

NIFTeTRUST

Certificate Policy

Table of Contents

1.	INTRODUCTION	9
1.1	OVERVIEW	9
1.2	DOCUMENT NAME AND IDENTIFICATION	9
1.3	PKI PARTICIPANTS	10
1.3.1	Certification Authorities	10
1.3.2	Registration Authorities	10
1.3.3	Subscribers	10
1.3.4	Relying Parties	11
1.3.5	Other Participants	11
1.4	CERTIFICATE USAGE	11
1.4.1	Appropriate Certificate Uses	11
1.4.2	Prohibited Certificate Uses	11
1.5	POLICY ADMINISTRATION	11
1.5.1	Organization Administering the Document	11
1.5.2	Contact Person	11
1.5.3	Person Determining CP/CPS Suitability for the Policy	12
1.5.4	CP/CPS Approval Procedures	12
1.6	DEFINITIONS AND ACRONYMS	12
1.6.1	Definitions	12
1.6.2	Acronyms	13
1.6.3	References	13
2	PUBLICATION AND REPOSITORY RESPONSIBILITIES	14
2.1	REPOSITORIES	14
2.2	PUBLICATION OF CERTIFICATION INFORMATION	14
2.3	TIME OR FREQUENCY OF PUBLICATION	14
2.4	ACCESS CONTROLS ON REPOSITORIES	14
3	IDENTIFICATION AND AUTHENTICATION	15
3.1	NAMING	15
3.1.1	Type of Names	15
3.1.2	Need for Names to be Meaningful	15
3.1.3	Anonymity or Pseudonymity of Subscribers	15
3.1.4	Rules for Interpreting Various Name Forms	15
3.1.5	Uniqueness of Names	15

3.1.6	Recognition, Authentication, and Role of Trademarks	15
3.2	INITIAL IDENTITY VALIDATION.....	16
3.2.1	Method to Prove Possession of Private Key	16
3.2.2	Authentication of Organization Identity	16
3.2.3	Authentication of Individual Identity	16
3.2.4	Non-verified Subscriber Information	17
3.2.5	Validation of Authority	17
3.2.6	Criteria for Interoperation	17
3.3	IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS	17
3.3.1	Identification and Authentication for Routine Re-key	17
3.3.2	Identification and Authentication for Re-Key after Revocation	17
3.4	IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST	17
4	CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS	19
4.1	CERTIFICATE APPLICATION	19
4.1.1	Who Can Submit a Certificate Application	19
4.1.2	Enrollment Process and Responsibilities	19
4.2	CERTIFICATE APPLICATION PROCESSING	19
4.2.1	Performing Identification and Authentication Functions	19
4.2.2	Approval or Rejection of Certificate Applications	19
4.2.3	Time to Process Certificate Applications	19
4.3	CERTIFICATE ISSUANCE	20
4.3.1	CA Actions during Certificate Issuance	20
4.3.2	Notifications to Subscriber by the CA of Issuance of Certificate	20
4.4	CERTIFICATE ACCEPTANCE.....	20
4.4.1	Conduct Constituting Certificate Acceptance	20
4.4.2	Publication of the Certificate by the CA.....	20
4.4.3	Notification of Certificate Issuance by the CA to Other Entities	20
4.5	KEY PAIR AND CERTIFICATE USAGE	20
4.5.1	Subscriber Private Key and Certificate Usage	20
4.5.2	Relying Party Public Key and Certificate Usage.....	20
4.6	CERTIFICATE RENEWAL	20
4.6.1	Circumstances for Certificate Renewal	20
4.6.2	Who May Request Renewal	21
4.6.3	Processing Certificate Renewal Requests	21
4.6.4	Notification of New Certificate Issuance to Subscriber	21
4.6.5	Conduct Constituting Acceptance of a Renewal Certificate	21
4.6.6	Publication of the Renewal Certificate by the CA	21

4.6.7	Notification of Certificate Issuance by the CA to Other Entities	21
4.7	CERTIFICATE RE-KEY	21
4.7.1	Circumstances for Certificate Re-key	21
4.7.2	Who May Request Certification of a New Public Key	21
4.7.3	Processing Certificate Re-keying Requests	22
4.7.4	Notification of Certificate Issuance to Subscriber	22
4.7.5	Conduct Constituting Acceptance of a Re-keyed Certificate	22
4.7.6	Publication of the Issued Certificate by the CA	22
4.7.7	Notification of Certificate Issuance by the CA to Other Entities	22
4.8	CERTIFICATE MODIFICATION	22
4.8.1	Circumstances for Certificate Modification	22
4.8.2	Who May Request Certificate Modification	22
4.8.3	Processing Certificate Modification Requests	22
4.8.4	Notification of New Certificate Issuance to Subscriber	23
4.8.5	Conduct Constituting Acceptance of Modified Certificate	23
4.8.6	Publication of the Modified Certificate by the CA	23
4.8.7	Notification of Certificate Modification by the CA to Other Entities	23
4.9	CERTIFICATE REVOCATION AND SUSPENSION	23
4.9.1	Circumstances for Revocation	23
4.9.2	Who Can Request Revocation	24
4.9.3	Procedure for Revocation Request	24
4.9.4	Revocation Request Grace Period	25
4.9.5	Time within which CA Must Process the Revocation Request	25
4.9.6	Revocation Checking Requirement for Relying Parties	25
4.9.7	CRL Issuance Frequency	25
4.9.8	Maximum Latency for CRLs	25
4.9.9	On-line Revocation/Status Checking Availability	25
4.9.10	On-line Revocation Checking Requirements	25
4.9.11	Other Forms of Revocation Advertisements Available	25
4.9.12	Special Requirements re Key Compromise	25
4.9.13	Circumstances for Suspension	25
4.9.14	Who Can Request Suspension	26
4.9.15	Procedure for Suspension Request	26
4.9.16	Limits on Suspension Period	26
4.10	CERTIFICATE STATUS SERVICES	26
4.10.1	Operational Characteristics	26
4.10.2	Service Availability	26

4.10.3	Operational Features	26
4.11	END OF SUBSCRIPTION	26
4.12	KEY ESCROW AND RECOVERY	26
4.12.1	Key Escrow and Recovery Policy Practices	26
4.12.2	Session Key Encapsulation and Recovery Policy and Practices.....	26
5	FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS	27
5.1	PHYSICAL CONTROLS.....	27
5.1.1	Site Location and Construction	27
5.1.2	Physical Access	27
5.1.3	Power and Air Conditioning	27
5.1.4	Water Exposures.....	27
5.1.5	Fire Prevention and Protection	28
5.1.6	Media Storage	28
5.1.7	Waste Disposal	28
5.1.8	Off-site Backup	28
5.2	PROCEDURAL CONTROLS	28
5.2.1	Trusted Roles	28
5.2.2	Number of Persons Required per Task	29
5.2.3	Identification and Authentication for each Role	29
5.2.4	Roles Requiring Separation of Duties	29
5.3	PERSONNEL CONTROLS.....	29
5.3.1	Qualifications, Experience, and Clearance Requirements	29
5.3.2	Background Check Procedures	29
5.3.3	Training Requirements	30
5.3.4	Retraining Frequency and Requirements	30
5.3.5	Job Rotation Frequency and Sequence	30
5.3.6	Sanctions for Unauthorized Actions	30
5.3.7	Independent Contractor Requirements.....	30
5.3.8	Documentation Supplied to Personnel	31
5.4	AUDIT LOGGING PROCEDURES	31
5.4.1	Types of Events Recorded	31
5.4.2	Frequency of Processing Log	31
5.4.3	Retention Period for Audit Log	31
5.4.4	Protection of Audit Log	31
5.4.5	Audit Log Backup Procedures	31
5.4.6	Audit Collection System (Internal vs. External)	32
5.4.7	Notification to Event-causing Subject	32

5.4.8	Vulnerability Assessments	32
5.5	RECORDS ARCHIVAL	32
5.5.1	Types of Records Archived	32
5.5.2	Retention Period for Archive.....	33
5.5.3	Protection of Archive	33
5.5.4	Archive Backup Procedures	33
5.5.5	Requirements for Time-stamping of Records	33
5.5.6	Archive Collection System (internal or external)	33
5.5.7	Procedures to Obtain and Verify Archive Information	33
5.6	KEY CHANGEOVER	34
5.7	COMPROMISE AND DISASTER RECOVERY	34
5.7.1	Incident and Compromise Handling Procedures	34
5.7.2	Computing Resources, Software, and/or Data Are Corrupted	34
5.7.3	Entity Private Key Compromise Procedures	34
5.7.4	Business Continuity Capabilities after a Disaster	34
5.8	CA OR RA TERMINATION	35
6	TECHNICAL SECURITY CONTROLS.....	36
6.1	KEY PAIR GENERATION AND INSTALLATION	36
6.1.1	Key Pair Generation	36
6.1.2	Private Key Delivery to Subscriber	36
6.1.3	Public Key Delivery to Certificate Issuer	36
6.1.4	CA Public Key Delivery to Relying Parties.....	36
6.1.5	Key Sizes	36
6.1.6	Public Key Parameters Generation and Quality Checking	36
6.1.7	Key Usage Purposes (as per X.509 v3 key usage field)	36
6.2	PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS	37
6.2.1	Cryptographic Module Standards and Controls	37
6.2.2	Private Key (n out of m) Multi-person Control	37
6.2.3	Private Key Escrow	37
6.2.4	Private Key Backup	37
6.2.5	Private Key Archival	37
6.2.6	Private Key Transfer into or from a Cryptographic Module	37
6.2.7	Private Key Storage on Cryptographic Module	38
6.2.8	Method of Activating Private Keys	38
6.2.9	Method of Deactivating Private Keys	38
6.2.10	Method of Destroying Private Keys	38
6.2.11	Cryptographic Module Rating	38

6.3	OTHER ASPECTS OF KEY PAIR MANAGEMENT	38
6.3.1	Public Key Archival	38
6.3.2	Certificate Operational Periods and Key Pair Usage Periods	38
6.4	ACTIVATION DATA	39
6.4.1	Activation Data Generation and Installation	39
6.4.2	Activation Data Protection	39
6.4.3	Other Aspects of Activation Data	39
6.5	COMPUTER SECURITY CONTROLS	39
6.5.1	Specific Computer Security Technical Requirements	39
6.5.2	Computer Security Rating	39
6.6	LIFE CYCLE TECHNICAL CONTROLS	39
6.6.1	System Development Controls	39
6.6.2	Security Management Controls	40
6.6.3	Life Cycle Security Controls	40
6.7	NETWORK SECURITY CONTROLS	40
6.8	TIME-STAMPING	40
7	CERTIFICATE, CRL, AND OCSP PROFILES	41
7.1	CERTIFICATE PROFILE	41
7.1.1	Version Number(s)	41
7.1.2	Certificate Extensions	41
7.1.3	Algorithm Object Identifiers	41
7.1.4	Name Forms	41
7.1.5	Name Constraints	41
7.1.6	Certificate Policy Object Identifier	41
7.1.7	Usage of Policy Constraints Extension	41
7.1.8	Policy Qualifiers Syntax and Semantics	41
7.1.9	Processing Semantics for the Critical Certificate Policies Extension	41
7.2	CRL PROFILE	42
7.2.1	Version number(s)	42
7.2.2	CRL and CRL Entry Extensions	42
7.3	OCSP PROFILE	42
7.3.1	Version Number(s)	42
7.3.2	OCSP Extensions	42
8	COMPLIANCE AUDIT AND OTHER ASSESSMENTS	43
8.1	FREQUENCY AND CIRCUMSTANCES OF ASSESSMENT	43
8.2	IDENTITY/QUALIFICATIONS OF ASSESSOR	43
8.3	ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY	43

8.4	TOPICS COVERED BY ASSESSMENT.....	43
8.5	ACTIONS TAKEN AS A RESULT OF DEFICIENCY	43
8.6	COMMUNICATIONS OF RESULTS	43
8.7	SELF-AUDITS	43
9	OTHER BUSINESS AND LEGAL MATTERS	44
9.1	FEES	44
9.1.1	Certificate Issuance or Renewal Fees	44
9.1.2	Certificate Access Fees	44
9.1.3	Revocation or Status Information Access Fees	44
9.1.4	Fees for Other Services	44
9.1.5	Refund Policy	44
9.2	FINANCIAL RESPONSIBILITY	44
9.2.1	Insurance Coverage	44
9.2.2	Other Assets	44
9.2.3	Insurance or Warranty Coverage for End-Entities	44
9.3	CONFIDENTIALITY OF BUSINESS INFORMATION	44
9.3.1	Scope of Confidential Information	44
9.3.2	Information Not Within the Scope of Confidential Information	45
9.3.3	Responsibility to Protect Confidential Information.....	45
9.4	PRIVACY OF PERSONAL INFORMATION	45
9.4.1	Privacy Plan	45
9.4.2	Information Treated as Private	45
9.4.3	Information Not Deemed Private	45
9.4.4	Responsibility to Protect Private Information	45
9.4.5	Notice and Consent to Use Private Information	45
9.4.6	Disclosure Pursuant to Judicial or Administrative Process	45
9.4.7	Other Information Disclosure Circumstances.....	45
9.5	INTELLECTUAL PROPERTY RIGHTS	45
9.6	REPRESENTATIONS AND WARRANTIES	46
9.6.1	CA Representations and Warranties	46
9.6.2	RA Representations and Warranties.....	46
9.6.3	Subscriber Representations and Warranties	46
9.6.4	Relying Party Representations and Warranties	47
9.6.5	Representations and Warranties of Other Participants	47
9.7	DISCLAIMERS OF WARRANTIES	48
9.8	LIMITATIONS OF LIABILITY.....	48
9.9	INDEMNITIES.....	48

9.9.1	Indemnification by NIFT	48
9.9.2	Indemnification by Subscribers	48
9.9.3	Indemnification by Relying Parties	49
9.10	TERM AND TERMINATION	49
9.10.1	Term	49
9.10.2	Termination	49
9.10.3	Effect of Termination and Survival	49
9.11	INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS	49
9.12	AMENDMENTS	49
9.12.1	Procedure for Amendment.....	49
9.12.2	Notification Mechanism and Period	49
9.12.3	Circumstances under which OID Must Be Changed	49
9.13	DISPUTE RESOLUTION PROVISIONS.....	49
9.14	GOVERNING LAW	50
9.15	COMPLIANCE WITH APPLICABLE LAW	50
9.16	MISCELLANEOUS PROVISIONS	50
9.16.1	Entire Agreement	50
9.16.2	Assignment	50
9.16.3	Severability	50
9.16.4	Enforcement (attorneys' fees and waiver of rights)	50
9.16.5	Force Majeure	51
9.17	Certificate Policy Management	52

1. INTRODUCTION

1.1 OVERVIEW

This document is the NIFT (Pvt) Ltd. (“NIFT”) Certificate Policy/Certification Practices Statement (CP/CPS) for Private PKI Services that outlines, in RFC 3647 format, the principles and practices related to NIFT’s certification of non-cross-certified and non-publicly trusted X.509 digital certificates.

This Private PKI CP/CPS also applies to the various communities relying on NIFT’s non-publicly trusted certificates, including both the financial and non financial institutions.

This CP/CPS is only one of several documents that control NIFT’s certification services. Other important documents include both private and public documents, such as NIFT’s agreements with its customers, External Program CPs, relying party agreements, Registration Authority Agreements, any applicable Registration Authority Practices Statement (RPS), and NIFT’s privacy policy. NIFT may provide additional certificate policies or certification practice statements. These supplemental policies and statements are available to applicable users or relying parties.

NIFT’s practices for the issuance and management of Verified Certificates are governed in accordance with version 1.4 of the Verified Certificates Requirements.

Users can find the VC Terms of Use (“VC Terms”) in section 9.6.3 of this document.

NIFT’s practices for the issuance and management of Certificates issued for the MATTER program are governed in accordance with the current MATTER Certificate Policy.

1.2 DOCUMENT NAME AND IDENTIFICATION

This document is the NIFT Certificate Policy/Certification Practices Statement for Private PKI Services and has been approved for publication by the NIFT Certificate Policy Authority (CPA) as of the date indicated on the cover page.

The Object Identifier (OID) representing this document is 1.3.6.1.4.1.60140.5.

Object Identifier(s) (OID) for Private PKI External Programs are specified in their respective CPs (or guidelines) and used within the NIFT Private PKI hierarchy when issuing Certificates for those programs.

Date	Changes	Version
01-June-2015	Initial draft.	1.0
13-June-2018	Document updated throughout in order to publish the document on the NIFT Legal Repository.	1.1
13-May-2019	Added updates throughout the document for the financial institutions.	2.0
29-July-2019	Integrated Certification Practices Statement with Certificate Policy.	3.0
29-September-2023	Clarification of Verified Certificates practices, including disclosure of Problem Reporting Mechanism and updated version of Verified Certificates Requirements.	3.5

1.3 PKI PARTICIPANTS

1.3.1 Certification Authorities

NIFT is a certification authority (CA) that issues digital certificates. As a CA, NIFT performs functions associated with both Private PKI Services and public key operations, including receiving applicable certificate requests, issuing, revoking and renewing a digital certificate, and maintaining, issuing, and publishing CRLs and OCSP responses. General information about NIFT's products and services are available at <https://www.NIFT.pk>.

NIFT Root Certificate Authorities and Intermediate CAs under the control of NIFT are managed by the NIFT Certificate Policy Authority (CPA) which is composed of members of NIFT management appointed by NIFT's executive management. The CPA is responsible for this CP/CPS as well as overseeing the review and conformance of CA practices with respective External Program CPs with their own respective Policy Management Authorities and legal agreements.

1.3.2 Registration Authorities

NIFT may delegate the performance of certain functions to Registration Authorities (RA) and other third parties to request certificates and/or perform identification and authentication for end-user certificates. The specific role of an RA or delegated third party varies greatly between entities, ranging from simple translation services to actual assistance in gathering and verifying Applicant information. Some RAs operate identity management systems (IdMs) and may manage the certificate lifecycle for end-users.

Specific roles of each RA under a Private PKI depend highly on the Private PKI party and External Program if applicable. RAs and other Delegated Third Parties for Private PKI External Programs are defined within their respective CP documents, guidelines, and within the legal agreements between the parties. Parties identified in those documents functioning in these roles are required to abide by those definitions as enforced in the additional supportive documentation including technical specifications.

1.3.3 Subscribers

Subscribers use NIFT's services and PKI to support transactions and communications. Subscribers are not always the party identified in a certificate, such as when certificates are issued to an organization's employees. The *Subject* of a certificate is the party named in the certificate. A *Subscriber*, as used herein, refers to both the Subject of the certificate and the entity that contracted with NIFT for the certificate's issuance.

Subscribers for Private PKI External Programs are defined within their respective CP documents, guidelines, and within the legal agreements between the associated parties. Parties identified in those documents as functioning in these roles are required to abide by those definitions as enforced in the additional supportive documentation including the technical specifications.

1.3.4 Relying Parties

Relying parties are entities that act in reliance on a certificate and/or digital signature issued by NIFT. Relying parties are defined by the community supported by the Private PKI infrastructure and by contract with NIFT.

1.3.5 Other Participants

Other Participants are defined in their respective CPs, guidelines, and by contract with NIFT.

1.4 CERTIFICATE USAGE

A *digital certificate* (or *certificate*) is formatted data that cryptographically binds an identified subscriber with a Public Key. A digital certificate allows an entity taking part in an electronic transaction to prove its identity to other participants in such transaction.

The respective Private PKI CPs set forth policies governing the use of NIFT Private PKI Certificates by Subscribers and Relying Parties in the associated program.

1.4.1 Appropriate Certificate Uses

Certificates issued pursuant to this CP/CPS may be used for all legal authentication, encryption, access control, and digital signature purposes, as designated by the key usage and extended key usage fields found within the certificate. However, the sensitivity of the information processed or protected by a certificate varies greatly, and each relying party must evaluate the application environment and associated risks before deciding on whether to use a certificate issued under this CP/CPS. The exact use of each Certificate is left to the discretion of the community for which the PKI is operated.

1.4.2 Prohibited Certificate Uses

Certificates do not guarantee that the Subject is trustworthy, honest, reputable in its business dealings, compliant with any laws, or safe to do business with. A certificate only establishes that the information in the certificate was verified as reasonably correct when the certificate issued.

1.5 POLICY AUTHORITY ADMINISTRATION

1.5.1 Organization Administering the Document

This CP/CPS and the documents referenced herein are maintained by the CPA, which can be contacted at:

NIFT (Pvt) Ltd.
5th Floor AWT Plaza
I.I Chundrigar Road
Karachi - 72400

1.5.2 Contact Person

Attn: Imran Ashraf
NIFT (Pvt) Ltd.
5th Floor AWT Plaza
I.I Chundrigar Road
Karachi - 72400
021-111-112-222

Verified Certificates Revocation Reporting Contact Person

Attn: Professional Services Organization
NIFTeTRUST
NIFT (Pvt) Ltd.
5th Floor AWT Plaza
I.I Chundrigar Road
Karachi - 72400
021-111-112-222

For anyone listed in section 4.9.2 of the Verified Certificates Requirements that needs assistance with revocation or an investigative report, NIFT provides this page for reporting and submitting requests with all of the necessary information as outlined in section 4.9 of this CP/CPS: helpdesk@nift.pk

If the problem reporting page is unavailable, there is a system outage, you have questions, or you believe our findings are incorrect please contact ssl@nift.pk.

Entities submitting certificate revocation requests must list their identity and explain the reason for requesting revocation. NIFT or an RA will authenticate and log each revocation request according to Section 4.9 of this CP/CPS. NIFT will always revoke a Verified Certificates if the request is authenticated as

originating from the Subscriber or the Affiliated Organization listed in the Certificate. If revocation is requested by someone other than an authorized representative of the Subscriber or Affiliated Organization, NIFT or an RA will investigate the alleged basis for the revocation request prior to taking action in accordance with Section 4.9.1 and 4.9.3 of the Verified Certificates Requirements.

1.5.3 Person Determining CP/CPS Suitability for the Policy

The CPA determines the suitability and applicability of this CP/CPS based on the contract with the customer for which the PKI is operated and any relevant audits. The CPA is responsible for the PKI's compliance with this CP/CPS.

1.5.4 CP/CPS Approval Procedures

The CPA approves the CP/CPS and any amendments. Amendments are made after the CPA has reviewed the amendments' consistency with relevant contracts. The CPA determines whether an amendment to this CP/CPS is consistent with a contract, requires notice, or requires an OID change. External PMAs managing a CP (or requirements document) that this CP/CPS conforms to by contract, approve this CP/CPS for each CA that issues certificates under their respective CPs (or requirements document). That process is described in the applicable CPs and other supporting documents specified in the legal agreements.

1.6 DEFINITIONS AND ACRONYMS

1.6.1 Definitions

"Applicant" means an entity applying for a certificate.

"Combined Mark" means a mark consisting of a graphic design, stylized logo, or image, with words and/or letters having a particular stylized appearance. For greater certainty, a "Combined Mark" includes marks made up of both word and design elements.

"Design Mark" means a mark consisting of a graphic design, stylized logo, or image, without words and/or letters. For greater certainty, a "Design Mark" includes marks made up solely of design elements.

"External Program" means a community relying on or contracting with NIFT's non-publicly trusted certificate hierarchy and Certificates which may or may not maintain its own CP or guidelines document with which this CP/CPS is compliant. May also be described in this document as "External Private PKI Program."

"Key Pair" means a Private Key and associated Public Key.

"Mark" means a Combined Mark, Design Mark, or Word Mark. Marks may either be registered with a Trademark Office or created through government action.

"OCSP Responder" means an online software application operated under the authority of NIFT and connected to its repository for processing certificate status requests.

"Private Key" means 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.

"Public Key" means 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.

"Relying Party" means an entity that relies upon either the information contained within a certificate or a time-stamp token.

“Subscriber” means either the entity identified as the subject in the certificate or the entity that is receiving NIFT’s time-stamping services.

“Superior Entity” An entity above a certain entity within the PKI.

1.6.2 Acronyms

CA	Certificate Authority or Certification Authority
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSR	Certificate Signing Request
CPA	NIFT Certificate Policy Authority
FIPS	(US Government) Federal Information Processing Standard
HSM	Hardware Security Module
IdM	Identity Management System
ITU	International Telecommunication Union
ITU-T	ITU Telecommunication Standardization Sector
OCSP	Online Certificate Status Protocol
OCF	Open Connectivity Foundation
OID	Object Identifier
PKI	Public Key Infrastructure
PKCS	Public Key Cryptography Standard
PMA	Policy Management Authority
RA	Registration Authority
RPS	Registration Authority Practices Statement
SHA	Secure Hashing Algorithm
SSL	Secure Sockets Layer
TLS	Transport Layer Security
URL	Uniform Resource Locator
VC	Verified Certificates
X.509	The ITU-T standard for Certificates and their corresponding authentication framework

1.6.3 References

No stipulation for this CP/CPS. References for the External Programs are included in their respective CPs, guidelines, relevant legal agreements, requirements, and technical guidance documents.

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 REPOSITORIES

CRLs and OCSP responses are available through online resources 24 hours a day, 7 days a week with systems described in Section 5 to minimize downtime.

CRL will be used to communicate revocations of VCs to maintain privacy when requested by Subscribers.

2.2 PUBLICATION OF CERTIFICATION INFORMATION

The NIFT certificate services and the repository are accessible through several means of communication:

- On the web via URIs included in the certificates themselves
- By email to support@NIFT.pk

- By mail addressed to: NIFT (Pvt) Ltd., 5th Floor AWT Plaza I.I. Chundrigar Road Karachi 72400
- By telephone Tel: 021 – 111-112-222

NIFT protects information not intended for public dissemination through the request process listed above.

2.3 TIME OR FREQUENCY OF PUBLICATION

CRLs for end-user certificates are issued before the nextUpdate period listed in the CRL endpoints in the certificate. CRLs for CA Certificates are issued in accordance with the applicable customer agreement. Typically, this is every 6 months and also within 18 hours if a CA Certificate is revoked. Under special circumstances, NIFT may publish new CRLs prior to the scheduled issuance of the next CRL. New or modified versions of this CP/CPS, Subscriber Agreements, or Relying Party Warranties are typically published within seven days after their approval.

2.4 ACCESS CONTROLS ON REPOSITORIES

Read-only access to the repository is unrestricted. Logical and physical controls internal to NIFT prevent unauthorized write access to repositories.

3 IDENTIFICATION AND AUTHENTICATION

3.1 NAMING

3.1.1 Type of Names

Certificates are issued with a subject Distinguished Name (DN) that complies with ITU X.500 standards. Some certificates may have a null subject DN if it includes at least one alternative name form that is marked critical. Policies on certificate field and extension information are specified in a separate Certificate Profile document or technical specification of the program.

3.1.2 Need for Names to be Meaningful

NIFT uses distinguished names to identify the subject (i.e. person, organization, device, or object) or issuer of the certificate.

Where required by the applicable CP or guidelines, Subscriber certificates will contain meaningful names with commonly understood semantics permitting the determination of the identity of the organization that is the Subject of the certificate by NIFT and by designated RAs. RAs will describe this process in their associated RPS.

The subject name in CA Certificates match the issuer name in certificates issued by such NIFT CAs, as required by [RFC 5280].

3.1.3 Anonymity or Pseudonymity of Subscribers

Except where required otherwise by the applicable CP or guidelines, NIFT may issue anonymous and pseudonymous end-entity certificates provided that they are not prohibited by policy and that any applicable name space uniqueness requirements are met.

3.1.4 Rules for Interpreting Various Name Forms

Distinguished Names in certificates are interpreted using X.500 standards and ASN.1 syntax. See RFC 2253 and RFC 2616 for further information on how X.500 distinguished names in certificates are interpreted as Uniform Resource Identifiers and HTTP references.

3.1.5 Uniqueness of Names

The uniqueness of each subject name in a certificate depends on the contract with the customer. Typically, uniqueness is maintained through the domain name in the certificate, email address in the certificate, or combination of the certificate's Subject information.

RAs are required to enforce name uniqueness in communities where they participate.

3.1.6 Recognition, Authentication, and Role of Trademarks

Subscribers may not request certificates with content that infringes on the intellectual property rights of another entity. Unless otherwise specifically stated in an agreement with a customer, NIFT does not verify an Applicant's right to use a trademark and does not resolve trademark disputes. NIFT may reject any application or require revocation of any certificate that is part of a trademark dispute.

NIFT will not issue a certificate knowing that it infringes the trademark of another. Certificate Applicants cannot use names in their Certificate Applications that infringe upon the Intellectual Property Rights of others. With the exception of VCs and their Marks as specified in the VC Requirements in section 3, NIFT is not required to determine whether a Certificate Applicant has Intellectual Property Rights in the name appearing in a Certificate Application or is in good standing with a Trademark Office.

NIFT is not required to arbitrate, mediate, or otherwise resolve any dispute concerning the ownership of any intellectual property rights, including, without limitation, rights in a domain name, trade name, trademark, or service mark. RAs operating under this program must specify how they meet the requirements of the applicable CP or guidelines in their respective RPS.

3.2 INITIAL IDENTITY VALIDATION

NIFT may use any legal means of communication or investigation to ascertain the identity of an organizational or individual Applicant. NIFT may refuse to issue a certificate in its sole discretion. Participating RAs must specify the validation methods used to verify identity information in their applicable RPS.

3.2.1 Method to Prove Possession of Private Key

NIFT establishes that the Applicant holds or controls the Private Key corresponding to the Public Key by performing signature verification or decryption on data purported to have been digitally signed or encrypted with the Private Key by using the Public Key associated with the certificate request.

Certificates generated by NIFT require proof that the Subscriber possesses the private key. Typically, the RA verifies this by verifying the subscriber's digital signature on the PKCS #10 Certificate Signing Request (CSR) with the public key in the CSR. If NIFT generates the key pair on behalf of the subscriber, proof of possession by the subscriber is not required.

The process of proving possession of the private key for end-entity certificates by RAs will be described in their respective RPS.

3.2.2 Authentication of Organization Identity

Authentication of Organization identity is set forth in the applicable customer agreement or requirements as specified in the agreements/contracts. Verification procedures depend on the community ordering the certificate. Where applicable, NIFT's certificate issuance process authenticates the identity of the organization named in the respective Digital Certificate Subscriber Agreement and per the requirements of the associated External Program and CP.

NIFT may request documents to assist with validating certificate requests in accordance with the standards set forth by the agreements/contracts. These documents will be used in accordance with 9.4 of this CP/CPS.

For certificates issued by RAs, the practices that fulfill the requirements will be described in the respective RPS.

3.2.2.1 Authentication of Self Signed Root CA Certificates

NIFT issues a self-signed root CA Certificate when participating in a Private PKI program upon approval and fulfillment of the CP requirements from that program.

3.2.2.2 Authentication of Sub-CA Certificates

NIFT issues a sub-CA Certificate when participating in a Private PKI program upon approval and fulfillment of the CP requirements from that program.

3.2.2.3 Authentication of Manufacturer CA Certificates

NIFT issues a Manufacturer CA Certificate when participating in a Private PKI program upon approval and fulfillment of the CP requirements from that program.

3.2.2.4 Authentication of Marks in Verified Certificates

NIFT issues VCs with a Mark upon completing the relevant requirements listed in the VC Requirements as referenced in section 1.1.

3.2.3 Authentication of Individual Identity

Verification of individual identities depends on the requirements of the community ordering the certificates. Verification may include confirmation of an email address, through record checks of the individual's identity, or other similar means.

RAs participating under NIFT will detail their practices to meet the requirements of the applicable CP or guidelines in their respective RPS.

3.2.3.1 Authentication for Role-based Client Certificates

NIFT may issue certificates that identify a specific role that the Subscriber holds instead of a specific individual (e.g., Chief Information Officer is a unique individual whereas Program Analyst is not). These role-based certificates are used when non-repudiation is desired. A sponsor of the role-based certificates is verified in accordance with Section 3.2.3 above. If applicable, the RA must specify how devices are authenticated in the RPS.

3.2.3.2 Authentication for Group Client Certificates

NIFT issues group certificates (a certificate that corresponds to a Private Key that is shared by multiple Subscribers) if several entities are acting in one capacity and if non-repudiation is not required. A sponsor for the group certificate is verified under Section 3.2.3 before the certificate is issued. The sponsor must maintain and continuously update a list of Subscribers with access to the private key and account for the time period during which each Subscriber had control of the key. If applicable, the RA must specify how these groups are authenticated in the RPS.

3.2.3.3 Authentication of Devices

If applicable, the RA must specify how devices are authenticated in the RPS.

3.2.3.4 Verification Subject Identity in Verified Certificates

Before issuing a Verified Certificates to an Applicant, a CA shall successfully complete verification of the Applicant's identity and domain(s) to be included in the Verified Certificates according to the VC Requirements section 3 and profile attributes as described in section 7.

3.2.4 Non-verified Subscriber Information

Private client certificates may contain non-verified subscriber information.

3.2.5 Validation of Authority

NIFT or an RA may verify the authorization of a certificate request dependent upon the stipulations in the relevant contracts and CPs.

3.2.6 Criteria for Interoperation No stipulation

3.3 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS

3.3.1 Identification and Authentication for Routine Re-key

Subscribers may request re-key of a certificate prior to a certificate's expiration. After receiving a request for re-key, NIFT creates a new certificate with the same certificate contents except for a new Public Key and, optionally, an extended validity period. If the certificate has an extended validity period, NIFT may perform some revalidation of the Applicant but may also rely on information previously provided or obtained. Validation requirements for Re-key requests will be performed in accordance with the program requirements associated with the contract agreements, CP, and relevant technical requirement documents.

If an RA performs validation for a Re-key, they will specify the practices to meet the requirements of the contractual agreements, the CP, this CP/CPS, and the associated technical requirement documents in their RPS.

3.3.2 Identification and Authentication for Re-Key after Revocation No stipulation.

3.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST

NIFT or an RA authenticates all revocation requests per the CP and relevant legal agreements. NIFT may authenticate revocation requests by referencing the use of the Private Key corresponding to the certificate's Public Key, regardless of whether the associated Private Key is compromised.

If an RA performs validation for a revocation, they will specify the practices to meet the requirements of the contractual agreements, the CP, this CP/CPS, and the associated technical requirement documents in their RPS.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 CERTIFICATE APPLICATION

4.1.1 Who Can Submit a Certificate Application

Either the Applicant or an individual authorized to request certificates on behalf of the Applicant may submit certificate requests. Applicants are responsible for any data that the Applicant or an agent of the Applicant supplies to NIFT or an RA.

4.1.2 Enrollment Process and Responsibilities

In no particular order, the enrollment process may include:

- Submitting a certificate application including the required documentation from the associated program,
- Generating a key pair,
- Delivering the public key of the key pair to NIFT,
- Agreeing to the applicable Subscriber Agreement, and
- Paying any applicable fees.

4.2 CERTIFICATE APPLICATION PROCESSING

4.2.1 Performing Identification and Authentication Functions

After receiving a certificate application, NIFT or an RA verifies the application information and other information in accordance with Section 3.2. If an RA assists in the verification, the RA must create and maintain records sufficient to establish that it has performed its required verification tasks and communicate the completion of such performance to NIFT in accordance with sections 5.4 and 5.5. After verification is complete, NIFT or the RA evaluates the corpus of information and decides whether or not to issue the certificate. NIFT considers a source's availability, purpose, and reputation when determining whether a third party source is reasonably reliable.

Prior to issuing a Verified Certificates, NIFT checks the DNS for the existence of a CAA record for each dNSName in the subjectAltName extension of the certificate to be issued, as specified in accordance with section 3.2.15 of the Verified Certificates Requirements. NIFT processes the "issueVC" property tag and may dispatch reports of issuance requests to the contact(s) listed in an "iodef" property tag.

The Certification Authority CAA identifying domains for CAs that NIFT recognizes: are "NIFT.PK", "NIFT.ne.jp", "cybertrust.ne.jp", "symantec.com", "thawte.com", "geotrust.com", "rapidssl.com", "digitalcertvalidation.com", and any domain containing those identifying domains as suffixes (e.g example.NIFT.PK).

4.2.2 Approval or Rejection of Certificate Applications

NIFT may reject a certificate application if NIFT believes that issuing the certificate could damage or diminish NIFT's reputation or business or it does not fulfill the requirements of the associated legal agreements or CP. RAs may only approve a Certificate Application after verifying the applicant meets all requirements listed in the applicable CP or guidelines.

4.2.3 Time to Process Certificate Applications

As specified in the relevant customer agreement. If the timeframe is not specified, NIFT will usually complete the validation process and issue or reject a certificate application within two working days after

receiving all of the necessary details and documentation from the Applicant, although events outside of the control of NIFT can delay the issuance process.

4.3 CERTIFICATE ISSUANCE

4.3.1 CA Actions during Certificate Issuance

Issuance is completed using the appropriate CA Certificate after fulfilling the requirements of the associated legal agreements and CP. After issuance is complete, the certificate is stored in a database and sent to the Subscriber.

4.3.2 Notifications to Subscriber by the CA of Issuance of Certificate

NIFT may deliver certificates in any secure manner within a reasonable time after issuance allowed by the associated legal agreements, CP, and technical requirements. Generally, NIFT delivers certificates by providing the Subscriber a hypertext link to a user id/password-protected location where the subscriber may log in and download the certificate or via email to the email address designated by the Subscriber during the application process.

4.4 CERTIFICATE ACCEPTANCE

Acceptance criteria is specified in the applicable CP or guidelines. At a minimum, a legal agreement specifying the limits on use and trust on the certificate is required. In the case of the automated issuance of end entity certificates the Subscriber is the end entity. The manufacturer in this case ensures that these responsibilities are followed.

4.4.1 Conduct Constituting Certificate Acceptance

Subscribers are solely responsible for installing the issued certificate on the Subscriber's computer or hardware security module. Certificates are considered accepted 30 days after the certificate's issuance, or earlier upon use of the certificate when evidence exists that the Subscriber used the certificate.

4.4.2 Publication of the Certificate by the CA

NIFT publishes end-entity certificates by delivering them to the Subscriber and through the methods described in section 2.1.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

RAs may receive notification of a certificate's issuance if the RA was involved in the issuance process. The applicable community is notified when a CA Certificate is issued for that community.

4.5 KEY PAIR AND CERTIFICATE USAGE

4.5.1 Subscriber Private Key and Certificate Usage

Subscribers are obligated to protect their Private Keys from unauthorized use or disclosure, discontinue using a Private Key after expiration or revocation of the associated certificate, and use certificates in accordance with their intended purpose as specified in the applicable legal agreement, this CP/CPS, the associated CP, and/or the KeyUsage field extensions in the certificate.

4.5.2 Relying Party Public Key and Certificate Usage

NIFT does not warrant that any third-party software will support or enforce the controls and requirements found herein. A Relying Party should use discretion when relying on a certificate and should consider the totality of the circumstances and risk of loss prior to relying on a certificate. If the circumstances indicate that additional assurances are required, the Relying Party must obtain such assurances before using the certificate.

4.6 CERTIFICATE RENEWAL

Certificate renewal means the issuance of a new certificate without changing the Public Key or other information in the certificate.

4.6.1 Circumstances for Certificate Renewal

NIFT may renew a certificate if:

- the associated Public Key has not reached the end of its validity period,
- the Subscriber and attributes are consistent, and
- the associated Private Key remains uncompromised.

NIFT may also renew a certificate if a CA Certificate is re-keyed or as otherwise necessary to provide services to a customer. NIFT may notify Subscribers prior to a certificate's expiration date. Certificate renewal requires payment of additional fees. In all cases, any renewal requirements are specified by the applicable CP or guidelines.

4.6.2 Who May Request Renewal

Only the certificate subject or an authorized representative of the certificate subject may request renewal of the Subscriber's certificates. NIFT may renew a certificate without a corresponding request if the signing certificate is re-keyed.

4.6.3 Processing Certificate Renewal Requests

Renewal application requirements and procedures are generally the same as those used during the certificate's original issuance as specified by the program CP. NIFT may refuse to renew a certificate if it cannot verify any rechecked information. If an individual is renewing a client certificate and the relevant information has not changed, then NIFT does not require any additional identity vetting. If the Private Key and domain information has not changed, the Subscriber may renew an SSL/TLS server certificate using a previously issued certificate or provided CSR.

RAs must confirm the identity of the Subscriber in accordance with the requirements in the relevant CP. These practices will be described in the RA's RPS.

4.6.4 Notification of New Certificate Issuance to Subscriber

NIFT may deliver the certificate in any secure fashion as required by the relevant CP, typically by email or by providing the Subscriber a hypertext link to a user id/password-protected location where the Subscriber may log in and download the certificate and in accordance of section 2.1.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

Renewed certificates are considered accepted 30 days after the certificate's renewal, or earlier upon use of the certificate when evidence exists that the Subscriber used the certificate.

4.6.6 Publication of the Renewal Certificate by the CA

NIFT publishes a renewed certificate by delivering it to the Subscriber in the method prescribed in the relevant CP and in accordance of section 2.1.

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

RAs may receive notification of a certificate's renewal if the RA was involved in the issuance process. The applicable community is notified when a CA Certificate is issued for that community.

4.7 CERTIFICATE RE-KEY

4.7.1 Circumstances for Certificate Re-key

Re-keying a certificate consists of creating a new certificate with a new Public Key and serial number while keeping the subject information the same. The new certificate may have a different validity date, key identifiers, CRL and OCSP distribution points, and signing key. CA keys may be re-keyed by a CA during recovery from key compromise. A CA Certificate may be re-keyed after expiration. The original CA Certificate may be revoked, but cannot be further re-keyed, renewed, or modified.

4.7.2 Who May Request Certification of a New Public Key

NIFT will only accept re-key requests from the subject of the certificate or the PKI sponsor. NIFT may initiate a certificate re-key at the request of the certificate subject or in NIFT's own discretion.

4.7.3 Processing Certificate Re-keying Requests

NIFT may re-use existing verification information unless re-verification and authentication is required by contract or if NIFT believes that the information has become inaccurate. NIFT or the RA will confirm the identity of the Subscriber in accordance with the requirements specified in the CP and contracts for the authentication of an original Certificate Application. The RAs will describe this practice in their respective RPS.

CA Certificate re-key requests will be approved according to the requirements in the associated contract, guidelines, requirements, and CP.

4.7.4 Notification of Certificate Issuance to Subscriber

NIFT notifies the Subscriber within a reasonable time after the certificate issues or per the requirements within the legal agreements and External Program CP.

4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate

Issued certificates are considered accepted 30 days after the certificate is re-keyed, or earlier upon use of the certificate when evidence exists that the Subscriber used the certificate.

4.7.6 Publication of the Issued Certificate by the CA

NIFT publishes re-keyed certificates by delivering them to Subscribers or per the requirements within the legal agreements and program CP.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

RAs may receive notification of a certificate's re-key if the RA was involved in the issuance process. The applicable community is notified when a CA Certificate is issued for that community.

4.8 CERTIFICATE MODIFICATION

4.8.1 Circumstances for Certificate Modification

Modifying a certificate means creating a new certificate for the same subject with information that differs slightly from the old certificate (e.g., changes to email address or non-essential parts of names or attributes) provided that the modification otherwise complies with the relevant CP and this CP/CPS. The new certificate may have the same or a different subject public key.

NIFT or an RA may modify certificates in the following circumstances:

- For a Subscriber organization name change or other Subscriber characteristic change

- To extend the validity period to maintain continuity of certificate usage in certain programs based on circumstances allowed in the CP; or
- To correct subject name attributes or extension settings.

The original certificate may be revoked, but cannot be further re-keyed, renewed, or modified.

4.8.2 Who May Request Certificate Modification

NIFT or an RA modifies certificates at the request of certain certificate subjects or in its own discretion or according to the relevant CP. NIFT does not make certificate modification services available to all Subscribers.

RAs that modify certificates will specify the compliant practice in their RPS according to this CP/CPS and the CP for the certificate type and subject.

4.8.3 Processing Certificate Modification Requests

After receiving a request for modification, NIFT or an RA verifies any changed information in accordance with section 3.2 of this CP/CPS and the applicable CP or guidelines.

RAs that modify certificates will specify the compliant practice in their RPS according to this CP/CPS and the CP for the certificate type and subject.

4.8.4 Notification of New Certificate Issuance to Subscriber

NIFT notifies the Subscriber within a reasonable time after the certificate issues or by the timeframe specified in the applicable CP or guidelines. RAs will specify the timeframe in their RPS based on compliant practices with this CP/CPS and the applicable CP or guidelines.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

Modified certificates are considered accepted 30 days after the certificate is modified, or earlier upon use of the certificate when evidence exists that the Subscriber used the certificate.

4.8.6 Publication of the Modified Certificate by the CA

NIFT publishes modified certificates by delivering them to Subscribers based on section 2.1.

4.8.7 Notification of Certificate Modification by the CA to Other Entities

RAs may receive notification of a certificate's modification if the RA was involved in the issuance process. The applicable community is notified when a CA Certificate is issued for that community.

4.9 CERTIFICATE REVOCATION AND SUSPENSION

4.9.1 Circumstances for Revocation

Revocation of a certificate permanently ends the operational period of the certificate prior to the certificate reaching the end of its stated validity period. Prior to revoking a certificate, NIFT verifies the identity and authority of the entity requesting revocation. NIFT may revoke any certificate in its sole discretion, including if NIFT believes that:

1. The Subscriber requested revocation of its certificate;
2. The Subscriber did not authorize the original certificate request and did not retroactively grant authorization;

3. Either the Private Key associated with the certificate or the Private Key used to sign the certificate was compromised or misused;
4. The Subscriber breached a material obligation under the CP/CPS or the relevant agreement;
5. Either the Subscriber's or NIFT's obligations under the CP/CPS are delayed or prevented by circumstances beyond the party's reasonable control, including computer or communication failure, and, as a result, another entity's information is materially threatened or compromised;
6. The Subscriber, sponsor, or other entity that was issued the certificate has lost its rights to a name, trademark, device, IP address, domain name, or other attribute that was associated with the certificate;
7. The certificate was not issued in accordance with the CP/CPS or applicable industry standards;
8. NIFT received a lawful and binding order from a government or regulatory body to revoke the certificate;
9. NIFT ceased operations and did not arrange for another certificate authority to provide revocation support for the certificates;
10. NIFT's right to manage certificates under applicable industry standards was terminated (unless arrangements have been made to continue revocation services and maintain the CRL/OCSP Repository);
11. Any information appearing in the certificate was or became inaccurate or misleading;
12. The technical content or format of the certificate presents an unacceptable risk; or
13. The Subscriber was added as a denied party or prohibited person to a blacklist or is operating from a destination prohibited under the laws of Government of Pakistan.

NIFT processes revocation requests in accordance with instructions from the RA and Subscribers. Generally, NIFT revokes certificates in a reasonable timeframe after receiving an approved revocation request – generally within 24 hours.

If NIFT or the RA makes the decision to revoke, the associated certificate will be revoked and distributed via OCSP or CRL (as applicable). Revocation information for certificates are included on all new publications of the certificate status information until the certificates expire.

4.9.2 Who Can Request Revocation

Any appropriately authorized party as defined in the relevant legal contract or CP, such as a recognized representative of a subscriber or cross-signed partner, may request revocation of a certificate. NIFT may revoke a certificate without receiving a request and without reason. Third parties may request certificate revocation for problems related to fraud, misuse, or compromise. Certificate revocation requests must identify the entity requesting revocation and specify the reason for revocation.

4.9.3 Procedure for Revocation Request

For certificates handled by NIFT, the process for a revocation request generally flows as follows (additional steps may be followed to meet community expectations):

1. NIFT logs the identity of entity making the request or problem report and the reason for requesting revocation. NIFT may also include its own reasons for revocation in the log.

2. NIFT may request confirmation of the revocation from the Subscriber or a known administrator; where applicable, via out-of-band communication (e.g., telephone, fax, etc.).
3. If the request is authenticated as originating from the Subscriber, NIFT revokes the certificate.
4. For requests from third parties, NIFT personnel begin investigating the request and decide whether revocation is appropriate based on the following criteria:
 - a. the nature of the alleged problem,
 - b. the number of reports received about a particular certificate,
 - c. the identity of the complainants (for example, complaints from a law enforcement official that a web site is engaged in illegal activities have more weight than a complaint from a consumer alleging they never received the goods they ordered), and
 - d. relevant legislation.
5. If NIFT determines that revocation is appropriate, NIFT personnel revoke the certificate and update the CRL.

NIFT maintains a continuous ability to internally respond to any high priority revocation requests. If appropriate, NIFT forwards complaints to law enforcement.

Revocation requests may originate from subscribers, external authorities operating the program applicable to the certificates, RAs, and resellers. NIFT may require an entity requesting revocation to authenticate itself prior to processing the revocation.

Upon revocation of a certificate, NIFT publishes the revocation information using OCSP or CRLs, depending on the contents of the issued certificate.

4.9.4 Revocation Request Grace Period

Subscribers are required to request revocation within one day after detecting the loss or compromise of the Private Key. NIFT may grant and extend revocation grace periods on a case-by-case basis.

4.9.5 Time within which CA Must Process the Revocation Request

NIFT will revoke a CA Certificate within a reasonable time after receiving clear instructions from the CPA. Other certificates are revoked as quickly as practical after validating the revocation request.

NIFT begins the investigation of a certificate revocation request promptly after receipt. RAs that accept revocation requests should promptly provide the request to NIFT via their system or through email. There is no stipulation about when certificate revocation requests are completed. Such timing depends largely on the availability of information supporting authorization of the certificate revocation request and the expected impact of revocation.

4.9.6 Revocation Checking Requirement for Relying Parties

Relying Parties must check the status of certificates on which they wish to rely on by checking the certificate status using CRLs or OCSP responses, as applicable.

4.9.7 CRL Issuance Frequency

Where applicable, CRLs for end entity certificates are generally published at least every 24 hours.

NIFT may issue CRLs periodically, even if there are no changes to be made, to ensure timeliness of information. Certificate status information may be issued more frequently than the issuance frequency described below.

External CAs under this program may be required to update and reissue CRLs at a more frequent rate as specified by the relevant agreements, contracts, technical specification documentation, and CP.

4.9.8 Maximum Latency for CRLs

CRLs for certificates issued to end entity subscribers are posted automatically to the online repository within a commercially reasonable time after generation or per requirements in legal agreements and CP, usually within minutes of generation. Regularly scheduled CRLs are posted prior to the nextUpdate field in the previously issued CRL of the same scope.

4.9.9 On-line Revocation/Status Checking Availability

If specified in the certificate, NIFT provides OCSP response information for issued certificates.

4.9.10 On-line Revocation Checking Requirements

A Relying Party for NIFT Private PKI Certificates must check the status of a certificate on which they wish to rely on with methods as specified in this section.

4.9.11 Other Forms of Revocation Advertisements Available

No stipulation.

4.9.12 Special Requirements re Key Compromise

Revocation information for CA Certificates are published after creation of the appropriate CRL and OCSP information, as applicable. Typically, revocation information for CA Certificates is published within 24 hours of notification based on the requirements of the contracts and relevant CP.

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

Certificate status information may be available via CRL and OCSP responder. The Repository is available via HTTP or another accessible transfer protocol as specified in section 2.1. The serial number of a revoked certificate remains on the CRL until one additional CRL is published after the end of the certificate's validity period.

4.10.2 Service Availability

Certificate status services are available on a continuous basis.

4.10.3 Operational Features

OCSP Responders may not be available for all certificate types. For those that are required, they will be configured per the profile requirements of the associated CP section 7.

4.11 END OF SUBSCRIPTION

A Subscriber's subscription service ends if its certificate expires or is revoked or if the applicable Subscriber Agreement expires without renewal.

4.12 KEY ESCROW AND RECOVERY

4.12.1 Key Escrow and Recovery Policy Practices

No stipulation.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

No stipulation.

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 PHYSICAL CONTROLS

5.1.1 Site Location and Construction

NIFT performs its CA operations from secure and geographically diverse commercial data centers. The data centers are equipped with logical and physical controls that make NIFT's CA operations inaccessible to non-trusted personnel as described in section 5.1.2. NIFT operates under a security policy designed to detect, deter, and prevent unauthorized access to NIFT's operations.

5.1.2 Physical Access

NIFT protects its equipment from unauthorized access and implements physical controls to reduce the risk of equipment tampering. The secure parts of NIFT CA hosting facilities are protected using physical access controls making them accessible only to appropriately authorized individuals in layers of security as described here. Access to secure areas of the buildings requires the use of an "access" or "pass" card. The buildings are equipped with motion detecting sensors, and the exterior and internal passageways of the buildings are under constant video surveillance in each subsequent area. NIFT securely stores all removable media and paper containing sensitive plain-text information related to its CA operations in secure containers in accordance with its Data Classification Policy.

Access to the data centers housing the CA platforms requires two-factor authentication—the individual must have an authorized access card and pass biometric access control authenticators. These biometric authentication access systems log each use of the access card that specify which layers of security they have access to based on their trusted role status and designated responsibilities described in section 5.2.1.

NIFT deactivates and securely stores its CA hardware equipment when not in use. Activation data must either be memorized or recorded and stored in a manner commensurate with the security afforded the cryptographic module. Activation data is never stored with the cryptographic module, removable hardware, or account used to administer NIFT's private keys. Cryptographic hardware includes a mechanism to lock the hardware after a certain number of failed login attempts.

NIFT personnel perform periodic security checks of the data center to verify that:

1. NIFT's equipment is in a state appropriate to the current mode of operation,
2. Any security containers are properly secured,
3. Physical security systems (e.g., door locks) are functioning properly, and
4. The area is secured against unauthorized access.

NIFT's administrators are responsible for making these checks and must sign off that all necessary physical protection mechanisms are in place and activated. The identity of the individual making the check is logged.

5.1.3 Power and Air Conditioning

Data centers have primary and secondary power supplies that ensure continuous and uninterrupted access to electric power. Uninterrupted power supplies (UPS) and diesel generators provide redundant backup power. NIFT monitors capacity demands and makes projections about future capacity requirements to ensure that adequate processing power and storage are available. NIFT's data center facilities use multiple load-balanced HVAC systems for heating, cooling, and air ventilation through perforated-tile raised flooring to prevent overheating and to maintain a suitable humidity level for sensitive computer systems.

5.1.4 Water Exposures

The cabinets housing NIFT's CA systems are located on raised flooring, and the data centers are equipped with monitoring systems to detect excess moisture.

5.1.5 Fire Prevention and Protection

The data centers are equipped with fire suppression mechanisms.

5.1.6 Media Storage

NIFT protects its media from accidental damage and unauthorized physical access. Backup files are created on a regular basis. NIFT's backup files are maintained at locations separate from NIFT's primary data operations facility.

5.1.7 Waste Disposal

CA media and documentation that are no longer needed for operations are destroyed in a secure manner. All unnecessary copies of printed sensitive information are shredded on-site before disposal.

5.1.8 Off-site Backup

NIFT maintains at least one full backup and makes regular backup copies of any information necessary to recover from a system failure. Backup copies of CA Private Keys and activation data are stored for disaster recovery purposes off-site in safe deposit boxes that are accessible only by trusted personnel.

5.2 PROCEDURAL CONTROLS

5.2.1 Trusted Roles

Personnel acting in trusted roles include CA and RA system administration personnel, and personnel involved with identity vetting and the issuance and revocation of certificates. The functions and duties performed by persons in trusted roles are distributed so that one person alone cannot circumvent security measures or subvert the security and trustworthiness of the PKI operations. All personnel in trusted roles must be free from conflicts of interest that might prejudice the impartiality of the NIFT PKI's operations. Trusted roles are appointed by senior management. A list of personnel appointed to trusted roles by NIFT is maintained and reviewed annually. RAs may have different requirements for appointing trusted roles. The process used by RAs for appointing and governing Trusted Roles is specified in the applicable RPS.

3.2.3.5 CA Administrators

The CA Administrator installs and configures the CA software, including key generation, key backup, and key management. The CA Administrator performs and securely stores regular system backups of the CA system. Administrators do not issue certificates to Subscribers.

3.2.3.6 Registration Officers – Validation and Vetting Personnel

The Registration Officer role is responsible for issuing and revoking certificates, including enrollment, identity verification, and compliance with required issuance and revocation steps such as managing the certificate request queue and completing certificate approval checklists as identity vetting tasks are successfully completed. This role can be both internal to NIFT or another group as specified in section 1.3.2.

3.2.3.7 System Administrators/ System Engineers (Operator)

The System Administrator / System Engineer installs and configures system hardware, including servers, routers, firewalls, and network configurations. The System Administrator / System Engineer also keeps CA and RA systems updated with software patches and other maintenance needed for system stability and recoverability.

3.2.3.8 Internal Auditors

Internal Auditors are responsible for reviewing, maintaining, and archiving audit logs and performing or overseeing internal compliance audits to determine if NIFT is operating in accordance with this CP/CPS.

5.2.2 Number of Persons Required per Task

CA keys will be under personnel controls according to the requirements in the relevant legal agreements, CPs, technical specification documents, requirement(s), and this CP/CPS.

Unless otherwise specified by the documents referenced above, NIFT requires that at least two people acting in a trusted role (one the CA Administrator and the other not an Internal Auditor) take action requiring a trusted role, such as activating NIFT's Private Keys, generating a CA key pair, or backing up a NIFT private key. The Internal Auditor may serve to fulfill the requirement of multiparty control for physical access to the CA system but not logical access.

5.2.3 Identification and Authentication for each Role

All personnel are required to authenticate themselves to CA and RA systems before they are allowed access to systems necessary to perform their trusted roles. External RA system access and control by trusted roles are specified in the respective RPS.

5.2.4 Roles Requiring Separation of Duties

Roles requiring a separation of duties include:

1. Those performing authorization functions such as the verification of information in certificate applications and approvals of certificate applications and revocation requests,
2. Those performing backups, recording, and record keeping functions;
3. Those performing audit, review, oversight, or reconciliation functions; and
4. Those performing duties related to CA key management or CA administration.

For RAs, the separation of duties for trusted roles are addressed in their respective RPS.

5.3 PERSONNEL CONTROLS

5.3.1 Qualifications, Experience, and Clearance Requirements

The CPA is responsible and accountable for NIFT's PKI operations and ensures compliance with this CP/CPS. NIFT's personnel and management practices provide reasonable assurance of the trustworthiness and competence of its employees and of the satisfactory performance of their duties.

For Trusted Roles maintained by RAs external to NIFT, these requirements will be addressed in their respective RPS.

5.3.2 Background Check Procedures

NIFT and RAs verify the identity of each employee appointed to a trusted role and performs a background check prior to allowing such person to act in a trusted role.

NIFT requires each individual to appear in-person before a human resources employee whose responsibility it is to verify identity. The human resources employee verifies the individual's identity using government-issued photo identification (e.g., passports and/or driver's licenses reviewed, Employment Eligibility Verification, or comparable procedure for the jurisdiction in which the individual's identity is being verified). Background checks include employment history, education, character references, social security number, previous residences, driving records and criminal background. Checks of previous residences are over the past three years. All other checks are for the previous five years.

The highest education degree obtained is verified regardless of the date awarded. Based upon the information obtained during the background check, the human resources department makes an adjudication decision, with the assistance of legal counsel when necessary, as to whether the individual is suitable for the position to which they will be assigned. Background checks are refreshed and readjudication occurs at least every five years.

For Trusted Roles maintained by RAs external to NIFT, these requirements will be addressed in their respective RPS.

5.3.3 Training Requirements

NIFT provides skills training to all employees involved in NIFT's PKI operations. The training relates to the person's job functions and covers:

1. basic Public Key Infrastructure (PKI) knowledge,
2. software versions used by NIFT,
3. authentication and verification policies and procedures,
4. NIFT security principals and mechanisms,
5. disaster recovery and business continuity procedures,
6. common threats to the validation process, including phishing and other social engineering tactics, and
7. applicable industry and government guidelines.

Training is provided via a mentoring process involving senior members of the team to which the employee belongs.

NIFT maintains records of who received training and what level of training was completed. Registration Officers must have the minimum skills necessary to satisfactorily perform validation duties before being granted validation privileges. Where competence is demonstrated in lieu of training, NIFT maintains supporting documentation.

5.3.4 Retraining Frequency and Requirements

Employees must maintain skill levels that are consistent with industry-relevant training and performance programs in order to continue acting in trusted roles. NIFT makes all employees acting in trusted roles aware of any changes to NIFT's operations. If NIFT's operations change, NIFT will provide documented training, in accordance with an executed training plan, to all employees acting in trusted roles.

5.3.5 Job Rotation Frequency and Sequence No stipulation.

5.3.6 Sanctions for Unauthorized Actions

NIFT employees and agents failing to comply with this CP/CPS, whether through negligence or malicious intent, are subject to administrative or disciplinary actions, including termination of employment or agency and criminal sanctions. If a person in a trusted role is cited by management for unauthorized or inappropriate actions, the person will be immediately removed from the trusted role pending management review. After management has reviewed and discussed the incident with the employee involved, management may reassign that employee to a non-trusted role or dismiss the individual from employment as appropriate.

5.3.7 Independent Contractor Requirements

Independent contractors who are assigned to perform trusted roles are subject to the duties and requirements specified for such roles in this Section 5.3 and are subject to sanctions stated above in Section 5.3.6. Otherwise, independent contractors and consultants are escorted and directly supervised by Trusted Persons when they are given access to NIFT and any of its secure facilities.

5.3.8 Documentation Supplied to Personnel

Personnel in trusted roles are provided with the documentation necessary to perform their duties. Personnel are also given access to information on internal systems and security documentation, identity vetting policies and procedures, discipline-specific books, treatises and periodicals, and other information.

For Trusted Roles maintained by RAs external to NIFT, these requirements will be addressed in their respective RPS and will include the relevant CP, this CP/CPS, and technical specification documents.

5.4 AUDIT LOGGING PROCEDURES

5.4.1 Types of Events Recorded

NIFT's systems require identification and authentication at system logon with a unique username and password. Important system actions are logged to establish the accountability of the operators who initiate such actions.

NIFT enables all essential event auditing capabilities of its CA applications in order to record the events listed below. If NIFT's applications cannot automatically record an event, NIFT or an RA implements manual procedures to satisfy the requirements. For each event, NIFT records the relevant (i) date and time, (ii) type of event, (iii) success or failure, and (iv) user or system that caused the event or initiated the action. Event records are available to auditors as proof of NIFT's or RA practices.

In generally, NIFT audits all activities related to the CA, including security events, authentication to systems, data entry, key generation, private key storage, etc. The systems audited are dependent on platform as well as requirements specified by the community of interest. Anomalies in the system are investigated and tracked.

5.4.2 Frequency of Processing Log

When checking logs, the administrator may perform the checks using automated tools. During these checks, the administrator (1) checks whether anyone has tampered with the log, (2) scans for anomalies or specific conditions, including any evidence of malicious activity, and (3) prepares a written summary of the review. Any anomalies or irregularities found in the logs are investigated. The summaries include recommendations to NIFT's operations management committee and are made available to NIFT's auditors upon request. NIFT documents any actions taken as a result of a review.

5.4.3 Retention Period for Audit Log No stipulation.

5.4.4 Protection of Audit Log

CA audit log information is retained on equipment until after it is copied by a system administrator. NIFT's CA systems are configured to ensure that (i) only authorized people have read access to logs, (ii) only authorized people may archive audit logs, and (iii) audit logs are not modified. Audit logs are protected from destruction prior to the end of the audit log retention period and are retained securely on-site until transferred to a backup site. NIFT's off-site storage location is a safe and secure location that is separate from the location where the data was generated.

5.4.5 Audit Log Backup Procedures No stipulation.

5.4.6 Audit Collection System (Internal vs. External)

Automatic audit processes begin on system startup and end at system shutdown. If an automated audit system fails and the integrity of the system or confidentiality of the information protected by the system is at risk, NIFT's Administrators, External Program PMAs, and the CPA shall be notified and the CPA will consider suspending the CA's or RA's operations until the problem is remedied.

5.4.7 Notification to Event-causing Subject No stipulation.

5.4.8 Vulnerability Assessments

NIFT performs annual risk assessments that identify and assess reasonably foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any certificate data or certificate issuance process. NIFT also routinely assesses the sufficiency of the policies, procedures, information systems, technology, and other arrangements that NIFT has in place to control such risks. NIFT's Internal Auditors review the security audit data checks for continuity. NIFT's audit log monitoring tools alert the appropriate personnel of any events, such as repeated failed actions, requests for privileged information, attempted access of system files, and unauthenticated responses.

5.5 RECORDS ARCHIVAL

NIFT complies with all record retention policies that apply by law. NIFT includes sufficient detail in all archived records to show that a certificate was issued in accordance with this CP/CPS.

5.5.1 Types of Records Archived

NIFT retains the following information in its archives (as such information pertains to NIFT's CA operations in the CP and legal agreements):

1. Accreditations of NIFT,
2. CP and CPS versions,
3. Contractual obligations and other agreements concerning the operation of the CA,
4. System and equipment configurations, modifications, and updates,
5. Rejection or acceptance of a certificate request,
6. Certificate issuance, re-key, renewal, and revocation requests,
7. Sufficient identity authentication data to satisfy the identification requirements of Section 3.2, including information about telephone calls made for verification purposes,
8. Any documentation related to the receipt or acceptance of a certificate or token,
9. Subscriber Agreements,
10. Issued certificates,
11. A record of certificate re-keys,
12. CRL and OCSP entries,
13. Data or applications necessary to verify an archive's contents,
14. Compliance auditor reports,
15. Changes to NIFT's audit parameters,
16. Any attempt to delete or modify audit logs,
17. Key generation, destruction, storage, backup, and recovery,
18. Access to Private Keys for key recovery purposes,
19. Export of Private Keys,
20. Approval or rejection of a certificate status change request,
21. Appointment of an individual to a trusted role,
22. Destruction of a cryptographic module,
23. Certificate compromise notifications,
24. Remedial action taken as a result of violations of physical security, and
25. Violations of the CP/CPS.

5.5.2 Retention Period for Archive

Archive records are kept in accordance with the community requirements. This time-frame may range between 1 and 10.5 years.

For records maintained by external RAs, the materials will be maintained for availability upon request by appropriately identified parties and per the requirements of the associated legal agreements, CP, and this CP/CPS.

5.5.3 Protection of Archive

Archive records are stored at a secure off-site location and are maintained in a manner that prevents unauthorized modification, substitution, or destruction. Archives are not released except as allowed by the CPA or as required by law. NIFT maintains any software application required to process the archive data until the data is either destroyed or transferred to a newer medium.

If NIFT needs to transfer any media to a different archive site or equipment, NIFT will maintain both archived locations and/or pieces of equipment until the transfer are complete. All transfers to new archives will occur in a secure manner.

5.5.4 Archive Backup Procedures No stipulation.

5.5.5 Requirements for Time-stamping of Records

NIFT automatically time-stamps archived records with system time (non-cryptographic method) as they are created. NIFT synchronizes its system time at least every eight hours using a real time value distributed by a recognized UTC(k) laboratory or National Measurement Institute.

5.5.6 Archive Collection System (internal or external)

Archive information is collected internally by NIFT. External information from RAs is not typically collected or controlled by NIFT.

5.5.7 Procedures to Obtain and Verify Archive Information

Details concerning the creation and storage of archive information are found in section 5.5.4. After receiving a request made for a proper purpose by a Customer, its agent, or a party involved in a dispute over a transaction involving the PKI, NIFT may elect to retrieve the information from archival. NIFT may elect to transmit the relevant information via a secure electronic method or courier, or it may also refuse to provide the information in its discretion and may require prior payment of all costs associated with the data.

5.6 KEY CHANGEOVER

Key changeover procedures enable the smooth transition from expiring CA Certificates to new CA Certificates. Towards the end of a CA Private Key's lifetime, NIFT ceases using the expiring CA Private Key to sign certificates and uses the old Private Key only to sign CRLs, OCSP responses, and OCSP responder certificates. A new CA signing key pair is commissioned and all subsequently issued certificates and CRLs are signed with the new private signing key. Both the old and the new key pairs may be concurrently active. This key changeover process helps minimize any adverse effects from CA Certificate expiration.

A CA Certificate may be renewed if permitted by the applicable community. NIFT renews CA Certificates pursuant to the instructions of the community's governing body and that community's CP.

5.7 COMPROMISE AND DISASTER RECOVERY

5.7.1 Incident and Compromise Handling Procedures

NIFT maintains internal procedures to guide personnel in response to security incidents, natural disasters, and similar events that may give rise to system compromise. These include, but are not limited to the following internally maintained documents:

- Disaster Recovery Plan,
- Business Continuity Plan (DR/BCP); and
- Operational Management Policies and Procedures
- Other internal documented process and procedure resources

NIFT reviews, tests, and updates its incident response plans and procedures on at least an annual basis.

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

NIFT makes regular system backups on at least a weekly basis and maintains backup copies of its Private Keys, which are stored in a secure, off-site location. If NIFT discovers that any of its computing resources, software, or data operations have been compromised, NIFT assesses the threats and risks that the compromise presents to the integrity or security of its operations or those of affected parties. If NIFT determines that a continued operation could pose a significant risk to Relying Parties or Subscribers, NIFT suspends such operation until it determines that the risk is mitigated.

5.7.3 Entity Private Key Compromise Procedures

If NIFT suspects that one of its Private Keys has been comprised or lost, then an emergency response team will convene and assess the situation to determine the degree and scope of the incident and take appropriate action. NIFT may generate a new key pair and sign a new certificate. If a disaster physically damages NIFT's equipment and destroys all copies of NIFT's signature keys, then NIFT will provide notice to affected parties at the earliest feasible time.

5.7.4 Business Continuity Capabilities after a Disaster

To maintain the integrity of its services, NIFT implements data backup and recovery procedures as part of its Business Continuity Management Plan (BCMP). Stated goals of the BCMP are to ensure that certificate status services be only minimally affected by any disaster involving NIFT's primary facility and that NIFT be capable of maintaining other services or resuming them as quickly as possible following a disaster. NIFT reviews, tests, and updates the BCMP and supporting procedures at least annually.

NIFT's systems are redundantly configured at its primary facility and are mirrored at a separate, geographically diverse location for failover in the event of a disaster. If a disaster causes NIFT's primary CA operations to become inoperative, NIFT will re-initiate its operations at its secondary location giving priority to the provision of certificate status information and time stamping capabilities, if affected.

5.8 CA OR RA TERMINATION

Before terminating its CA activities, NIFT will:

1. Provide notice and information about the termination by sending notice by email to its customers; and
2. Transfer all responsibilities to a qualified successor entity.

If a qualified successor entity does not exist, NIFT will:

1. transfer those functions capable of being transferred to a reliable third party and arrange to preserve all relevant records with a reliable third party or a government, regulatory, or legal body with appropriate authority;

2. revoke all certificates that are still un-revoked or un-expired on a date as specified in the notice and publish final CRLs;
3. destroy all Private Keys; and
4. make other necessary arrangements that are in accordance with this CP/CPS.

NIFT has made arrangements to cover the costs associated with fulfilling these requirements in case NIFT becomes bankrupt or is unable to cover the costs. Any requirements of this section that are varied by contract apply only the contracting parties.

6 TECHNICAL SECURITY CONTROLS

6.1 KEY PAIR GENERATION AND INSTALLATION

6.1.1 Key Pair Generation

CA key pairs are generated by trusted roles and using a cryptographic hardware device or per section 5.2.2. Typically, if hardware is required, the cryptographic hardware is evaluated to FIPS 140-1 Level 3 and EAL 4+. Community requirements may specify a lower version of control or optional uses of technology aside from hardware. NIFT creates auditable evidence during the key generation process to prove that the CP/CPS was followed, and role separation was enforced during the key generation process per section 5.2.2.

6.1.2 Private Key Delivery to Subscriber

Subscriber key pair generation is performed by the Subscriber, an external CA, an RA, or NIFT. If the Subscribers themselves generate private keys, then private key delivery to a Subscriber is unnecessary.

When NIFT or a CA generate key pairs on behalf of the Subscriber, the private key is delivered securely to the Subscriber based on the requirements of the associated legal agreements, CP, technical specification documents, and this CP/CPS.

6.1.3 Public Key Delivery to Certificate Issuer

Subscribers generate key pairs and may submit the Public Key to NIFT in a CSR as part of the certificate request process. The Subscriber's signature on the request is authenticated prior to issuing the certificate.

6.1.4 CA Public Key Delivery to Relying Parties No stipulation.

6.1.5 Key Sizes

Key sizes are specified in the applicable certificate profile document.

6.1.6 Public Key Parameters Generation and Quality Checking

NIFT uses cryptomodules based on the requirements of the associated legal agreements, CP, technical specification documents, and this CP/CPS.

Unless specified by another standard or requirement as specified above, the cryptographic modules may conform to FIPS 186-2 and provides random number generation and on-board generation of up to 4096-bit RSA Public Keys and a wide range of ECC curves.

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

NIFT's certificates may include key usage extension fields that specify the intended use of the certificate and technically limit the certificate's functionality in X.509v3 compliant software. The use of a specific key is determined by the key usage extension in the X.509 certificate and by the requirements specified by the relevant legal agreements, CP, and technical specification documents. Subscriber certificates assert key usages based on the intended application of the key pair. In particular certificates to be used for digital signatures (including authentication) set the digitalSignature and/or nonRepudiation bits. Certificates to be used for key or data encryption shall set the keyEncipherment and/or dataEncipherment bits. Certificates to be used for key agreement shall set the keyAgreement bit.

Key usage bits and extended key usages are specified in the certificate profile for each type of certificate as set forth in relevant profiled document.

6.2 PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

6.2.1 Cryptographic Module Standards and Controls

CA Private keys are generally protected using FIPS 140-2 Level 3 systems. External Program communities may elect a different standard for key protection, in which case that standard prevails. Private key holders must take necessary precautions to prevent the loss, disclosure, modification, or unauthorized use of such Private Keys in accordance with the relevant CP and contractual obligations specified in the appropriate legal agreements.

RAs with cryptographic modules will protect the Private Keys at the level specified in the relevant CP, legal agreements, this CP/CPS, and technical specification documents. These practices will be stated in their respective RPS.

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

NIFT's authentication mechanisms are protected securely when not in use based on the requirements of the associated legal agreements, CP, technical specification documents, and this CP/CPS.

If otherwise not stated in one of the above documents, backups of CA Private Keys are securely stored off-site and require two-person access. Re-activation of a backed-up CA Private Key (unwrapping) requires the same security and multi-person control as when performing other sensitive CA Private Key operations based on section 5.2.2.

6.2.3 Private Key Escrow

No stipulation.

6.2.4 Private Key Backup

No stipulation.

6.2.5 Private Key Archival

No stipulation.

6.2.6 Private Key Transfer into or from a Cryptographic Module

CA private keys are transferred from one cryptographic module to another to perform CA key backup procedures in section 6.3.4

All other keys are generated by and in a cryptographic module when it is in hardware. These practices will be based on the requirements of the associated legal agreements, CP, technical specification documents, and this CP/CPS. In the event that a private key is to be transported from one cryptographic module to another, the private key is encrypted during transport; private keys never exist in plaintext form outside the cryptographic module boundary.

Private or symmetric keys used to encrypt other private keys for transport are protected from disclosure.

Entry of a private key into a cryptographic module uses mechanisms to prevent loss, theft, modification, unauthorized disclosure, or unauthorized use of such private key.

When NIFT generates CA or RA private keys on one hardware cryptographic module and transfers them into another device, NIFT securely transfers such private keys into the second cryptographic module in a manner that prevents loss, theft, modification, unauthorized disclosure, or unauthorized use of such private keys. Such transfers shall be limited to making backup copies of the private keys on tokens.

If NIFT pre-generates private keys and transfers them into a hardware token, NIFT will securely transfer such private keys into the token in a manner that prevents the loss, theft, modification, unauthorized disclosure, or unauthorized use of such private keys.

6.2.7 Private Key Storage on Cryptographic Module

No stipulation beyond that specified in FIPS 140-2.

6.2.8 Method of Activating Private Keys

NIFT's Private Keys are activated according to the specifications of the cryptographic module manufacturer. These practices will be based on the requirements of the associated legal agreements, CP, technical specification documents, and this CP/CPS.. Activation data entry is protected from disclosure.

NIFT protects the activation data for their private keys against loss, theft, modification, disclosure, or unauthorized use.

CA administrators are authenticated to the cryptographic token or account before the activation of the associated private key(s). Entry of activation data is protected from disclosure (i.e., the data is not be displayed while it is entered). Subscribers are solely responsible for protecting their Private Keys. Subscribers should use a strong password or equivalent authentication method to prevent unauthorized access or use of the Subscriber's Private Key. At a minimum, Subscribers are required to authenticate themselves to the cryptographic module before activating their private keys.

6.2.9 Method of Deactivating Private Keys

NIFT's Private Keys are deactivated via logout procedures on the applicable HSM device or account when not in use. NIFT never leaves its HSM devices or accounts in an active unlocked or unattended state. Subscribers should deactivate their Private Keys via logout and removal procedures when not in use.

6.2.10 Method of Destroying Private Keys

NIFT/RA personnel, acting in trusted roles, destroy CA, RA, and status server Private Keys when no longer needed. Subscribers shall destroy their Private Keys when the corresponding certificate is revoked or expired or if the Private Key is no longer needed. NIFT may destroy a Private Key by deleting it from all known storage partitions. NIFT also zeroizes the HSM device and associated backup tokens according to the specifications of the hardware manufacturer. This reinitializes the device and overwrites the data with binary zeros.

CA keys associated with an External Program will be destroyed according to the requirements in the relevant legal agreements, CPs, technical specification documents, requirement(s), and this CP/CPS.

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

NIFT archives copies of Public Keys in accordance with Section 5.5 and per the associated CP requirements or other program documentation.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

The certificate validity period (i.e., certificate operational period and key pair usage period) are set to the time limits set forth in the relevant certificate profile.

For VC Certificates, the validity period shall not exceed stated timeframes in the VC Requirements.

PKI Participants must cease all use of their key pairs after their usage periods have expired.

6.4 ACTIVATION DATA

6.4.1 Activation Data Generation and Installation

NIFT activates the cryptographic module containing its CA Private Keys according to the specifications of the hardware manufacturer. All NIFT personnel and Subscribers are instructed to use strong passwords and to protect PINs and passwords. NIFT employees are required to create non-dictionary, alphanumeric passwords with a minimum length. If NIFT uses passwords as activation data for a signing key, NIFT will change the activation data change upon re-key of the CA Certificate.

6.4.2 Activation Data Protection

NIFT protects data used to unlock private keys from disclosure using a combination of cryptographic and physical access control mechanisms. Protection mechanisms include keeping activation mechanisms secure using role-based physical control. All NIFT personnel are instructed to memorize and not to write down their password or share it with another individual. NIFT locks accounts used to access secure CA processes if a certain number of failed password attempts occur. NIFT protects the activation data for its private keys using methods that protect against the loss, theft, modification, unauthorized disclosure, or unauthorized use of such private keys. These details are maintained in the disaster recovery procedures. NIFT maintains an audit trail of Secret Shares, and Shareholders participate in the maintenance of an audit trail.

6.4.3 Other Aspects of Activation Data

NIFT will follow the requirements of the associated legal agreements, CPs, and technical specification documents. If RAs handle activation data, they will follow the requirements of their associated legal agreements, the CP, this CP/CPS, and the related technical specification documents and state those practices in their respective RPS.

6.5 COMPUTER SECURITY CONTROLS

6.5.1 Specific Computer Security Technical Requirements

Computer security controls are required to ensure CA operations are performed as specified in the relevant contract agreements, CPs, and technical specification documents.

NIFT secures its CA systems and authenticates and protects communications between its systems and trusted roles. NIFT's CA servers and support-and-vetting workstations run on trustworthy systems that are configured and hardened using industry best practices.

6.5.2 Computer Security Rating No stipulation.

6.6 LIFE CYCLE TECHNICAL CONTROLS

6.6.1 System Development Controls

NIFT has mechanisms in place to control and monitor the acquisition and development of its CA systems. These practices will be based on the requirements of the associated legal agreements, CP, technical specification documents, and this CP/CPS..

Change requests require the approval of at least one administrator who is different from the person submitting the request. NIFT only installs software on CA systems if the software is part of the CA's operation. CA hardware and software are dedicated to performing operations of the CA.

Vendors are selected based on their reputation in the market, ability to deliver quality product, and likelihood of remaining viable in the future. Management is involved in the vendor selection and purchase decision process. Non-PKI hardware and software is purchased without identifying the purpose for which the component will be used. All hardware and software (if applicable) are shipped under standard conditions to ensure delivery of the component directly to a trusted employee who ensures that the equipment is installed without opportunity for tampering.

Some of the PKI software components used by NIFT are developed in-house or by consultants using standard software development methodologies. All such software is designed and developed in a controlled environment and subjected to quality assurance review. Other software is purchased commercial off-the-shelf (COTS). Quality assurance is maintained throughout the process through testing and documentation or by purchasing from trusted vendors as discussed above.

Updates of equipment and software are purchased or developed in the same manner as the original equipment or software and are installed and tested by trusted and trained personnel. All hardware and software essential to NIFT's operations is scanned for malicious code on first use and periodically thereafter.

6.6.2 Security Management Controls

NIFT has mechanisms in place to control and monitor the security-related configurations of its CA systems. When loading software onto a CA system, NIFT verifies that the software is the correct version and is supplied by the vendor free of any modifications. NIFT verifies the integrity of software used with its CA processes at least once a week.

6.6.3 Life Cycle Security Controls

No stipulation.

6.7 NETWORK SECURITY CONTROLS

NIFT documents and controls the configuration of its systems, including any upgrades or modifications made. These practices will be based on the requirements of the associated legal agreements, CP, technical specification documents, and this CP/CPS.

NIFT's CA system is connected to one internal network and is protected by firewalls and Network Address Translation for all internal IP addresses (e.g., 192.168.x.x). NIFT's customer support and vetting workstations are also protected by firewall(s) and only use internal IP addresses. Root Keys maintained on hardware are kept offline and brought online only when necessary to sign certificate-issuing subordinate CAs, OCSP responses, OCSP Responder Certificates, or periodic CRLs. Firewalls and boundary control devices are configured to allow access only by the addresses, ports, protocols and commands required for the trustworthy provision of PKI services by such systems. NIFT's security policy is to block all ports and protocols and open only ports necessary to enable CA functions. All CA equipment is configured with a minimum number of services and all unused network ports and services are disabled. NIFT's network configuration is available for review on-site by its auditors and consultants under an appropriate non-disclosure agreement.

6.8 TIME-STAMPING

When required by a legal contract, CP, and technical specification requirements documents Certificates, CRLs, and other revocation database entries contain time and date information. Such time information need not be

cryptographic-based. Asserted times are accurate to within three minutes. Electronic or manual procedures may be used to maintain system time.

7 CERTIFICATE, CRL, AND OCSP PROFILES

NIFT uses the ITU X.509, version 3 standard to construct digital certificates for use within the NIFT PKI. Specific certificate profiles are specified in NIFT's profile documentation, technical specification documents, and in the relevant community's CP or requirements document.

7.1 CERTIFICATE PROFILE

7.1.1 Version Number(s)

All certificates are X.509 version 3 certificates.

7.1.2 Certificate Extensions

As agreed to with the customer and as listed in the CP and technical specification documents or requirements document(s).

7.1.3 Algorithm Object Identifiers

Algorithm object identifiers are specified in the relevant certificate profile document or requirements document(s). NIFT recommends the following:

sha256WithRSAEncryption	[iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11]
ecdsa-with-sha256	iso(1) member-body(2) us(840)ansi-x962(10045)signatures(4)ecdsa-with-SHA2(3)ecdsawith-SHA256(2)
ecdsa-with-sha384	[iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures (4) ecdsa-with-SHA2 (3) 3]

7.1.4 Name Forms

Name forms are specified in the relevant certificate profile document or requirements document(s).

7.1.5 Name Constraints

Certificates assert the name constraints specified in the relevant certificate profile document or requirements document(s).

7.1.6 Certificate Policy Object Identifier

Policy OIDs are identified in the relevant certificate profile document or requirements document(s).

Verified Certificates issued in accordance with this document will assert UNDER the following Policy OIDs:
1.3.6.1.4.1.60140.

7.1.7 Usage of Policy Constraints Extension

Policy constraints are specified in the relevant certificate profile document.

7.1.8 Policy Qualifiers Syntax and Semantics

Policy qualifiers are NIFT may include brief statements in certificates about the limitations of liability and other terms associated with the use of a certificate in the Policy Qualifier field of the Certificates Policy extension.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

As agreed to with the customer and as listed in the CP and technical specification documents.

7.2 CRL PROFILE

7.2.1 Version number(s)

NIFT issues version 2 CRLs that contain the following fields:

Field	Value
Issuer Signature Algorithm	sha-1WithRSAEncryption [1 2 840 113549 1 1 5] OR sha-256WithRSAEncryption [1 2 840 113549 1 1 11] OR ecdsa-with-sha256 [1 2 840 10045 4 3 2] OR ecdsa-with-sha384 [1 2 840 10045 4 3 3]
Issuer Distinguished Name	[As appropriate]
thisUpdate	CRL issue date in UTC format
nextUpdate	Date when the next CRL will issue in UTC format.
Revoked Certificates List	List of revoked certificates, including the serial number and revocation date
Issuer's Signature	[Signature]

7.2.2 CRL and CRL Entry Extensions CRLs

have the following extensions:

Extension	Value
CRL Number	Never repeated monotonically increasing integer
Authority Key Identifier	Same as the Authority Key Identifier listed in the certificate
Invalidity Date	Optional date in UTC format
Reason Code	Optional reason for revocation

7.3 OCSP PROFILE

7.3.1 Version Number(s)

NIFT's OCSP responders conform to version 1 of RFC 2560.

7.3.2 OCSP Extensions

Extensions are set in accordance with RFC 2560.

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1 FREQUENCY AND CIRCUMSTANCES OF ASSESSMENT

Audits referencing this CP/CPS shall cover NIFT's CA systems, Sub CAs, and OCSP Responders.

RAs must comply with the audit requirements as specified in the legal agreements, the CP, relevant technical specification requirements, and this CP/CPS. How those audit requirements are met will be stipulated in their RPS.

8.2 IDENTITY/QUALIFICATIONS OF ASSESSOR

As agreed to with the customer in the relevant legal agreements, CP, and technical specification documents. RAs must comply with the audit requirements as specified in the legal agreements, the CP, relevant technical specification requirements, and this CP/CPS. How those audit requirements are met will be stipulated in their RPS.

8.3 ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY

As agreed to with the customer in the relevant legal agreements, CP, requirement(s), and technical specification documents.

RAs must comply with the audit requirements as specified in the legal agreements, the CP, relevant technical specification requirements, and this CP/CPS. How those audit requirements are met will be stipulated in their RPS.

8.4 TOPICS COVERED BY ASSESSMENT

Any audit covers NIFT's business practices disclosure, the integrity of NIFT's PKI operations, and NIFT's compliance with relevant standards.

RAs must comply with the audit requirements as specified in the legal agreements, the CP, relevant technical specification requirements, and this CP/CPS. How those audit requirements are met will be stipulated in their RPS.

8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY

If an audit reports a material noncompliance with applicable law, this CP/CPS, or any other contractual obligations related to NIFT's services, then (1) the auditor will document the discrepancy, (2) the auditor will promptly notify NIFT, and (3) NIFT will develop a plan to cure the noncompliance. NIFT will submit the plan to the CPA and/or governing bodies established for the programs for approval and to any third party that NIFT is legally obligated to satisfy. The CPA may require additional action if necessary to rectify any significant issues created by the non-compliance, including requiring revocation of affected certificates.

RAs must comply with the audit requirements as specified in the legal agreements, the CP, relevant technical specification requirements, and this CP/CPS. How those audit requirements are met will be stipulated in their RPS.

8.6 COMMUNICATIONS OF RESULTS

The results of each audit are reported to the CPA and to any third party entities which are entitled by law, regulation, or agreement to receive a copy of the audit results. NIFT may elect to share the audit report results with other entities in its sole discretion.

8.7 SELF-AUDITS

No stipulation.

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 FEES

9.1.1 Certificate Issuance or Renewal Fees

NIFT charges fees for certificate issuance and renewal. NIFT may change its fees in accordance with the applicable customer agreement.

9.1.2 Certificate Access Fees

If not specified in the relevant legal agreements or CP of an associated third party, NIFT may charge a reasonable fee for access to its certificate databases.

9.1.3 Revocation or Status Information Access Fees

NIFT does not charge a certificate revocation fee or a fee for checking the validity status of an issued certificate using a CRL. NIFT may charge a fee for providing certificate status information via OSCP.

9.1.4 Fees for Other Services

No stipulation.

9.1.5 Refund Policy

As set forth in the relevant customer agreement with NIFT.

9.2 FINANCIAL RESPONSIBILITY

9.2.1 Insurance Coverage

NIFT maintains Commercial General Liability insurance with a policy limit of at least PKR 10 million in coverage and Professional Liability/Errors & Omissions insurance with a policy limit of at least PKR 2 million in coverage. Insurance is carried through companies rated no less than A- as to Policy Holder's Rating in the current edition of Best's Insurance Guide (or with an association of companies, each of the members of which are so rated).

9.2.2 Other Assets

As set forth in the relevant legal agreements.

9.2.3 Insurance or Warranty Coverage for End-Entities

No stipulation.

9.3 CONFIDENTIALITY OF BUSINESS INFORMATION

9.3.1 Scope of Confidential Information

The following information is considered confidential and protected against disclosure using a reasonable degree of care:

- Private Keys;
- Activation data used to access Private Keys or to gain access to the CA system;
- Business continuity, incident response, contingency, and disaster recovery plans;
- Other security practices used to protect the confidentiality, integrity, or availability of information;
- Information held by NIFT as private information in accordance with Section 9.4;
- Audit logs and archive records; and
- Transaction records, financial audit records, and audit trail records and any audit reports (with the exception of an auditor's letter confirming the effectiveness of the controls set forth in this CP/CPS).

9.3.2 Information Not Within the Scope of Confidential Information

Any information not listed as confidential is considered public information. Published certificate and revocation data is considered public information.

9.3.3 Responsibility to Protect Confidential Information

NIFT's employees, agents, and contractors are responsible for protecting confidential information and are contractually obligated to do so. Employees receive training on how to handle confidential information. RAs are contractually required to protect confidential information.

9.4 PRIVACY OF PERSONAL INFORMATION

9.4.1 Privacy Plan

NIFT follows the Data Protection Act of Pakistan (draft) and NIFT privacy policy posted on its website when handling personal information. Personal information is only disclosed when the disclosure is required by law or when requested by the subject of the personal information.

9.4.2 Information Treated as Private

NIFT treats all personal information about an individual that is not publicly available in the contents of a certificate or CRL as private information. NIFT protects private information using appropriate safeguards and a reasonable degree of care. RAs may have a different standard of care as specified in their RPS.

9.4.3 Information Not Deemed Private

Private information does not include certificates, CRLs, or their contents.

9.4.4 Responsibility to Protect Private Information

NIFT employees and contractors are expected to handle personal information in strict confidence and meet the requirements of US and European law concerning the protection of personal data. All sensitive information is securely stored and protected against accidental disclosure.

9.4.5 Notice and Consent to Use Private Information

Personal information obtained from an applicant during the application or identity verification process is considered private information if the information is not included in a certificate. NIFT will only use private information after obtaining the subject's consent or as required by applicable law or regulation. All Subscribers must consent to the global transfer and publication of any personal data contained in a certificate.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

NIFT may disclose private information, without notice, if NIFT believes the disclosure is required by law or regulation.

9.4.7 Other Information Disclosure Circumstances

No stipulation.

9.5 INTELLECTUAL PROPERTY RIGHTS

NIFT and/or its business partners own the intellectual property rights in NIFT's services, including the certificates, trademarks used in providing the services, and this CP/CPS. "NIFT" is a registered trademark of NIFT (Pvt) Ltd.

Certificate and revocation information are the property of NIFT. NIFT grants permission to reproduce and distribute certificates on a non-exclusive and royalty-free basis, provided that they are reproduced and distributed in full. NIFT does not allow derivative works of its certificates or products without prior written permission. Private and Public Keys remain the property of the Subscribers who rightfully hold them. All secret shares (distributed elements) of the NIFT Private Keys are the property of NIFT.

All intellectual property of entities participating in the NIFT Private PKI remains the property of its respective owners as per the relevant legal agreements.

9.6 REPRESENTATIONS AND WARRANTIES

9.6.1 CA Representations and Warranties

Except as expressly stated in this CP/CPS or in a separate agreement with a Subscriber, NIFT does not make any representations regarding its products or services. NIFT represents, to the extent specified in this CP/CPS, that:

NIFT:

- NIFT complies, in all material aspects, with this CP/CPS and all applicable laws and regulations,
- NIFT publishes and updates CRLs and OCSP responses on a regular basis,
- Does not warrant the accuracy, authenticity, completeness, or fitness of any unverified information,
- Is not responsible for information contained in a certificate except as stated in this CP/CPS,
- Does not warrant the quality, function, or performance of any software or hardware device, and
- Is not responsible for failing to comply with this CP/CPS because of circumstances outside of NIFT's control.

9.6.2 RA Representations and Warranties

RA's represent that:

1. The RA's certificate issuance and management services conform to this CP/CPS,
2. Information provided by the RA does not contain any false or misleading information,
3. Translations performed by the RA are an accurate translation of the original information, and
4. All certificates requested by the RA meet the requirements of this CP/CPS. NIFT's agreement with the RA may contain additional representations.

9.6.3 Subscriber Representations and Warranties

Subscribers are solely responsible for any misrepresentations they make to third parties and for all transactions that use the Subscriber's Private Key, regardless of whether such use was authorized. Subscribers are required to notify NIFT and any applicable RA if a change occurs that could affect the status of the certificate. Subscribers represent to NIFT, Application Software Vendors, and Relying Parties that, for each certificate, the Subscriber will:

1. Securely generate its Private Keys and protect its Private Keys from compromise,
2. Provide accurate and complete information when communicating with NIFT and RAs,
3. Confirm the accuracy of the certificate data prior to using the certificate,
4. Promptly cease using a certificate and notify NIFT if (i) any information that was submitted to NIFT/the RA or is included in a certificate change or becomes misleading or (ii) there is any actual or suspected misuse or compromise of the Private Key associated with the certificate,
5. Ensure that individuals using certificates on behalf of an organization have received security training appropriate to the certificate,
6. Use the certificate only for authorized and legal purposes, consistent with the certificate purpose, this CP/CPS, any applicable CP or guidelines, and the relevant Subscriber Agreement, including only installing SSL certificates on servers accessible at the domain listed in the certificate and not using

code signing certificates to sign malicious code or any code that is downloaded without a user's consent, and

7. Promptly cease using the certificate and related Private Key after the certificate's expiration.

For VC participants, Applicants can find the VC Terms of Use ("VC Terms") in Appendix D of the VC Requirements, which is available at https://bimigroup.org/resources/VC_Guidelines_latest.pdf

9.6.4 Relying Party Representations and Warranties

Each Relying Party represents that, prior to relying on a NIFT certificate, it:

1. Obtained sufficient knowledge on the use of digital certificates and PKI,
2. Studied the applicable limitations on the usage of certificates and agrees to NIFT's limitations on liability related to the use of certificates,
3. Has read, understands, and agrees to the NIFT Relying Party Agreement and this CP/CPS,
4. Verified both the NIFT certificate and the certificates in the certificate chain using the relevant CRL or OCSP,
5. Will not use a NIFT certificate if the certificate has expired or been revoked, and
6. Will take all reasonable steps to minimize the risk associated with relying on a digital signature, including only relying on a NIFT certificate after considering:
 - a. applicable law and the legal requirements for identification of a party, protection of the confidentiality or privacy of information, and enforceability of the transaction;
 - b. the intended use of the certificate as listed in the certificate or this CP/CPS,
 - c. the data listed in the certificate,
 - d. the economic value of the transaction or communication,
 - e. the potential loss or damage that would be caused by an erroneous identification or a loss of confidentiality or privacy of information in the application, transaction, or communication,
 - f. the Relying Party's previous course of dealing with the Subscriber,
 - g. the Relying Party's understanding of trade, including experience with computer-based methods of trade, and
 - h. any other indicia of reliability or unreliability pertaining to the Subscriber and/or the application, communication, or transaction.

Any unauthorized reliance on a certificate is at a party's own risk.

9.6.5 Representations and Warranties of Other Participants

No stipulation.

9.7 DISCLAIMERS OF WARRANTIES

EXCEPT AS EXPRESSLY STATED IN SECTION 9.6.1, ALL CERTIFICATES AND ANY RELATED SOFTWARE AND SERVICES ARE PROVIDED "AS IS" AND "AS AVAILABLE". TO THE MAXIMUM EXTENT PERMITTED BY LAW, NIFT DISCLAIMS ALL EXPRESS AND IMPLIED WARRANTIES, INCLUDING ALL WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT. NIFT DOES NOT WARRANT THAT ANY SERVICE OR PRODUCT WILL MEET ANY EXPECTATIONS OR THAT ACCESS TO CERTIFICATES WILL BE TIMELY OR ERROR-FREE. NIFT does not guarantee the availability of any products or services and may modify or discontinue any product or service offering at any time. A fiduciary duty is not created simply because an entity uses NIFT's services.

9.8 LIMITATIONS OF LIABILITY

NOTHING HEREIN LIMITS LIABILITY RELATED TO (I) DEATH OR PERSONAL INJURY RESULTING FROM NIFT'S NEGLIGENCE OR (II) FRAUD COMMITTED BY NIFT. EXCEPT AS STATED ABOVE, ANY ENTITY USING A NIFT CERTIFICATE OR SERVICE WAIVES ALL LIABILITY OF NIFT RELATED TO SUCH USE, PROVIDED THAT NIFT HAS MATERIALLY COMPLIED WITH THIS CP/CPS IN PROVIDING THE CERTIFICATE OR SERVICE. Subscriber agreements and agreements with relying parties may contain different limitations on liability, in which case the agreement controls.

All liability is limited to actual and legally provable damages. NIFT is not liable for:

1. Any indirect, consequential, special, or punitive damages or any loss of profit, revenue, data, or opportunity, even if NIFT is aware of the possibility of such damages;
2. Liability related to fraud or willful misconduct of the Applicant;
3. Liability related to use of a certificate that exceeds the limitations on use, value, or transactions as stated either in the certificate or this CP/CPS;
4. Liability related to the security, usability, or integrity of products not supplied by NIFT, including the Subscriber's and Relying Party's hardware; or
5. Liability related to the compromise of a Subscriber's Private Key.

The limitations in this section apply to the maximum extent permitted by law and apply regardless of (i) the reason for or nature of the liability, including tort claims, (ii) the number of claims of liability, (iii) the extent or nature of the damages, (iv) whether NIFT failed to follow any provision of this CP/CPS, or (v) whether any provision of this CP/CPS was proven ineffective.

The disclaimers and limitations on liabilities in this CP/CPS are fundamental terms to the use of NIFT's certificates and services.

9.9 INDEMNITIES

9.9.1 Indemnification by NIFT

As set forth in the relevant customer agreement.

9.9.2 Indemnification by Subscribers

To the extent permitted by law, each Subscriber shall indemnify NIFT, its partners, and any cross-signed entities, and their respective directors, officers, employees, agents, and contractors against any loss, damage,

or expense, including reasonable attorney's fees, related to (i) any misrepresentation or omission of material fact by Subscriber, regardless of whether the misrepresentation or omission was intentional or unintentional;

- Subscriber's breach of the Subscriber Agreement, this CP/CPS, or applicable law;
- The compromise or unauthorized use of a certificate or Private Key caused by the Subscriber's negligence or intentional acts; or
- Subscriber's misuse of the certificate or Private Key.

9.9.3 Indemnification by Relying Parties

To the extent permitted by law, each Relying Party shall indemnify NIFT, its partners, and any cross-signed entities, and their respective directors, officers, employees, agents, and contractors against any loss, damage, or expense, including reasonable attorney's fees, related to the Relying Party's (i) breach of the Relying Party Agreement, an End-User License Agreement, this CP/CPS, or applicable law; (ii) unreasonable reliance on a certificate; or (iii) failure to check the certificate's status prior to use.

9.10 TERM AND TERMINATION

9.10.1 Term

This CP/CPS and any amendments to the CP/CPS are effective when adopted by the CPA and remain in effect until replaced with a newer version.

9.10.2 Termination

This CP/CPS and any amendments remain in effect until replaced by a newer version.

9.10.3 Effect of Termination and Survival

NIFT will communicate the conditions and effect of this CP/CPS's termination via email or the NIFT repository. The communication will specify which provisions survive termination. At a minimum, all responsibilities related to protecting confidential information will survive termination. All agreements remain effective until the certificate is revoked or expired, even if this CP/CPS terminates.

9.11 INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS

NIFT accepts notices related to this CP/CPS at the locations specified in Section 2.2. Notices are deemed effective after the sender receives a valid and digitally signed acknowledgment of receipt from NIFT. If an acknowledgement of receipt is not received within five days, the sender must resend the notice in paper form to the street address specified in Section 2.2 using either a courier service that confirms delivery or via certified or registered mail with postage prepaid and return receipt requested. NIFT may allow other forms of notice in the relevant customer agreement.

9.12 AMENDMENTS

9.12.1 Procedure for Amendment

This CP/CPS is periodically reviewed and updated by the CPA. Controls are in place to reasonably ensure that this CP/CPS is not amended and published without the prior authorization of the CPA.

9.12.2 Notification Mechanism and Period

NIFT does not guarantee or set a notice-and-comment period and may make changes to this CP/CPS without notice and without changing the version number. Major changes affecting accredited certificates

are announced and approved by the accrediting agency prior to becoming effective. The CPA is responsible for determining what constitutes a material change of the CP/CPS.

9.12.3 Circumstances under which OID Must Be Changed

The CPA is solely responsible for determining whether an amendment to the CP/CPS requires an OID change upon the notification from relevant PMAs.

9.13 DISPUTE RESOLUTION PROVISIONS

Parties are required to notify NIFT and attempt to resolve disputes directly with NIFT before resorting to any dispute resolution mechanism, including adjudication or any type of alternative dispute resolution.

9.14 GOVERNING LAW

For Verified Certificates:

The laws of the Government of Pakistan shall govern the interpretation, construction, and enforcement of this CP/CPS and all proceedings related hereunder, including tort claims, without regard to any conflicts of law principles, and shall have jurisdiction over such proceedings.

9.15 COMPLIANCE WITH APPLICABLE LAW

For Verified Certificates:

This CP/CPS is subject to all applicable laws and regulations, of Government of Pakistan. Subject to section 9.4.5's Notice and Consent to Use Private Information contained in Certificates, each Issuer CA shall (i) be licensed in each jurisdiction where it operates where licensing is required by the law of such jurisdiction for the issuance of Certificates, and (ii) meet the requirements of European data protection laws and shall establish and maintain appropriate technical and organization measures against unauthorized or unlawful processing of personal data and against the loss, damage, or destruction of personal data.

For all other Certificate types:

This CP/CPS is subject to all applicable laws and regulations, of Government of Pakistan.

9.16 MISCELLANEOUS PROVISIONS

9.16.1 Entire Agreement

NIFT contractually obligates any entity operating under this CP/CPS to comply with this CP/CPS and applicable industry guidelines. NIFT also requires each party using its products and services to enter into an agreement that delineates the terms associated with the product or service. If an agreement has provisions that differ from this CP/CPS, then the agreement with that party controls, but solely with respect to that party. Third parties may not rely on or bring action to enforce such agreement.

9.16.2 Assignment

Any entities operating under this CP/CPS may not assign their rights or obligations without the prior written consent of NIFT. Unless specified otherwise in a contract with a party, NIFT does not provide notice of assignment.

9.16.3 Severability

If any provision of this CP/CPS is held invalid or unenforceable by a competent court or tribunal, the remainder of the CP/CPS will remain valid and enforceable. Each provision of this CP/CPS that provides for a limitation of liability, disclaimer of a warranty, or an exclusion of damages is severable and independent of any other provision.

9.16.4 Enforcement (attorneys' fees and waiver of rights)

NIFT may seek indemnification and attorneys' fees from a party for damages, losses, and expenses related to that party's conduct. NIFT's failure to enforce a provision of this CP/CPS does not waive NIFT's right to enforce the same provision later or right to enforce any other provision of this CP/CPS. To be effective, waivers must be in writing and signed by NIFT.

9.16.5 Force Majeure

NIFT is not liable for any delay or failure to perform an obligation under this CP/CPS to the extent that the delay or failure is caused by an occurrence beyond NIFT's reasonable control. The operation of the Internet is beyond NIFT's reasonable control.

Clauses for force majeure will be added to the extent of applicable law for relevant parties and affiliates within the associated legal agreements.

9.17 Certificate Policy Management

NIFT CPA conducts assessment to determine the adequacy of the CP to address local regulations, business risks and compliance with NIFT Certificate Practice Statement.