of the hierarchy—is what validates the CA.

Under the hierarchical trust the public key of the root CA is known to every entity. The relying party validates its trustworthiness of the root CA directly with NIFTeTRUST via CRL and OCSP services. Any end entity's certificate can be verified by verifying the certification path of certificates that leads back to the root CA. Therefore NIFTeTRUST root CA (PCA) is the first party to the relying party.



1.2 Document Name and Identification

This document is the NIFTeTRUST Trust Network (NTN) Certification Practice Statement (CPS). NTN Certificates contain object identifier values corresponding to the applicable NTN Class of Certificate as listed in section 1.2 of the NTN CP. Therefore, NIFTeTRUST has not assigned this CPS an object identifier value. Certificate Policy Object Identifiers are used in accordance with Section 7.1.6.

1.3 PKI Participants

1.3.1 Certification Authorities

The term Certification Authority (CA) is an umbrella term that refers to all entities authorized to issue public key certificates within the NTN. The CA term encompasses a subcategory of issuers called Primary Certification Authorities (PCA). PCAs act as roots of four domains[5], one for each class of Certificate. Each PCA is a NIFTeTRUST entity. Subordinate to the PCAs are Certification Authorities that issue Certificates to end-user Subscribers or other CAs.

NIFTeTRUST also operates the NIFTeTRUST Class 3 Internal Administrator CA hierarchy that is limited to NIFTeTRUST internal administrative uses.

NIFTeTRUST also operates the “NIFTeTRUST Universal Root Certification Authority”. The Universal Root CAs issue Class 3 and selected Class 2 Subordinate CAs.

NIFTeTRUST enterprise customers may operate their own CAs as subordinate CAs to a public NTN PCA. Such a customer enters into a contractual relationship with NIFTeTRUST to abide by all the requirements of the NTN CP and the NTN CPS. These subordinate CAs may, however implement a more restrictive practices based on their internal requirements.

1.3.2 Registration Authorities

A Registration Authority is an entity that performs identification and authentication of certificate applicants for end-user certificates, initiates or passes along revocation requests for certificates for end-user certificates, and approves applications for renewal or re-keying certificates on behalf of a NTN CA. NIFTeTRUST may act as an RA for certificates it issues.

1.3.3 Subscribers

Subscribers under the NTN include all end users (including entities) of certificates issued by a NTN CA. A subscriber is the entity named as the end-user Subscriber of a certificate. End-user Subscribers may be individuals, organizations, or infrastructure components such as firewalls, routers, trusted servers or other devices used to secure communications within an Organization.

In some cases certificates are issued directly to individuals or entities for their own use. However, there commonly exist other situations where the party requiring a certificate is different from the subject to whom the credential applies. For example, an organization may require certificates for its employees to allow them to represent the organization in electronic transactions/business. In such situations the entity subscribing for the issuance of certificates (i.e. paying for them, either through subscription to a specific service, or as the issuer itself) is different from the entity which is the subject of the certificate (generally, the holder of the credential). Two different terms are used in this CPS to distinguish between these two roles: "Subscriber", is the entity which contracts with NIFTeTRUST for the issuance of credentials and; “Subject", is the person to whom the credential is bound. The Subscriber bears ultimate responsibility for the use of the credential but the Subject is the individual that is authenticated when the credential is presented.

When ‘Subject’ is used, it is to indicate a distinction from the Subscriber. When “Subscriber” is used it may mean just the Subscriber as a distinct entity but may also use the term to embrace the two. The context of its use in this CPS will invoke the correct understanding.

CAs are technically also subscribers of certificates within the NTN, either as a PCA issuing a self-signed Certificate to itself, or as a CA issued a Certificate by a superior CA. References to “end entities” and “subscribers” in this CPS, however, apply only to end-user Subscribers.

1.3.4 Relying Parties

A Relying Party is an individual or entity that acts in reliance of a certificate and/or a digital signature issued under the NTN. A Relying party may, or may not also be a Subscriber within the NTN.

1.3.5 Other Participants

Not applicable

1.4 Certificate Usage

1.4.1 Appropriate Certificate Usages

1.4.1.1 Certificates Issued to Individuals

Individual Certificates are normally used by individuals to sign and encrypt e-mail and to authenticate to applications (client authentication). While the most common usages for individual certificates are included in Table 1 below, an individual certificate may be used for other purposes, provided that a Relying Party is able to reasonably rely on that certificate and the usage is not otherwise prohibited by law, the NTN CP, the CPS under which the certificate has been issued and any agreements with Subscribers.

Certificate Class	**Assurance Level**			**Usage**		
	Low assurance level	**Medium assurance level**	**High assurance level**	**Signing**	**Encryption**	**Client Authentication**
Class 1 Certificates	✓			✓	✓	✓
Class 2 Certificates		✓		✓	✓	✓

Table 1. Individual Certificate Usage

1.4.1.2 Assurance levels

Low assurance certificates are certificates that should not be used for authentication purposes or to support Non-repudiation. The digital signature provides modest assurances that the e-mail originated from a sender with a certain e-mail address. The Certificate, however, provides no proof of the identity of the Subscriber. The encryption application enables a Relying Party to use the Subscriber's Certificate to encrypt messages to the Subscriber, although the sending Relying Party cannot be sure that the recipient is in fact the person named in the Certificate.

Medium assurance certificates are certificates that are suitable for securing some inter- and intraorganizational, commercial, and personal e-mail requiring a medium level of assurances of the Subscriber identity, in relation to Class 1 and 3.

1.4.2 Prohibited Certificate Uses

Certificates shall be used only to the extent the use is consistent with applicable law, and in particular shall be used only to the extent permitted by applicable export or import laws.

NIFTeTRUST Certificates 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. Also, Class 1 Certificates shall not be used as proof of identity or as support of non-repudiation of identity or authority. Client Certificates are intended for client applications and shall not be used as server or organizational Certificates.

CA Certificates may not be used for any functions except CA functions. In addition, end-user Subscriber Certificates shall not be used as CA Certificates.

NIFTeTRUST periodically rekeys Intermediate CAs. Third party applications or platforms that have an Intermediate CA embedded as a root certificate may not operate as designed after the Intermediate CA has been rekeyed. NIFTeTRUST therefore does not warrant the use of Intermediate CAs as root certificates and recommends that Intermediate CAs not be embedded into applications and/or platforms as root certificates. NIFTeTRUST recommends the use of PCA Roots as root certificates.

1.5 Policy Administration

1.5.1 Organization Administering the Document

NIFT (Pvt.) Ltd.
5th Floor AWT Plaza,
I. I. Chundrigar Road,
Karachi – 74200
Pakistan.

1.5.2 Contact Person

Information Security Services Manager / PKI Policy Manger
NIFTeTRUST Trust Network Policy Management Authority c/o NIFT (Pvt.) Ltd.
5th Floor AWT Plaza,

I. I. Chundrigar Road,
Karachi – 74200
Pakistan.
+009221-111-112-222 Ext. 200 (Voice)
+009221-9921-3145

1.5.3 Person Determining CP Suitability for the Policy

The NTN Policy Management Authority (PMA) determines the suitability and applicability of this CPS. PMA is comprised of Information Security Services Manager (PKI Policy Manger), Key Manager and Root Authority Key Manager.

.

1.5.4 CPS Approval Procedure

Approval of this CPS and subsequent amendments shall be made by the PMA. Amendments shall either be in the form of a document containing an amended form of the CPS or an update notice. Amended versions or updates shall be linked to the Practices Updates and Notices section of the NIFTeTRUST Repository located at: www.niftetrust.com/Downloads/NIFT-CPS.pdf. Updates supersede any designated or conflicting provisions of the referenced version of the CPS. The PMA shall determine whether changes to the CPS require a change in the Certificate policy object identifiers of the Certificate policies corresponding to each Class of Certificate. PKI Policy Manager is the final authority for approving Certificate practice statement (CPS).

1.5.5 CA environmental controls

PMA is responsible to make sure that this CPS has well defined CA environmental controls, Key life-cycle management and certificate lifecycle controls.

1.5.6 Business service application with CP

PMA has ensured that CA business service application of NIFTeTRUST is using appropriate CP.

1.5.7 Termination of certification policies

PMA has approved following procedure for the termination of (Certificate Policy)

a. PMA will inform Manager PSO and CEO 60 days in advance for any such planned termination.
b. Incase of unplanned termination manager PSO and the CEO will be informed within 1 hour time.
c. Manager PSO will be responsible to inform all the customers via corporate email within 24 hrs time when he received such information.
d. All other concerned parties including any relying party will be notified via a broadcast message through NIFTeTRUST web site. NIFTeTRUST will also employ 2 well known newspapers (1 English and 1 Urdu) to broadcast this news.

1.5.8 Certificate Policy

NIFTeTRUST PMA is not responsible for its public CP and will rely on international CPs of DigiCert, Sectigo or any local CP defined by ECAC under MoIT.

1.5.9 Review

PMA shell review CPS at the end of each calendar year. However, in case of any major change request (CR) PMA may approve sub releases anytime during the current year.

1.5.9 Risk Assessment

PMA shell conduct business risk assessment once in each calendar year.

1.6 Definitions and Acronyms

See Appendix A for a table of acronyms and definitions.

2 Publication and Repository Responsibilities

2.1 Repositories

NIFTeTRUST is responsible for the repository functions for its own CAs and the CAs of its Enterprise Customers (Managed PKI customers). NIFTeTRUST publishes Certificates it issues to end-user Subscribers in the repository in accordance with CPS.

Upon revocation of an end-user Subscriber's Certificate, NIFTeTRUST publishes notice of such revocation in the repository. NIFTeTRUST issues CRLs for its own CAs and the CAs of Service Centers and Enterprise Customers within its Sub-domain, pursuant to the provisions of this CPS. In addition, Enterprise Customers who have contracted for Online Certificate Status Protocol ("OCSP") services, NIFTeTRUST provides OCSP services pursuant to the provisions of this CPS.

2.2 Publication of Certificate Information

NIFTeTRUST maintains a web-based repository that permits Relying Parties to make online inquiries regarding revocation and other Certificate status information. NIFTeTRUST provides Relying Parties with information on how to find the appropriate repository to check Certificate status and, if OCSP (Online Certificate Status Protocol) is available, how to find the right OCSP responder.

NIFTeTRUST publishes the Certificates it issues on behalf of its own CAs, and the CAs of Client Service Centers in their Sub-domain. Upon revocation of an end-user Subscriber's Certificate, NIFTeTRUST shall publish notice of such revocation in the repository. In addition, NIFTeTRUST issues Certificate Revocation Lists (CRLs) and, if available, provide OCSP services (Online Certificate Status Protocol) for its own CAs and the CAs of Service Centers within its Sub-domain.

NIFTeTRUST will at all times publish a current version of:

- The NTN CP
- This NTN CPS,

- Subscriber Agreements,
- Relying Party Agreements

NIFTeTRUST is responsible for the repository function for:

- NIFTeTRUST Public Primary Certification Authorities (PCAs) and NIFTeTRUST Infrastructure/Administrative CAs supporting the NTN, and
- NIFTeTRUST CAs and Enterprise Customers' CAs that issue Certificates within NIFTeTRUST Sub-domain of the NTN.

NIFTeTRUST publishes certain CA information in the repository section of NIFTeTRUST web site at www.niftetrust.com/Downloads/NIFT-CPS.pdf. as described below.

NIFTeTRUST publishes the NTN CP, this CPS, Subscriber Agreements, and Relying Party Agreements in the repository section of NIFTeTRUST web site.

NIFTeTRUST publishes Certificates in accordance with Table 3 below.

Certificate Type	***Publication Requirements***
NTN PCA and NTN Issuing Root CA Certificates	Available to Relying Parties through inclusion in current browser software and as part of a Certificate Chain that can be obtained with the end-user Subscriber Certificate through the query functions described below.
NTN Issuing CA Certificates	Available to Relying Parties as part of a Certificate Chain that can be obtained with the end-user Subscriber Certificate through the query functions described below.
Certificate of the NTN CA supporting Managed PKI Lite Certificates and CA Certificates of Managed PKI Customers	Available through query to of the LDAP directory server at *directory.niftetrust.com*.
NIFTeTRUST OCSP Responder Certificates	Available through query of the LDAP directory server at *directory.niftetrust.com*.
End-User Subscriber Certificates issued through Managed PKI Customers.	Made available through the query functions listed above, although at the discretion of the Managed PKI Customer, the Certificate may be accessible only via a search using the Certificate's serial number.
End-User Subscriber Certificates issued by NIFTeTRUST Class 3 Organizational VIP Device CA	Not available through public query

Table 3 – Certificate Publication Requirements

2.3 Time or Frequency of Publication

Updates to this CPS are published in accordance with Section 9.12. Updates to Subscriber Agreements and Relying Party Agreements are published as necessary. Certificates are published upon issuance. Certificate status information is published in accordance with the provisions of this CPS.

2.4 Access Controls on Repositories

Information published in the repository portion of the NIFTeTRUST web site is publicly-accessible information. Read only access to such information is unrestricted. NIFTeTRUST requires persons to agree to a Relying Party Agreement or CRL Usage Agreement as a condition to accessing Certificates, Certificate status information, or CRLs. NIFTeTRUST has implemented logical and physical security measures to prevent unauthorized persons from adding, deleting, or modifying repository entries.

3 Identification and Authentication

3.1 Naming

Unless where indicated otherwise in this NTN CP, this CPS or the content of the digital certificate, names appearing in Certificates issued under NTN are authenticated.

3.1.1 Type of Names

NTN CA Certificates contain an X.501 Distinguished Name (DN) in the Issuer and Subject fields. NTN CA Distinguished Names consist of the components specified in Table 4 below.

Attribute	***Value***
Country (C) =	2-letter ISO country code or not used.
Organization (O) =	’ NIFTeTRUST Corporation”, or <organization name>[8]
Organizational Unit (O J) =	NIFTeTRUST CA Certificates may contain multiple OU attributes. Such attributes
	may contain one or more of the following:
	CA Name
	NIFTeTRUST Trust Network
	A statement referencing the applicable Relying Party Agreement
	governing terms of use of the Certificate
	A copyright notice.
	Text to describe the type of Certificate.
State or Province (S) =	Not used.

Locality (L) =	Not used except for the NIFTeTRUST Commercial Software Publishers CA,
	which uses “Internet.”
Common Name (CN) =	This attribute includes the CA Name (if the CA Name is not specified in an
	OU attribute) or is not used.

Table 4 – Distinguished Name Attributes in CA Certificates

End-user Subscriber Certificates contain an X.501 DN in the Subject name field and consist of the components specified in Table 5 below.

Attribute ***Value*** Country (C) =	2 letter ISO country code or not used. Organization (O) =
The Organization attribute is used as follows:	“NIFTeTRUST Corporation” for OCSP
Responder and optionally for	individual Certificates[9] that do not have an organization
affiliation.	
• Subscriber organizational name for web server Certificates and	individual
Certificates that have an organization affiliation.	Organizational Unit (OU) = NIFTeTRUST
end-user Subscriber Certificates may contain multiple OU	attributes. Such attributes may
contain one or more of the following:	Subscriber organizational unit (for organizational
Certificates and	individual Certificates that have an organization affiliation)
• NIFTeTRUST Trust Network	
• A statement referencing the applicable Relying Party Agreement	governing
terms of use of the Certificate	
• A copyright notice	
• “Authenticated by NIFTeTRUST[10]” and “Member, NIFTeTRUST Trust	
	Network” in Certificates whose applications were authenticated by
	NIFTeTRUST
• “Persona Not Validated” for Class 1 Individual Certificates	
• Text to describe the type of Certificate. 11	
• “No organization affiliation” (for code signing certificates issued to	individuals)
State or Province (S) =	Indicates the Subscriber’s State or Province (State is not a required field in
certificates issued to individuals).	
Locality (L) =	Indicates the Subscriber’s Locality (Locality is not a required field in
certificates issued to individuals).	Common Name (CN) = This attribute includes:
• The OCSP Responder Name (for OCSP Responder Certificates)	
• Domain name (for web server Certificates)	
• Organization name (for code/object signing Certificates)	
• Person’s name (for individual Certificates or code-signing certificates	issued to
individuals).	
• “Persona Not Validated” for Class 1 individual Certificates[12]	E-Mail Address (E) = E-mail
address for Class 1 individual Certificates and generally for MPKI	
	Subscriber Certificates.
	Optional e-mail address for Class 3 organizational e-mail signing
	Certificates

Table 5 – Distinguished Name Attributes in End User Subscriber Certificates

The Common Name (CN=) component of the Subject distinguished name of end-user Subscriber Certificates is authenticated in the case of Class 1-2 Certificates.

- The authenticated Common Name value included in the Subject DN of Organizational Certificates is a domain name) or the legal name of the organization or unit within the organization.

- The authenticated Common Name value included in the Subject DN of a Class 3 Organizational ASB Certificate, however, is the generally accepted personal name of the organizational representative authorized to use the organization's private key, and the organization (O=) component is the legal name of the organization.

- The Common Name value included in the Subject DN of individual Certificates represents the individual's generally accepted personal name.

3.1.2 Need for Names to be Meaningful

Class 2 end-user Subscriber Certificates contain names with commonly understood semantics permitting the determination of the identity of the individual or organization that is the Subject of the Certificate.

NTN CA certificates contain names with commonly understood semantics permitting the determination of the identity of the CA that is the Subject of the Certificate.

3.1.3 Anonymity or Pseudonymity of Subscribers

The identity of Class 1 individual Subscribers is not authenticated. Class 1 subscribers may use pseudonyms. Unless when required by law or requested by a State or Government authority to protect the identity of certain end user subscribers (e.g., minors, or sensitive government employee information), Class 2 Subscribers are not permitted to use pseudonyms (names other than a Subscriber's true personal or organizational name). Each request for anonymity in a certificate will be evaluated on its merits by the PMA and, if allowed the certificate will indicate that identity has been authenticated but is protected.

3.1.4 Uniqueness of Names

NIFTeTRUST ensures that Subject Distinguished Name (DN) of the Subscriber is unique within the domain of a specific CA through automated components of the Subscriber enrollment process. It is possible for a Subscriber to have two or more certificates with the same Subject DN.

3.1.5 Recognition, Authentication, and Role of Trademarks

Certificate Applicants are prohibited from using names in their Certificate Applications that infringe upon the Intellectual Property Rights of others. NIFTeTRUST, however, does not verify whether a Certificate Applicant has Intellectual Property Rights in the name appearing in a Certificate Application or arbitrates, mediate, or otherwise resolve any dispute concerning the ownership of any domain name, trade name, trademark, or service mark. NIFTeTRUST is entitled, without liability to any Certificate Applicant, to reject or suspend any Certificate Application because of such dispute.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

The certificate applicant must demonstrate that it rightfully holds the private key corresponding to the public key to be listed in the Certificate. The method to prove possession of a private key shall be PKCS #10, another cryptographically equivalent demonstration, or another NIFTeTRUST-approved method. This requirement does not apply where a key pair is generated by a CA on behalf of a Subscriber, for example where pre-generated keys are placed on smart cards.

3.2.2 Authentication of Organization identity

Whenever a certificate contains an organization name, the identity of the organization and other enrollment information provided by Certificate Applicants (except for Non-verified Subscriber Information) is confirmed in accordance with the procedures set forth in NIFTeTRUST documented Validation Procedures.

At a minimum NIFTeTRUST shall:

- Determine that the organization exists by using at least one third party identity proofing service or database, or alternatively, organizational documentation issued by or filed with the applicable government agency or competent authority that confirms the existence of the organization,

- Confirm by telephone, confirmatory postal mail, or comparable procedure to the Certificate Applicant certain information about the organization, that the organization has authorized the Certificate Application and that the person submitting the Certificate Application on behalf of the Certificate Applicant is authorized to do so.

  When a certificate includes the name of an individual as an authorized representative of the Organization, the employment of that individual and his/her authority to act on behalf of the Organization shall also be confirmed.

Where a domain name or e-mail address is included in the certificate NIFTeTRUST authenticates the Organization’s right to use that domain name either as a fully qualified Domain name or an e-mail domain

.

Additional checks necessary to satisfy rules and regulations governed by law of Pakistan are performed by NIFTeTRUST and Affiliates when required.

Additional procedures are performed for specific types of Certificates as described in Table 6 below.

Certificate Type	***Additional Procedures***
Authenticated Content Signing (ACS) Certificate	Before NIFTeTRUST digitally signs any content using ACS it authenticates that the content is the original content signed by the Organization using its Code Signing Certificate.
Class 3 organizational e-mail signing Certificates	NIFTeTRUST authenticates the Organization’s ownership of e-mail domain name.

Table 6 – Specific Authentication Procedures

3.2.3 Authentication of Individual Identity

Authentication of individual identity differs according to the Class of Certificate. The minimum authentication standard for each class of NTN certificate is explained in Table 7 below.

Certificate Class	**Authentication of Identity**

Class 1	No identity authentication. Email addresses validation – Limited confirmation that the certificate subscriber has access to the email address. NIFTeTRUST performs a challenge-response type of procedure in which NIFTeTRUST sends email to the email address to be included in the certificate, containing unpredictable information such as a randomly generated PIN/Password unique to the owner of the email address. The owner of the email address (the subscriber of the certificate) demonstrates control over the email address by using the information within the email, to then proceed with accessing a portal with the unique information sent in the email, to download and install the certificate.
Class 2	Authenticate identity by: Manual check performed by the enterprise administrator customer for each subscriber requesting a certificate, "in which the subscriber receives the certificate via an email sent to the address provided during enrollment" or Passcode-based authentication where a randomly-generated passcode is delivered out-of-band by the enterprise administrator customer to the subscriber entitled to enroll for the certificate, and the subscriber provides this passcode at enrollment time. Or Comparing information provided by the subscriber to information contained in business records or databases (customer directories such as Active Directory or LDAP.

Table 7. Authentication of individual identity

3.2.4 Validation of Authority

Whenever an individual's name is associated with an Organization name in a certificate in such a way to indicate the individual's affiliation or authorization to act on behalf of the Organization the NIFTeTRUST or a RA:

- determines that the Organization exists by using at least one third party identity proofing service or database, or alternatively, organizational documentation issued by or filed with the applicable government that confirms the existence of the organization, and

- Uses information contained in the business records or databases of business information (employee or customer directories) of an RA approving certificates to its own affiliated individuals or confirms by telephone, confirmatory postal mail, or comparable procedure to the organization, the employment with the Organization of the individual submitting the Certificate Application and, when appropriate, his/her authority to act on behalf of the Organization.

3.2.5 Criteria for Interoperation

NIFTeTRUST may provide interoperation services that allow a non-NTN CA to be able to interoperate with the NTN by unilaterally certifying that CA. CAs enabled to interoperate in this way will comply with the NTN CP as supplemented by additional policies when required.

NIFTeTRUST shall only allow interoperation with the NTN of a non-NTN CA in circumstances where the CA, at a minimum:

- Enters into a contractual agreement with NIFTeTRUST

- Operates under a CPS that meets NTN requirements for the classes of certificates it will issues
- Passes a compliance assessment before being allowed to interoperate
- Passes an annual compliance assessment for ongoing eligibility to interoperate.

3.3 Identification and Authentication for Re-key Requests

Prior to the expiration of an existing Subscriber's Certificate, it is necessary for the Subscriber to obtain a new certificate to maintain continuity of Certificate usage. NIFTeTRUST generally requires that the Subscriber generate a new key pair to replace the expiring key pair (technically defined as "rekey") However, in certain cases (i.e., for web server certificates) Subscribers may request a new certificate for an existing key pair (technically defined as "renewal").

Generally speaking, both "Rekey" and "Renewal" are commonly described as "Certificate Renewal", focusing on the fact that the old Certificate is being replaced with a new Certificate and not emphasizing whether or not a new key pair is generated. For all Classes and Types of NTN Certificates, except for Class 3 Server Certificates, this distinction is not important as a new key pair is always generated as part of NIFTeTRUST end-user Subscriber Certificate replacement process. However, for Class 3 Server Certificates, because the Subscriber key pair is generated on the web server and most web server key generation tools permit the creation of a new Certificate Request for an existing key pair, there is a distinction between "rekey" and "renewal."

3.3.1 Identification and Authentication for Routine Re-key

Re-key procedures ensure that the person or organization seeking to rekey an end user Subscriber Certificate is in fact the Subscriber of the Certificate.

One acceptable procedure is through the use of a Challenge Phrase (or the equivalent thereof), or proof of possession of the private key. Subscribers choose and submit with their enrollment information a Challenge Phrase. Upon renewal of a Certificate, if a Subscriber correctly submits the Subscriber's Challenge Phrase (or the equivalent thereof) with the Subscriber's re-enrollment information, and the enrollment information (including Corporate and Technical contact information) has not changed, a renewal Certificate is automatically issued. As an alternative to using a challenge phrase (or equivalent) NIFTeTRUST may send an e-mail message to the e-mail address associated with the verified corporate contact for the certificate being renewed, requesting confirmation of the Certificate renewal order and authorization to issue the Certificate. Upon receipt of confirmation authorizing issuance of the Certificate, NIFTeTRUST will issue the Certificate if the enrollment information (including Corporate and Technical contact information[15]) has not changed.

After rekeying or renewal in this fashion, and on at least alternative instances of subsequent rekeying or renewal thereafter, NIFTeTRUST or the RA reconfirms the identity of the Subscriber in accordance with the identification and authentication requirements of an original Certificate Application.

3.3.2 Identification and Authentication for Re-key After Revocation

Re-key/renewal after revocation is not permitted if the revocation occurred because:

- the Certificate (other than a Class 1 Certificate) was issued to a person other than the one named as the Subject of the Certificate, or
- the Certificate (other than a Class 1 Certificate) was issued without the authorization of the person or entity named as the Subject of such Certificate, or the entity approving the Subscriber's Certificate Application discovers or has reason to believe that a material fact in the Certificate Application is false. or
- For any other reason deemed necessary by NIFTeTRUST to protect the NTN

Subject to the foregoing paragraph, renewal of an Organizational or CA Certificate following revocation of the Certificate is permissible as long as renewal procedures ensure that the Organization or CA seeking renewal is in fact the Subscriber of the Certificate. Renewed Organizational Certificates shall contain the same Subject DN as the Subject DN of the Organizational Certificate being renewed.

Renewal of an individual Certificate following revocation must ensure that the person seeking renewal is, in fact, the Subscriber. One acceptable procedure is the use of a Challenge Phrase (or the equivalent thereof). Other than this procedure or another NIFTeTRUST-approved procedure, the requirements for the identification and authentication of an original Certificate Application shall be used for renewing a Certificate following revocation.

3.4 Identification and Authentication for Revocation Request

Prior to the revocation of a Certificate, NIFTeTRUST verifies that the revocation has been requested by the Certificate's Subscriber, the entity that approved the Certificate Application.

Acceptable procedures for authenticating the revocation requests of a Subscriber include:

- Having the Subscriber for certain certificate types submit the Subscriber's Challenge Phrase (or the equivalent thereof), and revoking the Certificate automatically if it matches the Challenge Phrase (or the equivalent thereof) on record, (Note that this option may not be available to all customers.)
- Receiving a message from the Subscriber that requests revocation and contains a digital signature verifiable with reference to the Certificate to be revoked,
- Communication with the Subscriber providing reasonable assurances in light of the Class of Certificate that the person or organization requesting revocation is, in fact the Subscriber. Such communication, depending on the circumstances, may include one or more of the following: telephone, facsimile, e-mail, postal mail, or courier service.

MPKI Administrators are entitled to request the revocation of end-user Subscriber Certificates within respective sub-domain. NIFTeTRUST authenticates the identity of Administrators via access control using SSL and client authentication before permitting them to perform revocation functions, or another NTN approved procedure.

RAs using an Automated Administration Software Module may submit bulk revocation requests to NIFTeTRUST. Such requests shall be authenticated via a digitally signed request signed with the private key in the RA's Automated Administration hardware token.

The requests to revoke a CA Certificate shall be authenticated by NIFTeTRUST to ensure that the revocation has in fact been requested by the CA.

4 Certificate Life-Cycle Operational Requirements

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application?

Below is a list of people who may submit certificate applications:

- Any individual who is the subject of the certificate,
- Any authorized representative of an Organization or entity,
- Any authorized representative of a CA,

- Any authorized representative of an RA.

4.1.2 Enrollment Process and Responsibilities

4.1.2.1 End-User Certificate Subscribers

All end-user Certificate Subscribers shall manifest assent to the relevant Subscriber Agreement that contains representations and warranties described in Section 9.6.3 and undergo an enrollment process consisting of:

- completing a Certificate Application and providing true and correct information,
- generating, or arranging to have generated, a key pair,
- delivering his, her, or its public key, directly or through an RA, to NIFTeTRUST,
- demonstrating possession and/or exclusive control of the private key corresponding to the public key delivered to NIFTeTRUST.

4.1.2.2 CA and RA Certificates

Subscribers of CA and RA Certificates enter into a contract with NIFTeTRUST. CA and RA Applicants shall provide their credentials to demonstrate their identity and provide contact information during the contracting process. During this contracting process or, at the latest, prior to the Key Generation Ceremony to create a CA or RA key pair, the applicant shall cooperate with NIFTeTRUST to determine the appropriate distinguished name and the content of the Certificates to be issued by the applicant.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

NIFTeTRUST or an RA shall perform identification and authentication of all required Subscriber information in terms of Section 3.2.

4.2.2 Approval or Rejection of Certificate Applications

NIFTeTRUST or an RA will approve an application for a certificate if the following criteria are met:

- Successful identification and authentication of all required Subscriber information in terms of Section 3.2
- Payment has been received.

NIFTeTRUST or an RA will reject a certificate application if:

- Identification and authentication of all required Subscriber information in terms of Section 3.2 cannot be completed, or
- The Subscriber fails to furnish supporting documentation upon request, or
- The Subscriber fails to respond to notices within a specified time, or
- Payment has not been received, or
- The RA believes that issuing a certificate to the Subscriber may bring the NTN into disrepute.

4.2.3 Time to Process Certificate Applications

NIFTeTRUST begins processing certificate applications within a reasonable time of receipt. There is no time stipulation to complete the processing of an application unless otherwise indicated in the relevant Subscriber Agreement, CPS or other Agreement between NTN participants. A certificate application remains active until rejected.

4.3 Certificate Issuance

4.3.1 CA Actions during Certificate Issuance

A Certificate is created and issued following the approval of a Certificate Application by NIFTeTRUST or following receipt of an RA's request to issue the Certificate. NIFTeTRUST creates and issues to a Cert ificate Applicant a Certificate based on the information in a Certificate Application following approval of such Certificate Application.

4.3.2 Notifications to Subscriber by the CA of Issuance of Certificate

NIFTeTRUST shall, either directly or through an RA, notify Subscribers that they have created such Certificates, and provide Subscribers with access to the Certificates by notifying them that their Certificates are available. Certificates shall be made available to end-user Subscribers, either by allowing them to download them from a web site or via a message sent to the Subscriber containing the Certificate.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

The following conduct constitutes certificate acceptance:

- Downloading a Certificate or installing a Certificate from a message attaching it constitutes the Subscriber's acceptance of the Certificate.
- Failure of the Subscriber to object to the certificate or its content constitutes certificate acceptance.

4.4.2 Publication of the Certificate by the CA

NIFTeTRUST publishes the Certificates it issues in a publicly accessible repository.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

RAs may receive notification of the issuance of certificates they approve.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

Use of the Private Key corresponding to the public key in the certificate shall only be permitted once the Subscriber has agreed to the Subscriber Agreement and accepted the certificate. The certificate shall be used lawfully in accordance with NIFTeTRUST Subscriber Agreement the terms of the NTN CP and this CPS. Certificate use must be consistent with the *KeyUsage* field extensions included in the certificate (e.g., if Digital Signature is not enabled then the certificate must not be used for signing).

Subscribers shall protect their private keys from unauthorized use and shall discontinue use of the private key following expiration or revocation of the certificate. Parties other than the Subscriber shall not archive the Subscriber Private Key except as set forth in section 4.12.

4.5.2 Relying Party Public Key and Certificate Usage

Relying parties shall assent to the terms of the applicable Relying Party Agreement as a condition of relying on the certificate.

Reliance on a certificate must be reasonable under the circumstances. If the circumstances indicate a need for additional assurances, the Relying Party must obtain such assurances for such reliance to be deemed reasonable.

Before any act of reliance, Relying Parties shall independently assess:

- the appropriateness of the use of a Certificate for any given purpose and determine that the Certificate will, in fact, be used for an appropriate purpose that is not prohibited or otherwise restricted by this CPS. NIFTeTRUST is not responsible for assessing the appropriateness of the use of a Certificate.

- That the certificate is being used in accordance with the *KeyUsage* field extensions included in the certificate (e.g., if Digital Signature is not enabled then the certificate may not be relied upon for validating a Subscriber’s signature).

- The status of the certificate and all the CAs in the chain that issued the certificate. If any of the Certificates in the Certificate Chain have been revoked, the Relying Party is solely responsible to investigate whether reliance on a digital signature performed by an end-user Subscriber Certificate prior to revocation of a Certificate in the Certificate chain is reasonable. Any such reliance is made solely at the risk of the Relying party.

Assuming that the use of the Certificate is appropriate, Relying Parties shall utilize the appropriate software and/or hardware to perform digital signature verification or other cryptographic operations they wish to perform, as a condition of relying on Certificates in connection with each such operation. Such operations include identifying a Certificate Chain and verifying the digital signatures on all Certificates in the Certificate Chain.

4.6 Certificate Renewal

Certificate renewal is the issuance of a new certificate to the subscriber without changing the public key or any other information in the certificate. Certificate renewal is supported for Class 3 certificates where the key pair is generated on a web server as most web server key generation tools permit the creation of a new Certificate Request for an existing key pair.

4.6.1 Circumstances for Certificate Renewal

Prior to the expiration of an existing Subscriber's Certificate, it is necessary for the Subscriber to renew a new certificate to maintain continuity of Certificate usage. A certificate may also be renewed after expiration.

4.6.2 Who May Request Renewal

Only the subscriber for an individual certificate or an authorized representative for an Organizational certificate may request certificate renewal.

4.6.3 Processing Certificate Renewal Requests

Renewal procedures ensure that the person or organization seeking to renew an end-user Subscriber Certificate is in fact the Subscriber (or authorized by the Subscriber) of the Certificate.

One acceptable procedure is through the use of a Challenge Phrase (or the equivalent thereof), or proof of possession of the private key. Subscribers choose and submit with their enrollment information a Challenge Phrase (or the equivalent thereof). Upon renewal of a Certificate, if a Subscriber correctly submits the Subscriber's Challenge Phrase (or the equivalent thereof) with the Subscriber's reenrollment information, and the enrollment information (including Corporate and Technical contact information) has not changed, a renewal Certificate is automatically issued. As an alternative to using a challenge phrase (or equivalent) NIFTeTRUST may send an e-mail message to the e-mail address associated with the verified corporate contact for the certificate being renewed, requesting confirmation of the Certificate renewal order and authorization to issue the Certificate. Upon receipt of confirmation authorizing issuance of the Certificate, NIFTeTRUST will issue the Certificate if the enrollment information (including Corporate and Technical contact information) has not changed.

After renewal in this fashion, and on at least alternative instances of subsequent renewal thereafter, NIFTeTRUST or an RA shall reconfirm the identity of the Subscriber in accordance with the requirements specified in this CPS for the authentication of an original Certificate Application.

In circumstances where:

- The challenge phrase is correctly used for the subsequent renewal certificate, or a confirmatory response is obtained to an e-mail to the corporate contact, and:
- The certificate Distinguished Name has not been changed, and
- The Corporate and Technical Contact information remains unchanged from that which was previously verified,

NIFTeTRUST will not have to reconfirm by telephone, confirmatory postal mail, or comparable procedure to the Certificate Applicant certain information about the organization, that the organization has authorized the Certificate Application and that the person submitting the Certificate Application on behalf of the Certificate Applicant is authorized to do so.

Other than this procedure or another NIFTeTRUST-approved procedure, the requirements for the authentication of an original Certificate Application shall be used for renewing an end-user Subscriber Certificate.

4.6.4 Notification of New Certificate Issuance to Subscriber

Notification of issuance of certificate renewal to the Subscriber is in accordance with Section 4.3.2

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

Conduct constituting Acceptance of a renewed certificate is in accordance with Section 4.4.1

4.6.6 Publication of the Renewal Certificate by the CA

The renewed certificate is published in NIFTeTRUST publicly accessible repository.

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

RAs may receive notification of the issuance of certificates they approve.

4.7 Certificate Re-Key

Certificate rekey is the application for the issuance of a new certificate that certifies the new public key. Certificate rekey is supported for all certificate Classes.

4.7.1 Circumstances for Certificate Re-Key

Prior to the expiration of an existing Subscriber's Certificate, it is necessary for the Subscriber to re-key the certificate to maintain continuity of Certificate usage. A certificate may also be re-keyed after expiration.

4.7.2 Who May Request Certification of a New Public Key

Only the subscriber for an individual certificate or an authorized representative for an Organizational certificate may request certificate renewal

4.7.3 Processing Certificate Re-Keying Requests

Re-key procedures ensure that the person or organization seeking to renew an end-user Subscriber Certificate is in fact the Subscriber (or authorized by the Subscriber) of the Certificate.

One acceptable procedure is through the use of a Challenge Phrase (or the equivalent thereof), or proof of possession of the private key. Subscribers choose and submit with their enrollment information a Challenge Phrase (or the equivalent thereof). Upon renewal of a Certificate, if a

Subscriber correctly submits the Subscriber's Challenge Phrase (or the equivalent thereof) with the Subscriber's reenrollment information, and the enrollment information (including contact information) has not changed, a renewal Certificate is automatically issued. Subject to the provisions of Section 3.3.1, after re-keying in this fashion, and on at least alternative instances of subsequent re-keying thereafter, NIFTeTRUST or an RA shall reconfirm the identity of the Subscriber in accordance with the requirements specified in this CPS for the authentication of an original Certificate Application.

Other than this procedure or another NIFTeTRUST-approved procedure, the requirements for the authentication of an original Certificate Application shall be used for re-keying an end-user Subscriber Certificate.

4.7.4 Notification of New Certificate Issuance to Subscriber

Notification of issuance of a re-keyed certificate to the Subscriber is in accordance with Section 4.3.2

4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

Conduct constituting Acceptance of a re-keyed certificate is in accordance with Section 4.4.1

4.7.6 Publication of the Re-Keyed Certificate by the CA

The re-keyed certificate is published in NIFTeTRUST publicly accessible repository.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

RAs may receive notification of the issuance of certificates they approve.

4.8 Certificate Modification

4.8.1 Circumstances for Certificate Modification

Certificate modification refers to the application for the issuance of a new certificate due to changes in the information in an existing certificate (other than the subscriber's public key).

Certificate modification is considered a Certificate Application in terms of Section 4.1.

4.8.2 Who May Request Certificate Modification

See Section 4.1.1.

4.8.3 Processing Certificate Modification Requests

NIFTeTRUST or an RA shall perform identification and authentication of all required Subscriber information in terms of Section 3.2.

4.8.4 Notification of New Certificate Issuance to Subscriber

See Section 4.3.2.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

See Section 4.4.1.

4.8.6 Publication of the Modified Certificate by the CA

See Section 4.4.2.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

See Section 4.4.3.

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for Revocation

Only in the circumstances listed below, will an end-user Subscriber certificate be revoked by NIFTeTRUST (or by the Subscriber) and published on a CRL. Upon request from a subscriber who can no longer use (or no longer wishes to use) a certificate for a reason other than one mentioned below, NIFTeTRUST will flag the certificate as inactive in its database but will not publish the certificate on a CRL.

An end-user Subscriber Certificate is revoked if:

- NIFTeTRUST, a Customer, or a Subscriber has reason to believe or strongly suspects that there has been a Compromise of a Subscriber’s private key,
- NIFTeTRUST or a Customer has reason to believe that the Subscriber has materially breached a material obligation, representation, or warranty under the applicable Subscriber Agreement,
- The Subscriber Agreement with the Subscriber has been terminated,
- The affiliation between an Enterprise Customer with a Subscriber is terminated or has otherwise ended,
- NIFTeTRUST or a Customer has reason to believe that the Certificate was issued in a manner not materially in accordance with the procedures required by the applicable CPS, the Certificate (other than a Class 1 Certificate) was issued to a person other than the one named as the Subject of the Certificate, or the Certificate (other than a Class 1 Certificate) was issued without the authorization of the person named as the Subject of such Certificate,
- NIFTeTRUST or a Customer has reason to believe that a material fact in the Certificate Application is false,
- NIFTeTRUST or a Customer determines that a material prerequisite to Certificate Issuance was neither satisfied nor waived,
- In the case of Class 2 organizational Certificates, the Subscriber’s organization name changes,
- The information within the Certificate, other than Non-verified Subscriber Information, is incorrect or has changed,
- The Subscriber identity has not been successfully re-verified in accordance with section 6.3.2,
- The Subscriber has not submitted payment when due, or
- The continued use of that certificate is harmful to the NTN.

When considering whether certificate usage is harmful to the NTN, NIFTeTRUST considers, among other things, the following:

- The nature and number of complaints received
- The identity of the complainant(s)
- Relevant legislation in force
- Responses to the alleged harmful use from the Subscriber

When considering whether the use of a Code Signing Certificate is harmful to the NTN, NIFTeTRUST additionally considers, among other things, the following:

- The name of the code being signed
- The behaviour of the code
- Methods of distributing the code
- Disclosures made to recipients of the code Any additional allegations made about the code

NIFTeTRUST may also revoke an Administrator Certificate if the Administrator’s authority to act as Administrator has been terminated or otherwise has ended.

NIFTeTRUST Subscriber Agreements require end-user Subscribers to immediately notify NIFTeTRUST of a known or suspected compromise of its private key.

4.9.2 Who Can Request Revocation

Individual Subscribers can request the revocation of their own individual Certificates through an authorized representative of NIFTeTRUST or an RA. In the case of organizational Certificates, a duly authorized representative of the organization shall be entitled to request the revocation of Certificates issued to the organization. A duly authorized representative of NIFTeTRUST or a RA shall be entitled to request the revocation of an RA Administrator's Certificate. The entity that approved a Subscriber's Certificate Application shall also be entitled to revoke or request the revocation of the Subscriber's Certificate.

Only NIFTeTRUST is entitled to request or initiate the revocation of the Certificates issued to its own CAs. RAs are entitled, through their duly authorized representatives, to request the revocation of their own Certificates, and their Superior Entities shall be entitled to request or initiate the revocation of their Certificates.

4.9.3 Procedure for Revocation Request

4.9.3.1 Procedure for Requesting the Revocation of an End-User Subscriber Certificate

An end-user Subscriber requesting revocation is required to communicate the request to NIFTeTRUST or the Customer approving the Subscriber's Certificate Application, who in turn will initiate revocation of the certificate promptly. For Enterprise customers, the Subscriber is required to communicate the request to the Enterprise Administrator who will communicate the revocation request to NIFTeTRUST for processing. Communication of such revocation request shall be in accordance with CPS. Non-Enterprise customers shall communicate a revocation request in accordance with CPS.

Where an Enterprise Customer initiates revocation of an end-user Subscriber Certificate upon its own initiative, the Managed PKI Customer or ASB Customer instructs NIFTeTRUST to revoke the Certificate.

4.9.3.2 CABF Requirements for Certificate Revocation Process

EV SSL Certificates, EV Code Signing, and domain-validated and organization-validated SSL Certificates conform to the CA / Browser Forum requirements as set forth in the NTN Supplemental Procedures, Appendix.

4.9.3.3 Procedure for Requesting the Revocation of a CA or RA Certificate

A CA or RA requesting revocation of its CA or RA Certificate is required to communicate the request to NIFTeTRUST. NIFTeTRUST will then revoke the Certificate. NIFTeTRUST may also initiate CA or RA Certificate revocation.

4.9.4 Revocation Request Grace Period

Revocation requests shall be submitted as promptly as possible within a commercially reasonable time.

4.9.5 Time within Which CA Must Process the Revocation Request

NIFTeTRUST takes commercially reasonable steps to process revocation requests without delay.

4.9.6 Revocation Checking Requirements for Relying Parties

Relying Parties shall check the status of Certificates on which they wish to rely. One method by which Relying Parties may check Certificate status is by consulting the most recent CRL from the CA that issued the Certificate on which the Relying Party wishes to rely. Alternatively, Relying Parties may meet this requirement either by checking Certificate status using the applicable web-based repository or by using OCSP (if available). CAs shall provide Relying Parties with information on how to find the appropriate CRL, web-based repository, or OCSP responder (where available) to check for revocation status.

4.9.7 CRL Issuance Frequency

CRLs for end-user Subscriber Certificates are issued at least once per day. CRLs for CA Certificates shall be issued at least annually, but also whenever a CA Certificate is revoked.

CRLs for Authenticated Content Signing (ACS) Root CAs are published annually and also whenever a CA Certificate is revoked.

If a Certificate listed in a CRL expires, it may be removed from later-issued CRLs after the Certificate's expiration.

4.9.7.1 CABF Requirements for CRL Issuance

CRL issuance for EV SSL Certificates, EV Code Signing, and domain-validated and organization-validated SSL Certificates conform to the CA / Browser Forum requirements as set forth in the NTN Supplemental Procedures, Appendix.

4.9.8 Maximum Latency for CRLs

CRLs are posted to the repository within a commercially reasonable time after generation. This is generally done automatically within minutes of generation.

4.9.9 On-Line Revocation/Status Checking Availability

Online revocation and other Certificate status information are available via a web-based repository and, where offered, OCSP. In addition to publishing CRLs, NIFTeTRUST provides Certificate status information through query functions in the NIFTeTRUST Repository.

Certificate status information for Individual Certificates is available through web-based query functions accessible through the NIFTeTRUST Repository at

http://onsite-root.niftetrust.com/ejbca/retrieve/list_certs.jsp
http://onsite-root.niftetrust.com/ejbca/retrieve/check_status.jsp

NIFTeTRUST also provides OCSP Certificate status information. Enterprise Customers who contract for OCSP services may check Certificate status through the use of OCSP. The URL for the relevant OCSP Responder is communicated to the Enterprise Customer.

4.9.9.1 CABF Requirements for OCSP Availability

OCSP availability for EV SSL Certificates, EV Code Signing, and domain-validated and organization validated SSL Certificates conform to the CA / Browser Forum requirements as set forth in the NTN Supplemental Procedures, Appendix.

4.9.10 On-Line Revocation Checking Requirements

A relying party must check the status of a certificate on which he/she/it wishes to rely. If a Relying Party does not check the status of a Certificate on which the Relying Party wishes to rely by consulting the most recent relevant CRL, the Relying Party shall check Certificate status by consulting the applicable repository or by requesting Certificate status using the applicable OCSP responder (where OCSP services are available).

4.9.11 Other Forms of Revocation Advertisements Available

Not applicable.

4.9.12 Special Requirements regarding Key Compromise

NIFTeTRUST uses commercially reasonable efforts to notify potential Relying Parties if it discovers, or have reason to believe, that there has been a Compromise of the private key of one of their own CAs or one of the CAs within their sub-domains.

4.9.13 Circumstances for Suspension

Not applicable.

4.9.14 Who Can Request Suspension

Not applicable.

4.9.15 Procedure for Suspension Request

Not applicable.

4.9.16 Limits on Suspension Period

Not applicable.

4.10 Certificate Status Services

4.10.1 Operational Characteristics

The Status of public certificates is available via CRL at NIFTeTRUST website, LDAP directory and via an OCSP responder (where available).

4.10.2 Service Availability

Certificate Status Services are available 24/7 without scheduled interruption.

Certificate status services for EV SSL Certificates, EV Code Signing, and Organization-validated and Domain-validated SSL Certificates, conform to the CA / Browser Forum requirements as set forth in the NTN Supplemental Procedures, Appendix.

4.10.3 Optional Features

OCSP is an optional status service feature that is not available for all products and must be specifically enabled for other products.

4.11 End of Subscription

A subscriber may end a subscription for a NIFTeTRUST certificate by:

- Allowing his/her/its certificate to expire without renewing or re-keying that certificate
- Revoking of his/her/its certificate before certificate expiration without replacing the certificates.

4.12 Key Escrow and Recovery

With the exception of enterprises deploying Managed PKI Key Management Services no NTN participant may escrow CA, RA or end-user Subscriber private keys.

Enterprise customers using the Key Escrow option within the NIFTeTRUST Managed PKI Service can escrow copies of the private keys of Subscribers whose Certificate Applications they approve. The enterprise customer may escrow keys either within the enterprise's premises or

NIFTeTRUST secure data center. If operated out of the enterprise's premises, NIFTeTRUST does not store copies of Subscriber private keys but nevertheless plays an important role in the Subscriber key recovery process.

4.12.1 Key Escrow and Recovery Policy and Practices

Enterprise customers using the Key Escrow option within the NIFTeTRUST Managed PKI service (or an equivalent service approved by NIFTeTRUST) are permitted to escrow end-user Subscribers' private key. Escrowed private keys shall be stored in encrypted form using the Managed PKI Key Manager software. Except for enterprise customers using the Managed PKI Key Manager Service (or an equivalent service approved by NIFTeTRUST), the private keys of CAs or end-user Subscribers shall not be escrowed.

End-user Subscriber private keys shall only be recovered under the circumstances permitted within the Managed PKI Key Management Service Administrator's Guide, under which:

- Enterprise customers using Managed PKI Key Manager shall confirm the identity of any person purporting to be the Subscriber to ensure that a purported Subscriber request for the Subscriber's private key is, in fact, from the Subscriber and not an imposter,

- Enterprise customers shall recover a Subscriber's private key without the Subscriber's authority only for their legitimate and lawful purposes, such as to comply with judicial or administrative process or a search warrant, and not for any illegal, fraudulent, or other wrongful purpose, and

- Such Enterprise customers shall have personnel controls in place to prevent Key Management Service Administrators and other persons from obtaining unauthorized access to private keys.

It is recommended that Enterprise Customers using the Key Escrow option within the NIFTeTRUST Managed PKI Service:

- Notify the subscribers that their private keys are escrowed

- Protect subscribers' escrowed keys from unauthorized disclosure,

- Protect all information, including the administrator's own key(s) that could be used to recover subscribers' escrowed keys.

- Release subscribers' escrowed keys only for properly authenticated and authorized requests for recovery.

- Revoke the Subscriber's Key pair prior to recovering the encryption key under certain circumstances such as to discontinue the use of a lost certificate.

- Not be required to communicate any information concerning a key recovery to the subscriber except when the subscriber him/herself has requested recovery.

- Not disclose or allow to be disclosed escrowed keys or escrowed key-related information to any third party unless required by the law, government rule, or regulation; by the enterprise's organization policy; or by order of a court of competent jurisdiction.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

Private keys are stored in the Key Manager database in encrypted form. Each Subscriber's private key is individually encrypted with its own triple-DES symmetric key. A Key Escrow Record (KER) is generated then the triple-DES key is combined with a random session key to form a session key mask (MSK). The resulting MSK together with the certificate request information is securely sent and stored in the Managed PKI database at NIFTeTRUST. The KER (containing the end user's private key) and the individual session key are stored in the Key Manager database and all residual key material is destroyed.

The Managed PKI database is operated out of NIFTeTRUST secure data center. The enterprise customer may choose to operate the Key Manager database either on the enterprise's premises or out of NIFTeTRUST secure data center.

Recovery of a private key and digital certificate requires the Managed PKI administrator to securely log on to the Managed PKI Control Center, select the appropriate key pair to recover and click a "recover" hyperlink. Only after an approved administrator clicks the “recover” link is the

MSK for that key pair returned from the Managed PKI database. The Key Manager retrieves the session key from the KMD and combines it with the MSK to regenerate the triple-DES key which was used to originally encrypt the private key, allowing recovery of the end user’s private key. As a final step, an encrypted PKCS#12 file is returned to the administrator and ultimately distributed to the end user.

5 Facility, Management, and Operational Controls

5.1 Physical Controls

NIFTeTRUST has implemented the NIFTeTRUST Physical Security Policy, which supports the security requirements of this CPS. Compliance with these policies is included in NIFTeTRUST independent audit requirements described in Section 8. NIFTeTRUST Physical Security Policy contains sensitive security information and is only available upon agreement with NIFTeTRUST. An overview of the requirements is described in the subsections following.

5.1.1 Site Location and Construction

NTN CA and RA operations are conducted within a physically protected environment that deters, prevents, and detects unauthorized use of, access to, or disclosure of sensitive information and systems whether covert or overt.

NIFTeTRUST also maintains disaster recovery facilities for its CA operations. NIFTeTRUST disaster recovery facilities are protected by multiple tiers of physical security comparable to those of NIFTeTRUST primary facility.

5.1.2 Physical Access

NTN CA systems are protected by a minimum of four tiers of physical security, with access to the lower tier required before gaining access to the higher tier.

Progressively restrictive physical access privileges control access to each tier. Sensitive CA operational activity, any activity related to the lifecycle of the certification process such as authentication, verification, and issuance, occur within very restrictive physical tiers. Access to each tier requires the use of a proximity card employee badge. Physical access is automatically logged and video recorded. Additional tiers enforce individual access control through the use of two factor authentication including biometrics. Unescorted personnel, including untrusted employees or visitors, are not allowed into such secured areas.

The physical security system includes additional tiers for key management security which serves to protect both online and offline storage of CSUs and keying material. Areas used to create and store cryptographic material enforce dual control, each through the use of two factor authentication including biometrics. Online CSUs are protected through the use of locked cabinets. Offline CSUs are protected through the use of locked safes, cabinets and containers. Access to CSUs and keying material is restricted in accordance with NIFTeTRUST segregation of duties requirements. The opening and closing of cabinets or containers in these tiers is logged for audit purposes.

5.1.3 Power and Air Conditioning

NIFTeTRUST secure facilities are equipped with primary and backup:

power systems to ensure continuous, uninterrupted access to electric power and
heating/ ventilation/ air conditioning systems to control temperature and relative humidity.

5.1.4 Water Exposures

NIFTeTRUST has taken reasonable precautions to minimize the impact of water exposure to NIFTeTRUST systems.

5.1.5 Fire Prevention and Protection

NIFTeTRUST has taken reasonable precautions to prevent and extinguish fires or other damaging exposure to flame or smoke. NIFTeTRUST fire prevention and protection measures have been designed to comply with local fire safety regulations.

5.1.6 Media Storage

All media containing production software and data, audit, archive, or backup information is stored within NIFTeTRUST facilities or in a secure off-site storage facility with appropriate physical and logical access controls designed to limit access to authorized personnel and protect such media from accidental damage (e.g., water, fire, and electromagnetic).

5.1.7 Waste Disposal

Sensitive documents and materials are shredded before disposal. Media used to collect or transmit sensitive information are rendered unreadable before disposal. Cryptographic devices are physically destroyed in accordance the manufacturers' guidance prior to disposal. Other waste is disposed of in accordance with NIFTeTRUST normal waste disposal requirements.

5.1.8 Off-Site Backup

NIFTeTRUST performs routine backups of critical system data, audit log data, and other sensitive information. Offsite backup media are stored in a physically secure manner using a bonded third party storage facility and NIFTeTRUST disaster recovery facility.

5.2 Procedural Controls

5.2.1 Trusted Roles

Trusted Persons include all employees, contractors, and consultants that have access to or control authentication or cryptographic operations that may materially affect:

- the validation of information in Certificate Applications;
- the acceptance, rejection, or other processing of Certificate Applications, revocation requests, renewal requests, or enrollment information;
- the issuance, or revocation of Certificates, including personnel having access to restricted portions of its repository;
- the handling of Subscriber information or requests.

Trusted Persons include, but are not limited to:

- customer service personnel,
- cryptographic business operations personnel, security personnel,

- system administration personnel,
- designated engineering personnel, and
- executives that are designated to manage infrastructural trustworthiness.

NIFTeTRUST considers the categories of personnel identified in this section as Trusted Persons having a Trusted Position. Persons seeking to become Trusted Persons by obtaining a Trusted Position must successfully complete the screening requirements set out in this CPS.

5.2.2 Number of Persons Required per Task

NIFTeTRUST has established, maintains, and enforces rigorous control procedures to ensure the segregation of duties based on job responsibility and to ensure that multiple Trusted Persons are required to perform sensitive tasks.

Policy and control procedures are in place to ensure segregation of duties based on job responsibilities. The most sensitive tasks, such as access to and management of CA cryptographic hardware (cryptographic signing unit or CSU) and associated key material, require multiple Trusted Persons.

These internal control procedures are designed to ensure that at a minimum, two trusted personnel are required to have either physical or logical access to the device. Access to CA cryptographic hardware is strictly enforced by multiple Trusted Persons throughout its lifecycle, from incoming receipt and inspection to final logical and/or physical destruction. Once a module is activated with operational keys, further access controls are invoked to maintain split control over both physical and logical access to the device. Persons with physical access to modules do not hold “Secret Shares” and vice versa.

Other manual operations such as the validation and issuance of Class 3 Certificates, not issued by an automated validation and issuance system, require the participation of at least two (2) Trusted Persons, or a combination of at least one trusted person and an automated validation and issuance process. Manual operations for Key Recovery may optionally require the validation of two (2) authorized Administrators.

5.2.3 Identification and Authentication for Each Role

For all personnel seeking to become Trusted Persons, verification of identity is performed through the personal (physical) presence of such personnel before Trusted Persons performing NIFTeTRUST HR or security functions and a check of well-recognized forms of identification (e.g., passports and driver’s licenses). Identity is further confirmed through the background checking procedures in CPS.

NIFTeTRUST ensures that personnel have achieved Trusted Status and departmental approval has been given before such personnel are:

- issued access devices and granted access to the required facilities;
- issued electronic credentials to access and perform specific functions on NTN CA, RA, or other IT systems.

5.2.4 Roles Requiring Separation of Duties

Roles requiring Separation of duties include (but are not limited to)

- the validation of information in Certificate Applications;   the acceptance, rejection, or other processing of Certificate Applications, revocation requests, key recovery requests or renewal requests, or enrollment information;

- the issuance, or revocation of Certificates, including personnel having access to restricted portions of the repository;
- the handling of Subscriber information or requests
- the generation, issuing or destruction of a CA certificate
- the loading of a CA to a Production environment

5.3 Personnel Controls

Personnel seeking to become Trusted Persons must present proof of the requisite background, qualifications, and experience needed to perform their prospective job responsibilities competently and satisfactorily, as well as proof of any government clearances, if any, necessary to perform certification services under government contracts. Background checks are repeated at least every 5 years for personnel holding Trusted Positions.

5.3.1 Qualifications, Experience, and Clearance Requirements

NIFTeTRUST requires that personnel seeking to become Trusted Persons present proof of the requisite background, qualifications, and experience needed to perform their prospective job responsibilities competently and satisfactorily, as well as proof of any government clearances, if any, necessary to perform certification services under government contracts.

5.3.2 Background Check Procedures

Prior to commencement of employment in a Trusted Role, NIFTeTRUST conducts background checks which include the following:

- confirmation of previous employment,
- check of professional reference,
- confirmation of the highest or most relevant educational degree obtained,
- search of criminal records (local, state or provincial, and national),
- check of credit/financial records, search of driver's license records, and
- search of Social Security Administration records.

To the extent that any of the requirements imposed by this section cannot be met due to a prohibition or limitation in local law or other circumstances, NIFTeTRUST will utilize a substitute investigative technique permitted by law that provides substantially similar information, including but not limited to obtaining a background check performed by the applicable governmental agency.

The factors revealed in a background check that may be considered grounds for rejecting candidates for Trusted Positions or for taking action against an existing Trusted Person generally include (but are not limited to) the following:

- Misrepresentations made by the candidate or Trusted Person,
- Highly unfavourable or unreliable professional references,
- Certain criminal convictions, and
- Indications of a lack of financial responsibility.

Reports containing such information are evaluated by human resources and security personnel, who determine the appropriate course of action in light of the type, magnitude, and frequency of the behavior uncovered by the background check. Such actions may include measures up to and including the cancellation of offers of employment made to candidates for Trusted Positions or the termination of existing Trusted Persons.

The use of information revealed in a background check to take such actions is subject to the applicable federal, state, and local laws.

5.3.3 Training Requirements

NIFTeTRUST provides its personnel with training upon hire as well as the requisite on-the-job training needed for them to perform their job responsibilities competently and satisfactorily. NIFTeTRUST maintains records of such training. NIFTeTRUST periodically reviews and enhances its training programs as necessary.

NIFTeTRUST training programs are tailored to the individual's responsibilities and include the following as relevant:

- Basic PKI concepts,
- Job responsibilities,
- NIFTeTRUST security and operational policies and procedures,
- Use and operation of deployed hardware and software,
- Incident and Compromise reporting and handling, and
- Disaster recovery and business continuity procedures.

5.3.3.1 CABF Requirements for Training and Skill Level

For EV SSL Certificates, EV Code Signing, and Organization-validated and Domain-validated SSL Certificates, personnel training is provided as set forth in the NTN Supplemental Procedures, Appendix.

5.3.4 Retraining Frequency and Requirements

NIFTeTRUST provides refresher training and updates to their personnel to the extent and frequency required to ensure that such personnel maintain the required level of proficiency to perform their job responsibilities competently and satisfactorily.

5.3.5 Job Rotation Frequency and Sequence

Not applicable

5.3.6 Sanctions for Unauthorized Actions

Appropriate disciplinary actions are taken for unauthorized actions or other violations of NIFTeTRUST policies and procedures. Disciplinary actions may include measures up to and including termination and are commensurate with the frequency and severity of the unauthorized actions.

5.3.7 Independent Contractor Requirements

In limited circumstances, independent contractors or consultants may be used to fill Trusted Positions. Any such contractor or consultant is held to the same functional and security criteria that apply to a NIFTeTRUST employees in a comparable position.

Independent contractors and consultants who have not completed or passed the background check procedures specified in CPS § 5.3.2 are permitted access to NIFTeTRUST secure facilities only to the extent they are escorted and directly supervised by Trusted Persons at all times.

5.3.8 Documentation Supplied to Personnel

NIFTeTRUST provides its employees the requisite training and other documentation needed to perform their job responsibilities competently and satisfactorily.

5.4 Audit Logging Procedures

5.4.1 Types of Events Recorded

NIFTeTRUST manually or automatically logs the following significant events:

- CA key life cycle management events, including:
  - Key generation, backup, storage, recovery, archival, and destruction
  - Cryptographic device life cycle management events.
- CA and Subscriber certificate life cycle management events, including:
  - Certificate Applications, renewal, rekey, and revocation
  - Successful or unsuccessful processing of requests
  - Generation and issuance of Certificates and CRLs.
- Security-related events including:
  - Successful and unsuccessful PKI system access attempts
  - PKI and security system actions performed by NIFTeTRUST personnel
  - Security sensitive files or records read, written or deleted
  - Security profile changes
  - System crashes, hardware failures and other anomalies
  - Firewall and router activity
  - CA facility visitor entry/exit.

Log entries include the following elements:

- Date and time of the entry
- Serial or sequence number of entry, for automatic journal entries
- Identity of the entity making the journal entry
- Description/kind of entry.

NIFTeTRUST RAs and Enterprise Administrators log Certificate Application information including:

- Kind of identification document(s) presented by the Certificate Applicant
- Record of unique identification data, numbers, or a combination thereof (e.g., Certificate Applicant's driver's license number) of identification documents, if applicable
- Storage location of copies of applications and identification documents
- Identity of entity accepting the application
- Method used to validate identification documents, if any

- Name of receiving CA or submitting RA, if applicable.

EV SSL Certificates, EV Code Signing, and domain-validated and organization-validated SSL Certificates conform to the CA /Browser Forum requirements as set forth in the NTN Supplemental Procedures Appendix.

5.4.2 Frequency of Processing Log

The CA system is continuously monitored to provide real time alerts of significant security and operational events for review by designated system security personnel. Monthly reviews of the audit logs include verifying that the logs have not been tampered with and thoroughly investigating any alerts or irregularities detected in the logs. Actions taken based on audit log reviews are also documented.

5.4.3 Retention Period for Audit Log

Audit logs shall be retained onsite for at least two (2) months after processing and thereafter archived in accordance with Section 5.5.2.

5.4.4 Protection of Audit Log

Audit logs are protected with an electronic audit log system that includes mechanisms to protect the log files from unauthorized viewing, modification, deletion, or other tampering.

5.4.5 Audit Log Backup Procedures

Incremental backups of audit logs are created daily and full backups are performed weekly.

5.4.6 Audit Collection System (Internal vs. External)

Automated audit data is generated and recorded at the application, network and operating system level. Manually generated audit data is recorded by NIFTeTRUST personnel.

5.4.7 Notification to Event-Causing Subject

Where an event is logged by the audit collection system, no notice is required to be given to the individual, organization, device, or application that caused the event.

5.4.8 Vulnerability Assessments

Events in the audit process are logged, in part, to monitor system vulnerabilities. Logical security vulnerability assessments (“LSVAs”) are performed, reviewed, and revised following an examination of these monitored events. LSVAs are based on real-time automated logging data and are performed on a daily, monthly, and annual basis. An annual LSVA will be an input into an entity’s annual Compliance Audit.

5.5 Records Archival

5.5.1 Types of Records Archived

NIFTeTRUST archives:

- All audit data collected in terms of Section 5.4
- Certificate application information
- Documentation supporting certificate applications
- Certificate lifecycle information e.g., revocation, rekey and renewal application information

5.5.2 Retention Period for Archive

Records shall be retained for at least the time periods set forth below following the date the Certificate expires or is revoked.

- Five (5) years for Class 1 Certificates,
- Ten (10) years and six (6) months for Class 2 and Class 3 Certificates

5.5.3 Protection of Archive

NIFTeTRUST protects the archive so that only authorized Trusted Persons are able to obtain access to the archive. The archive is protected against unauthorized viewing, modification, deletion, or other tampering by storage within a Trustworthy System. The media holding the archive data and the applications required to process the archive data shall be maintained to ensure that the archive data can be accessed for the time period set forth in this CPS.

5.5.4 Archive Backup Procedures

NIFTeTRUST incrementally backs up electronic archives of its issued Certificate information on a daily basis and performs full backups on a weekly basis. Copies of paper-based records shall be maintained in an off-site secure facility.

5.5.5 Requirements for Time-Stamping of Records

Certificates, CRLs, and other revocation database entries shall contain time and date information. Such time information need not be cryptographic-based.

5.5.6 Archive Collection System (Internal or External)

NIFTeTRUST archive collection systems are internal, except for enterprise RA Customers. NIFTeTRUST assists its enterprise RAs in preserving an audit trail. Such an archive collection system therefore is external to that enterprise RA.

5.5.7 Procedures to Obtain and Verify Archive Information

Only authorized Trusted Personnel are able to obtain access to the archive. The integrity of the information is verified when it is restored.

5.6 Key Changeover

NTN CA key pairs are retired from service at the end of their respective maximum lifetimes as defined in this CPS. NTN CA Certificates may be renewed as long as the cumulative certified lifetime of the CA key pair does not exceed the maximum CA key pair lifetime. New CA key pairs will be generated as necessary, for example to replace CA key pairs that are being retired, to supplement existing, active key pairs and to support new services.

Prior to the expiration of the CA Certificate for a Superior CA, key changeover procedures are enacted to facilitate a smooth transition for entities within the Superior CA's hierarchy from the old

Superior CA key pair to new CA key pair(s). NIFTeTRUST CA key changeover process requires that:

- A Superior CA ceases to issue new Subordinate CA Certificates no later than 60 days before the point in time ("Stop Issuance Date") where the remaining lifetime of Superior CA key pair equals the approved Certificate Validity Period for the specific type(s) of Certificates issued by Subordinate CAs in the Superior CA's hierarchy.

- Upon successful validation of Subordinate CA (or end-user Subscriber) Certificate requests received after the "Stop Issuance Date," Certificates will be signed with a new CA key pair.

The Superior CA continues to issue CRLs signed with the original Superior CA private key until the expiration date of the last Certificate issued using the original key pair has been reached

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

Backups of the following CA information shall be kept in off-site storage and made available in the event of a Compromise or disaster: Certificate Application data, audit data, and database records for all Certificates issued. Back-ups of CA private keys shall be generated and maintained in accordance with CP § 6.2.4. NIFTeTRUST maintains backups of the foregoing CA information for their own CAs, as well as the CAs of Enterprise Customers within its Sub-domain.

5.7.2 Computing Resources, Software, and/or Data Are Corrupted

In the event of the corruption of computing resources, software, and/or data, such an occurrence is reported to NIFTeTRUST Security and NIFTeTRUST incident handling procedures are enacted. Such procedures require appropriate escalation, incident investigation, and incident response. If necessary, NIFTeTRUST key compromise or disaster recovery procedures will be enacted.

5.7.3 Entity Private Key Compromise Procedures

Upon the suspected or known Compromise of a NTN CA, NIFTeTRUST infrastructure or Customer CA private key, NIFTeTRUST Key Compromise Response procedures are enacted by the NIFTeTRUST Security Incident Response Team (SSIRT). This team, which includes Security, Cryptographic Business Operations, Production Services personnel, and other NIFTeTRUST management representatives, assesses the situation, develops an action plan, and implements the action plan with approval from NIFTeTRUST executive management.

If CA Certificate revocation is required, the following procedures are performed:

- The Certificate's revoked status is communicated to Relying Parties through the NIFTeTRUST Repository in accordance with CPS.

- Commercially reasonable efforts will be made to provide additional notice of the revocation to all affected NTN Participants, and
- The CA will generate a new key pair in accordance with CPS, except where the CA is being terminated in accordance with CPS.

5.7.4 Business Continuity Capabilities after a Disaster

NIFTeTRUST has created and maintains business continuity plans so that in the event of a business disruption, critical business functions may be resumed. NIFTeTRUST maintains a Disaster Recovery Facility (DRF) located at a facility geographically separate from the primary Production Facility.

The DRF is a hardened facility designed to federal government and military specifications and is also specifically equipped to meet NIFTeTRUST security standards.

In the event of a natural or man-made disaster requiring permanent cessation of operations from NIFTeTRUST primary facility, the Corporate NIFTeTRUST Business Continuity Team and the NIFTeTRUST Authentication Operations Incident Management Team will coordinate with cross functional management teams to make the decision to formally declare a disaster situation and manage the incident. Once a disaster situation is declared, restoration of NIFTeTRUST Production services functionality at the DRF will be initiated.

NIFTeTRUST has developed a Disaster Recovery Plan (DRP) for its managed PKI services including the NTN PKI service. The DRP identifies conditions for activating the plan and what constitutes an acceptable system outage and recovery time. The DRP defines the procedures for the teams to reconstitute NIFTeTRUST NTN operations using backup data and backup copies of the NTN keys.

Additionally, for EV SSL Certificates, EV Code Signing, and Organization-validated and Domain-validated SSL Certificates, NIFTeTRUST DRP includes the CA / Browser Forum requirements as set forth in the NTN Supplemental Procedures, Appendix B1, Appendix C and Appendix D, respectively.

The target recovery time for restoring critical Production service functionality is no greater than 24 hours.

NIFTeTRUST conducts at least one disaster recovery test per calendar year to ensure functionality of services at the DRF. Formal Business Continuity Exercises are also conducted yearly in coordination with the Corporate NIFTeTRUST Business Continuity Team where procedures for additional types of scenarios (e.g. pandemic, earthquake, flood, power outage) are tested and evaluated.

NIFTeTRUST takes significant steps to develop, maintain, and test sound business recovery plans, and NIFTeTRUST planning for a disaster or significant business disruption is consistent with many of the best practices established within the industry.

NIFTeTRUST maintains redundant hardware and backups of its CA and infrastructure system software at its disaster recovery facility. In addition, CA private keys are backed up and maintained for disaster recovery purposes in accordance with CPS.

NIFTeTRUST maintains offsite backups of important CA information for NTN CAs as well as the CAs of Service Centers, and Enterprise Customers, within NIFTeTRUST Sub-domain. Such information includes, but is not limited to: Certificate Application data, audit data (per Section 4.5), and database records for all Certificates issued.

5.8 CA or RA Termination

In the event that it is necessary for a NTN CA, or Enterprise Customer CA to cease operation, NIFTeTRUST makes a commercially reasonable effort to notify Subscribers, Relying Parties, and other affected entities of such termination in advance of the CA termination. Where CA termination is required, NIFTeTRUST and, in the case of a Customer CA, the applicable Customer, will develop a termination plan to minimize disruption to Customers, Subscribers, and Relying Parties. Such termination plans may address the following, as applicable:

- Provision of notice to parties affected by the termination, such as Subscribers, Relying Parties, and Customers, informing them of the status of the CA,
- Handling the cost of such notice,
- The revocation of the Certificate issued to the CA by NIFTeTRUST,
- The preservation of the CA's archives and records for the time periods required in this CPS,
- The continuation of Subscriber and customer support services,
- The continuation of revocation services, such as the issuance of CRLs or the maintenance of online status checking services,
- The revocation of unexpired unrevoked Certificates of end-user Subscribers and subordinate CAs, if necessary,
- Refunding (if necessary) Subscribers whose unexpired unrevoked Certificates are revoked under the termination plan or provision, or alternatively, the issuance of replacement Certificates by a successor CA,
- Disposition of the CA's private key and the hardware tokens containing such private key, and Provisions needed for the transition of the CA's services to a successor CA.

5.9 Data Security

For the issuance of EV SSL Certificates, EV Code Signing, and Organization-validated and Domainvalidated SSL Certificates, NIFTeTRUST conforms to the CA / Browser Forum requirements for Data Security as set forth in the NTN Supplemental Procedures, Appendix B1, Appendix C and Appendix D, respectively.

6 Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

CA key pair generation is performed by multiple pre-selected, trained and trusted individuals using Trustworthy Systems and processes that provide for the security and required cryptographic strength for the generated keys. For PCA and Issuing Root CAs, the cryptographic modules used for key generation meet the requirements of FIPS 140-1 level 3. For other CAs (including NTN CAs and Managed PKI Customer CAs), the cryptographic modules used meet the requirements of at least FIPS 140-1 level 2.

All CA key pairs are generated in pre-planned Key Generation Ceremonies in accordance with the requirements of the Key Ceremony Reference Guide, the CA Key Management Tool User's

Guide, and the NIFTeTRUST SAR Guide. The activities performed in each key generation ceremony are recorded, dated and signed by all individuals involved. These records are kept for audit and tracking purposes for a length of time deemed appropriate by NIFTeTRUST Management.

Generation of RA key pairs is generally performed by the RA using a FIPS 140-1 level 1 certified cryptographic module provided with their browser software.

Enterprise Customers generate the key pair used by their Automated Administration servers. NIFTeTRUST recommends that Automated Administration server key pair generation be performed using a FIPS 140-1 level 2 certified cryptographic module.

Generation of end-user Subscriber key pairs is generally performed by the Subscriber. For Class 1 Certificates, Class 2 Certificates, and Class 3 Code/Object Signing Certificates, the Subscriber typically uses a FIPS 140-1 level 1 certified cryptographic module provided with their browser software for key generation. For server Certificates, the Subscriber typically uses the key generation utility provided with the web server software.

For ACS Application IDs, NIFTeTRUST generates a key pair on behalf of the Subscriber using a random numbers seed generated on a cryptographic module that, at a minimum, meets the requirements of FIPS 140-1 level 3.

Supplementary practices in Appendix B and C identify additional requirements for Certificates conforming to the CA/ Browser Forum requirements.

6.1.2 Private Key Delivery to Subscriber

When end-user Subscriber key pairs are generated by the end-user Subscriber, private key delivery to a Subscriber is not applicable. For ACS Application IDs, private key delivery to a Subscriber is also not applicable.

Where RA or end-user Subscriber key pairs are pre-generated by NIFTeTRUST on hardware tokens or smart cards, such devices are distributed to the RA or end-user Subscriber using a commercial delivery service and tamper evident packaging. The data required to activate the device is communicated to the RA or end-user Subscriber using an out of band process. The distribution of such devices is logged by NIFTeTRUST.

Where end-user Subscriber key pairs are pre-generated by Enterprise Customers on hardware tokens or smart cards, such devices are distributed to the end-user Subscriber using a commercial delivery service and tamper evident packaging. The required activation data required to activate the device is communicated to the RA or end-user Subscriber using an out of band process. The distribution of such devices is logged by the Enterprise Customer.

For Enterprise Customers using Managed PKI Key Manager for key recovery services, the Customer may generate encryption key pairs (on behalf of Subscribers whose Certificate Applications they approve) and transmit such key pairs to Subscribers via a password protected PKCS #12 file.

6.1.3 Public Key Delivery to Certificate Issuer

End-user Subscribers and RAs submit their public key to NIFTeTRUST for certification electronically through the use of a PKCS#10 Certificate Signing Request (CSR) or other digitally signed package in a session secured by Secure Sockets Layer (SSL). Where CA, RA, or end-user Subscriber key pairs are generated by NIFTeTRUST, this requirement is not applicable.

6.1.4 CA Public Key Delivery to Relying Parties

NIFTeTRUST makes the CA Certificates for its PCAs and root CAs available to Subscribers and Relying Parties through their inclusion in web browser software. As new PCA and root CA Certificates are generated, NIFTeTRUST provides such new Certificates to the browser manufacturers for inclusion in new browser releases and updates.

NIFTeTRUST generally provides the full certificate chain (including the issuing CA and any CAs in the chain) to the end-user Subscriber upon Certificate issuance. NTN CA Certificates may also be downloaded from the LDAP Directory at *directory.niftetrust.com*.

6.1.5 Key Sizes

Key pairs shall be of sufficient length to prevent others from determining the key pair's private key using cryptanalysis during the period of expected utilization of such key pairs. The NIFTeTRUST Standard for minimum key sizes is the use of key pair's equivalent in strength to 2048 bit RSA for PCAs and CAs. The following table lists NIFTeTRUST Root key pairs and strengths:

Public Key	**Signature**		
Algorithm	**Algorithm**	**Class**	**Generation**
2048 bit RSA	SHA256	Class 1, 2, 3 PCAs	G1 PCAs
		Class 3 PCA	G1 PCA
	SHA256	Class 1, 2 and Class 3 Universal Root PCA	G1 PCAs
384 bit ECC	SHA384	Class 1, 2, 3 PCAs	G2 PCAs
4096 bit RSA	SHA384	Class 3 PCA	G3 PCA
2048_256 bit DSA	SHA256	Class 1, 2, 3 PCAs	G4 PCAs

Table: NIFTeTRUST Root CAs and Key Sizes

All Classes of NTN PCAs and CAs, and RAs and end entity certificates use either SHA-1 or SHA-2 for digital signature hash algorithm and certain versions of NIFTeTRUST Processing Center support the use of SHA-256 and SHA-384 has algorithms in end-entity Subscriber Certificates.

	Validity period ending on or before 31 Dec 2013	**Validity period ending after 31 Dec 2013**
Digest algorithm	SHA-256, SHA-384 or SHA-512	SHA-256, SHA-384 or SHA-512
Minimum RSA modulus size (bits)	2048	2048
Minimum DSA modulus size (bits)	2048	2048
ECC curve	NIST P-256, P-384 or P-521	NIST P-256, P-384 or P-521

Table 4C – Algorithms and key sizes for Subscriber Certificates

NIFTeTRUST CAs reserve the right to reject a certificate request if the requested Public Key does not meet the minimum algorithm key sizes set forth in this section.

6.1.6 Public Key Parameters Generation and Quality Checking

Not applicable.

6.1.7 Key Usage Purposes (as per X.509 v3 Key Usage Field)

Refer to Section 7.1.2.1.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

NIFTeTRUST has implemented a combination of physical, logical, and procedural controls to ensure the security of NIFTeTRUST and Enterprise Customer CA private keys. Subscribers are required by contract to take necessary precautions to prevent the loss, disclosure, modification, or unauthorized use of private keys.

6.2.1 Cryptographic Module Standards and Controls

For PCA and Issuing Root CA key pair generation and CA private key storage, NIFTeTRUST uses hardware cryptographic modules that are certified at or meet the requirements of FIPS 140-1 Level 3.

6.2.2 Private Key (m out of n) Multi-Person Control

NIFTeTRUST has implemented technical and procedural mechanisms that require the participation of multiple trusted individuals to perform sensitive CA cryptographic operations. NIFTeTRUST uses Shares created and distributed for a particular hardware cryptographic module (n) is required to activate a CA private key stored on the module.

The threshold number of shares needed to sign a CA certificate is three (3). It should be noted that the number of shares distributed for disaster recovery tokens may be less than the number distributed for operational tokens, while the threshold number of required shares remains the same. Secret Shares are protected in accordance with this CPS.

6.2.3 Private Key Escrow

CA private keys are not escrowed. Escrow of private keys for end user subscribers is explained in more detail in Section 4.12.

6.2.4 Private Key Backup

NIFTeTRUST creates backup copies of CA private keys for routine recovery and disaster recovery purposes. Such keys are stored in encrypted form within hardware cryptographic modules and associated key storage devices. Cryptographic modules used for CA private key storage meet the requirements of this CPS. CA private keys are copied to backup hardware cryptographic modules in accordance with this CPS.

Modules containing onsite backup copies of CA private keys are subject to the requirements of CPS. Modules containing disaster recovery copies of CA private keys are subject to the requirements of this CPS.

NIFTeTRUST does not store copies of RA private keys. For the backup of end-user Subscriber private keys, see Section 6.2.3 and Section 4.12. For ACS Application IDs, NIFTeTRUST does not store copies of Subscriber private keys.

6.2.5 Private Key Archival

Upon expiration of a NTN CA Certificate, the key pair associated with the certificate will be securely retained for a period of at least 5 years using hardware cryptographic modules that meet the requirements of this

CPS. These CA key pairs shall not be used for any signing events after the expiration date of the corresponding CA Certificate, unless the CA Certificate has been renewed in terms of this CPS.

NIFTeTRUST does not archive copies of RA and Subscriber private keys.

6.2.6 Private Key Transfer Into or From a Cryptographic Module

NIFTeTRUST generates CA key pairs on the hardware cryptographic modules in which the keys will be used. In addition, NIFTeTRUST makes copies of such CA key pairs for routine recovery and disaster recovery purposes. Where CA key pairs are backed up to another hardware cryptographic module, such key pairs are transported between modules in encrypted form.

6.2.7 Private Key Storage on Cryptographic Module

CA or RA private keys held on hardware cryptographic modules shall be stored in encrypted form.

6.2.8 Method of Activating Private Key

All NIFTeTRUST sub-domain Participants shall protect the activation data for their private keys against loss, theft, modification, unauthorized disclosure, or unauthorized use.

6.2.8.1 Class 1 Certificates

The Standard for Class 1 private key protection is for Subscribers to take commerciallyreasonable measures for the physical protection of the Subscriber's workstation to prevent use of the workstation and its associated private key without the Subscriber's authorization. In addition,

NIFTeTRUST recommends that Subscribers use a password in accordance with Section 6.4.1 or security of equivalent strength to authenticate the Subscriber before the activation of the private key, which includes, for instance, a password to operate the private key, a Windows logon or screen saver password, or a network logon password.

6.2.8.2 Class 2 Certificates

The Standard for Class 2 Private Key protection is for Subscribers to:

- Use a password in accordance with Section 6.4.1 or security of equivalent strength to authenticate the Subscriber before the activation of the private key, which includes, for instance, a password to operate the private key, or a Windows logon or screen saver password; and

- Take commercially reasonable measures for the physical protection of the Subscriber's workstation to prevent use of the workstation and its associated private key without the Subscriber's authorization.

When deactivated, private keys shall be kept in encrypted form only.

6.2.8.3 Class 3 Certificates other than Administrator Certificates

The Standard for Class 3 private key protection (other than Administrators) is for Subscribers to:

- Use a smart card, biometric access device or security of equivalent strength to authenticate the Subscriber before the activation of the private key; and

- Take commercially reasonable measures for the physical protection of the Subscriber's workstation to prevent use of the workstation and its associated private key without the Subscriber's authorization.

Use of a password along with a smart card or biometric access device in accordance with Section 6.4.1 is recommended. When deactivated, private keys shall be kept in encrypted form only.

6.2.8.4 Administrators' Private Keys (Class 3)

The Standard for Administrators' private key protection requires them to:

- Use a smart card, biometric access device, password in accordance with Section 6.4.1, or security of equivalent strength to authenticate the Administrator before the activation of the private key, which includes, for instance, a password to operate the private key, a Windows logon or screen saver password, or a network logon password; and

- Take commercially reasonable measures for the physical protection of the Administrator's workstation to prevent use of the workstation and its associated private key without the Administrator's authorization.

NIFTeTRUST recommends that Administrators use a smart card, biometric access device, or security of equivalent strength along with the use of a password in accordance with Section 6.4.1 to authenticate the Administrator before the activation of the private key.

When deactivated, private keys shall be kept in encrypted form only.

6.2.8.5 Enterprise RAs using a Cryptographic Module (with Automated Administration or with Managed PKI Key Manager Service)

The Standard for private key protection for Administrators using such a cryptographic module requires them to:

- Use the cryptographic module along with a password in accordance with Section 6.4.1 to authenticate the Administrator before the activation of the private key; and

- Take commercially reasonable measures for the physical protection of the workstation housing the cryptographic module reader to prevent use of the workstation and the private key associated with the cryptographic module without the Administrator's authorization.

6.2.8.6 Private Keys Held by Processing Centers (Class 1-3)

An online CA's private key shall be activated by a threshold number of Shareholders, as defined in Section 6.2.2, supplying their activation data (stored on secure media). Once the private key is activated, the private key may be active for an indefinite period until it is deactivated when the CA goes offline. Similarly, a threshold number of Shareholders shall be required to supply their activation data in order to activate an offline CA's private key. Once the private key is activated, it shall be active only for one time.

6.2.9 Method of Deactivating Private Key

NTN CA private keys are deactivated upon removal from the token reader. RA private keys (used for authentication to the RA application) are deactivated upon system log off. RAs are required to log off their workstations when leaving their work area.

Client Administrators, RA, and end-user Subscriber private keys may be deactivated after each operation, upon logging off their system, or upon removal of a smart card from the smart card reader depending upon the authentication mechanism employed by the user. In all cases, end-user Subscribers have an obligation to adequately protect their private key(s) in accordance with this CPS. The private key associated with an ACS Application ID is deleted immediately after it has been used for code signing.

6.2.10 Method of Destroying Private Key

Where required, NIFTeTRUST destroys CA private keys in a manner that reasonably ensures that there are no residuals remains of the key that could lead to the reconstruction of the key. NIFTeTRUST utilizes the zeroization function of its hardware cryptographic modules and other appropriate means to ensure the complete destruction of CA private keys. When performed, CA key destruction activities are logged. The private key associated with an ACS Application ID is deleted immediately after it has been used for code signing.

6.2.11 Cryptographic Module Rating

See Section 6.2.1

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

NTN CA, RA and end-user Subscriber Certificates are backed up and archived as part of NIFTeTRUST routine backup procedures.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

The Operational Period of a Certificate ends upon its expiration or revocation. The Operational Period for key pairs is the same as the Operational Period for the associated Certificates, except that they may continue to be used for decryption and signature verification. The maximum Operational Periods for NIFTeTRUST Certificates for Certificates issued on or after the effective date of this CPS are set forth in Table 8 below[26]. End user Subscriber Certificates that are renewals of existing subscriber certificates may have a longer validity period (up to 3 months).

In addition, NTN CAs stops issuing new Certificates at an appropriate date prior to the expiration of the CA's Certificate such that no Certificate issued by a Subordinate CA expires after the expiration of any Superior CA Certificates.

Certificate Issued By: ***Validity Period***	self-signed (2048 bit RSA) Up to 30 years self-
signed (4096 bit RSA) Up to 50 years	self-signed (256 bit ECC) Up to 30 years self-signed (384
bit ECC) Up to 30 years	
Offline intermediate CA Generally 10	years but up to 15 years after renewal online CA
Generally 5 years but up to 10 years after	renewal[27]

Offline intermediate CA to online CA	Generally 5 years but up to 10 years after renewal[28]
Online CA to End-user Individual Subscriber	Normally up to 3 years, but under the conditions described below, up to 6 years[29] under the conditions described below with no option to renew or re-key. After 6 years new enrollment is required.
Online CA to End-Entity Organizational Subscriber	Normally up to 6 years[30] under the conditions described below with no option to renew or re-key. After 6 years new enrollment is required.

Table 8 – Certificate Operational Periods

Except as noted in this section, NIFTeTRUST sub-domain participants shall cease all use of their key pairs after their usage periods have expired.

Certificates issued by CAs to end-user Subscribers may have Operational Periods longer than three years, up to six years, if the following requirements are met:

- Protection of the Subscriber key pairs in relation to its operational environment for Organizational Certificates, operation within the enhanced protection of a data center and for Individual Certificates, the Subscribers' key pairs reside on a hardware token, such as a smart card,

- Subscribers are required to undergo re-authentication at least every 3 years under Section 3.2.3,

- If a Subscriber is unable to complete re-authentication procedures successfully or is unable to prove possession of such private key when required by the foregoing, the CA shall revoke the Subscriber's Certificate.

NIFTeTRUST also operates the "NIFTeTRUST Class 3 International Server CA", "Thawte SGC CA" and the "Class 3 Open Financial Exchange CA" which are online CAs signed by a PCA. The validity of these CAs may exceed the validity periods described in Table 8 above to ensure continued interoperability of certificates offering SGC and OFX capability.

6.3.2.1 CABF Validity Period Requirements

EV SSL Certificates, EV Code Signing, and domain-validated and organization-validated SSL Certificates conform to the CA /Browser Forum requirements as set forth in the NTN Supplemental Procedures, Appendix B1, Appendix C and Appendix D, respectively.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

Activation data (Secret Shares) used to protect tokens containing NTN CA private keys is generated in accordance with the requirements of CPS § 6.2.2 and the Key Ceremony Reference Guide. The creation and distribution of Secret Shares is logged.

RAs are required to select strong passwords to protect their private keys. NIFTeTRUST password selection guidelines require that passwords:

- be generated by the user;
- have at least fifteen characters;
- have at least one alphabetic and one numeric character;
- have at least one lower-case letter;
- not contain many occurrences of the same character;

- not be the same as the operator's profile name; and not contain a long substring of the user's profile name.

NIFTeTRUST strongly recommends that Enterprise Administrators, RAs, and end-user Subscribers choose passwords that meet the same requirements. NIFTeTRUST also recommends the use of two factor authentication mechanisms (e.g., token and passphrase, biometric and token, or biometric and passphrase) for private key activation.

6.4.2 Activation Data Protection

NIFTeTRUST Shareholders are required to safeguard their Secret Shares and sign an agreement acknowledging their Shareholder responsibilities.

RAs are required to store their Administrator/RA private keys in encrypted form using password protection and their browser's “high security” option.

NIFTeTRUST strongly recommends that Client Administrators, RAs and end-user Subscribers store their private keys in encrypted form and protect their private keys through the use of a hardware token and/or strong passphrase. The use of two factor authentication mechanisms (e.g., token and passphrase, biometric and token, or biometric and passphrase) is encouraged.

6.4.3 Other Aspects of Activation Data

6.4.3.1 Activation Data Transmission

To the extent activation data for private keys are transmitted, NTN Participants shall protect the transmission using methods that protect against the loss, theft, modification, unauthorized disclosure, or unauthorized use of such private keys. To the extent Windows or network logon user name/password combination is used as activation data for an end-user Subscriber, the passwords transferred across a network shall be protected against access by unauthorized users.

6.4.3.2 Activation Data Destruction

Activation data for CA private keys shall be decommissioned using methods that protect against the loss, theft, modification, unauthorized disclosure, or unauthorized use of the private keys protected by such activation data. After the record retention periods in Section 5.5.2 lapse, NIFTeTRUST shall decommission activation data by overwriting and/or physical destruction.

6.5 Computer Security Controls

NIFTeTRUST performs all CA and RA functions using Trustworthy Systems that meet the requirements of NIFTeTRUST SAR Guide. Enterprise Customers must use Trustworthy Systems.

6.5.1 Specific Computer Security Technical Requirements

NIFTeTRUST ensures that the systems maintaining CA software and data files are Trustworthy Systems secure from unauthorized access. In addition, NIFTeTRUST limits access to production servers to those individuals with a valid business reason for such access. General application users do not have accounts on production servers.

NIFTeTRUST production network is logically separated from other components. This separation prevents network access except through defined application processes. NIFTeTRUST uses firewalls to protect the production network from internal and external intrusion and limit the nature and source of network activities that may access production systems.

NIFTeTRUST requires the use of passwords that have a minimum character length and a combination of alphanumeric and special characters. NIFTeTRUST requires that passwords be changed on a periodic basis.

Direct access to NIFTeTRUST databases supporting NIFTeTRUST CA Operations is limited to Trusted Persons in NIFTeTRUST Production Operations group having a valid business reason for such access.

6.5.1.1 CABF Requirements for System Security

EV SSL Certificates, EV Code Signing, and domain validated and organization validated SSL Certificates conform to the CA /Browser Forum requirements as set forth in the NTN Supplemental Procedures, Appendix.

6.5.2 Computer Security Rating

No stipulation.

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

Applications are developed and implemented by NIFTeTRUST in accordance with NIFTeTRUST systems development and change management standards. NIFTeTRUST also provides software to its Enterprise Customers for performing RA and certain CA functions. Such software is developed in accordance with NIFTeTRUST system development standards.

NIFTeTRUST developed software, when first loaded provides a method to verify that the software on the system originated from NIFTeTRUST, has not been modified prior to installation, and is the version intended for use.

6.6.2 Security Management Controls

NIFTeTRUST has mechanisms and/or policies in place to control and monitor the configuration of its CA systems. NIFTeTRUST creates a hash of all software packages and NIFTeTRUST software updates. This hash is used to verify the integrity of such software manually. Upon installation and periodically thereafter, NIFTeTRUST validates the integrity of its CA systems.

6.6.3 Life Cycle Security Controls

No stipulation

6.7 Network Security Controls

NIFTeTRUST performs all its CA and RA functions using networks secured in accordance with the Security and Audit Requirements (SAR) Guide to prevent unauthorized access and other malicious activity. NIFTeTRUST protects its communications of sensitive information through the use of encryption and digital signatures.

6.8 Time-Stamping

Certificates, CRLs, and other revocation database entries shall contain time and date information. Such time information need not be cryptographic-based.

7 Certificate, CRL, and OCSP Profiles

7.1 Certificate Profile

NIFTeTRUST Certificates generally conform to (a) ITU-T Recommendation X.509 (1997): Information Technology - Open Systems Interconnection - The Directory: Authentication Framework, June 1997 and (b) RFC 5280: Internet X.509 Public Key Infrastructure Certificate and CRL Profile, April 2002 (“RFC 5280”). As applicable to the Certificate type, NTN Certificates conform to the current version of the CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates.

At a minimum, X.509 Certificates shall contain the basic fields and indicated prescribed values or value constraints in Table 9 below:

Field	***Value or Value constraint***
Serial Number	Unique value per Issuer DN that exhibits at least 20 bits of entropy.
Signature Algorithm	Object identifier of the algorithm used to sign the certificate (See CP § 7.1.3)
Issuer DN	See Section 7.1.4
Valid From	Universal Coordinate Time base. Synchronized to Master Clock of U.S. Naval Observatory. Encoded in accordance with RFC 5280.
Valid To	Universal Coordinate Time base. Synchronized to Master Clock of U.S. Naval Observatory. Encoded in accordance with RFC 5280.
Subject DN	See CP § 7.1.4
Subject Public Key	Encoded in accordance with RFC 5280
Signature	Generated and encoded in accordance with RFC 5280

Table 9 – Certificate Profile Basic Fields

7.1.1 Version Number(s)

NIFTeTRUST Certificates are X.509 Version 3 Certificates although certain Root Certificates are permitted to be X.509 Version 1 Certificates to support legacy systems. CA certificates shall be X.509 Version 1 or Version 3 CA Certificates. End-user Subscriber Certificates shall be X.509 Version 3.

7.1.2 Certificate Extensions

NIFTeTRUST populates X.509 Version 3 NTN Certificates with the extensions required by Section 7.1.2.1-7.1.2.8. Private extensions are permissible, but the use of private extensions is not warranted under this CP and the applicable CPS unless specifically included by reference.

EV SSL certificate extension requirements are described in Appendix B3 to this CPS.

7.1.2.1 Key Usage

X.509 Version 3 Certificates are generally populated in accordance with RFC 5280: Internet X.509 Public Key Infrastructure Certificate and CRL Profile, April 2002. The criticality field of the KeyUsage extension is generally set to TRUE for CA certificates and may be set to either TRUE or FALSE for end entity Subscriber certificates.

Note: The non-Repudiation bit is not required to be set in these Certificates because the PKI industry has not yet reached a consensus as to what the non-Repudiation bit means. Until such a consensus emerges, the non-Repudiation bit might not be meaningful for potential Relying Parties. Moreover, the most commonly used applications do not always respect the non-Repudiation bit. Therefore, setting the bit might not help Relying Parties make a trust decision.

Consequently, this CPS does not require that the non-Repudiation bit be set. It may be set in the case of dual key pair signature Certificates issued through Managed PKI Key Manager, or as otherwise requested. Any dispute relating to non-repudiation arising from the use of a digital certificate is a matter solely between the Subscriber and the Relying Party(s). NIFTeTRUST shall incur no liability in relation thereto.

7.1.2.2 Certificate Policies Extension

The *CertificatePolicies* extension of X.509 Version 3 Certificates are populated with the object identifier for the NTN CP in accordance with CP Section 7.1.6 and with policy qualifiers set forth in CP Section 7.1.8. The criticality field of this extension shall be set to FALSE.

7.1.2.2.1 CABF Requirement for Certificate Policies Extension

EV SSL Certificates, EV Code Signing, and domain-validated and organization-validated SSL Certificates conform to the CA / Browser Forum requirements as set forth in the NTN Supplemental Procedures, Appendix B1, Appendix C, and Appendix D, respectively.

7.1.2.3 Subject Alternative Names

The *subjectAltName* extension of X.509 Version 3 Certificates are populated in accordance with RFC 5280 with the exception of those issued under Public Lite accounts which may optionally exclude the email address in *SubjectAltName*. The criticality field of this extension shall be set to FALSE.

7.1.2.4 Basic Constraints

NIFTeTRUST X.509 Version 3 CA Certificates *BasicConstraints* extension shall have the CA field set to TRUE. End-user Subscriber Certificates *BasicConstraints* extension shall have the CA field set to FALSE. The criticality field of this extension shall be set to TRUE for CA Certificates, but may be set to TRUE or FALSE for end-user Subscriber Certificates.

NIFTeTRUST X.509 Version 3 CA Certificates shall have a "*pathLenConstraint*" field of the

BasicConstraints extension set to the maximum number of CA certificates that may follow this Certificate in a certification path. CA Certificates issued to an online Enterprise Customer issuing end-user Subscriber Certificates shall have a "*pathLenConstraint*" field set to a value of "0" indicating that only an end-user Subscriber Certificate may follow in the certification path.

7.1.2.5 Extended Key Usage

By default, *ExtendedKeyUsage* is set as a non-critical extension. NTN CA Certificates do not include the *ExtendedKeyUsage* extension.

7.1.2.6 CRL Distribution Points

Most NIFTeTRUST X.509 Version 3 end user Subscriber Certificates and Intermediate CA Certificates include the *cRLDistributionPoints* extension containing the URL of the location where a Relying Party can obtain a CRL to check the CA Certificate's status. The criticality field of this extension is set to FALSE.

7.1.2.7 Authority Key Identifier

NIFTeTRUST generally populates the Authority Key Identifier extension of X.509 Version 3 end user Subscriber Certificates and Intermediate CA Certificates. When the certificate issuer contains the Subject Key Identifier extension, the Authority Key Identifier is composed of the 160-bit SHA-1 hash of the public key of the CA issuing the Certificate. Otherwise, the Authority Key Identifier extension includes the issuing CA's subject distinguished name and serial number. The criticality field of this extension is set to FALSE.

7.1.2.8 Subject Key Identifier

Where NIFTeTRUST populates X.509 Version 3 NTN Certificates with a *subjectKeyIdentifier* extension, the *keyIdentifier* based on the public key of the Subject of the Certificate is generated in accordance with one of the methods described in RFC 5280. Where this extension is used, the criticality field of this extension is set to FALSE.

7.1.3 Algorithm Object Identifiers

NIFTeTRUST Certificates are signed using one of following algorithms.

- ***sha256withRSAEncryption*** OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}

- ***ecdsa-with-Sha256*** OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) ansi-X962(10045) signatures(4) ecdsa-with-SHA2 (3) 2}

- ***ecdsa-with-Sha384*** OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) ansi-X962(10045) signatures(4) ecdsa-with-SHA2 (3) 3}

- ***sha-1WithRSAEncryption*** OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5}

- ***md5WithRSAEncryption*** OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 4}

Certificate signatures produced using these algorithms shall comply with RFC 3279.

sha256WithRSAEncryption will be used over *md5WithRSAEncryption*[34].

7.1.4 Name Forms

NIFTeTRUST populates NTN Certificates with an Issuer Name and Subject Distinguished Name in accordance with Section 3.1.1. The Issuer Name shall be populated in each Certificate issued containing the Country, Organization Name and the Common Name of the Issuer CA.

In addition, NIFTeTRUST may include within end-user Subscriber Certificates an additional Organizational Unit field that contains a notice stating that the terms of use of the Certificate are set forth in a URL which is a pointer to the applicable Relying Party Agreement. This OU must appear if a pointer to the applicable Relying Party Agreement is not included in the policy extension of the certificate.

7.1.5 Name Constraints

No stipulation

7.1.6 Certificate Policy Object Identifier

Where the Certificate Policies extension is used, Certificates contain the object identifier for the Certificate Policy corresponding to the appropriate Class of Certificate as set forth in the NTN CP Section1.2. For legacy Certificates issued prior to the publication of the NTN CP which include the Certificate Policies extension, Certificates refer to the NTN CPS.

7.1.6.1 CABF Requirements for Certificate Policy Object Identifier

EV SSL Certificates, EV Code Signing, and domain-validated and organization-validated SSL Certificates conform to the CA / Browser Forum requirements as set forth in the NTN Supplemental Procedures, Appendix B1, Appendix C and Appendix D, respectively.

7.1.7 Usage of Policy Constraints Extension

No stipulation

7.1.8 Policy Qualifiers Syntax and Semantics

NIFTeTRUST generally populates X.509 Version 3 NTN Certificates with a policy qualifier within the Certificate Policies extension. Generally, such Certificates contain a CPS pointer qualifier that points to the applicable Relying Party Agreement or the NTN CPS. In addition, some Certificates contain a User Notice Qualifier which points to the applicable Relying Party Agreement.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

No stipulation

7.2 CRL Profile

Version 2 CRLs conform to RFC 5280 and contain the basic fields and contents specified in Table 13 below:

Field	Value or Value constraint
Version	See Section 7.2.1.
Signature Algorithm	Algorithm used to sign the CRL in accordance with RFC 3279. (See CPS § 7.1.3)

Issuer	Entity who has signed and issued the CRL.
Effective Date	Issue date of the CRL. CRLs are effective upon issuance.
Next Update	Date by which the next CRL will be issued. CRL issuance frequency is in accordance with the requirements of Section 4.9.7.
Revoked Certificates	Listing of revoked certificates, including the Serial Number of the revoked Certificate and the Revocation Date.

Table 13 – CRL Profile Basic Fields

7.2.1 Version Number(s)

NIFTeTRUST supports both X.509 Version1 and Version 2 CRLs. Version 2 CRLs comply with the requirements of RFC 5280.

7.2.2 CRL and CRL Entry Extensions

No stipulation.

7.3 OCSP Profile

OCSP (Online Certificate Status Protocol) is a way to obtain timely information about the revocation status of a particular certificate. NIFTeTRUST validates:

- Class 2 Enterprise certificates using the Enterprise OCSP which conforms to RFC 2560, and
- Class 2 Enterprise certificates and Class 3 organization certificates using the NIFTeTRUST Trusted Global Validation (TGV) service which conforms to RFC 5019.

CABF Requirement for OCSP Signing

For EV SSL Certificates, EV Code Signing, and domain-validated and organization-validated SSL Certificates, NIFTeTRUST provides OCSP responses as set forth in the NTN Supplemental Procedures, Appendix B1, Appendix C, and Appendix D, respectively.

7.3.1 Version Number(s)

Version 1 of the OCSP specification as defined by RFC2560 and Version 1 of the OCSP specification as defined by RFC 5019 are supported.

7.3.2 OCSP Extensions

NIFTeTRUST TGV Service uses secure timestamp and validity period to establish the current freshness of each OCSP response. NIFTeTRUST does not use a nonce to establish the current freshness of each OCSP response and clients should not expect a nonce in the response to a request that contains a nonce. Instead, clients should use the local clock to check for response freshness.

8 Compliance Audit and Other Assessments

An annual WebTrust for Certification Authorities v2.0 or later or equivalent examination is performed for NIFTeTRUST data center operations and key management operations supporting NIFTeTRUST public and Managed PKI CA services including the NTN Root CAs, Class 3 Organizational CAs, Class 2 Organizational and Individual CAs, and Class 1 Individual CAs specified in Section 1.3.1. The external audit scheme of NIFTeTRUST Japan Inc.'s public CAs is ISAE3402/SSAE16 instead of WebTrust for Certification Authorities. Customer-specific CAs are not specifically audited as part of the audit of NIFTeTRUST operations unless required by the Customer. NIFTeTRUST shall be entitled to require that Enterprise Customers undergo a compliance audit under this CPS and audit programs for these types of Customers.

In addition to compliance audits, NIFTeTRUST shall be entitled to perform other reviews and investigations to ensure the trustworthiness of NIFTeTRUST Sub-domain of the NTN, which include, but are not limited to:

- NIFTeTRUST shall be entitled, within its sole and exclusive discretion, to perform at any time an "Exigent Audit/Investigation" on a Customer in the event NIFTeTRUST has reason to believe that the audited entity has failed to meet NTN Standards, has experienced an incident or compromise, or has acted or failed to act, such that the audited entity's failure, the incident or compromise, or the act or failure to act poses an actual or potential threat to the security or integrity of the NTN.

- NIFTeTRUST shall be entitled to perform "Supplemental Risk Management Reviews" on a Customer following incomplete or exceptional findings in a Compliance Audit or as part of the overall risk management process in the ordinary course of business.

NIFTeTRUST shall be entitled to delegate the performance of these audits, reviews, and investigations to a third party audit firm. Entities that are subject to an audit, review, or investigation shall provide reasonable cooperation with NIFTeTRUST and the personnel performing the audit, review, or investigation.

CABF Requirement for Self-Audits

For EV SSL Certificates, EV Code Signing, and Organization-validated and Domain-validated SSL Certificates, NIFTeTRUST shall conduct self-audits as set forth in the NTN Supplemental Procedures, Appendix B1, Appendix C, and Appendix D, respectively.

8.1 Frequency and Circumstances of Assessment

Compliance Audits are conducted at least annually at the sole expense of the audited entity. Audits are conducted over unbroken sequences of audit periods with each period no longer than one year duration.

8.2 Identity/Qualifications of Assessor

NIFTeTRUST CA compliance audits are performed by a public accounting firm that:

- Demonstrates proficiency in conducting the WebTrust for Certification Authorities v2.0 or later or equivalent,

- Demonstrates proficiency in public key infrastructure technology, information security tools and techniques, security auditing, and the third-party attestation function,

- Is accredited by the American Institute of Certified Public Accountants (AICPA), which requires the possession of certain skill sets, quality assurance measures such as peer review, competency testing, standards with respect to proper assignment of staff to engagements, and requirements for continuing professional education,

- Is bound by law, government regulation, or professional code of ethics; and

- maintains Professional Liability/Errors & Omissions insurance with policy limits of at least one million US dollars in coverage.

8.3 Assessor's Relationship to Assessed Entity

Compliance audits of NIFTeTRUST operations are performed by a public accounting firm that is independent of NIFTeTRUST.

8.4 Topics Covered by Assessment

The scope of NIFTeTRUST annual WebTrust for Certification Authorities (or equivalent) audit includes CA environmental controls, key management operations and Infrastructure/Administrative CA controls, certificate life cycle management and CA business practices disclosure.

8.5 Actions Taken as a Result of Deficiency

With respect to compliance audits of NIFTeTRUST operations, significant exceptions or deficiencies identified during the Compliance Audit will result in a determination of actions to be taken. This determination is made by NIFTeTRUST management with input from the auditor. NIFTeTRUST management is responsible for developing and implementing a corrective action plan. If NIFTeTRUST determines that such exceptions or deficiencies pose an immediate threat to the security or integrity of the NTN, a corrective action plan will be developed within 30 days and implemented within a commercially reasonable period of time. For less serious exceptions or deficiencies, NIFTeTRUST Management will evaluate the significance of such issues and determine the appropriate course of action.

8.6 Communications of Results

NIFTeTRUST makes its annual Audit Report publicly available no later than three (3) months after the end of the audit period. In the event of a delay greater than three months, NIFTeTRUST shall provide an explanatory letter signed by the Qualified Auditor.

9 Other Business and Legal Matters

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

NIFTeTRUST is entitled to charge end-user Subscribers for the issuance, management, and renewal of Certificates.

9.1.2 Certificate Access Fees

NIFTeTRUST does not charge a fee as a condition of making a Certificate available in a repository or otherwise making Certificates available to Relying Parties.

9.1.3 Revocation or Status Information Access Fees

NIFTeTRUST does not charge a fee as a condition of making the CRLs required by the CP available in a repository or otherwise available to Relying Parties. NIFTeTRUST is, however, entitled to charge a fee for providing customized CRLs, OCSP services, or other value-added revocation and status information services. NIFTeTRUST does not permit access to revocation information, Certificate status information, or time stamping in their repositories by third parties that provide products or services that utilize such Certificate status information without NIFTeTRUST prior express written consent.

9.1.4 Fees for Other Services

NIFTeTRUST does not charge a fee for access to this CPS. Any use made for purposes other than simply viewing the document, such as reproduction, redistribution, modification, or creation of derivative works, shall be subject to a license agreement with the entity holding the copyright to the document.

9.1.5 Refund Policy

Within NIFTeTRUST's Sub-domain, the following refund policy:

NIFTeTRUST adheres to, and stands behind, rigorous practices and policies in undertaking certification operations and in issuing certificates. Nevertheless, if for any reason a subscriber is not completely satisfied with the certificate issued to him, her, or it, the subscriber may request that NIFTeTRUST revoke the certificate within thirty (30) days of issuance and provide the subscriber with a refund. Following the initial thirty (30) day period, a subscriber may request that NIFTeTRUST revoke the certificate and provide a refund if NIFTeTRUST has breached a warranty or other material obligation under this CPS or the NetSure Protection Plan relating to the subscriber or the subscriber's certificate. After NIFTeTRUST revokes the subscriber's certificate, NIFTeTRUST will promptly credit the subscriber's credit card account (if the certificate was paid for via credit card) or otherwise reimburse the subscriber via check, for the full amount of the applicable fees paid for the certificate. To request a refund, please call customer service at +009221-111-112-222. This refund policy is not an exclusive remedy and does not limit other remedies that may be available to subscribers.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

Enterprise Customers are encouraged to maintain a commercially reasonable level of insurance coverage for errors and omissions, either through an errors and omissions insurance program with an insurance carrier or a self-insured retention. NIFTeTRUST maintains such errors and omissions insurance coverage.

9.2.2 Other Assets

Enterprise Customers shall have sufficient financial resources to maintain their operations and perform their duties, and they must be reasonably able to bear the risk of liability to Subscribers and Relying Parties. NIFTeTRUST's financial resources are set forth in disclosures appearing at:
http://www.nift.com.pk

9.2.3 Extended Warranty Coverage

The NetSure Protection Plan is an extended warranty program that provides Symantec SSL and code signing certificate subscribers with protection against loss or damage that is due to a defect in issuance of the certificate or other malfeasance caused by Symantec negligence or breach of its contractual obligations, provided that the subscriber of the certificate has fulfilled its obligations under the applicable service agreement. For general information concerning the NetSure Protection Plan, and a discussion of which Certificates are covered by it, see www.symantec.com/about/profile/policies/repository.jsp.

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

The following records of Subscribers shall, subject to Section 9.3.2, be kept confidential and private ("Confidential/Private Information"):

- CA application records, whether approved or disapproved,
- Certificate Application records,
- Private keys held by enterprise Customers using Managed PKI Key Manager and information needed to recover such Private Keys,
- Transactional records (both full records and the audit trail of transactions),
- Audit trail records created or retained by NIFTeTRUST or a Customer,
- Audit reports created by NIFTeTRUST or a Customer (to the extent such reports are maintained), or their respective auditors (whether internal or public),
- Contingency planning and disaster recovery plans, and
- Security measures controlling the operations of NIFTeTRUST hardware and software and the administration of Certificate services and designated enrollment services.

9.3.2 Information Not Within the Scope of Confidential Information

Certificates, Certificate revocation and other status information, NIFTeTRUST repositories and information contained within them are not considered Confidential/Private Information. Information not expressly deemed Confidential/Private Information under Section 9.3.1 shall be considered neither confidential nor private. This section is subject to applicable privacy laws.

9.3.3 Responsibility to Protect Confidential Information

NIFTeTRUST secures private information from compromise and disclosure to third parties.

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

Introduction
Welcome to **NIFT (Pvt) Ltd.**.
NIFT (Pvt) Ltd. ("us", "we", or "our") operates **www.nift.pk** (hereinafter referred to as **"Service"**).
Our Privacy Policy governs your visit to **www.nift.pk**, and explains how we collect, safeguard and disclose information that results from your use of our Service.

We use your data to provide and improve Service. By using Service, you agree to the collection and use of information in accordance with this policy. Unless otherwise defined in this Privacy Policy, the terms used in this Privacy Policy have the same meanings as in our Terms and Conditions.

Our Terms and Conditions (**"Terms"**) govern all use of our Service and together with the Privacy Policy constitutes your agreement with us (**"agreement"**).

2. **Definitions**

SERVICE means the www.nift.pk website operated by NIFT (Pvt) Ltd..

PERSONAL DATA means data about a living individual who can be identified from those data (or from those and other information either in our possession or likely to come into our possession).

USAGE DATA is data collected automatically either generated by the use of Service or from Service infrastructure itself (for example, the duration of a page visit).

COOKIES are small files stored on your device (computer or mobile device).

DATA CONTROLLER means a natural or legal person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed. For the purpose of this Privacy Policy, we are a Data Controller of your data.

DATA PROCESSORS (OR SERVICE PROVIDERS) means any natural or legal person who processes the data on behalf of the Data Controller. We may use the services of various Service Providers in order to process your data more effectively.

DATA SUBJECT is any living individual who is the subject of Personal Data.

THE USER is the individual using our Service. The User corresponds to the Data Subject, who is the subject of Personal Data.

3. **Information Collection and Use**

We collect several different types of information for various purposes to provide and improve our Service to you.

4. **Types of Data Collected**

Personal Data

While using our Service, we may ask you to provide us with certain personally identifiable information that can be used to contact or identify you (**"Personal Data"**). Personally identifiable information may include, but is not limited to:

0.1. Email address
0.2. First name and last name
0.3. Phone number
0.4. Address, Country, State, Province, ZIP/Postal code, City
0.5. Cookies and Usage Data

We may use your Personal Data to contact you with newsletters, marketing or promotional materials and other information that may be of interest to you. You may opt out of receiving any, or all, of these communications from us by following the unsubscribe link.

Usage Data

We may also collect information that your browser sends whenever you visit our Service or when you access Service by or through any device (**"Usage Data"**).

This Usage Data may include information such as your computer's Internet Protocol address (e.g. IP address), browser type, browser version, the pages of our Service that you visit, the time and date of your visit, the time spent on those pages, unique device identifiers and other diagnostic data.

When you access Service with a device, this Usage Data may include information such as the type of device you use, your device unique ID, the IP address of your device, your device operating system, the type of Internet browser you use, unique device identifiers and other diagnostic data.

Location Data

We may use and store information about your location if you give us permission to do so (**“Location Data”**). We use this data to provide features of our Service, to improve and customize our Service.

You can enable or disable location services when you use our Service at any time by way of your device settings.

Tracking Cookies Data

We use cookies and similar tracking technologies to track the activity on our Service and we hold certain information.

Cookies are files with a small amount of data which may include an anonymous unique identifier. Cookies are sent to your browser from a website and stored on your device. Other tracking technologies are also used such as beacons, tags and scripts to collect and track information and to improve and analyze our Service.

You can instruct your browser to refuse all cookies or to indicate when a cookie is being sent. However, if you do not accept cookies, you may not be able to use some portions of our Service.

Examples of Cookies we use:

0.1. **Session Cookies:** We use Session Cookies to operate our Service.

0.2. **Preference Cookies:** We use Preference Cookies to remember your preferences and various settings.

0.3. **Security Cookies:** We use Security Cookies for security purposes.

0.4. **Advertising Cookies:** Advertising Cookies are used to serve you with advertisements that may be relevant to you and your interests.

Other Data

While using our Service, we may also collect the following information: sex, age, date of birth, place of birth, passport details, citizenship, registration at place of residence and actual address, telephone number (work, mobile), details of documents on education, qualification, professional training, employment agreements, non-disclosure agreements, information on bonuses and compensation, information on marital status, family members, social security (or other taxpayer identification) number, office location and other data.

5. **Use of Data**

NIFT (Pvt) Ltd. uses the collected data for various purposes:

0.1. to provide and maintain our Service;

0.2. to notify you about changes to our Service;
0.3. to allow you to participate in interactive features of our Service when you choose to do so;
0.4. to provide customer support;
0.5. to gather analysis or valuable information so that we can improve our Service;
0.6. to monitor the usage of our Service;
0.7. to detect, prevent and address technical issues;
0.8. to fulfil any other purpose for which you provide it;
0.9. to carry out our obligations and enforce our rights arising from any contracts entered into between you and us, including for billing and collection;
0.10. to provide you with notices about your account and/or subscription, including expiration and renewal notices, email-instructions, etc.;
0.11. to provide you with news, special offers and general information about other goods, services and events which we offer that are similar to those that you have already purchased or enquired about unless you have opted not to receive such information;
0.12. in any other way we may describe when you provide the information;
0.13. for any other purpose with your consent.

6. **Retention of Data**

We will retain your Personal Data only for as long as is necessary for the purposes set out in this Privacy Policy. We will retain and use your Personal Data to the extent necessary to comply with our legal obligations (for example, if we are required to retain your data to comply with applicable laws), resolve disputes, and enforce our legal agreements and policies.

We will also retain Usage Data for internal analysis purposes. Usage Data is generally retained for a shorter period, except when this data is used to strengthen the security or to improve the functionality of our Service, or we are legally obligated to retain this data for longer time periods.

7. **Transfer of Data**

Your information, including Personal Data, may be transferred to – and maintained on – computers located outside of your state, province, country or other governmental jurisdiction where the data protection laws may differ from those of your jurisdiction.

If you are located outside Pakistan and choose to provide information to us, please note that we transfer the data, including Personal Data, to Pakistan and process it there.

Your consent to this Privacy Policy followed by your submission of such information represents your agreement to that transfer.

NIFT (Pvt) Ltd. will take all the steps reasonably necessary to ensure that your data is treated securely and in accordance with this Privacy Policy and no transfer of your Personal Data will take place to an organisation or a country unless there are adequate controls in place including the security of your data and other personal information.

8. **Disclosure of Data**

We may disclose personal information that we collect, or you provide:

0.1. **Disclosure for Law Enforcement.**

Under certain circumstances, we may be required to disclose your Personal Data if required to do so by law or in response to valid requests by public authorities.

0.2. **Business Transaction.**

If we or our subsidiaries are involved in a merger, acquisition or asset sale, your Personal Data may be transferred.

0.3. **Other cases. We may disclose your information also:**

0.3.1. to our subsidiaries and affiliates;

0.3.2. to contractors, service providers, and other third parties we use to support our business;

0.3.3. to fulfill the purpose for which you provide it;

0.3.4. for the purpose of including your company’s logo on our website;

0.3.5. for any other purpose disclosed by us when you provide the information;

0.3.6. with your consent in any other cases;

0.3.7. if we believe disclosure is necessary or appropriate to protect the rights, property, or safety of the Company, our customers, or others.

9. **Security of Data**

The security of your data is important to us but remember that no method of transmission over the Internet or method of electronic storage is 100% secure. While we strive to use commercially acceptable means to protect your Personal Data, we cannot guarantee its absolute security.

10. **Your Data Protection Rights Under General Data Protection Regulation (GDPR)**

If you are a resident of the European Union (EU) and European Economic Area (EEA), you have certain data protection rights, covered by GDPR.

We aim to take reasonable steps to allow you to correct, amend, delete, or limit the use of your Personal Data.

If you wish to be informed what Personal Data we hold about you and if you want it to be removed from our systems, please email us at **info@nift.pk**.

In certain circumstances, you have the following data protection rights:

0.1. the right to access, update or to delete the information we have on you;

0.2. the right of rectification. You have the right to have your information rectified if that information is inaccurate or incomplete;

0.3. the right to object. You have the right to object to our processing of your Personal Data;

0.4. the right of restriction. You have the right to request that we restrict the processing of your personal information;

0.5. the right to data portability. You have the right to be provided with a copy of your Personal Data in a structured, machine-readable and commonly used format;

0.6. the right to withdraw consent. You also have the right to withdraw your consent at any time where we rely on your consent to process your personal information;

Please note that we may ask you to verify your identity before responding to such requests. Please note, we may not able to provide Service without some necessary data.

You have the right to complain to a Data Protection Authority about our collection and use of your Personal Data. For more information, please contact your local data protection authority in the European Economic Area (EEA).

11. **Your Data Protection Rights under the Prevention Of Electronic Crimes Act, 2016**

Prevention Of Electronic Crimes Act, 2016 (PECA) is the first state law in the nation to require commercial websites and online services to post a privacy policy. The law’s reach stretches well beyond Pakistan to require a person or company in the Pakistan (and conceivable the world) that operates websites collecting personally identifiable information from Pakistan consumers to post a conspicuous privacy policy on its website stating exactly the information being collected and those individuals with whom it is being shared, and to comply with this policy.

According to PECA we agree to the following:

0.1. users can visit our site anonymously;

0.2. our Privacy Policy link includes the word "Privacy", and can easily be found on the home page of our website;

0.3. users will be notified of any privacy policy changes on our Privacy Policy Page;

0.4. users are able to change their personal information by emailing us at **info@nift.pk**.

Our Policy on "Do Not Track" Signals:

We honor Do Not Track signals and do not track, plant cookies, or use advertising when a Do Not Track browser mechanism is in place. Do Not Track is a preference you can set in your web browser to inform websites that you do not want to be tracked.

You can enable or disable Do Not Track by visiting the Preferences or Settings page of your web browser.

12. **Your Data Protection Rights under the prevention of electronic crimes act, 2016 (PECA)**

If you are a Pakistani resident, you are entitled to learn what data we collect about you, ask to delete your data and not to sell (share) it. To exercise your data protection rights, you can make certain requests and ask us:

0.1. What personal information we have about you. If you make this request, we will return to you:

0.0.1. The categories of personal information we have collected about you.

0.0.2. The categories of sources from which we collect your personal information.

0.0.3. The business or commercial purpose for collecting or selling your personal information.

0.0.4. The categories of third parties with whom we share personal information.

0.0.5. The specific pieces of personal information we have collected about you.

0.0.6. A list of categories of personal information that we have sold, along with the category of any other company we sold it to. If we have not sold your personal information, we will inform you of that fact.

0.0.7. A list of categories of personal information that we have disclosed for a business purpose, along with the category of any other company we shared it with.

Please note, you are entitled to ask us to provide you with this information up to two times in a rolling twelve-month period. When you make this request, the information provided may be limited to the personal information we collected about you in the previous 12 months.

0.2. To delete your personal information. If you make this request, we will delete the personal information we hold about you as of the date of your request from our records and direct any service providers to do the same. In some cases, deletion may be accomplished through de-identification of the information. If you choose to delete your personal information, you may not be able to use certain functions that require your personal information to operate.

0.3. To stop selling your personal information. We don't sell or rent your personal information to any third parties for any purpose. We do not sell your personal information for monetary consideration. However, under some circumstances, a transfer of personal information to a third party, or within our family of companies, without monetary consideration may be considered a "sale" under Pakistani law. You are the only owner of your Personal Data and can request disclosure or deletion at any time.

If you submit a request to stop selling your personal information, we will stop making such transfers.

Please note, if you ask us to delete or stop selling your data, it may impact your experience with us, and you may not be able to participate in certain programs or membership services which require the usage of your personal information to function. But in no circumstances, we will discriminate against you for exercising your rights.

To exercise your Pakistani data protection rights described above, please send your request(s) by email: **helpdesk@nift.pk**.

Your data protection rights, described above, are covered by the PECA, short for the Pakistan Electronic Crime Act. To find out more, visit the official MoIT or National Assembly website.

http://www.na.gov.pk/uploads/documents/1470910659_707.pdf

The PECA took effect on 19th August, 2016.

13. **Service Providers**

We may employ third party companies and individuals to facilitate our Service (**"Service Providers"**), provide Service on our behalf, perform Service-related services or assist us in analysing how our Service is used.

These third parties have access to your Personal Data only to perform these tasks on our behalf and are obligated not to disclose or use it for any other purpose.

14. **Analytics**

We may use third-party Service Providers to monitor and analyze the use of our Service.

15. **CI/CD tools**

We may use third-party Service Providers to automate the development process of our Service.

16. **Behavioral Remarketing**

We may use remarketing services to advertise on third party websites to you after you visited our Service. We and our third-party vendors use cookies to inform, optimise and serve ads based on your past visits to our Service.

17. **Payments**

We may provide paid products and/or services within Service. In that case, we use third-party services for payment processing (e.g. payment processors).

We will not store or collect your payment card details. That information is provided directly to our third-party payment processors whose use of your personal information is governed by their Privacy Policy. These payment processors adhere to the standards set by PCI-DSS as managed by the PCI Security Standards Council, which is a joint effort of brands like Visa, Mastercard, American Express and Discover. PCI-DSS requirements help ensure the secure handling of payment information.

18. **Links to Other Sites**

Our Service may contain links to other sites that are not operated by us. If you click a third party link, you will be directed to that third party's site. We strongly advise you to review the Privacy Policy of every site you visit.

We have no control over and assume no responsibility for the content, privacy policies or practices of any third party sites or services.

19. **Children's Privacy**

Our Services are not intended for use by children under the age of 18 (**"Child"** or **"Children"**).

We do not knowingly collect personally identifiable information from Children under 18. If you become aware that a Child has provided us with Personal Data, please contact us. If we become aware that we have collected Personal Data from Children without verification of parental consent, we take steps to remove that information from our servers.

20. **Changes to This Privacy Policy**

We may update our Privacy Policy from time to time. We will notify you of any changes by posting the new Privacy Policy on this page.

We will let you know via email and/or a prominent notice on our Service, prior to the change becoming effective and update “effective date” at the top of this Privacy Policy.

You are advised to review this Privacy Policy periodically for any changes. Changes to this Privacy Policy are effective when they are posted on this page.

21. **Contact Us**

If you have any questions about this Privacy Policy, please contact us by email: **info@nift.pk**.

9.4.2 Information Treated as Private

Any information about Subscribers that is not publicly available through the content of the issued certificate, certificate directory and online CRLs is treated as private

9.4.3 Information Not Deemed Private

Subject to local laws, all information made public in a certificate is deemed not private.

9.4.4 Responsibility to Protect Private Information

NTN participants receiving private information shall secure it from compromise and disclosure to third parties and shall comply with all local privacy laws in their jurisdiction.

9.4.5 Notice and Consent to Use Private Information

Unless where otherwise stated in this CPS, the applicable Privacy Policy or by agreement, private information will not be used without the consent of the party to whom that information applies. This section is subject to applicable privacy laws

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

NIFTeTRUST shall be entitled to disclose Confidential/Private Information if, in good faith, NIFTeTRUST believes that:

- disclosure is necessary in response to subpoenas and search warrants.
- disclosure is necessary in response to judicial, administrative, or other legal process during the discovery process in a civil or administrative action, such as subpoenas, interrogatories, requests for admission, and requests for production of documents.

This section is subject to applicable privacy laws.

9.4.7 Other Information Disclosure Circumstances

No Stipulation

9.5 Intellectual Property rights

The allocation of Intellectual Property Rights among NIFTeTRUST Sub-domain Participants other than Subscribers and Relying Parties is governed by the applicable agreements among such NIFTeTRUST Sub-domain Participants. The following subsections of Section 9.5 apply to the Intellectual Property Rights in relation to Subscribers and Relying Parties. Property Rights in Certificates and Revocation Information

CAs retains all Intellectual Property Rights in and to the Certificates and revocation information that they issue. NIFTeTRUST and Customers grant permission to reproduce and distribute Certificates on a nonexclusive royalty-free basis, provided that they are reproduced in full and that use of Certificates is subject to the Relying Party Agreement referenced in the Certificate. NIFTeTRUST and Customers shall grant permission to use revocation information to perform Relying Party functions subject to the applicable CRL Usage Agreement, Relying Party Agreement, or any other applicable agreements.

9.5.1 Property Rights in the CPS

NTN Participants acknowledge that NIFTeTRUST retains all Intellectual Property Rights in and to this CPS.

9.5.2 Property Rights in Names

A Certificate Applicant retains all rights it has (if any) in any trademark, service mark, or trade name contained in any Certificate Application and distinguished name within any Certificate issued to such Certificate Applicant.

9.5.3 Property Rights in Keys and Key Material

Key pairs corresponding to Certificates of CAs and end-user Subscribers are the property of the CAs and enduser Subscribers that are the respective Subjects of these Certificates, subject to the rights of enterprise Customers using Managed PKI Key Manager, regardless of the physical medium within which they are stored and protected, and such persons retain all Intellectual Property Rights in and to these key pairs. Without limiting the generality of the foregoing, NIFTeTRUST Root public keys and the Root Certificates containing them, including all PCA public keys and self-signed Certificates, are the property of NIFTeTRUST. NIFTeTRUST licenses software and hardware manufacturers to reproduce such root Certificates to place copies in trustworthy hardware devices or software. Finally, Secret Shares of a CA's private key are the property of the

CA, and the CA retains all Intellectual Property Right in and to such Secret Shares even though they cannot obtain physical possession of the those shares or the CA from NIFTeTRUST.

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

NIFTeTRUST warrants that:

- There are no material misrepresentations of fact in the Certificate known to or originating from the entities approving the Certificate Application or issuing the Certificate,

- There are no errors in the information in the Certificate that were introduced by the entities approving the Certificate Application or issuing the Certificate as a result of a failure to exercise reasonable care in managing the Certificate Application or creating the Certificate,

- Their Certificates meet all material requirements of this CPS, and

- Revocation services and use of a repository conform to the applicable CPS in all material aspects.

Subscriber Agreements may include additional representations and warranties.

9.6.1.1 CABF Warranties and Obligations

EV SSL Certificates, EV Code Signing, and domain-validated and organization-validated SSL Certificates conform to the CA / Browser Forum requirements as set forth in the NTN Supplemental Procedures, Appendix.

9.6.2 RA Representations and Warranties

RAs warrant that:

- There are no material misrepresentations of fact in the Certificate known to or originating from the entities approving the Certificate Application or issuing the Certificate,
- There are no errors in the information in the Certificate that were introduced by the entities approving the Certificate Application as a result of a failure to exercise reasonable care in managing the Certificate Application,
- Their Certificates meet all material requirements of this CPS, and
- Revocation services (when applicable) and use of a repository conform to the applicable CPS in all material aspects.

Subscriber Agreements may include additional representations and warranties.

9.6.3 Subscriber Representations and Warranties

Subscribers warrant that:

- Each digital signature created using the private key corresponding to the public key listed in the Certificate is the digital signature of the Subscriber and the Certificate has been accepted and is operational (not expired or revoked) at the time the digital signature is created,
- Their private key is protected and that no unauthorized person has ever had access to the Subscriber’s private key,
- All representations made by the Subscriber in the Certificate Application the Subscriber submitted are true,
- All information supplied by the Subscriber and contained in the Certificate is true,
- The Certificate is being used exclusively for authorized and legal purposes, consistent with this CPS, and
- The Subscriber is an end-user Subscriber and not a CA, and is not using the private key corresponding to any public key listed in the Certificate for purposes of digitally signing any Certificate (or any other format of certified public key) or CRL, as a CA or otherwise.

Subscriber Agreements may include additional representations and warranties.

9.6.4 Relying Party Representations and Warranties

Relying Party Agreements require Relying Parties to acknowledge that they have sufficient information to make an informed decision as to the extent to which they choose to rely on the information in a Certificate, that they are solely responsible for deciding whether or not to rely on such information, and that they shall bear the legal consequences of their failure to perform the Relying Party obligations in terms of this CPS.

Relying Party Agreements may include additional representations and warranties.

9.6.5 Representations and Warranties of Other Participants

No stipulation

9.7 Disclaimers of Warranties

To the extent permitted by applicable law, Subscriber Agreements and Relying Party Agreements shall disclaim NIFTeTRUST possible warranties, including any warranty of merchantability or fitness for a particular purpose, outside the context of the NetSure Protection Plan.

9.8 Limitations of Liability

To the extent NIFTeTRUST has issued and managed the Certificate(s) at issue in compliance with its Certificate Policy and its Certification Practice Statement, NIFTeTRUST shall have no liability to the Subscriber, any Relying Party, or any other third parties for any damages or losses suffered as a result of the use or reliance on such Certificate(s). To the extent permitted by applicable law, Subscriber Agreements and Relying Party Agreements shall limit NIFTeTRUST liability outside the context of the NetSure Protection Plan. Limitations of liability shall include an exclusion of indirect, special, incidental, and consequential damages. They shall also include the following liability caps limiting NIFTeTRUST damages concerning a specific Certificate:

Class	Liability Caps
Class 1	One Hundred U.S. Dollars ($ 100.00 US)
Class 2	Five Thousand U.S. Dollars ($ 5,000.00 US)
Class 3 **(Symantec)**	One Hundred Thousand U.S. Dollars ($ 100,000.00 US)

Table 14 – Liability Caps

The liability caps in Table 14 limit damages recoverable outside the context of the NIFT (Pvt) Ltd and NetSure Protection Plan. Amounts paid under the NetSure Protection Plan are subject to their own liability caps. The liability caps under the NetSure Protection Plan for different kinds of Certificates range from $10,000 US to $1,750,000 US. *See* the NetSure Protection Plan for more detail at www.symantec.com/about/profile/policies/repository.jsp.

The liability (and/or limitation thereof) of Subscribers shall be as set forth in the applicable Subscriber agreements.

The liability (and/or limitation thereof) of enterprise RAs and the applicable CA shall be set out in the agreement(s) between them.

The liability (and/or limitation thereof) of Relying Parties shall be as set forth in the applicable Relying Party Agreements.

NIFTeTRUST limitation of liability for EV certificates is further described in Appendix B1 to this CPS.

9.9 Indemnities

9.9.1 Indemnification by Subscribers

To the extent permitted by applicable law, Subscribers are required to indemnify NIFTeTRUST for:

- Falsehood or misrepresentation of fact by the Subscriber on the Subscriber's Certificate Application,

- Failure by the Subscriber to disclose a material fact on the Certificate Application, if the misrepresentation or omission was made negligently or with intent to deceive any party,

- The Subscriber's 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 unauthorized use of the Subscriber's private key, or

- The Subscriber's use of a name (including without limitation within a common name, domain name, or e-mail address) that infringes upon the Intellectual Property Rights of a third party.

The applicable Subscriber Agreement may include additional indemnity obligations.

9.9.2 Indemnification by Relying Parties

To the extent permitted by applicable law, Relying Party Agreements shall require Relying Parties to indemnify NIFTeTRUST for:

- The Relying Party's failure to perform the obligations of a Relying Party,

- The Relying Party's reliance on a Certificate that is not reasonable under the circumstances, or
- The Relying Party's failure to check the status of such Certificate to determine if the

  Certificate is expired or revoked.

The applicable Relying Party Agreement may include additional indemnity obligations.

9.9.3 Indemnification of Application Software Suppliers

Notwithstanding any limitations on its liability to Subscribers and Relying Parties, the CA understands and acknowledges that the Application Software Suppliers who have a Root Certificate distribution agreement in place with the NIFTeTRUST Root CA do not assume any obligation or potential liability of the CA under these Requirements or that otherwise might exist because of the issuance or maintenance of Certificates or reliance thereon by Relying Parties or others.

Thus the CA shall defend, indemnify, and hold harmless each Application Software Supplier for any and all claims, damages, and losses suffered by such Application Software Supplier related to a Certificate issued by the CA, regardless of the cause of action or legal theory involved. This does not apply, however, to any claim, damages, or loss suffered by such Application Software Supplier related to a Certificate issued by the CA where such claim, damage, or loss was directly caused by such Application Software Supplier's software displaying as not trustworthy a

Certificate that is still valid, or displaying as trustworthy: (1) a Certificate that has expired, or (2) a Certificate that has been revoked (but only in cases where the revocation status is currently available from the CA online, and the application software either failed to check such status or ignored an indication of revoked status).

9.10 Term and Termination

9.10.1 Term

The CPS becomes effective upon publication in the NIFTeTRUST Repository. Amendments to this CPS become effective upon publication in the NIFTeTRUST Repository.

9.10.2 Termination

This CPS as amended from time to time shall remain in force until it is replaced by a new version.

9.10.3 Effect of Termination and Survival

Upon termination of this CPS, NIFTeTRUST Sub-domain participants are nevertheless bound by its terms for all certificates issued for the remainder of the validity periods of such certificates.

9.11 Individual Notices and Communications with Participants

Unless otherwise specified by agreement between the parties, NIFTeTRUST Sub-domain participants shall use commercially reasonable methods to communicate with each other, taking into account the criticality and subject matter of the communication.

9.12 Amendments

9.12.1 Procedure for Amendment

Amendments to this CPS may be made by the NIFTeTRUST Policy Management Authority (PMA). Amendments shall either be in the form of a document containing an amended form of the CPS or an update. Amended versions or updates shall be linked to the Practices Updates and Notices section of the NIFTeTRUST Repository located at: *www.NIFTeTRUST.com/about/profile/policies/repository.jsp*. Updates supersede any designated or conflicting provisions of the referenced version of the CPS. The PMA shall determine whether changes to the CPS require a change in the Certificate policy object identifiers of the Certificate policies corresponding to each Class of Certificate.

9.12.2 Notification Mechanism and Period

NIFTeTRUST and the PMA reserve the right to amend the CPS without notification for amendments that are not material, including without limitation corrections of typographical errors, changes to

URLs, and changes to contact information. The PMA's decision to designate amendments as material or non-material shall be within the PMA's sole discretion

Proposed amendments to the CPS shall appear in the Practices Updates and Notices section of the NIFTeTRUST Repository, which is located at: www.nift.com.pk.

The PMA solicits proposed amendments to the CPS from other NIFTeTRUST Sub-domain participants. If the PMA considers such an amendment desirable and proposes to implement the amendment, the PMA shall provide notice of such amendment in accordance with this section.

Notwithstanding anything in the CPS to the contrary, if the PMA believes that material amendments to the CPS are necessary immediately to stop or prevent a breach of the security of the NTN or any portion of it, NIFTeTRUST and the PMA shall be entitled to make such amendments by publication in the NIFTeTRUST Repository. Suchamendmentswill be effective immediately upon publication. Within a reasonable time after publication, NIFTeTRUST shall provide notice to Affiliates of such amendments.

9.12.2.1 Comment Period

Except as otherwise stated, the comment period for any material amendments to the CPS shall be fifteen (15) days, starting on the date on which the amendments are posted on the NIFTeTRUST Repository. Any NIFTeTRUST Sub-domain participant shall be entitled to file comments with the PMA up until the end of the comment period.

9.12.2.2 Mechanism to Handle Comments

The PMA shall consider any comments on the proposed amendments. The PMA shall either (a) allow the proposed amendments to become effective without amendment, (b) amend the proposed amendments and republish them as a new amendment when required, or (c) withdraw the proposed amendments. The PMA is entitled to withdraw proposed amendments by notifying Affiliates and providing notice in the Practices Updates and Notices section of the NIFTeTRUST Repository. Unless proposed amendments are amended or withdrawn, they shall become effective upon the expiration of the comment period.

9.12.3 Circumstances under Which OID Must be changed

If the PMA determines that a change is necessary in the object identifier corresponding to a Certificate policy, the amendment shall contain new object identifiers for the Certificate policies corresponding to each Class of Certificate. Otherwise, amendments shall not require a change in Certificate policy object identifier.

9.13 Dispute Resolution Provisions

9.13.1 Disputes among NIFTeTRUST, Affiliates, and Customers

Disputes among NIFTeTRUST Sub-domain participants shall be resolved pursuant to provisions in the applicable agreements among the parties.

9.13.2 Disputes with End-User Subscribers or Relying Parties

To the extent permitted by applicable law, Subscriber Agreements and Relying Party Agreements shall contain a dispute resolution clause. Disputes involving NIFTeTRUST require an initial negotiation period of sixty (60) days followed by litigation in the federal or state court encompassing Santa Clara County, California, in the case of claimants who are U.S. residents, or, in the case of all other claimants, arbitration administered by the International Chamber of

Commerce (“ICC”) in accordance with the ICC Rules of Conciliation and Arbitration, unless otherwise approved by NIFTeTRUST.

9.14 Applicable Law and Jurisdiction

This Certificate Practice Statement is governed by the laws of the Islamic Republic of Pakistan. Disputes arising out of this Agreement are subject to the exclusive jurisdiction of the courts of Karachi, to which the Parties irrevocably submit. This choice of law is made to ensure uniform procedures and interpretation for all NTN Participants, no matter where they are located.

This governing law provision applies only to this CPS. Agreements incorporating the CPS by reference may have their own governing law provisions, provided that this Section 9.14 governs the enforceability, construction, interpretation, and validity of the terms of the CPS separate and apart from the remaining provisions of any such agreements, subject to any limitations appearing in applicable law.

This CPS is subject to applicable national, state, local and foreign laws, rules, regulations, ordinances, decrees, and orders including, but not limited to, restrictions on exporting or importing software, hardware, or technical information.

9.15 Compliance with Applicable Law

This CPS is subject to applicable national, state, local and foreign laws, rules, regulations, ordinances, decrees, and orders including, but not limited to, restrictions on exporting or importing software, hardware, or technical information. NIFTeTRUST licenses its CAs in each jurisdiction that it operates where licensing is required by the law of such jurisdiction for the issuance of Certificates.

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

Not applicable

9.16.2 Assignment

Not applicable

9.16.3 Severability

In the event that a clause or provision of this CPS is held to be unenforceable by a court of law or other tribunal having authority, the remainder of the CPS shall remain valid.

9.16.4 Enforcement (Attorney's Fees and Waiver of Rights)

Not applicable

9.16.5 Force Majeure

To the extent permitted by applicable law, Subscriber Agreements and Relying Party Agreements shall include a force majeure clause protecting NIFTeTRUST.

9.17 Other Provisions

Not applicable

Appendix A: Table of Acronyms and Definitions

Table of Acronyms

Term	Definition
AICPA	American Institute of Certified Public Accountants.
ANSI	The American National Standards Institute.
ACS	Authenticated Content Signing.
BIS	The United States Bureau of Industry and Science of the United States Department of Commerce.
CA	Certification Authority.
ccTLD	Country Code Top-Level Domain
CICA	Canadian Instituted of Chartered Accountants
CP	Certificate Policy.
CPS	Certification Practice Statement.

CRL	Certificate Revocation List.
DBA	Doing Business As
DNS	Domain Name System
EV	Extended Validation
FIPS	United State Federal Information Processing Standards.
FQDN	Fully Qualified Domain Name
ICC	International Chamber of Commerce.
IM	Instant Messaging
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
ISO	International Organization for Standardization
KRB	Key Recovery Block.
LSVA	Logical security vulnerability assessment.
NIST	(US Government) National Institute of Standards and Technology
OCSP	Online Certificate Status Protocol.
OID	Object Identifier
PCA	Primary Certification Authority.
PIN	Personal identification number.
PKCS	Public-Key Cryptography Standard.
PKI	Public Key Infrastructure.
PMA	Policy Management Authority.
QGIS	Qualified Government Information Source
QIIS	Qualified Independent Information Source
RA	Registration Authority.
RFC	Request for comment.
SAR	Security Audit Requirements
S/MIME	Secure multipurpose Internet mail extensions.
SSL	Secure Sockets Layer.
NTN	NIFTeTRUST Trust Network.

TLD	Top-Level Domain
TLS	Transport Layer Security

Definitions

Term	Definition
Administrator	A Trusted Person within the organization of a Processing Center, Service Center, Managed PKI Customer or Gateway Customer that performs validation and other CA or RA functions.
Administrator Certificate	A Certificate issued to an Administrator that may only be used to perform CA or RA functions.
Affiliate	A leading trusted third party, for example in the technology, telecommunications, or financial services industry, that has entered into an agreement with NIFTeTRUST to be a NTN distribution and services channel within a specific territory. In the CAB Forum context, the term "*Affiliate*" refers to: A corporation, partnership, joint venture or other entity controlling, controlled by, or under common control with another entity, or an agency, department, political subdivision, or any entity operating under the direct control of a Government Entity.
Affiliate Practices Legal Requirements Guidebook	A NIFTeTRUST document setting forth requirements for Affiliate CPSs, agreements, validation procedures, and privacy policies, as well as other requirements that Affiliates must meet.
Affiliated Individual	A natural person that is related to a Managed PKI Customer, Managed PKI Lite Customer, or Gateway Customer entity (i) as an officer, director, employee, partner, contractor, intern, or other person within the entity, (ii) as a member of a NIFTeTRUST registered community of interest, or (iii) as a person maintaining a relationship with the entity where the entity has business or other records providing appropriate assurances of the identity of such person.
Applicant	The Private Organization or Government Entity that applies for (or seeks renewal of) an EV Certificate naming it as the Subject.
Applicant Representative	An individual person employed by the Applicant for an EV certificate: (i) who signs and submits, or approves an EV Certificate Request on behalf of an Applicant, and/or (ii) who signs and submits a Subscriber Agreement on behalf of an Applicant.
Application Software Vendor	A developer of Internet browser software or other software that displays or uses certificates and distributes root certificates, such as KDE, Microsoft Corporation, Mozilla Corporation, Opera Software ASA, and Red Hat, Inc.
Applicant	The natural person or Legal Entity that applies for (or seeks renewal of) a Certificate. Once the Certificate issues, the Applicant is referred to as the Subscriber. For Certificates issued to devices, the Applicant is the entity that controls or operates the device named in the Certificate, even if the device is sending the actual certificate request.
Applicant Representative	A natural person or human sponsor who is either the Applicant, employed by the Applicant, or an authorized agent who has express authority to represent the Applicant: (i) who signs and submits, or approves a certificate request on behalf of the Applicant, and/or (ii) who signs and submits a Subscriber Agreement on behalf of the Applicant, and/or (iii) who acknowledges and agrees to the Certificate Terms of Use on behalf of the Applicant when the Applicant is an Affiliate of the CA.
Application Software Supplier	A supplier of Internet browser software or other relying-party application software that displays or uses Certificates and incorporates Root Certificates.
Attestation Letter	A letter attesting that Subject Information is correct written by an accountant, lawyer, government official, or other reliable third party customarily relied upon for such information.

Audit Report	A report from a Qualified Auditor stating the Qualified Auditor's opinion on whether an entity's processes and controls comply with the mandatory provisions of these Requirements.
Automated Administration	A procedure whereby Certificate Applications are approved automatically if enrollment information matches information contained in a database.
Automated Administration Software Module	Software provided by NIFT eTRUST that performs Automated Administration.
Certificate	A message that, at least, states a name or identifies the CA, identifies the Subscriber, contains the Subscriber's public key, identifies the Certificate's Operational Period, contains a Certificate serial number, and is digitally signed by the CA.
Certificate Applicant	An individual or organization that requests the issuance of a Certificate by a CA.
Certificate Application	A request from a Certificate Applicant (or authorized agent of the Certificate Applicant) to a CA for the issuance of a Certificate.
Certificate Approver	who has express authority to represent the Applicant of an EV Certificate to (i) act as a Certificate Requester and to authorize other employees or third parties to act as a Certificate Requester, and (ii) to approve EV Certificate Requests submitted by other Certificate Requesters.
Certificate Chain	An ordered list of Certificates containing an end-user Subscriber Certificate and CA Certificates, which terminates in a root Certificate.
Certificate Data	Certificate requests and data related thereto (whether obtained from the Applicant or otherwise) in the CA's possession or control or to which the CA has access.
Certificate Management Control Objectives	Criteria that an entity must meet in order to satisfy a Compliance Audit.

Term	Definition
Certificate Management Process	Processes, practices, and procedures associated with the use of keys, software, and hardware, by which the CA verifies Certificate Data, issues Certificates, maintains a Repository, and revokes Certificates.
Certificate Policies (CP)	This document, which is entitled "NIFT eTRUST Trust Network Certificate Policies" and is the principal statement of policy governing the NTN.
Certificate Problem Report	Complaint of suspected Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, or inappropriate conduct related to Certificates
Certificate Requester	A Certificate Requester is a natural person who is employed and authorized by the Applicant, or an authorized agent who has express authority to represent the Applicant or a third party (such as an ISP or hosting company) that completes and submits an EV Certificate Request on behalf of the Applicant.
Certificate Revocation List (CRL)	A periodically (or exigently) issued list, digitally signed by a CA, of identified Certificates that have been revoked prior to their expiration dates in accordance with CP § 3.4. The list generally indicates the CRL issuer's name, the date of issue, the date of the next scheduled CRL issue, the revoked Certificates' serial numbers, and the specific times and reasons for revocation.
Certificate Signing Request	A message conveying a request to have a Certificate issued.
Certification Authority (CA)	An entity authorized to issue, manage, revoke, and renew Certificates in the NTN.

Certification Practice Statement (CPS)	A statement of the practices that NIFT eTRUST or an Affiliate employs in approving or rejecting Certificate Applications and issuing, managing, and revoking Certificates, and requires its Managed PKI Customers and Gateway Customers to employ.
Challenge Phrase	A secret phrase chosen by a Certificate Applicant during enrollment for a Certificate. When issued a Certificate, the Certificate Applicant becomes a Subscriber and a CA or RA can use the Challenge Phrase to authenticate the Subscriber when the Subscriber seeks to revoke or renew the Subscriber's Certificate.
Class	A specified level of assurances as defined within the CP. See CP § 1.1.1.
Client Service Center	A Service Center that is an Affiliate providing client Certificates either in the Consumer or Enterprise line of business.
Compliance Audit	A periodic audit that a Processing Center, Service Center, Managed PKI Customer, or Gateway Customer undergoes to determine its conformance with NTN Standards that apply to it.
Compromise	A violation (or suspected violation) of a security policy, in which an unauthorized disclosure of, or loss of control over, sensitive information may have occurred. With respect to private keys, a Compromise is a loss, theft, disclosure, modification, unauthorized use, or other compromise of the security of such private key.
Confidential/Private Information	Information required to be kept confidential and private pursuant to CP § 2.8.1.
Contract Signer	A Contract Signer is a natural person who is employed by the Applicant, or an authorized agent who has express authority to represent the Applicant who has authority on behalf of the Applicant to sign Subscriber Agreements on behalf of the Applicant for an EV Certificate.
Country	A Country shall mean a Sovereign state as defined in the Guidelines.
CRL Usage Agreement	An agreement setting forth the terms and conditions under which a CRL or the information in it can be used.
Cross Certificate	A certificate that is used to establish a trust relationship between two Root CAs.
Customer	An organization that is either a Managed PKI Customer, or Gateway Customer.
Delegated Third Party	A natural person or Legal Entity that is not the CA but is authorized by the CA to assist in the Certificate Management Process by performing or fulfilling one or more of the CA requirements found herein.
Demand Deposit Account	A deposit account held at a bank or other financial institution, the funds deposited in which are payable on demand. The primary purpose of demand accounts is to facilitate cashless payments by means of check, bank draft, direct debit, electronic funds transfer, etc. Usage varies among countries, but a demand deposit account is commonly known as: a checking account, a share draft account, a current account, or a checking account.
Domain Authorization	Correspondence or other documentation provided by a Domain Name Registrant attesting to the authority of an Applicant to request a Certificate for a specific Domain Namespace.
Domain Name	The label assigned to a node in the Domain Name System.
Domain Namespace	The set of all possible Domain Names that are subordinate to a single node in the Domain Name System.
Domain Name Registrant	Sometimes referred to as the "owner" of a Domain Name, but more properly the person(s) or entity(ies) registered with a Domain Name Registrar as having the right to control how a Domain Name is used, such as the natural person or Legal Entity that is listed as the "Registrant" by WHOIS or the Domain Name Registrar.
Domain Name Registrar	A person or entity that registers Domain Names under the auspices of or by agreement with: (i) the

Term	Definition
	Internet Corporation for Assigned Names and Numbers (ICANN), (ii) a national Domain Name authority/registry, or (iii) a Network Information Center (including their affiliates, contractors, delegates, successors, or assigns).
Enterprise, as in Enterprise Service Center	A line of business that an Affiliate enters to provide Managed PKI services to Managed PKI Customers.
Enterprise EV Certificate:	An EV Certificate that an Managed PKI for SSL Customer authorizes NIFTeTRUST to issue at third and higher domain levels that contain the domain that have been verified by NIFTeTRUST.
Enterprise RA	A Managed PKI for SSL customer that can request multiple valid EV Certificates for Domains and Organizations verified by NIFTeTRUST for domains at third and higher domain levels that contain a domain that was verified by NIFTeTRUST in the original EV Certificate, in accordance with the requirements of these Guidelines.
Expiry Date	The "Not After" date in a Certificate that defines the end of a Certificate's validity period.
EV Certificate:	A digital certificate that contains information specified in the EV Guidelines and that has been validated in accordance with the Guidelines.
EV OID	An identifying number, called an "object identifier," that is included in the *certificatePolicies* field of an EV certificate that: (i) indicates which CA policy statement relates to that certificate, and which, (ii) by pre-agreement with one or more Application Software Vendor, marks the certificate as being an EV Certificate.
Exigent Audit/Investigation	An audit or investigation by NIFTeTRUST where NIFTeTRUST has reason to believe that an entitys failure to meet NTN Standards, an incident or Compromise relating to the entity, or an actual or potential threat to the security of the NTN posed by the entity has occurred.
Extended Validation	Validation Procedures defined by the Guidelines for Extended Validation Certificates published by a forum consisting of major certification authorities and browser vendors.
Fully-Qualified Domain Name	A Domain Name that includes the labels of all superior nodes in the Internet Domain Name System.
Government Entity	A government-operated legal entity, agency, department, ministry, branch, or similar element of the government of a country, or political subdivision within such country (such as a state, province, city, county, etc.).
Intellectual Property Rights	Rights under one or more of the following: any copyright, patent, trade secret, trademark, and any other intellectual property rights.
Intermediate Certification Authority (Intermediate CA)	A Certification Authority whose Certificate is located within a Certificate Chain between the Certificate of the root CA and the Certificate of the Certification Authority that issued the end -user Subscriber's Certificate.
Internal Server Name	A Server Name (which may or may not include an Unregistered Domain Name) that is not resolvable using the public DNS.
International Organization	An International Organization is an organization founded by a constituent document, e.g., charter, treaty, convention, or similar document, signed by, or on behalf of, a minimum of two or more Sovereign State governments.
Issuing CA	In relation to a particular Certificate, the CA that issued the Certificate. This could be either a Root CA or a Subordinate CA.
Key Compromise	A Private Key is said to be compromised if its value has been disclosed to an unauthorized person, an unauthorized person has had access to it, or there exists a practical technique by which an unauthorized person may discover its value.

Key Generation Ceremony	A procedure whereby a CA’s or RA’s key pair is generated, its private key is transferred into a cryptographic module, its private key is backed up, and/or its public key is certified.
Key Generation Script	A documented plan of procedures for the generation of a CA Key Pair.
Key Manager Administrator	An Administrator that performs key generation and recovery functions for a Managed PKI Customer using Managed PKI Key Manager.
Key Pair	The Private Key and its associated Public Key.
Key Recovery Block (KRB)	A data structure containing a Subscriber’s private key that is encrypted using an encryption key. KRBs are generated using Managed PKI Key Manager software.
Key Recovery Service	A NIFTeTRUST service that provides encryption keys needed to recover a Key Recovery Block as part of a Managed PKI Customer’s use of Managed PKI Key Manager to recover a Subscriber’s private key.
Legal Entity	An association, corporation, partnership, proprietorship, trust, government entity or other entity with legal standing in a country’s legal system.
Managed PKI	NIFTeTRUST’s fully integrated managed PKI service that allows enterprise Customers of NIFTeTRUST and its Affiliates to distribute Certificates to individuals, such as employees, partners, suppliers, and customers, as well as devices, such as servers, routers, and firewalls. Managed PKI permits enterprises to secure messaging, intranet , extranet, virtual private network, and e-commerce applications.

Term	Definition
Managed PKI Administrator	An Administrator that performs validation or other RA functions for an Managed PKI Customer.
Managed PKI Control Center	A web-based interface that permits Managed PKI Administrators to perform Manual Authentication of Certificate Applications
Managed PKI Key Manager	A key recovery solution for those Managed PKI Customers choosing to implement key recovery under a special Managed PKI Agreement.
Managed PKI Key Management Service Administrator’s Guide	A document setting forth the operational requirements and practices for Managed PKI Customers using Managed PKI Key Manager.
Manual Authentication	A procedure whereby Certificate Applications are reviewed and approved manually one-by-one by an Administrator using a web -based interface.
NetSure Protection Plan	An extended warranty program, which is described in CP § 9.2.3.
Nonverified Subscriber Information	Information submitted by a Certificate Applicant to a CA or RA, and included within a Certificate, that has not been confirmed by the CA or RA and for which the applicable CA and RA provide no assurances other than that the information was submitted by the Certificate Applicant.

Non-repudiation	An attribute of a communication that provides protection against a party to a communication falsely denying its origin, denying that it was submitted, or denying its delivery. Denial of origin includes the denial that a communication originated from the same source as a sequence of one or more prior messages, even if the identity associated with the sender is unknown. Note: only an adjudication by a court, arbitration panel, or other tribunal can ultimately prevent repudiation. For example, a digital signature verified with reference to a NTN Certificate may provide proof in support of a determination of Non-repudiation by a tribunal, but does not by itself constitute Non-repudiation.
Object Identifier	A unique alphanumeric or numeric identifier registered under the International Organization for Standardization's applicable standard for a specific object or object class.
OCSP (Online Certificate Status Protocol)	An online Certificate-checking protocol for providing Relying Parties with real-time Certificate status information.
OCSP Responder	An online server operated under the authority of the CA and connected to its Repository for processing Certificate status requests. See also, Online Certificate Status Protocol.
Offline CA	NTN PCAs, Issuing Root CAs and other designated intermediate CAs that are maintained offline for security reasons in order to protect them from possible attacks by intruders by way of the network. These CAs do not directly sign end user Subscriber Certificates.
Online CA	CAs that sign end user Subscriber Certificates are maintained online so as to provide continuous signing services.
Online Certificate Status Protocol (OCSP)	A protocol for providing Relying Parties with real-time Certificate status information.
Operational Period	The period starting with the date and time a Certificate is issued (or on a later date and time certain if stated in the Certificate) and ending with the date and time on which the Certificate expires or is earlier revoked.
Parent Company	**Parent Company:** A parent company is defined as a company that owns a majority of the Subsidiary Company and this can be verified by referencing a QIIS or from financial statement supplied by a registered Chartered Professional Accountant (CPA) or equivalent outside of the USA.
PKCS #10	Public-Key Cryptography Standard #10, developed by RSA Security Inc., which defines a structure for a Certificate Signing Request.
PKCS #12	Public-Key Cryptography Standard #12, developed by RSA Security Inc., which defines a secure means for the transfer of private keys.
Policy Management Authority (PMA)	The organization within NIFT eTRUST responsible for promulgating this policy throughout the NTN.
Primary Certification Authority (PCA)	A CA that acts as a root CA for a specific Class of Certificates, and issues Certificates to CAs subordinate to it.
Principal Individual(s)	Individuals of a Private Organization, Government Entity or Business Entity that are either owners, partners, managing members, directors or officers, as identified by their title of employment, or an employee, contractor or agent authorized by such entity or organization to conduct business related to the request, issuance and use of EV Certificates.
Private Key	The key of a Key Pair that is kept secret by the holder of the Key Pair, and that is used to create Digital Signatures and/or to decrypt electronic records or files that were encrypted with the corresponding Public Key.

Term	Definition

Processing Center	An organization (NIFTeTRUST or certain Affiliates) that creates a secure facility housing, among other things, the cryptographic modules used for the issuance of Certificates. In the Consumer and Web Site lines of business, Processing Centers act as CAs within the NTN and perform all Certificate lifecycle services of issuing, managing, revoking, and renewing Certificates. In the Enterprise line of business, Processing Centers provide lifecycle services on behalf of their Managed PKI Customers or the Managed PKI Customers of the Service Centers subordinate to them.
Public Key	The key of a Key Pair that may be publicly disclosed by the holder of the corresponding Private Key and that is used by a Relying Party to verify Digital Signatures created with the holder's corresponding Private Key and/or to encrypt messages so that they can be decrypted only with the holder's corresponding Private Key.
Public Key Infrastructure (PKI)	The architecture, organization, techniques, practices, and procedures that collectively support the implementation and operation of a Certificate-based public key cryptographic system. The NTN PKI consists of systems that collaborate to provide and implement the NTN.
Publicly-Trusted Certificate	A Certificate that is trusted by virtue of the fact that its corresponding Root Certificate is distributed as a trust anchor in widely -available application software.
Qualified Auditor	A natural person or Legal Entity that meets the requirements of Section 17.6 (Auditor Qualifications).
Registered Domain Name	A Domain Name that has been registered with a Domain Name Registrar.
Registration Agency	A Governmental Agency that registers business information in connection with an entity's business formation or authorization to conduct business under a license, charter or other certification. A Registration Agency MAY include, but is not limited (i) a State Department of Corporations or a Secretary of State; (ii) a licensing agency, such as a State Department of Insurance; or (iii) a chartering agency, such as a state office or department of financial regulation, banking or finance, or a federal agency such as the Comptroller of Currency (OCC) or Office of Thrift Supervision (OTC)
Registration Authority (RA)	An entity approved by a CA to assist Certificate Applicants in applying for Certificates, and to approve or reject Certificate Applications, revoke Certificates, or renew Certificates.
Regulated Financial Institution	A financial institution that is regulated, supervised, and examined by governmental, national, state or provincial, or local authorities having regulatory authority over such financial institution based on the governmental, national, state or provincial, or local laws under which such financial institution was organized and/or licensed.
Reliable Method of Communication	A method of communication, such as a postal/courier delivery address, telephone number, or email address, that was verified using a source other than the Applicant Representative.
Relying Party	An individual or organization that acts in reliance on a certificate and/or a digital signature.
Relying Party Agreement	An agreement used by a CA setting forth the terms and conditions under which an individual or organization acts as a Relying Party.
Repository	An online database containing publicly-disclosed PKI governance documents (such as Certificate Policies and Certification Practice Statements) and Certificate status information, either in the form of a CRL or an OCSP response.
Reseller	An entity marketing services on behalf of NIFTeTRUST or an Affiliate to specific markets.
Reserved IP Address	An IPv4 or IPv6 address that the IANA has marked as reserved: http://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xml http://www.iana.org/assignments/ipv6 -address-space/ipv6-address-space.xml
Retail Certificate	A Certificate issued by NIFTeTRUST or an Affiliate, acting as CA, to individuals or organizations applying one by one to NIFTeTRUST or an Affiliate on its web site.

Root CA	The top level Certification Authority whose Root Certificate is distributed by Application Software Suppliers and that issues Subordinate CA Certificates.
Root Certificate	The self-signed Certificate issued by the Root CA to identify itself and to facilitate verification of Certificates issued to its Subordinate CAs.
RSA	A public key cryptographic system invented by Rivest, Shamir and Adleman.
Secret Share	A portion of a CA private key or a portion of the activation data needed to operate a CA private key under a Secret Sharing arrangement.
Secret Sharing	The practice of splitting a CA private key or the activation data to operate a CA private key in order to enforce multi-person control over CA private key operations under CP § 6.2.2.
Secure Sockets Layer (SSL)	The industry-standard method for protecting Web communications developed by Netscape Communications Corporation. The SSL security protocol provides data encryption, server authentication, message integrity, and optional client authentication for a Transmission Control Protocol/Internet Protocol connection.
Security and Audit Requirements (SAR) Guide	A NIFT eTRUST document that sets forth the security and audit requirements and practices for Processing Centers and Service Centers.
Security and Practices Review	A review of an Affiliate performed by NIFT eTRUST before an Affiliate is permitted to become operational.
Service Center	An Affiliate that does not house Certificate signing units for the issuance of Certificates for the purpose of issuing Certificates of a specific Class or type, but rather relies on a Processing Center to perform issuance, management, revocation, and renewal of such Certificates.

Term	Definition
Sovereign State	A Sovereign state is a state, or country, that administers its own government, and is not dependent upon, or subject to, another power.
Sub-domain	The portion of the NTN under control of an entity and all entities subordinate to it within the NTN hierarchy.
Subject	The natural person, device, system, unit, or Legal Entity identified in a Certificate as the Subject and holder of a private key corresponding to a public key. The Subject is either the Subscriber or a device under the control and operation of the Subscriber. The term “Subject” can, in the case of an organizational Certificate, refer to the equipment or device that holds a private key. A Subject is assigned an unambiguous name, which is bound to the public key contained in the Subject’s Certificate.
Subject Identity Information	Information that identifies the Certificate Subject. Subject Identity Information does not include a domain name listed in the subjectAltName extension or the Subject commonName field.
Subordinate CA	A Certification Authority whose Certificate is signed by the Root CA, or another Subordinate CA.
Subscriber	In the case of an individual Certificate, a person who is the Subject of, and has been issued, a Certificate. In the case of an organizational Certificate, an organization that owns the equipment or device that is the Subject of, and that has been issued, a Certificate. A Subscriber is capable of using, and is authorized to use, the private key that corresponds to the public key listed in the Certificate.
Subscriber Agreement	An agreement used by a CA or RA setting forth the terms and conditions under which an individual or organization acts as a Subscriber.
Subsidiary Company	A subsidiary company is defined as a company that is majority owned by Applicant as verified by referencing a QIIS or from financial statement supplied by a registered Chartered Professional Accountant (CPA) or equivalent outside of the USA.
Superior Entity	An entity above a certain entity within a NTN hierarchy (the Class 1, 2, or 3 hierarchy).

Supplemental Risk Management Review	A review of an entity by NIFTeTRUST following incomplete or exceptional findings in a Compliance Audit of the entity or as part of the overall risk management process in the ordinary course of business.
NIFTeTRUST	Means, with respect to each pertinent portion of this CPS, NIFTeTRUST Corporation and/or any wholly owned NIFTeTRUST subsidiary responsible for the specific operations at issue.
NIFTeTRUST Digital Notarization Service	A service offered to Managed PKI Customers that provides a digitally signed assertion (a Digital Receipt) that a particular document or set of data existed at a particular point in time.
Terms of Use	Provisions regarding the safekeeping and acceptable uses of a Certificate issued in accordance with these Requirements when the Applicant/Subscriber is an Affiliate of the CA.
Trusted Person	An employee, contractor, or consultant of an entity within the NTN responsible for managing infrastructural trustworthiness of the entity, its products, its services, its facilities, and/or its practices as further defined in CP § 5.2.1.
Trusted Position	The positions within a NTN entity that must be held by a Trusted Person.
Trustworthy System	Computer hardware, software, and procedures that are reasonably secure from intrusion and misuse; provide a reasonable level of availability, reliability, and correct operation; are reasonably suited to performing their intended functions; and enforce the applicable security policy. A trustworthy system is not necessarily a "trusted system" as recognized in classified government nomenclature.
NIFTeTRUST Repository	NIFTeTRUST's database of Certificates and other relevant NIFTeTRUST Trust Network information accessible on -line.
NIFTeTRUST Trust Network (NTN)	The Certificate-based Public Key Infrastructure governed by the NIFTeTRUST Trust Network Certificate Policies, which enables the worldwide deployment and use of Certificates by NIFTeTRUST and its Affiliates, and their respective Customers, Subscribers, and Relying Parties.
NTN Participant	An individual or organization that is one or more of the following within the NTN: NIFTeTRUST, an Affiliate, a Customer, a Universal Service Center, a Reseller, a Subscriber, or a Relying Party.
NTN Standards	The business, legal, and technical requirements for issuing, managing, revoking, renewing, and using Certificates within the NTN.
Unregistered Domain Name	A Domain Name that is not a Registered Domain Name.
Valid Certificate	A Certificate that passes the validation procedure specified in RFC 5280.
Validation Specialists	Someone who performs the information verification duties specified by these Requirements.
Validity Period	The period of time measured from the date when the Certificate is issued until the Expiry Date.
Wildcard Certificate	A Certificate containing an asterisk (*) in the left-most position of any of the Subject Fully-Qualified Domain Names contained in the Certificate.

Appendix B: Supplemental Validation Procedures for Extended Validation (EV) SSL Certificates

The current version of the CA/Browser Forum Guidelines for the Issuance and Management of Extended Validation (EV) SSL Certificates can be accessed at https://cabforum.org/extended validation/

Appendix C: Minimum Cryptographic Algorithm and Key Sizes for EV Certificates

1. Root CA Certificates

	Minimum strength of algorithm
Digest algorithm	SHA-256, SHA-384 or SHA-512
RSA	2048 bit
ECC	256 or 384 bits

2. Subordinate CA Certificates

	Minimum strength of algorithm
Digest algorithm	SHA-256, SHA-384 or SHA-512
RSA	2048 bit
ECC	256 or 384 bits

3. Subscriber Certificates

	Minimum strength of algorithm
Digest algorithm	SHA-256, SHA-384 or SHA-512
RSA	2048 bit
ECC	256 or 384 bits

Appendix D: EV Certificates Required Certificate Extensions

1. Root CA Certificate

Root certificates generated after October 2006 MUST be X.509 v3.

(a) *basicConstraints*

If the certificate is v3 and is created after October 2006, this extension MUST appear as a critical extension in all CA certificates that contain Public Keys used to validate digital signatures on certificates. The CA field MUST be set true. The *pathLenConstraint* field SHOULD NOT be present.

(b) *keyUsage*

If the certificate is v3 and is created after October 2006, this extension MUST be present and MUST be marked critical. Bit positions for *CertSign* and *cRLSign* MUST be set. All other bit positions SHOULD NOT be set.

(c) *certificatePolicies*

This extension SHOULD NOT be present.

(d) ***extendedKeyUsage***

This extension is not present.

All other fields and extensions are set in accordance to RFC 5280.

2. Subordinate CA Certificate

(a) ***certificatePolicies***

MUST be present and SHOULD NOT be marked critical. The set of policy identifiers MUST include the identifier for NIFTeTRUST's EV policy.

certificatePolicies:policyIdentifier (Required) ○ the ***anyPolicy*** identifier if subordinate CA is controlled by NIFTeTRUST

(b) ***cRLDistributionPoint***

is always present and NOT marked critical. It contains the HTTP URL of NIFTeTRUST's CRL service.

(c) ***authorityInformationAccess***

MUST be present and MUST NOT be marked critical.

SHALL contain the HTTP URL of the Issuing CA's OCSP responder (accessMethod = 1.3.6.1.5.5.7.48.1). An HTTP accessMethod SHOULD be included for NIFTeTRUST's certificate (accessMethod = 1.3.6.1.5.5.7.48.2).

(d) ***basicConstraints***

This extension MUST be present and MUST be marked critical in all CA certificates that contain Public Keys used to validate digital signatures on certificates. The CA field MUST be set true. The *pathLenConstraint* field MAY be present.

(e) ***keyUsage***

This extension MUST be present and MUST be marked critical. Bit positions for *CertSign* and *cRLSign* MUST be set. All other bit positions MUST NOT be set.

All other fields and extensions MUST be set in accordance to RFC 5280.

3. Subscriber Certificate

(a) ***certificatePolicies***

MUST be present and SHOULD NOT be marked critical. The set of policyIdentifiers MUST include the identifier for NIFTeTRUST's EV policy.

certificatePolicies:policyIdentifier (Required) ○
EV policy OID

certificatePolicies:policyQualifiers:policyQualifierId (Required)
○ id-qt 2 [RFC 5280]

certificatePolicies:policyQualifiers:qualifier (Required) ○
URI to the Certificate Practice Statement

(b) *cRLDistributionPoint*

is always present and NOT marked critical. It contains the HTTP URL of NIFTeTRUST's CRL service.

(c) *authorityInformationAccess*

is always present and NOT marked critical. SHALL contain the HTTP URL of NIFTeTRUST's OCSP responder (accessMethod = 1.3.6.1.5.5.7.48.1). An HTTP accessMethod MAY be included for NIFTeTRUST's certificate (accessMethod = 1.3.6.1.5.5.7.48.2).

(d) *basicConstraints* (optional)

If present, the CA field MUST be set false.

(e) *keyUsage* (optional)

If present, bit positions for *CertSign* and *cRLSign* MUST NOT be set.

(f) *extKeyUsage*

Either the value *id-kp-serverAuth* [RFC5280] or *id-kp-clientAuth* [RFC5280] or both values MUST be present. Other values SHOULD NOT be present.

(f) *SubjectAltName*

Populated in accordance with RFC5280 and criticality is set to FALSE.

All other fields and extensions set in accordance to RFC 5280.

Appendix E: Supplemental Validation Procedures for Extended Validation (EV) Code-Signing Certificates

The current version of the CA/Browser Forum Guidelines for the Issuance and Management of Extended Validation (EV) Code Signing Certificates can be accessed at https://cabforum.org/evcode-signing-certificate-guidelines/