Relief Validation Limited

Certification Practice Statement

(Version 1.0.0)

Document Control

Title	Certification Practice Statement-RVL
Document Type	Public
Version	1.0.0
Approve Date	
Previous Version	NA
Previous Version Revised Date	NA
Pages	
Status	Final for CCA's Approval

Revision History

Sl.	Version	Section Affected	Modification

Table of Contents

1. Introduction

Relief Validation Limited (RVL) is a private limited company incorporated under Companies Act, 1994 of Bangladesh.The term “Certifying Authority” or CA as used in this CPS, refers to RVL-CA or RVLCA as the entity that holds the CA license from the Office of the Controller of Certifying Authorities (CCA)- ICT Division, Ministry of Post, Telecommunication and Information Technology, Bangladesh Government.

Bangladesh PKI is a hierarchical PKI with the trust chain starting from the Bangladesh Root Certifying Authority. Bangladesh Root CA is operated by the Office of Controller of Certifying Authorities (CCA). Below Bangladesh Root CA there are Certifying Authorities (CAs) licensed by the CCA to issue Digital Signature Certificates and e-Sign under the provisions of IT Act 2006 and relevant regulations and guidelines. These are also called Licensed CAs. RVL CA is a Licensed CA under Bangladesh Root CA.

1.1.1. Background

Bangladesh Root CA’s CP defines certificate policies to facilitate interoperability among subscribers and relying parties for e-commerce and e-governance in Bangladesh. The CP and Certifying Authorities (CAs) are governed by the CCA. Certificates issued by CAs contain one or more registered Certificate Policy Object Identifier (OID), which may be used by a Relying Party to decide whether a certificate can be trusted for a particular purpose.

1.1.2. Purpose

The Certification Practice Statement (CPS) of RVL CA details the practices and operational procedures implemented to meet the assurance requirements. This CPS is consistent with the Internet Engineering Task Force (IETF), Public Key Infrastructure X.509 (IETF PKIX) RFC 3647,Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practice Statement Framework. CCA issues license to operate as Certifying Authority subject to successful compliance audit of CA per the CPS.

1.2.3. Scope

The CPS is also defined as a statement of the practices that a Certification Authority employs in issuing, managing, revoking, and renewing or re-keying digital certificates, and in providing e-Sign, Digital Seal, Timestamp, and document management services.
Certificate users and relying parties must assure themselves, by reviewing this document, and any other information they deem necessary, that any certificate issued, or other service provided by a RVLCA under this Policy is suitable for the intended use.

All keys, key materials, and certificates issued under this policy are the property of RVL CA. Activities of the certification authority and other entities, and all certificates issued and used under this CPS, are intended solely for the conduct of applicable RVLCA policies, Government regulations, and CCA policies.

1.2. Document Name and Identification

Document Title: Relief Validation Limited Certification Practice Statement (RVL CPS)
Document Version: CPS-RVL v 1.0.0

Document OID: 2.16.50.1.12

Document Date: 03.01.2024

1.3. PKI Participants

This section identifies and describes some of the entities that participate within the RVLCA PKI. RVLCA conforms to this CPS and other obligations it undertakes through adjacent contracts when it provides its services.

1.3.1. PKI Authorities

1.3.1.1. Controller of Certifying Authorities (CCA)

The Controller of Certifying Authority (CCA) manages and operates the Root CA of Bangladesh and several Subordinate CAs. CCA issues digital certificates using a collection of centralized, automated systems including hardware, software, personnel, and operating procedures that create, sign public key certificates to its Sub CAs. The CA is responsible for issuing and managing certificates including:

- Approving the issuance of all certificates, including those issued to subordinate CAs andRAs.
- Publication of certificates.
- Revocation of certificates.
- Generation and destruction of CA signing keys.
- Establishing and maintaining the CA system.
- Establishing and maintaining the Certification Practice Statement (CPS).
- Maintaining, issuing, and publishing CRLs and OCSP responses.

General information about CCA and Its Subordinate CAs are available at www.cca.gov.bd.

1.3.1.2. Certifying Authorities (CA)

Certification Authorities (CA) are entities licensed by CCA to sign and issue certificates under the CCA PKI Trust Network. The CA will issue Digital Certificates to end entities or subscribers who request Digital Certificates. The Digital Certificates thus issued legally bind the subscriber's Public Key (hence the Private Key) with his/her Identity.

The CA also manages Suspension, Activation, Revocation and/or Re-issuance of Digital Certificates which constitutes the Certificate Life Cycle. Apart from this, the CA also publishes the Certificate Revocation List (CRL) which contains the list of certificates that have been revoked/suspended by the CA. Such Certificates should not be used / trusted by the relying applications.

1.3.1.3. Subordinate Certifying Authority (Sub-CA)

Certifying authority (CA) can create one or more Subordinate Certifying Authority (Sub-CA). The Sub-CA will be part of the same legal entity as the CA. The key-pair of the Sub-CA are managed and operated by RVLCA.

Creation of RVL Sub-CAs has been approved subject to the following conditions:

Sl No.	Name of Sub-CA	Types of Certificates Issued
1.	Relief Validation Limited Sub-CA for e-sign	Issuance of e-sign certificates to end users
2.	Relief Validation Limited Sub-CA for timestamp	Issuance of timestamp service
3.	Relief Validation Limited Sub-CA for System	Issuance for internal certificates for machines and workstations, dedicated Trusted roles who will perform CA operations, Signature Management Module (SAM)

1.3.2. PKI Services

(i) **Certificate Services:** RVLCA provides e-Sign based certificate service.
(ii) **CRL Services:** CA makes available CRL freely downloadable by subscribers and relying parties.

(iii) **OCSP (Online Certificate Status Protocol) Validation Services:** CA can provide OCSP validation services to relying parties for certificate status verification in real time.

(iv) **e-Sign Service:** The following type of e-Sign service can be provided by RVLCA:
a) Client Applicant based e-Sign

RVLCA provides e-Sign services for its clients**,** both i.e., organization and individual, for that RVL will issue necessary certificates as per regulation upon successful completion of e-KYC

The e-KYC service of RVLCA authenticates the subscriber through Facial and Biometric based verification according to e-Sign Service Guideline provided by CCA.

The e-Sign system of RVLCA will also be integrated with the application service system of the organizational clients. The organizational clients will need legal agreements with RVLCA to avail e-Sign service according to the prevailing e-Sign Service Guideline.

1.3.3. Registration Authority (RA)

For Individual onboarding, a Registration Authority (RA) is an automated feature, that approves registration through successful e-KYC. The RVL e-sign system enables automatic identity authentication upon successful e-KYC.
In case of failure of automatic identity verification, the RA of RVLCA verifies the identity physically performing KYC.

For organization and/or organizational authorized person onboarding, a Registration Authority is responsible for identification and authentication of certificate applicants manually but does not sign or issue certificates (i.e., an RA is delegated certain tasks on behalf of an authorized CA).

1.3.4. Subscribers

The Subscribers / Applicants are the End Entities who ask for Digital Certificates from CA and make use of them. The Subscribers raise request for Digital Certificates by filling in the application form and submitting the associated documentation for verification by the RAs

End Entities requesting for a Digital Certificate can be:

1. Individuals
2. Individuals representing Organizations.

1.3.5. Relying Parties

A Relying Party is any entity that relies on information provided by Certificate Authorities regarding a specific electronic transaction that the Relying Party uses to accept or reject its participation in the transaction. The Relying Party is responsible for deciding whether or how to check the validity of the certificate by checking the appropriate certificate status information. The Relying Party can use the certificate to verify the integrity of a digitally signed message, to identify the creator of a message, or to establish confidential communications with the holder of the certificate. A Relying Party may use information in the certificate (such as certificate policy identifiers) to determine the suitability of the certificate for a particular use.

1.3.6. Other Participants

1.3.6.1. Auditors and Assessors

Besides the auditor roles and functions of the various authorities, from time-to-time external third-party auditor entities are engaged as per ICT Act 2006, IT (CA) Rules 2010 and Auditing Guidelineof CCA to verify the compliance provisions of the RVLCA Managed PKI.

1.4. Certificate Usage

1.4.1. Appropriate Certificate Uses

The Digital Certificates issued under the RVLCA Trust Network are used for lawful purposes as further described in the Section 4.5 Key Pair and Certificate Usage in this CPS. Use of issued Digital Signature Certificates under the RVLCA Trust Network for other than usage mentioned inthis CPS is prohibited. The RVLCA either by its own judgment, or guided by the advice of a concerned RA, reserves the rights to revoke Digital Certificates of Subscriber, entity, or organization for indulging in illegal use or misuse of Digital Signature Certificates, among other reasons.

1.4.2. Prohibited Certificate Uses

The Digital Certificates issued under this CPS are not designed, intended, or authorized for use or resale as control equipment in hazardous circumstances or for users requiring fail-safe performance such as the operation of nuclear facilities, aircraft navigation or communication systems, etc. where failure could lead directly to death, personal injury, or severe environmental damage. Client Certificates are intended for client applications and shallnot be used as server or organizational Certificates.

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

1.5. Policy Administration

This section includes the name and mailing address of the organization that is responsible for the drafting, registering, maintaining, and updating of this document. It also includes the name, electronic mail address, telephone number of a contact person.

1.5.1. Organization Administering the Document

This CPS is administered by RVLCA and is revised with the approval of CCA.

1.5.2. Contact Person

RVLCA can be contacted at the following address:

RVL Certification Authority Manager
Relief Validation Limited
CA Manager
Tel: +8809606501227
Email: ca@reliefvalidation.com.bd
Website: www.reliefvalidation.com.bd

1.5.3. Person Determining CPS Suitability for the Policy

RVLCA Chief of CA Administration is responsible to administer and determine CPS suitability for the policy, provided the intended suitability is duly approved by the CCA.

1.5.4. CPS Approval Procedures

RVLCA CPS shall be submitted to CCA, Bangladesh for approval before commencing CA operations. The approved CPS shall be made available in RVLCA web portal.

Proposed changes to the CPS are divided into two classes. Simple changes (such as minor clarifications, spelling/grammatical errors, minor typographic errors) shall be noted as and when the error is found. All such errors (if any) are collected and the whole set treated as one proposedchange.

Large changes, such as material changes in policy, procedures, financial information (such as fees or liability caps), and any other changes are treated as proposed changes.

Any changes to the CPS arising due to changes in policies, procedures, or any updates to the Act or Guidelines defined by CCA; Bangladesh shall be approved by RVLCA Management. The updated CPS will be shared with CCA for approval. On obtaining the approval, the CPS will be published in RVLCA website. The RVLCA management must approve the proposed changes.

These changes are informed to the CCA, Bangladesh and upon approval by CCA, Bangladeshare adopted as the new CPS and updated on the RVLCA web portal.

1.6. Definitions and Acronyms

All definitions and acronyms are listed in Appendix A of this document.

2. Publication & PKI Repository Responsibilities

2.1. PKI Repositories

CA maintains Hypertext Transfer Protocol Secure (HTTPS), or LDAP based repositories thatcontain the following information:

a) CA Certificates Issued to their sub-CAs
b) Certificate Revocation List (CRL)
    a) Issued by the Licensed CA
    b) Issued by their sub-CAs
c) Digital Signature Certificates issued by CA/sub-CA

2.2. Publication of Certification Information

The Certification Practice Statement, CA-certificate, and certificate status information are available from the repository. CA maintains a repository and is available at https://www.reliefvalidation.com.bd/repository.html.

Certificate revocation list using this CPS will be hosted in a separate directory located under the URL https://www.reliefvalidation.com.bd/repository.html.

2.3. Time or Frequency of Publication

The RVL CA publishes certificates and other information promptly upon issuance or acceptance by it. It also publishes its CRL immediately after revocation of any certificate. Apart from this,CRLs will be generated every 24 hours.

2.4. Access Controls on Repositories

The RVLCA repositories are maintained by RVLCA and are accessible to authorized personnel. The RVLCA repositories are the source for the most current CRL and other information regarding Digital Certificates issued under the RVLCA Trust Network. The adding, deleting, or modifying repository entries can be performed only by listed authorized personnel of RVLCA. All others including subscribers and relying parties are only allowed to search/query the repository.

3. Identification and Authentication

The requirements for identification and authentication are specified under Information Technology Act 2006, Rules and Guidelines issued there under. Before issuing a Certificate, the CA ensure that all subject information in the certificate conforms to the requirements that has been verified in accordance with the procedures prescribed in this CPS.

3.1. Naming

3.1.1. Types of Names

The names in the Digital Certificates issued under the RVLCA Trust Network shall comply X.500 naming conventions as specified in Root CA Certificate Profile of Interoperability Guidelines published by CCA, Bangladesh. These Digital Certificates shall use

Distinguished Names (DN) to provide the identities to Subscribers, the RVLCA and the Partner for whom Sub-CA has been created under the RVLCA Trust Network. Subject specification for CA Certificate consists of following attributes –

Common Name (CN)
House Identifier
Street Address
Locality
State / Province
Postal Code
Organizational Unit (OU)
Organization (O)
Country (C)

3.1.2. Need for Names to be Meaningful

All subject names must be meaningful. The names provided on the digital certificate must be as accurate as possible when describing the person or organization or role within the organization. Digital certificates will not be issued for names that are not to be deemed meaningful by RVLCA.

The Subject and Issuer names contained in a certificate MUST be meaningful in the sense that the issuing CA has proper evidence of the existent association between these names and the entities to which they belong.

- For personal certificates, the CN DN attribute contains the legal name as presented in agovernment issued photo-identification.

RVLCA ensures that the Organization (O) and Organizational Unit (OU) attributes in the Subjectfield accurately identify the legal entity that is the subject of the certificate. Similarly, RVLCA usesnon-ambiguous designations in the Issuer field to identify itself as the Issuer of a certificate (e.g., RVL Certificate Authority).

3.1.3. Anonymity or Pseudonymity of Subscribers

Subscriber names cannot be anonymous or pseudonyms. The name provided in the CommonName field should be verifiable against the identity proofs.

3.1.4. Rules for Interpreting Various Name Forms

DNs shall be interpreted according to the X.501 standard:

a) Country [CountryName] (C) – This attribute contains a two-letter ISO 3166 country code.
b) Organization [OrganizationName] (O) – This attribute contains the name of anorganization.
c) Organizational Unit Name [OrganizationalUnitName] (OU) – This attribute contains thename of an organizational unit.
d) Common Name [CommonName] (CN) – This attribute contains a name of an object.

3.1.5. Uniqueness of Names

The Distinguished Names form the basis for the uniqueness of each assigned name, but

the same Applicant/Subscriber can have multiple Digital Certificates with the same DNs for different Digital Certificate purposes as specified in the CPS.

The Distinguished Names should be able to uniquely identify the Subscriber in public Repository in which it is published. Additionally, all the Digital Certificates under the RVLCA Trust Network shall be assigned a unique serial number, which will enable identification, suspension, activation, and revocation of the Digital Certificates when required.

3.1.6. Recognition, Authentication, and Role of Trademarks

Subscribers represent and warrant that all information supplied in the digital certificate applicationprocess is accurate and does not infringe or violate in any way the trademarks, service marks, trade name, company name, or any other Intellectual Property Rights of any third party. Subscribers also warrant that any material they supply or transmit is not libelous and does not constitute malicious falsehood or disparagement of goods or services, is not otherwise defamatory, is not immoral, obscene, is not illegal and does not advocate illegal activity, does notconstitute a violation of privacy and does not infringe any Intellectual Property Rights of RVLCA or a third party.

3.2. Initial Identity Validation

3.2.1. Method to Prove Possession of Private Key

As per client's request, the private key will be generated by the HSM and subsequently exported from the HSM using the HSM key encrypting key (KEK) and stored as encrypted blob (Binary Large Object) in the CA system under the sole control of e-Sign subscriber. They will remain encrypted when not in use.

3.2.2. Authentication of Organizational User Identity

An organization's identity as well as other enrolment information are required to be verified and confirmed by the Registration Authority (RA) of the RVLCA.
RVLCA will perform the verification of the identity of the organization along with the identity of the representatives of the organization. The organization concerned requires submitting the following documents to the RVL CA:

1. Certificate of Incorporation or equivalent
2. Trade License
3. BIN
4. TIN/eTIN

Documents required for the organization's authorized person:
1. Organizational Authorization Letter
2. Admin Authorization Letter

In addition to the above, the representative of the organization requires to be verified as per the procedure described in Clause 3.2.3.

3.2.3. Authentication of Individual Identity

For verification, the following documents are accepted by the RVLCA:

Photo ID: NID

For e-Sign certificates, the applicant will be verified through RVLCA e-KYC system based on Facial or Fingerprint matching as per CCA e-Sign guideline.

Authenticate identity by matching the identity provided by the Subscriber's information residing in the database of a CCA approved identity proofing service, such as a National Identity Verification through e-KYC system provided by RVLCA.

In case of failure of automatic identity verification, the RA of RVLCA verifies the identity physically performing KYC.

3.2.4. Device Certificates

RVLCA does not provide device certificate.

3.2.5. Non-verified Subscriber Information

Any non-verified information included in a certificate shall be designated as such in the certificate as per IOG guideline. No unverified information shall be included in any Class 2 certificate.

3.2.6. Validation of Authority

RVLCA Operator shall verify a Subscriber to authenticate his affiliation/association/ representation with the Organization for which he requested the certificate for. There must be at least one valid document which unambiguously corroborates the proof that the Subscriber's declared relationship with an organization is founded.

3.2.7. Criteria for Interoperation

Digital Certificates issued under the RVLCA hierarchy will be in accordance with the CCA's DigitalCertificate Interoperability Guidelines.

3.3. Identification and Authentication for Re-key Requests

3.3.1. Identification and Authentication for Routine Re-Key

Subscribers will be sent a notification email 30 days prior to the expiry of Digital Certificate. A Subscriber will be treated as being the same as stipulated in the Clause 3.2 will be applicable for Subscriber's Routine Authentication.

3.3.2. Identification and Authentication for Re-key after Revocation

When authenticating a Subscriber's identity for Re-key after certificate revocation, he will be treated as a fresh requestor. Clause 3.2 of this document will be followed to authenticate this Subscriber.

The procedure for re-authentication is the same with an initial registration.

3.4. Identification and Authentication for Revocation Request

For e-Sign, the certificate expiry time is much longer, usually 1-2 years. In that case, certificate

revocation may be required. Subscriber can ask for revocation of his/her certificate for reasons such as Private Key compromise. Prior to the revocation of a certificate, the CA verifies that the revocation has been requested by an authorized entity. For revocation of end-entity subscriber certificates issued from a RVLCA Managed PKI Service, the acceptable procedures for authenticating the revocation requests of a Subscriber include:

1. The subscriber can log-in to the RVLCA portal and request for revocation, stating his/her reason for revocation.
2. By signing a revocation request with the private key of the corresponding certificate, which is being requested for revocation, and sending the request to RVLCA via web portal. RVLCA will authenticate the revocation request using the requestor's public key to decrypt, also communicating with the requestor via phone/mail. The certificate, for which revocation is requested, must be a valid, non-expired and non-revoked certificate.

The CA has the authority to revoke the certificate specifying the revocation reason under the circumstances stated in the clause 4.9.1. After the revocation, the user will receive a notification via email, that notifies that his/her certificate has been revoked.

4. Certificate Life-Cycle Operational Requirements

Communication among the CA, RA, and subscriber are implemented with requisite security services (i.e., source authentication, integrity, non-repudiation, or confidentiality) applied to them commensurate with the assurance level of the certificate being managed.

When cryptography is used, CA implemented the mechanism, at least as strong as the certificates being managed, to secure web site using Secure Socket Layer (SSL) certificate and set up with appropriate algorithms and key sizes satisfies the integrity and confidentiality requirements for certificate management.

4.1. Certificate Application

The applicant intending to subscribe e-Sign certificate requires to submit an online application form filled with personal details, address, live photo, supporting documents (front and back part of NID). On receipt of the request and information in the prescribed format, CA carries out the verification of documents. The detailed requirements for e-Sign certificate applications are specified under Clause 3.2.3. For e-Sign certificates, certificate requests will be received from e-Sign system through secured API channel.

4.1.1. Who Can Submit a Certificate Application

Any person who owns a valid NID or authorized representative of an organizational entity can apply for a certificate to RVLCA. The e-Sign system will submit certificate requests through secured API.

4.1.2. Enrolment Process and Responsibilities

RVLCA Chief of CA Administration is responsible to establish an enrollment process for his CA team to assist in receiving a digital certificate application requested by a user. For e-Sign certificates, certificate request will be received from e-Sign system through secured API channel. Applicants will be verified through CCA approved e-KYC process.

4.2. Certificate Application Processing

4.2.1. Performing Identification and Authentication Functions

Guideline described in Clauses 3.2.3 is used to validate individual identity.

Validation of Organizational information and documents is done using the guideline described in Clause 3.2.2 in the event that certification is requested for an organization.

4.2.2. Approval or Rejection of Certificate Applications

From time to time, RVLCA may modify the requirements related to application information requested, based on RVLCA requirements, business context of the usage of certificates, or as it may be required by law with prior approval of CCA.

For individual certificate approval, following successful completion of all required validations of a certificate application, the application for a digital certificate is automatically approved by the RVLCA.

For organizational certificate approval, following successful verification of the entity physically, the application for a digital certificate is approved manually by the RVLCA.

4.2.3. Time to Process Certificate Applications

A request for certification is handled instantly. The certificate will be generated automatically and sent to e-Sign system through secured API.

4.3. Certificate Issuance

For individual certificate issuance process, after e-KYC, a certificate applicant submits a certificate application. Upon successful verification based on all required authentication procedures e-sign certificates, a contract is issued to the Subscriber which is to be accepted by push notification in the Mobile application. After acceptance of the contract, a certificate is confirmed by the end user using the push notification in the Mobile application. After confirmation a certificate is issued to the end user instantly.

For organization, CA verifies or refutes the information in the certificate application. The applicant's request for certificate issuance is reviewed by the CA which may result in approval or denial of certificate.

4.3.1. CA Actions during Certificate Issuance

For individual certificate issuance process, the RVL e-sign system signs a contract and issues the certificate to the subscriber. The subscribers receive a notification on the mobile application, where they agree and sign the certificate contract. The system also notifies the Subscriber of contract signing and certificate issuance through email. After confirmation from the mobile application, subscribers are then able to use the digital certificate. Certificates are checked to ensure that all fields and extensions are properly populated. After verification, generation, and acceptance, CA publishes the certificate in the repository.

For organizational certificate issuance process, CA verifies the source of a certificate request before issuance.

4.3.2. Notification to subscriber by the CA of Issuance of Certificate

The RVLCA signs a contract and issues the certificate to the subscriber. The subscribers receive a notification on mobile application where they agree and sign the contract back and confirm the receipt of the issued certificate. The system also notifies the Subscriber of contract signing and certificate issuance through email. After confirmation from the mobile application, RVL user portal makes the certificate available.

4.4. Certificate Acceptance

The certificate will be sent to e-Sign system through secured API and this event will be deemed as acceptance of the certificate.

4.4.1. Conduct Constituting Certificate Acceptance

The certificate will be considered as accepted by the subscriber when the subscriber confirms the push notification. An email will also be sent to the Subscriber for successful certificate issuance. The Subscriber can log in to the RVLCA Portal, check the details and can download the certificate from the portal. Subscribers accepting the contract and confirming the push notification is treated as certificate acceptance. There is no time limit within which the push notification on the Mobile application must be accepted for certificate issuance.

4.4.2. Publication of the Certificate by the CA

As RVLCA only issues e-Sign certificates, the subscriber certificates are not published in the repository.

4.4.3. Notification of Certificate Issuance by the CA to Other Entities

RVLCA does not follow any other means of notification or publication of information pertaining to issuing certificates for an entity except for the means as described in Clause 2.2 of this document.

4.5. Key Pair and Certificate Usage

4.5.1. Subscriber Private Key and Certificate Usage

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

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

4.5.2. Relying Party Public Key and Certificate Usage

Relying parties shall assent to the terms of the applicable Relying Party Agreement as a condition of relying on the certificate. Reliance on a certificate must be reasonable under the circumstances. If the circumstances indicate a need for additional assurances, the Relying Party must obtain such assurances for such reliance to be deemed reasonable.

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

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

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

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

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

4.6. Certificate Renewal

As per IT CA Rules 2010, RVLCA does not support renewal of certificates in any circumstances. It is treated as certificate Re-key.

4.6.1. Circumstance for Certificate Renewal

Refer to Section 4.7.1

4.6.2. Who May Request Renewal

Refer to Section 4.7.2

4.6.3. Processing Certificate Renewal Requests

Refer to Section 4.7.3

4.6.4. Notification of New Certificate Issuance to Subscriber

Refer to Section 4.7.4

4.6.5. Conduct Constituting Acceptance of a Renewal Certificate

Refer to Section 4.7.5

4.6.6. Publication of the Renewal Certificate by the CA

Refer to Section 4.7.6

4.6.7. Notification of Certificate Issuance by the CA to other Entities

Refer to Section 4.7.7

4.7. Certificate Re-key

Re-keying a certificate means that a new certificate is created that has the same characteristics and level as the old one, except that the new certificate has a new, different public key (corresponding to a new, different private key) and a different certificate serial number, and it may be assigned a different validity period.

4.7.1. Circumstance for Certificate Re-key

The following events warrant the circumstances for a Subscriber to apply for certificate re-key:

a) When the validity period of a particular certificate expires in just 30 days.
b) When the certificate is revoked, and the Subscriber applies again.

The corresponding RA may make reasonable efforts to inform the subscriber in advance about the expiration of the subscriber's certificate.

4.7.2. Who May Request Certification of a New Public Key

Only the subscriber for an individual certificate or an authorized representative for an organizational certificate may request a new certificate based on the new public key.

4.7.3. Processing Certificate Re-keying Requests

The person or organization seeking to re-key shall be authenticated as the Subscriber (or authorized by the Subscriber) of the certificate by one of the following procedures:

a) Proof of possession of the private key.

b) Subscribers choose and submit with their enrolment information a Challenge Phrase (or the equivalent thereof). Upon re-keying, if a Subscriber correctly submits the Subscriber's Challenge Phrase (or the equivalent thereof) with the Subscriber's re-enrolment information, and the enrolment information (including contact information) has not changed, a new certificate is issued.

Other than this procedure, the processing re-keying requests will be same as original requests as specified in Section 4.2 Certificate Application Processing.

4.7.4. Notification of New Certificate Issuance to Subscriber

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

Section 4.3.2.

4.7.5. Conduct Constituting Acceptance of a Re-keyed Certificate

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

4.7.6. Publication of the Re-keyed Certificate by the CA

The Digital Certificates accepted by the subscribers will be published in the RVLCA repository by the CA.

4.7.7. Notification of Certificate Issuance by the CA to other Entities

Subscribers are notified through email once their Digital Certificates are issued. No other entities are notified.

4.8. Certificate Modification

4.8.1. Circumstance for Certificate Modification

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

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

4.8.2. Who May Request Certificate Modification

Refer to Section 4.1.1.

4.8.3. Processing Certificate Modification Requests

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

4.8.4. Notification of New Certificate Issuance to Subscriber

Refer to Section 4.3.2.

4.8.5. Conduct Constituting Acceptance of a Modified Certificate

Refer to Section 4.4.1.

4.8.6. Publication of the Modified Certificate by the CA

Refer to Section 4.4.2.

4.8.7. Notification of Certificate Issuance by the CA to other Entities

Refer to Section 4.4.3.

4.9. Certificate Revocation and Suspension

For e-Sign, the certificate expiry time is much longer, usually 1-2 years. In that case, certificate revocation and suspension may be required.

Suspension is the process of making a certificate to make it invalid temporarily. Revocation is the process of making a certificate to be invalid permanently. RVLCA can activate the suspended certificates. The revoked certificates cannot be reused and are listed in the CRL.

The RVLCA reserves the right to revoke any of its issued digital certificates as per IT (CA) Rules 2010 or as instructed by the CCA. As per, the revoked Electronic Signature Certificate shall be added to the Certificate Revocation List (CRL). All revocation information is published in repository server where it is made publicly available when required for certificate verification processes.

4.9.1. Circumstances for Revocation

There are two distinct reasons that arise for which activities pertaining to revocation of a certificate are required for. In one instance, a revocation process takes place with the intentional and lawful request of the Subscriber to do so, and in the other instance, revocation process is enforced by the RVLCA owing to non-compliance of the terms and conditions set forth as binding upon the Subscriber.

Clause 3.4 of this document describes possible means of revocation requests made by a Subscriber within the scope of his lawful authority.

There are circumstances that lead the RVLCA to enforce its legal authorities to take steps for revoking a certificate, like:

a) When the information it contains or the implied assertions it carries are known orsuspected to be incorrect, inaccurate, wrong, or compromised.
b) If it is found that the Subscriber violates his/her obligations as agreed to comply with.
c) If any other entity presents against the Subscriber any evidence which substantiallycorroborates incidences of flagrant violation of obligations.
d) If subscriber contravened any provisions of the ICT ACT 2006 or IT (CA) rules 2010 (Rule 30)
e) The private key corresponding to the public key in the certificate has been lost, disclosed without authorization, stolen, or compromised in any way.
f) RVLCA suspects or determines that revocation of a Certificate is in the best interest of theintegrity of RVLCA,
g) There has been an improper or faulty issuance of a certificate due to:
    - A material prerequisite to the issuance of the Certificate not being satisfied.
    - A material fact in the Certificate is known, or reasonably believed, to be false.
    - If the subscriber has expired (i.e., dead)
    - The subscriber has been declared insolvent by a competent court or authority
    - Instructions from appropriate government authorities, court of law, or lawenforcement agencies.

4.9.2. Who Can Request Revocation

The following entities may request revocation of a subscriber digital certificate:

- The RVLCA upon notifying the Root CA.
- The subscriber/end entity user.

- Any other entity holding evidence of a revocation circumstance about that certificate.
- Law enforcement agency of Bangladesh Government

4.9.3. Procedure for Revocation Requests

4.9.3.1. Request from the Subscriber

The procedure for the subscriber to request the revocation of Digital Certificate is as follows:

- The subscriber generates the request for the Digital Certificate revocation and sends thedetails along with the reason for revocation.
- The RVL–CA verifies the request and then revokes the subscriber's certificate. The RVL– CA then updates the corresponding CRL with the list of all revoked certificates and publishes it to the repository.
- The subscriber can check the status of the revocation request on the RVLCA portal.

The validity of the request will be checked as follows:

- For requests from the subscriber signed using the private key, no further verification isdone.
- For requests submitted via the RVLCA portal using the user's own user-id and password, no further verification is done.
- For written requests which are signed and accompanied by police complaint, no further verification is done.
- For written requests which are signed and accompanied by a copy of attested identity proofwith the same signature, no further verification is done.

4.9.3.2. Request from government/courts/law enforcement

For revocation requests originating from entities such as the government/court/law enforcement agency, verification is based on the nature of documentation submitted in support of the requestand will be according to applicable laws.

4.9.3.3. Request from the RA

Not applicable for RVLCA.

4.9.4. Revocation Request Grace Period

There is no revocation grace period. Responsible parties must request revocation as soon as they identify the need for revocation.

4.9.5. Time within Which CA Must Process the Revocation Request

A Digital Certificate will be revoked by close of business day for revocations placed online by subscriber from his/her user login and if the request for revocation is received vide email/letter, verification of a revocation request is made, and the revocation will be done on once the verification of is satisfactory. Until the verification is in process, the Digital Certificate may be suspended.

Action on a revocation request made over a weekend or holiday may be delayed until the followingbusiness day of the RA.

4.9.6. Revocation Checking Requirement for Relying Parties

A relying party shall use the certificates issued under the RVLCA Trust Network only after checking the same with the latest CRL of the corresponding certificate issuer available at the repository. The RVL–CA or the RA shall not be liable to any damages/loss caused by the certificates or CRLs.

The repository is made available to the subscribers and public via the RVLCA portal. The repository contains all information of the subscribers' certificates relating to their validity, suspension, activation, and revocation through CRL. The relying party must check the certificate details online before they trust the certificates. RVL–CA or the RA shall not be held responsible for any loss/damage caused by certificates issued under the RVLCA Trust Network that are usedby the relying party.

4.9.7. CRL Issuance Frequency

The RVLCA will update and issue the CRL (including certificates issued) whenever certificates under their respective user groups are revoked or suspended. Irrespective of the occurrence of revocations or suspensions, CRL will be updated once in every 24 hours. The CRL issued shall be published to the repository immediately.

4.9.8. Maximum Latency for CRLs

There is no latency for Publishing CRLs as it is immediate. CRLs are generated as soon as any Suspension / Activation or Revocation of Certificates takes place. The CRLs are published onto the RVLCA web portal as soon as they are generated.

4.9.9. On-Line Revocation/Status Checking Availability

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

4.9.10. On-Line Revocation Checking Requirements

It is the responsibility of relying party to check certificate status. RVLCA will recommend relying party to check certificate status as and when required.

4.9.11. Other Forms of Revocation Advertisements Available

Other than implementation of CRLs and on-line revocation status, no other forms of on-linerevocation status will be provided by CA.

4.9.12. Special Requirements Related to Key Compromise

RVLCA uses reasonable efforts to notify potential Relying Parties if it discovers, or have reason to believe, that there has been a compromise of the private key of one of their own CAs or Sub- CAs.

4.9.13. Circumstances for Suspension

For e-Sign, the certificate expiry time is much longer, usually 1-2 years. In that case,

certificate suspension may be required. A certificate may put on hold (i.e., suspended) for a short period due to following circumstances –

a) Due to order from law enforcement agency, court, or Bangladesh Government.
b) Subscriber requests to suspend his/her certificate.
c) Suspicious activity of subscriber reported to RVLCA.
d) Any other circumstance which may lead RVLCA to suspend the certificate.

4.9.14. Who can Request Suspension

a) RVLCA
b) Subscriber/ End user
c) Any entity holding evidence of a suspension circumstance committed by any other entity
d) Law enforcement agency of Bangladesh Government

4.9.15. Procedure for Suspension Request

The subscribers and the RAs will request for the certificate suspension using the same procedures as for the certificate revocation specified in Section 4.9.3.

4.9.16. Limits on Suspension Period

The RVLCA reserves the right to revoke the suspended certificates of its subscribers if a request for activation of suspended certificate is not received within 15 days of the date of suspension.

4.9.17. Who Can Request for Activation of a Suspended Certificate

Activation is the process of making the applicant/subscriber's suspended certificate to be valid for use based on conditions as specified in this CPS. CA may initiate the request for activation for any suspended certificate. A certificate shall be activated only if the RVLCA is satisfied that the reason for suspension is no longer valid.

4.9.18. Procedure for Activation Request

The suspended certificates shall be re-activated upon approval by the RVLCA or when the sameparty that had the certificate suspended initiates the request. This should be done within 15 days after the Digital Certificate has been suspended. The RVLCA shall remove the re-activated certificates from the corresponding CRL listing and a new CRL will be generated and published to the repository.

4.10. Certificate Status Services

4.10.1. Operational Characteristics

The Status of public certificates is available via CRL at RVLCA's website, LDAP directory and viaan OCSP responder (where available).

4.10.2. Service Availability

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

4.10.3. Optional Features

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

4.11. End of Subscription

A Subscriber may end a subscription for a RVLCA certificate by:

a) Allowing his/her/its certificate to expire without renewing or re-keying that certificate, or
b) Revoking his/her/its certificate before certificate expiration without replacing the certificate.

4.12. Key Escrow and Recovery

4.12.1. Key Escrow and Recovery Policy and Practices

RVLCA does not practice Key Escrow for recovery.

4.12.2. Session Key Encapsulation and Recovery Policy and Practices

Session key recovery is not supported under this CPS.

5. Facility, Management, and Operational Controls

This section describes the physical, procedural, and personnel security controls of the RVLCA environment.

5.1. Physical Controls

5.1.1. Site Location and Construction

RVLCA is in a fully protected and restricted zone. The location of RVLCA office within the compound is always attended by at least one authorized person.

The system components and operation of CA are contained within a physically protected environment to deter, detect, and prevent unauthorized use of, access to, or disclosure of sensitiveinformation. The physical security standards are modeled as per the physical and operational security guidelines mentioned in the Information and Communication Technology Act (ICT) of 2006 of Bangladesh.

5.1.2. Physical Access

The RVLCA is housed at a restricted location in compliance with the ICT Act and regulation, where progressively restrictive physical access privileges control to each level is ensured. The site of operation is strictly restricted by multiple tiers initiated using access email, mobile phone number and photo ID. A logbook is maintained to keep physical entry records. Entry is further restricted by security doors that can only be accessed by the authorized personnel followed by two layers of biometric locks are enabled to reach the CA containment. Finally, the security of the server rack is maintained using a physical lock.

5.1.3. Power and Air Conditioning

CAs secure facilities are equipped with primary and backup power systems to ensure continuous, uninterrupted access to electric power and these secure facilities are equipped with air conditioning systems to control temperature and relative humidity.

PKI Repositories are provided with sufficient Uninterrupted Power for continuous CA operations.

5.1.4. Water Exposures

RVLCA has taken necessary measures to protect critical systems for the CA operation premises from any kind of water damage or water exposure.

5.1.5. Fire Prevention and Protection

Automatic fire detectors and extinguishers compliant with standard requirements specified by the fire brigade is installed in the RVLCA operating premises to prevent and protect the facility from fire. Also, the whole building is equipped with hand fire extinguishers on each floor. Guards and office employees are trained to use the hand fire extinguishers.

5.1.6. Media Storage

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

5.1.7. Waste Disposal

Sensitive documents and materials are shredded before disposal. Media used to collect or transmit sensitive information are rendered unreadable before disposal. Cryptographic devices are physically destroyed or zeroed in accordance with the manufacturers' guidance prior to disposal.

5.1.8. Off-Site Backup

RVLCA performs routine backups of critical system data, audit log data, and other sensitive information. Offsite backup media are stored in a physically secured location.

5.2. Procedural Controls

Procedures are established, documented, and implemented for all trusted and administrative roles required to operate the RVLCA Service. Where possible and appropriate duties associated with RVLCA specific operations are kept separate from general operations. This is accomplished through the assignment of different staff if possible, and with the use of separate physical and logical access controls.

There are a number of trusted roles assigned to different personnel involved in the operation of RVLCA operations. These roles have been defined and assigned by senior management and are periodically reviewed as part of the Information Security Management System operated by RVLCA. These reviews seek to reassign roles if necessary following staff changes or following company reorganization, to ensure no

potential security risks exists as a consequence of multiple roles held by individuals, and to ensure that no conflicts of interest exist where staffs are assignedmultiple roles.

The trusted roles defined for RVLCA personnel, and the policies employed in assigning staff members to these roles are designed to guarantee best practice is maintained in relation to information security, while at the same time providing flexibility required by the business in maximizing employee productivity.

5.2.1. Trusted Roles

RVLCA has designated several trusted roles for Certificate Authority operations.

A trusted role is one whose incumbent performs functions that can introduce security problems if not carried out properly, whether accidentally or maliciously. The people selected to fill these rolesmust be extraordinarily responsible or the integrity of the CA is weakened. The functionsperformed in these roles form the basis of trust for all uses of the CA. Two approaches are taken to increase the likelihood that these roles can be successfully carried out. The first ensures that the person filling the role is trustworthy and properly trained. The second distributes the functionsamong more than one person, so that any malicious activity would require collusion.

The requirements of this policy are drawn in terms of five roles listed below:

1. **CA Administrator** – authorized to design, operate, and maintain the PKI systems supporting the execution of PKI business and ensuring efficient and effective PKI operation.

2. **RA Administrator** – authorized to design, implement, operate, and maintain the customer & certificate lifecycle processes.

3. **IT Security Manager** – authorized to design, implement, operate and maintain a secure PKI operation ensuring customer trust.

4. **Database Administrator** – authorized to design, operate and maintain the database systemssupporting the execution of PKI business and ensuring efficient and effective PKI operation.

5. **Programmer** – authorized to design, develop / acquire, implement, operate and maintain the business applications, databases and reporting systems ensuring efficient and effective PKI business.

5.2.2. Number of Persons Required for Task

RVLCA maintains a policy and rigorous control procedures to ensure segregation of duties based on job responsibilities. The most sensitive tasks, such as access to and management of CA cryptographic hardware (HSM or Hardware Security Module) and associated key material requiremultiple trusted persons.

These internal control procedures are designed to ensure that at a minimum, two trusted personnel are required to have either physical or logical access to the device. Access to CA HSM is strictly enforced by multiple trusted persons throughout its lifecycle, from incoming receipt and inspection to final logical and/or physical destruction. Once a module is activated with operationalkeys, further access controls are invoked to maintain split control over both physical and logical access to the device. Persons with physical access

to modules do not hold “Shares” and vice-versa. Requirements for CA private key activation data and Shares are specified in policy documents.

5.2.3. Identification and Authentication for Each Role

All personnel seeking to become trusted persons are required to be in the payroll of CA. Thoroughbackground checks are carried out prior to engaging such personnel for CA Operations. The Certifying Authority follow the procedures approved by management for the background check and there are documented for audit purpose.

CA ensures that personnel have achieved trusted status and approval has been given before such personnel are:

1. Issued access devices and granted access to the required facilities
2. Issued electronic credentials to access and perform specific functions on CA’s IT systems.

5.2.4. Roles Requiring Separation of Duties

The RVLCA operations will be carried out by the individuals under the roles of CA Administrator, RA Administrator, System Administrator and Helpdesk. Separate individuals will be identified forthese roles to prevent same individual performing multiple duties under different roles.

5.3. Personnel Controls

RVLCA employees who possess expert knowledge will operate all services, experience, and qualifications necessary to perform allocated duties. In accordance with the requirements for specific duties, employees undergo a post security clearance prior to being granted permissionto partake in the service and or related operations.

5.3.1. Qualifications, Experience, and Clearance Requirements

RVLCA verifies qualifications, experience, and clearance as per recruitment procedure of RVL. RVL has a dedicated HR function that formulates & executes these types of activities. The RVLCA will grant the trusted status to the person after he/she has acquired the required skills and qualification to perform the trusted role. Personnel will be appointed to trusted roles (CA trusted roles) based on:

a) Having successfully completed an appropriate training program.
b) Having demonstrated the ability to perform their duties.
c) Being trustworthy.
d) Having no other duties that would interfere or conflict with their duties for thetrusted role.
e) Having not been previously relieved of duties for reasons of negligence or non-performance of duties.
f) Having not been denied a security clearance or had a security clearance revoked for cause.
g) Having not been convicted of an offense; and
h) Being appointed in writing by an appointing authority.

5.3.2. Background Check Procedures

RVLCA conducts background checking as per recruitment procedure of RVLCA. RVLCA has a dedicated HR function that formulates & executes these types of activities. Prior to

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

a) Confirmation of previous employment.
b) Check of professional reference.
c) Confirmation of the highest or most relevant educational degree obtained.
d) Search of criminal records (state and national).
e) Check of credit/financial/insolvency records.

The personnel shall be rejected for the trusted role if any of the above checks reveals misrepresentation or indicates that the concerned individual is not suitable for the correspondingtrusted role. The background will be rechecked every three years.

5.3.3. Training Requirements

RVLCA provides its personnel with training upon hire as well as the requisite on-the-job training needed for them to perform their job responsibilities competently and satisfactorily. RVLCA maintains records of such training. RVLCA periodically reviews and enhances its training programs as necessary. RVLCA training programs are tailored to the individual's responsibilitiesand include the following as relevant:

a) CA security principles and mechanisms.
b) All PKI software versions in use on the CA system.
c) All PKI duties they are expected to perform.
d) Subscriber verification requirements.
e) Incident and Compromise reporting and handling.
f) Disaster recovery and business continuity procedures.

5.3.4. Retraining Frequency and Requirements

Training (awareness) is conducted to make the trusted personnel aware of any significant changeto the operations, and the executions of such plans are documented. Such changes are CA software or hardware upgrade, changes in automated security systems, and relocation ofequipment.

RVLCA will review the training plans for the personnel in all the trusted roles on a yearly basis. Periodic security awareness and any new technological changes training is provided on an ongoingbasis, based on the newer versions or releases of the products.

5.3.5. Job Rotation Frequency and Sequence

RVLCA personnel will undergo job rotation practices as per the Human Resources Policy of RVL.

5.3.6. Sanctions for Unauthorized Actions

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

5.3.7. Independent Contractor Requirements

No independent contractors shall be used to fill any of the trusted positions of RFLCA, however solutions or hardware vendors (herein after Independent Contractors and Consultants) may be used time to time for only maintenance purpose and their background and authenticity shall be checked by RVLCA approved procedures. After passing the background check independent contractors and consultants are permitted to access RVLCA secure facilities only to the extentthey are escorted and directly always supervised by Trusted Persons.

5.3.8. Documentation Supplied to Personnel

All the relevant documents relating to CA operation required for trusted personnel to perform theirduties such as Certificate Policy, the applicable CPS, Verification Guidelines, User Manuals, Administrator Manual, Policies or Contracts etc. are made available to CA personnel. CAmaintains the documents identifying all personnel who received training and the level of training completed.

5.4. Audit Logging Procedures

Audit log files are generated for all events relating to the security of the CAs. The security audit logs are automatically collected or if not possible, a logbook, paper form, or other physical mechanism are used. All security audits logs, both electronic and non-electronic, are retained andmade available during compliance audits. The security audit logs for each auditable event defined in this section shall be maintained in accordance with Section 5.5.2.

5.4.1. Types of Events Recorded

RVLCA logs the following significant events:

a) CA key life cycle management events, including:
   - Key generation, backup, storage, recovery, archival, and destruction.
   - Cryptographic device life cycle management events.

b) CA and Subscriber certificate life cycle management events, including:
   - Certificate applications, renewal, re-key, and revocation.
   - Successful or unsuccessful processing of requests.
   - Generation and issuance of certificates and CRLs.

c) Security-related events including:
   - Successful and unsuccessful PKI system access attempts.
   - PKI and security system actions performed by RVLCA personnel.
   - Security sensitive files or records read, written or deleted.
   - Security profile changes.
   - System crashes, hardware failures and other anomalies.
   - Network device activity.
   - CA facility visitor entry/exit.

Log entries include the following elements:

a) Date and time of the entry.
b) Serial or sequence number of entries, for automatic journal entries.
c) Identity of the entity making the journal entry.
d) Type of entry.

RVLRAs log certificate application information including:

a) Type of identification document(s) presented by the certificate applicant.
b) Record of unique identification data, numbers, or a combination thereof (e.g., certificate applicant's driving license number) of identification documents, if applicable.
c) Storage location of copies of applications and identification documents.
d) Identity of entity accepting the application.
e) Method used to validate identification documents, if any.
f) Name of receiving CA or submitting RA, if applicable.

5.4.2. Frequency of Processing Logs

Audit logs are processed at least once per quarter.

5.4.3. Retention Period for Audit Logs

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

5.4.4. Protection of Audit Logs

Only authorized RVLCA personnel are allowed to view and process audit logs. Unauthorized access to the audit logs is restricted by physical and logical access control systems and such access will be logged.

5.4.5. Audit Log Backup Procedures

Full backups of audit logs will be performed as per the RVLCA Backup Policy.

5.4.6. Audit Collection System (Internal vs. External)

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

5.4.7. Notification to Event-Causing Subject

This CPS imposes no requirement to provide notice (that an event was audited) to the individual,organization, device, or application that caused the event.

5.4.8. Vulnerability Assessments

RVLCA performs vulnerability assessments on annual basis. Such vulnerability assessmentsfocused on internal and external threats that could result in unauthorized access, tampering, modification, alteration, or destruction of the Certificate issuance process.

The Vulnerability Assessments also included application scanning, as well as Penetration Test assessment annually. Any negative results out of such reports are under corrective actions for such negative result to ensure no common security vulnerabilities shall exist on public facing websites, hosted in the network.

The results of such vulnerability assessment tests are used to enhance the security of the environment.

5.5. Records Archival

5.5.1. Types of Records Archived

RVLCA archives:

a) All audit data collected in terms of Section 5.4.
b) Certificate application information.
c) Subscriber identity authentication data as per Section 3.2.3
d) Certificate lifecycle information, e.g., revocation, re-key, and renewal applicationinformation.

5.5.2. Retention Period of Archive

All data and records pertaining to the Subscriber, the various states of the Certificate lifecycle andthe corresponding application form and the supporting Documents are all archived and retained for a period of 7 years.

5.5.3. Protection of Archive

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

5.5.4. Archive Backup Procedures

RVLCA incrementally backs up electronic archives of its issued certificate information daily and performs full backups on a weekly basis.

5.5.5. Requirements for Timestamping of Records

Archived records are time stamped such that order of events can be determined.

Certificates, CRLs, other revocation databases and usage entries contain time and date information provided by System time, which is synchronized with NTP Server as available.

5.5.6. Archive Collection System (Internal vs. External)

The archive collection system is internal to the CA.

5.5.7. Procedures to Obtain and Verify Archived Information

Archived media is verified just after archival operation. Also, archived data are verified for integrityonce a year. Additionally, the archived information may be made available to the CCA upon request.

5.6. Key Changeover

The keys of RVLCA, Partner for whom Sub-CA has been created, RAs and Subscriber will be changed periodically. The key change will be processed as per Section 6.1.1 Key Pair Generation specified in this CPS.

Key changeover for RVLCA/Sub-CA can happen under the following circumstances:

c) When the RVLCA/Sub-CA certificate is due for expiry
d) When the RVLCA/Sub-CA key is compromised
e) When CCA Bangladesh mandates the CA's to procure a new key due to change in CAcertificate profile. This will eventually lead to changes in Sub-CA keys.

The RVLCA will provide reasonable notice to the Subscriber's relying parties of any change to anew key pair used by the RVLCA to sign Digital Certificates under the RVLCA Trust Network. There will be no key change of the Subscriber's Certificate unless there is a compromise.

Digital Certificates will be issued to the Subscribers of RVLCA Trust Network for a specified period. The Subscribers will generate a new private-public key-pair before or after the expirationof the Certificate and submit the public key along with the new application to the corresponding RVL–CA or RA for generating a new Certificate. This process is carried out preferably before theexisting Digital Certificate expires.

The period of maximum validity of the Certificates will be as mentioned below unless otherwise mentioned in this CPS:

a) RVLCA Certifying Authority's keys and associated Certificates – 10 years.
b) The keys of the partner for whom Sub-CA have been created and associate Certificates –5 years not exceeding the expiry period of RVLCA Digital Certificate.
c) Subscriber Digital Certificate key (class 2): 2 years.
d) Subscriber Digital Certificate key (class 3) – 2 years.
e) e-Sign Digital Certificate key – As per CCA Guidelines.

5.7. Compromise and Disaster Recovery

Organizations are regularly faced with events that may disrupt their normal business activities or may lead to loss of information and assets. These events may be the result of natural disasters, accidents, equipment failures, or deliberate actions. This section details the procedures RVLCA employs in the event of a compromise or disaster.

5.7.1. Incident and Compromise Handling Procedures

If RVLCA detects a potential hacking attempt or other form of compromise, it will perform an investigation to determine the nature and the degree of damage. If the CA key is suspected of compromise, the procedures outlined in Section 5.7.3 shall be followed. Otherwise,the scope of potential damage shall be assessed in order to determine if the CA needs to be rebuilt, only some certificates need to be revoked, and/or the CA key needs to be declared compromised.

RVLCA will inform CCA if any of the following cases occur:

a) Suspected or detected compromise of the CA system.
b) Physical or electronic attempts to penetrate the CA system.
c) Denial of service attacks on the CA system; or
d) Any incident preventing CA from issuing a CRL within 24 hours of the time specified in the next update field of its currently valid CRL. RVLCA will make all efforts to restore capabilityto issue CRL as quickly as possible.

5.7.2. Computing Resources, Software, and/or Data are corrupted

RVLCA has a Disaster Recovery center as per the guidelines of IT Act and CCA. The

disaster recovery site will be made operational using the latest available backup data.

If CA equipment is damaged or rendered inoperative, but the signature keys are not destroyed, CA makes all efforts to establish the operation as quickly as possible, giving priority to the abilityto generate CRL or make use of Disaster Recovery facility for CRL generation. Additionally, appropriate investigations will be carried out to identify the root cause for any such event and corrective measures are taken within an agreed upon timeframe.

If both primary and Disaster recovery sites cannot be used to establish revocation capability in areasonable timeframe, the CA may request for revocation of its certificate(s) to CCA.

5.7.3. Entity Private Key Compromise Procedures

If RVLCA signature keys are compromised, lost, or suspected to be compromised, CCA shall benotified at the earliest feasible time so that CCA can revoke the CA certificate. RVLCA will follow the procedures as mentioned below:

a) RVLCA will revoke all Certificates ever issued using those compromised keys, notify all owners of Certificates (by email) of that revocation, and offer to issue the Certificates to the customers with an alternative or new private signing key.
b) A CA key pair shall be generated by RVLCA in accordance with procedures set forth in this applicable CPS.
c) New CA certificates shall be requested in accordance with the initial registration processset forth by Root CA.
d) If the CA can obtain accurate information on the certificates, it has issued and that are still valid (i.e., not expired or revoked), the CA may re-issue those certificates with the not After date in the certificate as in original certificates; and

e) The CA shall also investigate what caused the compromise or loss, and what measuresmust be taken to preclude recurrence.

5.7.4. Business Continuity Capabilities after a Disaster

RVLCA shall implement a disaster recovery site, which is physically separate from the RVLCA principal secure facilities. Development, implementation, and testing a disaster recovery plan to mitigate the effects of any kind of natural or man-made disaster is in progress. This plan shall be regularly tested, verified, and updated to be operational in the event of a disaster.

Detailed disaster recovery plans shall be in place as stipulated by the regulatory authority to address the restoration of information systems services and key business functions. RVLCA's disaster recovery site shall contain the physical security protections and operational controls required by the RVLCA Security and Audit Requirements Guide to provide for a secure and sound backup operational setup.

In the event of a natural or man-made disaster requiring temporary or permanent cessation of operations from the RVLCA primary facility, the RVLCA disaster recovery process shall be initiated by the RVLCA Emergency Response Team.

RVLCA has the capability to restore or recover essential operations within twenty-four (24) hoursfollowing a disaster with, at a minimum, support for the following functions:

a) Certificate issuance,
b) Certificate revocation,

c) Publication of revocation information, and
d) Provision of key recovery information for Enterprise Customers using RVLCA Managed PKI Key Manager.

The RVLCA disaster recovery database shall be synchronized regularly with the production database within the time limits set forth in the RVLCA Security and Audit Requirements Guide. RVLCA disaster recovery equipment shall be protected by physical security protections comparable to the physical security tiers specified in Section 5.1.1.

The RVLCA disaster recovery plan shall be designed to provide full recovery within one week following the disaster occurring at the RVLCA primary site. RVLCA shall test its equipment at its primary site to support CA/RA functions following all but a major disaster that would render the entire facility inoperable. Results of such tests shall be reviewed and kept for audit and planning purposes. Where possible, operations are resumed at the RVLCA primary site as soon as possible following a major disaster.

RVLCA shall maintain redundant hardware and backups of its CA and infrastructure system software at its disaster recovery facility. In addition, CA private keys shall be backed up and maintained for disaster recovery purposes in accordance with Section 6.2.4.

RVLCA maintains offsite backups of important CA information. Such information includes, but is not limited to the certificate application data, audit data (per Section 5.4), and database records for all certificates issued.

5.8. CA, RA and Sub-CA Termination

The RVLCA and the Partner for whom Sub-CA has been created shall reserve the right to terminate its operations at any time with reasonable notice as stated in Section 5.8.1 below to all affected parties. The RVLCA will take the necessary steps to destroy all copies of the private keys and notify the details of such activity to CCA (in case of RVLCA) as specified by Rule 22 (9) of IT(CA) Rules 2010.

RVLCA will reserve the right to terminate the operations of the Sub-CA when it receives a notification for withdrawal of Sub-CA operations or when there is no request for renewal of the Sub-CA agreement. In such a case RVLCA will communicate the decision to terminate Sub-CA services to the Partner for whom Sub-CA has been created via email.

The RVLCA will take necessary steps to destroy the private key and notify the details of such activity to the Partner for whom Sub-CA has been created.

In case of RA termination, the RVLCA takes the responsibility of certificate Revocation, Suspension or Activation requests arising from the Subscribers belonging to that RA, until all the certificates issued under that RA expire. No new Certificate requests or routine re-key requests will be accepted from the terminated RA. All new certificate requests shall be raised under a new RA.

5.8.1. Requirements Prior to Cessation

The following obligations will be followed by RVLCA and the Partner for whom Sub-CA has been created to reduce the impact of termination of service by providing for timely notice, transfer of responsibilities to succeeding entities, maintenance of records, etc. Before ceasing the operations, RVLCA will perform the following operations as specified in IT (CA) Rules 2010 – Rule22:

a) Notify CCA of its intention to cease acting as RVLCA. Such notice shall be made at leastninety (90) days before ceasing to act as RVLCA or ninety days before the date of expiryof license.

b) Advertise sixty days before the expiry of license or ceasing to act as Certifying Authority,as the case may be by publishing notice of the intention in such daily newspaper or electronic media and website and in such manner as the Controller may determine.

c) Notify its intention to cease acting as a Certifying Authority to the subscribers and Cross Certifying Authority of each unrevoked or unexpired Digital Certificate issued by it;provided that the notice shall be given 60 (sixty) days before ceasing to act as a CertifyingAuthority or 60(sixty) days before the date of expiry of Digital Certificate, as the case maybe the notice shall be sent to the Controller, affected subscribers and Cross Certifying Authorities by electronically signed e-mail and registered post.

d) After the date of expiry as mentioned in the license, the Certifying Authority shall destroy the certificate signing private key and inform the date and time of destruction of the privatekey to the Controller.

e) Revoke all Certificates that remain unrevoked or unexpired at the end of the sixty (60) daynotice period, whether the Subscribers have requested revocation. This is to enable

the Subscribers to find alternate means of certification and thereby prevent unduedisruption to their business.

f) Give notice of the revocation to each affected Subscriber.

g) Make a reasonable effort to ensure that discontinuing its certification services will cause minimal disruption to its Subscribers and to persons duly needing to verify Digital Signatures by reference to the public keys contained in outstanding Certificates.

h) Make reasonable arrangements for preserving the records for 10 years.

Before ceasing the operations, the Partner for whom Sub-CA has been created:

a) Notifies RVLCA of its intention to cease acting as a Partner for whom Sub-CA has been created. Such notice will be made at least ninety (90) days before ceasing to act as the Partner for whom Sub-CA has been created or ninety days before the date of expiry of license. RVLCA may require additional statements to verify compliance with this provision.

b) Provides a sixty (60) day notice to the Subscriber of each unrevoked or unexpired Certificate of its intention to cease acting as the Partner for whom Sub-CA has been created.

c) Initiates revocation of all Certificates through its RA that remain unrevoked or unexpired at the end of the sixty (60) day notice period, whether the Subscribers have requested revocation. This is to enable the Subscribers to find alternate means of certification and thereby prevent undue disruption to their business.

d) Give notice of the revocation to each affected Subscriber.

e) Make a reasonable effort to ensure that discontinuing its certification services will cause minimal disruption to its Subscribers and to persons duly needing to verify Digital Signatures by reference to the public keys contained in outstanding Certificates.

f) Make reasonable arrangements for preserving the records for 10 years.

6. Technical Security Controls

The RVLCA private keys are protected within a hardware security module ("HSM"). The use of a HSM, with FIPS-140 level 3 capabilities ensures that RVLCA are adhering to the highest industrystandard regarding the generation and protection of the Operational CAs' private keys. Access to the modules within the RVLCA environment including the Operational CAs' private keys are restricted using token/smartcards and associated pass phrases. These smartcards and pass phrases are allocated among the multiple members of the RVLCA management team. Such allocation ensures that no one member of the team holds total control over any component of thesystem.

6.1. Key Pair Generation and Installation

6.1.1. Key Pair Generation

The private-public key pairs of RVLCA and the Partner for whom Sub-CA has been created will be generated by RVLCA confidentially using the standards specified in the Bangladesh Information and Communication Technology Act 2006 (Amended in 2013), IT (CA) Rules 2010 and Interoperability Guidelines published by CCA. RA's key pair generation follows the same process as key generation for subscribers under Class 3 certificates. The key generation will be conducted in a secure and trustworthy environment. The Certificate and key generation shall be documented and witnessed for authentication purpose. The size of the Key pair for RA will be the same as that of the subscriber.

Subscribers will be required to generate private/public key pairs generated on a secure medium.The key pair size will be as prescribed in the Interoperability Guidelines published by CCA.

The RVLCA and the Partner for whom Sub-CA has been created will generate encryption private-public RSA key pairs for Subscribers. The key size of the encryption certificate of the subscriber will be equivalent to the Subscriber's Signing Certificate as per the Interoperability Guidelines published by CCA.

6.1.2. Private Key Delivery to Subscriber

For e-sign certificates, the key pair will be generated at e-Sign system and stored in HSM in encrypted form in accordance with the e-Sign Guideline for certifying authorities (CA's) 2020 & Digital certificate interoperability guideline v 1.7. Therefore, physical, or online delivery of private key by RVLCA is not applicable here.

6.1.3. Public Key Delivery to Certificate Issuer

RVLCA operate as an e-Sign service provider. For e-Sign certificates where certificates along with public key is delivered to e-Sign system, RVLCA will keep subscriber's public key and will publish in its website.

6.1.4. CA Public Key Delivery to Relying Parties

The Digital Certificate of the RVLCA or the Partner for whom Sub-CA has been created will be published in the RVLCA repository. The relying parties can connect to the RVLCA repository andfetch the Digital Certificate of RVLCA or the Partner for whom Sub-CA has been created.

6.1.5. Key Sizes

As per CCA Interoperability Guidelines, key size will be 2048 bits RSA or higher.

6.1.6. Public Key Parameters Generation and Quality Checking

RSA keys shall be generated in accordance with FIPS 140-2 Level 3.

Key parameters generation: Whichever entity is generating the key pair i.e., CA or subscriber, its application will generate the parameters used to create public keys.

Key parameters quality checking: The application software used by subscriber should check the quality of parameter in the case of key pair generation.

6.1.7. Key Usage Purposes (as per X.509 V3 Key Usage Field)

Key Usage purposes will be set based on RFC 5280 and the CCA Digital Certificate Interoperability Guidelines. The use of a specific key is constrained by the key usage extension in the X.509 certificate. All certificates shall include a critical key usage extension.

In particular:

a) Certificates used for authentication set the digitalSignature bit
b) Certificates used for key encryption set the keyEncipherment bit
c) Certificates used for data encryption set the dataEncipherment bit
d) Certificates used for digital signatures set the digitalSignature, nonRepudiation bit
e) CA certificates set cRLSign and keyCertSign bits
f) Certificates used for key agreement set the keyAgreement bit.

6.2. Private Key Protection and Cryptographic Module Engineering Controls

RVLCA has implemented a combination of physical, logical, and procedural controls to ensure the security of CA private keys. Subscribers are required to take necessary precautions to preventthe loss, disclosure, modification, or unauthorized use of private keys.

6.2.1. Cryptographic Module Standards and Controls

For CA key pair generation and CA private key storage, RVLCA uses hardware cryptographic modules that are certified at or meet the requirements of FIPS 140-2 Level 3.

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

RVLCA has implemented technical and procedural mechanisms that require the participation of multiple trusted individuals to perform sensitive CA cryptographic operations. RVLCA uses “Secret Sharing” to split the activation data needed to make use of a CA private key into separate parts called “Secret Shares” which are held by trained and trusted individuals called “Shareholders.” A threshold number of Secret Shares (m) out of the total number of Secret Sharescreated and distributed for a particular hardware cryptographic module (n) is required to activatea CA private key stored on the module.

The threshold number of shares needed to sign a CA certificate is 2 (two). It should be noted that the number of shares distributed for disaster recovery tokens may be less than the number distributed for operational tokens, while the threshold number of required shares remains the same. Secret Shares are protected in accordance with this CPS.

6.2.3. Private Key Escrow

The CA private keys are not escrowed.

6.2.4. Private Key Backup

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

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

RVLCA does not store copies of RA private keys. For the backup of end-user Subscriber privatekeys, see Section 6.2.3 and Section 4.12.

6.2.5. Private Key Archival

RVLCA does not archive subscriber private key.

6.2.6. Private Key Transfer into or from a Cryptographic Module

RVLCA generates CA key pairs on the hardware cryptographic modules in which the keys will beused. In addition, RVLCA makes copies of such CA key pairs for routine recovery and disaster recovery purposes. Where the CA key pairs are backed up to another hardware cryptographic module, they are transported between modules in encrypted form. Importing and exporting process of the private key requires at least two persons with Trusted Role.

6.2.7. Private Key Storage on Cryptographic Module

CA stores Private Keys in hardware cryptographic module and keys are not accessible without authentication mechanism that follows FIPS 140-2 level 3 rating of the cryptographicmodule.

6.2.8. Method of Activating Private Key

RVLCA's private key is activated by the main stakeholders and authorized personnel, as definedin clause 6.2.2, supplying their activation data. The user must be authenticated to the cryptographic module before the activation of any private key(s). Acceptable means of authentication include but are not limited to passphrases, Personal Identification Numbers (PINs)or biometrics.

6.2.9. Method of Deactivating Private Key

Cryptographic module that has been activated is never left unattended or otherwise available to unauthorized access. After use, cryptographic modules are deactivated. RVLCA private keys are deactivated upon removal from the token reader. After deactivation, the use of the cryptographic modules-based CA key pair requires the presence of the trusted roles with the activation data to reactivate said CA key pair.

6.2.10. Method of Destroying Private Key

Private signature keys will be destroyed when they are no longer needed, or when the certificatesto which they correspond expire or are revoked. Destroying private key inside cryptographic modules requires destroying the key(s) inside the HSM using the 'zeroization' function of the cryptographic modules in a manner that any information cannot be used to recover any part of the private key. All the private key back-ups are destroyed in a manner that any information cannotbe used to recover any part of the private key. If the functions of cryptographic modules are not accessible to destroy the key contained inside, then the cryptographic modules will be physically destroyed. The destruction operation is realized in a physically secure environment.

6.2.11. Cryptographic Module Rating

See Section 6.2.1.

6.3. Other Aspects of Key Pair Management

This section considers other areas of key management. Subsections may be applicableto issuing CAs, repositories, subject CAs, RAs, Subscribers, and other participants.

6.3.1. Public Key Archival

Public keys of all issued certificates are archived as a part of certificate archival according to procedures outlined in section 5.5 of this CPS.

6.3.2. Certificate Operational Periods and Key Pair Usage Periods

RVLCA's root certificate has a validity of ten years. For subscribers, the maximum validity period for a certificate is maximum 24 (twenty-four) months. For e-Sign certificates, the validity will be according to CCA e-Sign guidelines.

6.4. Activation Data

6.4.1. Activation Data Generation and Installation

The activation data used to unlock private keys is protected from disclosure by a combination of cryptographic and physical access control mechanisms. Activation data holders are responsible for their accountability and protection. Activation data (Secret Shares) used to protect tokens containing RVLCA private keys is generated in accordance with the requirements of Section 6.2.2.The creation and distribution of Secret Shares is logged.

When they are not used, activation data are always stored in a safe for which access is controlledby holders in limited roles.

6.4.2. Activation Data Protection

Activation data for cryptographic modules shall be secured at the level of the data that the associated cryptographic module is used to protect and shall not be stored with the cryptographicmodule.

Activation data for Private Keys associated with certificates asserting individual identities shall never be shared.

Activation data for Private Keys associated with certificates asserting organizational identities shall be restricted to those in the organization authorized to use the Private Keys.

6.4.3. Other Aspects of Activation Data

CA changes the activation data whenever the HSM is re-keyed or returned from maintenance. Before sending a cryptographic module for maintenance, all sensitive information contained in the cryptographic module is destroyed.

Subscribers are responsible to ensure the protection of their activation data.

6.5. Computer Security Controls

6.5.1. Specific Computer Security Technical Requirements

The following computer security functions are provided by the operating system, or through acombination of operating system, software, and physical safeguards.

a) Require authenticated logins for trusted roles
b) Provide Discretionary Access Control
c) Provide a security audit capability
d) Require a trusted path for identification and authentication
e) Provide domain isolation for process
f) Provide self-protection for the operating system

CA computer systems are configured with minimum required accounts and network services. CAhas implemented a combination of physical and logical security controls to ensure that the CA administration is net carried out with less than two-person control.

6.5.2. Computer Security Rating

No stipulation.

6.6. Life-Cycle Technical Controls

6.6.1. System Development Controls

The system development controls for the CA are as follows:

a) Hardware and software are purchased in such a way so as to reduce the likelihood that any particular component was tampered with.
b) All hardware must be shipped or delivered via controlled methods that provide a continuous chain of accountability, from the purchase location to the operations location.
c) The hardware and software are dedicated to performing the PKI activities. There are no other applications; hardware devices, network connections, or component software installed which are not part of the PKI operation.
d) Proper care is taken to prevent malicious software from being loaded onto the equipment.Only applications required performing the PKI operations is obtained from sources authorized by local policy.
e) CA hardware and software are scanned for malicious code on first use and periodically thereafter.

6.6.2. Security Management Controls

The configuration of the CA system as well as any modification and upgrade are documented and controlled. There is a mechanism for detecting unauthorized modification to the CA software or configuration. A formal configuration management methodology is used for installation and ongoing maintenance of the CA system. The CA software, when first loaded, is verified as beingthat supplied from the vendor, with no modifications, and be the version intended for use.

6.6.3. Life Cycle Security Controls

Capacity demands are monitored, and projections of future capacity requirements made to ensurethat adequate processing power and storage are available.

6.7. Network Security Controls

RVLCA signing server is always disconnected from all non-CA networks. It is internal to the CA's PKI system network. RVLCA employs appropriate security measures to ensure that they are guarded against denial of service and intrusion attacks. Such measures include the use of hardware firewalls, hardware filtering routers, and intrusion detection systems. Unused network ports and services are turned off. Protocols that provide network security attack vector(s) is not permitted through the boundary control devices.

All boundary control devices used to protect the network on which PKI equipment is hosted will deny all but the necessary services to the PKI equipment even if those services are enabled for other devices on the network.

6.8. Time Stamping

System time for RVLCA computers is updated using the Network Time Protocol (NTP) to synchronize system clocks at least once every eight hours (Windows default). The synchronization of NTP is provided from CCA facility.

All components shall regularly synchronize with the time service. Time derived from the

time service shall be used for establishing the time of:

- Initial validity time of a Subscriber's Certificate
- Revocation of a Subscriber's Certificate
- Posting of CRL updates
- OCSP or other CSP responses

Electronic or manual procedures may be used to maintain system time. Clock adjustments are auditable events as listed in Section 5.4.1.

7. Certificate, CRL and OCSP Profiles

7.1. Certificate Profile

CPS defines RVLCA's Certificate Profile. RVLCA certificates conform to the Digital CertificateInteroperability Guidelines published by Office of the CCA, along with:

a) ITU-T Recommendation X.509 Version 3 and
b) RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate RevocationList (CRL) Profile, May 2008.

7.1.1. Version Number

Digital Certificate X.509 v3 and CRL v2 are supported.

7.1.2. Certificate Extensions

X509v3 Certificate extensions are supported. Interoperability guideline from CCA will supersedein this case.

7.1.3. Algorithm Object Identifiers

SHA256 with RSA Encryption.

7.1.4. Name Forms

Name fields and extensions shall be consistent with section 3.1

7.1.5. Name Constraints

Anonymous and pseudo names are not supported.

7.1.6. Certificate Policy Object Identifier

Where the Certificate Policies extension is used, Certificates contain the object identifier for theCertificate Policy corresponding to the appropriate Class of Certificate as set forth in this CPS.

7.1.7. Usage of Policy Constraints Extension

Not Applicable.

7.1.8. Policy Qualifiers Syntax and Semantics

RVLCA populates X.509 Version 3 Certificates with a policy qualifier within the Certificate Policiesextension. Generally, such Certificates contain a CPS pointer qualifier that points to the applicable Relying Party Agreement or the RVLCA CPS. In addition, some Certificates contain a User NoticeQualifier that points to the applicable Relying Party Agreement.

7.1.9. Processing Semantics for the Critical Certificate Policies Extension

Not Applicable.

7.2. CRL Profiles

RVLCA issues CRLs as per directions from Digital Certificate Interoperability Guideline publishedby Office of the CCA that conform to RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, May 2008.

7.2.1. Version Number(s)

The version number of certificate revocation list in accordance with the RFC5280 will be specified the value of version to be 2.

7.2.2. CRL and CRL Entry Extensions

The RVLCA supports and uses the following CRL and CRL entry extensions:

- CRL Number: monotonically increasing sequence number for each CRL issued by the CA;
- X509v3 CRL Reason Code: non-critical extension, carrying the revocation reason codeas specified in RFC3647.

7.3. OCSP Profiles

The Online Certificate Status Protocol [OCSP] is the way for subscribers to obtain information about the revocation status of a RVLCA issued Certificates. CCA uses OCSP to provideinformation about all its Certificates. The OCSP responses MUST conform to RFC6960.

7.3.1. Version Number(s)

RVLCA issue Version 1 OCSP responses.

7.3.2. Fields in OCSP Responses

Fields in The OCSP requests and responses shall be compliant with the requirements of RFC.

7.3.3. OCSP Extensions

No Stipulation.

8. Compliance Audit and Other Assessments

An annual External Audit for Certification Authorities examination is performed as per the IT (CA)Rules 2010 by empaneled auditor under CCA for RVLCA data center operations and key management operations supporting RVLCA Managed PKI services. In addition to external audits,RVLCA shall perform internal audit twice in a year and submit audit reports to Office of the CCA to comply with the IT (CA) Rules 2010.

In addition to compliance audits, the RVLCA shall be entitled to perform other reviews and investigations to ensure the trustworthiness of the RVLCA Managed PKI, which include, but are not limited to:

a) RVLCA shall be entitled, within its sole and exclusive discretion, to perform at any time an"Exigent Audit/Investigation" in the event RVLCA has reason to believe that the audited entity has failed to meet RVLCA Managed PKI Standards, has experienced an incident orcompromise, or has acted or failed to act, such that the audited entity's failure, the incident or compromise, or the act or failure to act poses an actual or potential threat to the securityor integrity of the RVLCAPKI.

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

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

8.1. Frequency or Circumstances of Assessment

External assessments required to be conducted in accordance with this CPS shall be performed on an annual basis and internal assessments shall be performed twice in a year.

8.2. Identity/Qualifications of Assessor

The annual audit will be performed by the empaneled external auditor, who is recognized by the Controller of Certifying Authorities. RVLCA top management will decide the composition of the internal audit team when an audit for RVLCA becomes due.

8.3. Assessor's Relationship to Assessed Entity

The external auditing firm involved in the preparing the audit reports will be independent of the party being audited and will not be a software or hardware vendor which is or has been providing services or supplying equipment to the party being audited. The auditing firm and the party beingaudited will not have any current or planned financial, legal or other relationship, other than that of an auditor and the audited party. The office of CCA determines whether an auditor meets this requirement.

8.4. Topics Covered by Assessment

The scope of RVLCA's annual Audit for compliance with the Bangladesh Information and Communication Technology Act 2006, IT (CA) Rules 2010 and CCA Audit Guidelines includes CA environmental controls, key management operations and Infrastructure/Administrative CA controls, certificate life cycle management and CA business practices disclosure.

8.5. Actions Taken as a Result of Deficiency

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

8.6. Communication of Results

On completion of audit by an empaneled auditor, Auditor submit an Audit Report, including identification of corrective measures taken or being taken by CA, to the office of CCA and a copy to CA. The report identifies the version of the CPS used for the assessment.

9. Other Business and Legal Matters

9.1. Fees

9.1.1. Certificate Issuance or Renewal Fees

RVLCA has established a structure for fees/charges it wishes to propose against certificate issuance and renewal. The fee structure is available in RVLCA site (https://www.reliefvalidation.com.bd). This fee structure is established as per guideline from the office of the CCA.

9.1.2. Certificate Access Fees

RVLCA is not charging any fees to relying parties or other public for accessing the certificate information from the repository. The certificate search facility is provided free of cost at its website (https://www.reliefvalidation.com.bd).

9.1.3. Revocation or Status Information Access Fees

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

9.1.4. Fees for Other Services

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

9.1.5. Refund Policy

All payments made by the customer are non-refundable, except as explicitly outlined in the "Terms of Purchase" agreement or mutually agreed upon by both parties.

9.2. Financial Responsibility

The RVLCA does not make any representation and does not give any warranties on the financial transactions, which the subscribers and the relying parties undergo using the Digital Certificate obtained from the RVLCA. The subscribers and the relying parties shall be responsible for any loss, damages or any consequences due to such transactions.

RVLCA is not the agent, fiduciary or other representative of any subscriber and/or certificate holder and must not be represented by the subscriber and/or certificate holder to be so.Subscribers and/or certificate holders have no authority to bind RVLCA by contract or otherwise,to any obligation.

9.2.1. Insurance Coverage

No Insurance coverage is accepted by RVLCA.

9.2.2. Other Assets

RVLCA shall also maintain reasonable and sufficient financial resources to maintain operations, fulfill duties, and address commercially reasonable liability obligations to PKI Participants described in Section 1.3 of this CPS.

9.2.3. Insurance or Warranty Coverage for End Entities

RVLCA does not offer protection to end entities that extends beyond the protections provided in this CPS. Subscribers should refer to the Subscriber Agreement that they have with RVLCA located at https://www.reliefvalidation.com.bd/docs/RVL_PKI_agreement.pdf. Relying Parties should refer to the Relying Party Agreement located at https://www.reliefvalidation.com.bd/docs/RVL_CA_Relying_Party_Agreement.pdf

9.3. Confidentiality of Business Information

9.3.1. Scope of Confidential Information

RVLCA keeps the following types of information confidential and maintains reasonable controlsto prevent the exposure of such records to non-trusted personnel.

a) CA application records, whether approved or disapproved,
b) Certificate Application records,
c) Private keys held by enterprise Customers using RVLCA Managed PKI Key

Manager andinformation needed to recover such Private Keys,
d) Transactional records (both full records and the audit trail of transactions),
e) Audit trail records created or retained by RVLCA or a Customer,
f) Audit reports created by RVL or a Customer (to the extent such reports are maintained),or their respective auditors (whether internal or public),
g) Contingency planning and disaster recovery plans
h) Security measures controlling the operations of RVLCA hardware and software and theadministration of Certificate services and designated enrolment services, and
i) Any other information classified as Confidential as per the information classificationguideline of RVLCA.

9.3.2. Information Not Within the Scope of Confidential Information

Notwithstanding Section 9.3.1, Confidential Information does not include information which:
a) was already lawfully disclosed by RVLCA prior to RVLCA being required to treat theinformation as confidential.
b) is lawfully received from a third party who is not bound by a duty of confidentiality.
c) has become public knowledge, other than through a breach of an obligation of confidence under this CPS.
d) was independently developed or released by RVLCA without reference to Confidential Information.
e) is information that the RVLCA Managed PKI Participant provides for inclusion within a Certificate.
f) is information indicating that a Certificate has been Revoked or Suspended, though notincluding the reason behind this Certificate Status; or
g) includes any information relating to the RVLCA Managed PKI Participant's use of theRepository.

9.3.3. Responsibility to Protect Confidential Information

RVLCA observes applicable rules on the protection of personal data deemed by law or the RVLCA privacy policy (see Section 9.4 of this CPS) to be confidential.

9.4. Privacy of Personal Information

9.4.1. Privacy Plan

RVLCA has implemented a privacy policy, which complies with this CPS. The RVLCA privacy policy is published at https://reliefvalidation.com.bd/docs/privacy_policy.pdf.

9.4.2. Information Treated as Private

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

9.4.3. Information Not Treated as Private

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

9.4.4. Responsibility to Protect Private Information

RVLCA acknowledges its responsibilities to protect privacy of customer information by co-

signingagreement with customer during handing over certificate. RVLCA describes all its measures it establishes to protect any kind of unlawful use of customer information and to prevent them fromleaking out to third parties.

9.4.5. Notice and Consent to Use Private Information

Subscriber Agreement is signed between RVLCA and Subscriber which contains a clause to protect each other's confidential/personal information from leaking out to any third party and anyuse of it will require consent from the other party. For e-Sign certificates, the submission of e-Sign request to e-Sign system will be deemed as such agreement.

9.4.6. Disclosure Pursuant to Judicial or Administrative Process

While it is the responsibility of RVLCA to protect private and confidential information of its Subscribers, it is compelled to, in reasonable situation to release information of a Subscriber to comply with the law of land.

9.4.7. Other Information Disclosure Circumstances

All other information disclosure circumstance shall be governed by the requirements of laws of Bangladesh concerning the protection of personal data.

9.5. Intellectual Property Rights

All Intellectual Property Rights in the RVLCA Service and any associated documentation (including all functional and performance specifications (the "Specifications")) shall vest in Relief Validation Limited and/or its licensors. For the purposes of this document, "Intellectual Property Rights" shall mean all patents, copyrights (including copyright in computer software), design rights, trademarks, trade names, service marks, know-how, trade secrets and technical data, together with all goodwill attaching or relating thereto and all other industrial or intellectual property rights of whatever nature arising anywhere in the world, (and whether any such rights are registered or unregistered, including any application for registration in respect of any such rights).

The subscriber and each relying party shall ensure that in using the RVLCA Services it will do nothing illegal or infringe upon any third-party rights and in particular will ensure that any material that it supplies or transmits is not illegal, libelous, and does not infringe upon any Intellectual Property Right of RVLCA or any third party.

The subscriber and relying parties are given a non-exclusive, non-transferable, royalty free, limited license to use the Intellectual Property Rights in the RVLCA Service only to the extent andsolely for the purpose of availing of the RVLCA Service. The granting of this limited license is conditional on the subscriber's and relying parties' agreement to and compliance with all of the terms and conditions of RVLCA CPS.

Nothing in this document shall be taken or inferred as any endorsement by RVLCA of the subscriber, its business, goods, or services.

9.6. Representations and Warranties

9.6.1. CA Representations and Warranties

RVLCA makes to all Subscribers and relying parties' certain representations regarding

its public service, as described below. RVLCA reserves its right to modify such representations as it sees fit or required by law.

Except as expressly stated in this CPS or in a separate agreement with Subscriber, to the extentspecified in the relevant sections of the CPS, RVLCA represents, in all material aspects, to:

a) Comply with this CPS and its internal or published policies and procedures

b) Comply with applicable laws and regulations.
c) Provide infrastructure and certification services, including but not limited to the establishment and operation of the RVLCA Repository and web site for the operation of PKI services.
d) Provide trust mechanisms, including a key generation mechanism, key protection, and secret sharing procedures regarding its own infrastructure.
e) Provide prompt notice in case of compromise of its Private Key(s).
f) Provide and validate application procedures for the various types of Certificates that it maymake publicly available.
g) Issue digital Certificates in accordance with this CPS and fulfill its obligations presentedherein.
h) Upon receipt of a request from an RA operating within the RVLCA network; act promptlyto issue a RVLCA Certificate in accordance with this CPS.
i) Upon receipt of a request for revocation from an RA operating within the RVLCA network; act promptly to revoke a RVLCA Certificate in accordance with this RVLCA CPS.
j) Publish accepted Certificates in accordance with this CPS.
k) Provide support to Subscribers and relying parties as described in this CPS.
l) Revoke Certificates according to this CPS.
m) Provide for the expiration and renewal of Certificates according to this CPS.
n) Make available a copy of this CPS and applicable policies to requesting parties.

As the RVLCA network may include RAs that operate under RVLCA practices and procedures RVLCA warrants the integrity of any Certificate issued under its own root within the limits of the RVLCA insurance policy and in accordance with this CPS.

The Subscriber also acknowledges that RVLCA has no further obligations under this CPS.

9.6.2. RA Representations and Warranties

A RVLCA RA operates under the policies and practices detailed in this CPS and also the associated Web Host Reseller agreement and EPKI Manager Account agreement. The RA is bound under contract to:

a) Receive applications for RVLCA Certificates in accordance with this CPS.
b) Perform all verification actions prescribed by the RVLCA validation procedures and thisCPS.
c) Receive, verify, and relay to RVLCA all requests for revocation of a RVLCA Certificate in accordance with the RVLCA revocation procedures and the CPS.
d) Act according to relevant laws and regulations.

9.6.3. Subscriber Representations and Warranties

Subscribers represent and warrant that when submitting to RVLCA and using a domain and distinguished name (and all other Certificate application information) they do not interfere with orinfringe any rights of any third parties in any jurisdiction with respect to their trademarks, service marks, trade names, company names, or any other intellectual property right, and that

they are not seeking to use the domain and distinguished names for any unlawful purpose, including, without limitation, tortious interference with contract or prospective business advantage, unfair competition, injuring the reputation of another, and confusing or misleading a person, whether natural or incorporated.

Upon accepting a Certificate, the Subscriber represents to RVLCA and to relying parties that at the time of acceptance and until further notice:

a) Digital signatures created using the Private Key corresponding to the Public Key included in the Certificate is the digital signature of the Subscriber and the Certificate has been accepted and is properly operational at the time the digital signature is created.
b) No unauthorized person has ever had access to the Subscriber's Private Key.
c) All representations made by the Subscriber to RVLCA regarding the information contained in the Certificate are accurate and true.
d) All information contained in the Certificate is accurate and true to the best of the Subscriber's knowledge or to the extent that the Subscriber had notice of such informationwhilst the Subscriber shall act promptly to notify RVLCA of any material inaccuracies in such information.
e) The Certificate is used exclusively for authorized and legal purposes, consistent with thisCPS.
f) It will use a RVLCA Certificate only in conjunction with the entity named in the organizationfield of a digital Certificate (if applicable).
g) The Subscriber retains control of his/her Private Key, uses a trustworthy system, and takesreasonable precautions to prevent its loss, disclosure, modification, or unauthorized use.
h) The Subscriber is an end-user Subscriber and not a CA and will not use the Private Key corresponding to any Public Key listed in the Certificate for purposes of signing any Certificate (or any other format of certified Public Key) or CRL, as a CA or otherwise, unless expressly agreed in writing between Subscriber and RVLCA.
i) The Subscriber agrees with the terms and conditions of this CPS and other agreements and policy statements of RVLCA.
j) The Subscriber abides by the laws applicable in his/her country or territory including those related to intellectual property protection, viruses, accessing computer systems etc.
k) The Subscriber complies with all export laws and regulations for dual usage goods as maybe applicable.

In all cases and for all types of RVLCA Certificates the Subscriber has a continuous obligation to monitor the accuracy of the submitted information and notify RVLCA of any such changes.

9.6.4. Relying Party Representations and Warranties

A party relying on a RVLCA Certificate accepts that to reasonably rely on a RVLCA Certificate they must:

a) Minimize the risk of relying on a digital signature created by an invalid, revoked, expired or rejected Certificate; the Relying Party must have reasonably made the effort to acquire sufficient knowledge on using digital Certificates and PKI.
b) Study the limitations to the usage of digital Certificates and be aware through the Relying Party agreement the maximum value of the transactions that can be made using a RVLCAdigital Certificate.
c) Read and agree with the terms of the RVLCA CPS and Relying Party agreement.

d) Verify a RVLCA Certificate by referring to the relevant CRL and the CRLs of intermediate CA and root CA or by checking the OCSP response using the RVLCA OCSP responder.
e) Trust a RVLCA Certificate only if it is valid and has not been revoked or has expired.
f) Rely on a RVLCA Certificate, only as may be reasonable under the circumstances listed in this section and other relevant sections of this CPS.

9.6.5. Representations and Warranties of Other Participants

No warranty is extended by RVLCA to other parties other than specifically mentioned in this CPS.

9.7. Disclaimer of Warranties

To the extent permitted by applicable law and any other related agreements, RVLCA disclaims all warranties other than any express warranties contained in such agreements or set forth in this CPS.

9.8. Limitations of Liability

RVLCA limit liabilities if RVLCA meet the liability requirements stated in ICT Act 2006 (amended 2013) and IT (CA) Rules 2000 made there under. RVLCA is responsible for verificationof any Subscriber to whom it has issued a certificate and to all relying parties who reasonably relyon such certificate in accordance with this CPS, for damages suffered by such persons that are caused by the failure of the RVLCA to comply with the terms of its CPS or its Subscriber Agreement, and sustained by such persons as a result of the use of or reliance on the certificate.

The verification requirements for certificate issuance by RVLCA are as specified under ICT Act 2006 (amended 2013) and IT (CA) Rules 2000 made there under and reasonable effort by CA. CA cannot guarantee the activities or conduct of the subscribers.

CA shall not be liable for any indirect, exemplary, special, punitive, incidental, and consequentiallosses, damages, claims, liabilities, charges, costs, expenses or injuries (including withoutlimitation loss of use, data, revenue, profits, business and for any claims of Subscribers or Usersor other third parties including Relying parties).

CA shall not be liable for any delay, default, failure, breach of its obligations under the SubscribersAgreement, Relying Party Terms & Conditions and Registration Authority Agreement.

9.9. Indemnities

The RVLCA does not make any representation and does not give any warranties on the financial transactions which the Subscribers and the relying parties perform using the Digital Certificate obtained under the RVLCA Trust Network. The Subscribers and the relying parties shall be responsible for any losses, damages or any consequences due to such transactions.

9.9.1. Indemnification by Subscribers

By accepting a Digital Certificate, the Subscriber agrees to indemnify and hold RVLCA, as well as its agent(s) and contractors harmless from any acts or omissions resulting in liability, any lossor damage, and any suits and expenses of any kind, including reasonable attorneys' fees, that RVLCA, and the above mentioned parties may incur, that are caused by the use or publication ofa Certificate, and that arises from:

a) Any false or misrepresented data supplied by the Subscriber or agent(s).
b) Failure by the Subscriber to disclose a material fact on the Certificate Application, if the misrepresentation or omission was made negligently or with intent to deceive any party.
c) Failure to protect the Subscriber's confidential data including their Private Key, or failure to take reasonable precautions necessary to prevent the compromise, loss, disclosure, modification, or unauthorized use of the Subscriber's confidential data.
d) Breaking any laws applicable in his/her country or territory including those related to intellectual property protection, viruses, accessing computer systems etc.

9.9.2. Indemnification by Relying Parties

To the extent permitted by applicable law, relying party agreement requires, relying parties toindemnify RVLCA for:

a) The relying party's failure to perform the representations and warranties as outlined in thesection 9.6.4 of this CPS.
b) The relying party's reliance on a certificate that is not reasonable under the circumstances,or
c) The relying party's failure to check the status of such certificate to determine if thecertificate is expired or revoked.

9.10. Term and Termination

9.10.1. Term

The term of this CPS, including amendments and addenda, begins upon publication to the Repository and remains in effect until replaced with a new CPS.

9.10.2. Termination

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

9.10.3. Effect of Termination and Survival

Upon termination of this CPS, RVLCA Managed PKI participants are nevertheless bound by its terms for all certificates issued for the remainder of the validity periods of such certificates.

9.11. Individual Notices and Communications with Participants

Unless otherwise specified by agreement between the parties, RVLCA uses commercially reasonable methods to communicate, taking into account the criticality and subject matter of thecommunication.

9.12. Amendments

9.12.1. Procedure for Amendment

Amendments to this CPS shall be made by RVLCA and approved by Controller of Certifying Authorities, Bangladesh. The amendments shall either be in whole CPS document form or an update. Amended versions or updates shall be linked to the RVLCA Repository located at: RVLCAWebsite. Updates always supersede any designated or conflicting provisions of the referenced version of the CPS.

9.12.2. Notification Mechanisms and Period

RVLCA reserves the right to amend the CPS without notification for amendments that are not material, including without limitation corrections of typographical errors, changes to URLs, and changes to contact information. Such amendments will be effective immediately upon publication.

9.12.3. Circumstances under Which OID Must Be Changed

If RVLCA determines that a change is necessary in the object identifier corresponding to Certificate Policy or CPS, the amendment shall contain new object identifiers for the Certificate Policies. Otherwise, amendments shall not require a change in Certificate Policy object identifier.

9.13. Dispute Resolution Procedures

9.13.1. Disputes among RVLCA and Customers

Disputes among RVLCA Managed PKI participants shall be resolved pursuant to provisions in the applicable agreements among the parties. However, if the disputes are not resolved within one hundred twenty (120) days after the initial notice then the matter will be referred to competentcourt of law.

9.13.2. Disputes with End-User Subscribers or Relying Parties

To the extent permitted by applicable law, RVLCA's Subscriber Agreements and Relying Party Agreements contain, and other Subscriber Agreements shall contain, a dispute resolution clause.

9.14. Governing Law

The laws of the Peoples' Republic of Bangladesh shall govern the enforceability, construction, interpretation, and validity of this CPS. This is in accordance with the Information and Communication Technology Act, 2006 (Amended in 2013).

9.15. Compliance with Applicable Law

This CPS is subject to applicable national, state, local and foreign laws, rules, regulations in accordance with the Information and Communication Technology Act, 2006 (Amended in 2013) and IT (CA) Rules 2010.

9.16. Miscellaneous Provisions

9.16.1. Entire Agreement

This CPS Guidelines and all documents referred to herein contain the entire and exclusive agreement and understanding between the parties on the subject matter of the Agreement. This guideline supersedes all prior agreements, arrangements, understandings, communications, representations, and arrangements relating thereto. Except as may be expressly included in this CPS Guidelines, no oral or written representation, agreement, communication, understanding, or promise related to the subject matter is given or implied from anything previously said or written in negotiations between the parties.

9.16.2 Assignment

Parties to this CPS may not assign any of their rights or obligations under this CPS or applicableagreements without the written consent of RVLCA.

9.16.3. Severability

If any term or provision or part of the Subscriber Agreement and/or any document contemplated herein is declared illegal or unenforceable, in whole or part, it will be enforced to the maximum extent permissible, and the remainder of the Subscriber Agreement will remain in full force and effect to the fullest extent permitted by law and the parties hereto agree to replace the illegal or unenforceable provisions with valid provisions which are as close as possible to the Parties' original intentions in their respective meaning, purpose, and commercial effect.

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

RVLCA reserves the right to seek indemnification and attorneys' fees from any party related to that party's conduct described in Section 9.9. Except where an express time frame is set forth in this CPS, no delay or omission by any party to exercise any right, remedy or power it has under this CPS shall impair or be construed as a waiver of such right, remedy or power. A waiver by anyparty of any breach or covenant in this CPS shall not be construed to be a waiver of any other orsucceeding breach or covenant. Bilateral agreements between RVLCA and the parties to this CPS may contain additional provisions governing enforcement.

9.16.5. Force Majeure

RVLCA accepts no liability for any breach of warranty, delay or failure in performance that resultsfrom events beyond its control such as acts of God, acts of war, acts of terrorism, civil unrest, strikes, flood, epidemics, power or telecommunication services failure, fire, and other natural disasters; any provision of any applicable law, regulation or order; civil, government or military authority; the failure of any electrical communication or other system operated by any other partyover which it has no control; or other similar causes beyond its reasonable control and without itsfault or negligence.

9.17. Other Provisions

This CPS shall be binding upon the successors, executors, heirs, representatives, administrators,and assigns, whether express, implied, or apparent, of the parties that this

CPS applies to. The rights and obligations detailed in this CPS are assignable by the parties, by operation of law (including as a result of merger or a transfer of a controlling interest in voting securities) or otherwise, provided such assignment is undertaken consistent with this CPS articles on termination or cessation of operations, and provided that such assignment does not effect a novation of any other debts or obligations the assigning party owes to other parties at the time ofsuch assignment.

Appendix: Definitions and Acronyms

Term	Description
(Certificate)	A person.
Activation Data	Data values, other than keys, that are required to operate cryptographic modules and that need to be protected (e.g., a PIN, a passphrase, or a manually held key share).
Administrator (PKI)	A Trusted Person within the organization of a Processing Centre that performs validation and other CA or RA functions.
Administrator Certificate	A Certificate issued to an Administrator that may only be used to perform CA or RA functions.
Application Software Vendor	A developer of Internet browser software or other software that displays or uses certificates and distributes root certificates, such as KDE, Microsoft Corporation, Mozilla Corporation, Opera Software ASA, and Red Hat, Inc.
Assurance Level	A specified level of assurances as defined within this CPS.
Asymmetric Cryptography	A class of Cryptography in which a Key Pair is used – a Private Key to create signatures and to decrypt messages, and a Public Key to encrypt messages and verify signatures. It has two main advantages: For n users, only n Key Pairs are needed; and Public Keys can be widely distributed with no requirement for confidentiality; but most methods which can achieve good security require significant computing resources. (See Symmetric Cryptography)
Audit	Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures.
Authorization	The granting of rights, including the ability to access specific information or resources.
Authorized Party	(Certificate purpose) An Individual or Device with authority to conduct certain actions or make certain assertions.
Automated Administration	A procedure whereby Certificate Applications are approved automatically if enrolment information matches information contained in a database.
Automated Administration Software Module	Software provided by RVLCA that performs Automated Administration.
Backup	Copy of files and programs made to facilitate recovery if necessary.
Binding	Process of associating two related elements of information.
Business Day	Any day other than a Saturday, Sunday or public holiday (including public service holidays) for the whole of RVLCA.
CA-certificate	A certificate for a CA's public key.
Certificate	See X.509 Certificate.
Certificate Applicant	An individual or organization that requests the issuance of a Certificate by a CA.
Certificate Application	A request from a Certificate Applicant (or authorized agent of the Certificate Applicant) to a CA for the issuance of a Certificate.

Term	Description
Certificate Chain	An ordered list of Certificates containing an end-user Subscriber Certificate and CA certificates, which terminates in a root Certificate.
Certificate Management Control Objectives	Criteria that an entity must meet in order to satisfy compliance audit.
Certificate Profile	The specification of the fields to be included in a Certificate and the contents of each, as set in the relevant Certificate Policy.
Certificate Re-key	Within the RVLCAPKI, Certificate Re-key is defined as the issuance of a new certificate to replace an existing valid certificate, with a new serial number, validity, and public key, but with no other Subscriber information changed.
Certificate Renewal	Within the RVLCAPKI, Certificate Renewal is defined as the issuance of a new certificate to replace an existing valid certificate, with a new serial number and extended validity but with no other Subscriber information changed
Certificate Revocation List (CRL)	A signed, time-stamped list of serial numbers of the Public Key Certificates of Subscribers (other than Certification Authorities) that have been revoked prior to their scheduled Expiry.
Certificate Signing Request (CSR)	A message conveying a request to have a Certificate issued.
Certificate Policy (CP)	A named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements.
Certification Authority Owner (CAO)	The legal entity responsible for the Certification Authority.
Certification Authority (CA)	A Certification Authority (CA) is an entity and/or an automated system, as the case may be, is responsible to issue, manage, revoke, and renew Certificates in the RVLCA PKI.
Certification Authority Manager (CAM)	The CA individual who is responsible for overseeing the management of the CA.
Certification Path	An ordered sequence of certificates that, together with the public key of the initial object in the path, can be processed to obtain that of the final object in the path.
Certification Practice Statement (CPS)	A statement of the practices that a CA employs in issuing, managing, revoking, and renewing or re-keying certificates.
Challenge Phrase	A secret phrase chosen by a Certificate Applicant during enrolment for a Certificate. When issued a Certificate, the Certificate Applicant becomes a Subscriber, and a CA or RA can use the Challenge Phrase to authenticate the Subscriber when the Subscriber seeks to revoke or renew the Subscriber's Certificate.
Compromise	A violation (or suspected violation) of a security policy, in which an unauthorized disclosure of, or loss of control over, sensitive information may have occurred. With respect to private keys, a Compromise is a loss, theft, disclosure, modification, unauthorized use, or other compromise of the security of such private key.
CRL Usage Agreement	An agreement setting forth the terms and conditions under which a CRL or the information in it can be used.
Cross Certification	The process undertaken by Certification Authorities to establish a trust relationship. When two Certification Authorities are cross-certified, they agree to trust and rely upon each other's public key certificates and keys as if they had issued them themselves. The two Certification Authorities exchange cross- certificates, enabling their respective users to interact securely.
Cryptographic Module	The set of hardware, software, firmware, or some combination thereof that implements cryptographic logic or processes, including cryptographic algorithms, and is contained within the cryptographic boundary of the module.
Device (Certificate)	(Certificate purpose) A device, host, service, or process. For example, a network device, firewall, server, personal computer, handheld digital device, Smartphone, access point, website, service, process, socket, interface, or the like.
Digital Signature	A method of using Cryptography to link an exclusive identity to an electronic document or transaction to accomplish what a written signature accomplishes in a paper document. A digital signature also verifies that the contents of themessage

Term	Description
	or document have not been altered.
Distinguished Name (DN)	A unique identifier assigned to each Certificate Applicant, having the structure required by the Certificate Profile.
EncryptionCertificate	A Certificate containing a Public Key that is used to encrypt electronic messages, files, documents, or data transmissions, or to establish or exchange a session key for these same purposes.
End Entity	A Relying Party or a Subscriber.
Hardware Security Module	A hardware device incorporating tamper protection, used to securely generate and store cryptographic keys.
Hashing	The process of subjecting a set of data to a sequence of mathematical operations to compute a numeric value that will later be compared to ensure the original data has not been altered.
Identification	The process of establishing the identity of an entity, by: • Establishing that a given name of an entity corresponds to a real-world identity of an entity, and Establishing that an entity applying for or seeking access under that nameis, in fact, the named entity.
Intellectual Property Rights	Rights under one or more of the following: any copyright, patent, trade secret, trademark, and any other intellectual property rights.
Intermediate Certification Authority (Intermediate CA)	A Certification Authority whose Certificate is located within a Certificate Chain between the Certificate of the root CA and the Certificate of the Certification Authority that issued the end user Subscriber's Certificate.
Issuing Certification Authority (Issuing CA)	In the context of a particular certificate, or when the phrase "the issuing CA" is used, the issuing CA is the CA that issued the certificate. In the context of the RVLCAPKI hierarchy of CAs, or when the phrase "an Issuing CA" is used, an Issuing CA is a CA that issues End-Entity Certificates and does not issue CA-certificates.
Key	A sequence of symbols that controls the operation of a cryptographic transformation.
Key Escrow	The process of entrusting a Private Key to a third party (an Escrow Agent such as an organization or government) and providing another third party with a legal right to obtain the Key from the Escrow Agent in certain circumstances.
Key Exchange	The process of exchanging public keys in order to establish secure communications.
Key Pair	A matching Private Key and Public Key which are mathematically linked such that one will decrypt Cipher text produced with the other. In many cryptosystems, including those used here, the converse is also true, i.e. either key can be used to decrypt Cipher text produced with the other.
Managed PKI	RVLCA fully integrated managed PKI service that allows enterprise Customers of RVLCA and its Partners to distribute certificates to individuals, such as employees, partners, suppliers, and customers, as well as devices, such as servers, routers, and firewalls. RVLCA Managed PKI permits enterprises to secure messaging, intranet, extranet, virtual private network, and ecommerceapplications.
Managed PKI Administrator	An Administrator that performs validation or other RA functions for RVLCA Managed PKI Customer.
Manual Authentication	A procedure whereby Certificate Applications are reviewed and approved manually one-by-one by an Administrator using a web-based interface.
No verified Subscriber Information	Information submitted by a Certificate Applicant to a CA or RA, and included withina Certificate, that has not been confirmed by the CA or RA and for which the applicable CA and RA provide no assurances other than that the information was submitted by the Certificate Applicant.
Non-repudiation	An attribute of a communication that provides protection against a party to a communication falsely denying its origin, denying that it was submitted, or denying its delivery. Denial of origin includes the denial that a communication originated from the same source as a sequence of one or more prior messages, even if the

Term	Description
	identity associated with the sender is unknown. Note: only adjudication by a court, arbitration panel, or other tribunal can ultimately prevent repudiation. For example,a digital signature verified with reference to a RVLCA Managed PKI Certificate may provide proof in support of a determination of non-repudiation by a tribunal, but does not by itself constitute Non-repudiation.
Offline CA	RVLCAs, Root CAs and other designated intermediate CAs that are maintained offline for security reasons in order to protect them from possible attacks by intruders by way of the network. These CAs do not directly sign end user Subscriber Certificates.
Online CA	CAs that sign end user Subscriber Certificates are maintained online so as to provide continuous signing services.
Online Certificate Status Protocol (OCSP)	A protocol for providing Relying Parties with real-time Certificate status information.
Operational Period	The period starting with the date and time a Certificate is issued (or on a later date and time certain if stated in the Certificate) and ending with the date and time on which the Certificate expires or is earlier revoked.
PKCS #10	Public-Key Cryptography Standard #10, developed by RSA Security Inc., which defines a structure for a Certificate Signing Request.
PKCS #12	Public-Key Cryptography Standard #12, developed by RSA Security Inc., which defines a secure means for the transfer of private keys.
Policy Authority (PA)	The entity responsible for the approval of a Certificate Policy and the associated Certification Practice Statement, Subscriber Agreement and Relying Party Agreement.
Private Key	That Key of an entity's Key Pair which should only be used by that entity and should not be disclosed to any other entity.
Private Signing Key	See Private Authentication Key.
Processing Centre	An organization (RVLCA or certain other entities) that creates a secure facility housing, among other things, the cryptographic modules used for the issuance of Certificates.
Public Key	That Key of an entity's Key Pair which can be made public.
Public Key Infrastructure (PKI)	The architecture, organization, techniques, practices, and procedures that collectively support the implementation and operation of a Certificate-based public key cryptographic system.
Public-Key Cryptography Standards (PKCS)	A series of cryptographic standards dealing with public-key issues, published by RSA Laboratories.
Registration Authority (RA)	A Registration Authority (RA) is an entity and/or an automated system, as the case may be, is responsible for identification and authentication of certificate applicants in the RVLCA PKI.
Registration Authority Manager (RAM)	The RA individual who is responsible for overseeing the management of the RA.
Registration Information	Information that an applicant is required to disclose for the purpose of obtaining keys and certificates.
Relying Party	A recipient of a certificate which relies on that certificate for authentication or confidentiality and/or any digital signatures verified using that certificate.
Relying Party Agreement	An agreement used by a CA setting forth the terms and conditions under whichan individual or organization acts as a Relying Party.
Repudiation	The denial or attempted denial of involvement by a party in all or part of an electronic Transaction.
Revoke	The process undertaken by the CA, generally in response to a request by an RA,to invalidate a certificate. A subscriber may request revocation through the RA.
Root Certification Authority (Root CA)	The CA which is the highest trusted element in the PKI.

Term	Description
RVLCA Repository	RVLCA database of Certificates and other relevant RVLCA Managed PKI information accessible online.
RVLCA ManagedPKI Participant	An individual or organization that is one or more of the following within the RVLCA Managed PKI CA hierarchy: RVLCA, a Subscriber, or a Relying Party.
RVLCA ManagedPKI Standards	The business, legal, and technical requirements for issuing, managing, revoking, renewing, and using Certificates within the RVLCAPKI.
Secret Share	A portion of a CA private key or a portion of the activation data needed to operatea CA private key under a Secret Sharing arrangement.
Secret Sharing	The practice of splitting a CA private key or the activation data to operate a CA private key in order to enforce multi-person control over CA private key operations under Section 6.2 of the CP and CPS
Secure Sockets Layer (SSL)	The industry-standard method for protecting Web communications developed by Netscape Communications Corporation. The SSL security protocol provides data encryption, server authentication, message integrity, and optional client authentication for a Transmission Control Protocol/Internet Protocol connection.
Session Key	A Symmetric Cryptography Key generated specifically for use within a single transaction or session.
Subject	The holder of a private key corresponding to a public key. The term “Subject” can, in the case of an organizational Certificate, refer to the equipment or device that holds a private key. A Subject is assigned an unambiguous name, which is bound to the public key contained in the Subject’s Certificate.
Subordinate CA	In a hierarchical PKI, a CA whose certificate signature key is certified by another CA, and whose activities are constrained by that other CA. (see Superior CA)
Subscriber	In the case of an individual Certificate, a person who is the Subject of, and has been issued, a Certificate. In the case of an organizational Certificate, an organization that owns the equipment or device that is the Subject of, and that has been issued, a Certificate. A Subscriber is capable of using, and is authorized to use, the private key that corresponds to the public key listed in the Certificate.
Subscriber Agreement	An agreement used by a CA or RA setting forth the terms and conditions underwhich an individual or organization acts as a Subscriber.
Superior CA	In a hierarchical PKI, a CA who has certified the certificate signature key of another CA, and who constrains the activities of that CA. (see Subordinate CA)
Token	Media capable of storing the Private Key of a Subscriber. Tokens include secure tokens and other devices such as smart cards.
Trusted Person	An employee, contractor, or consultant of an entity within the RVLCA Managed PKI responsible for managing infrastructural trustworthiness of the entity, its products, its services, its facilities, and/or its practices as further defined in CP.
Trusted Position	The positions within a RVLCA Managed PKI entity that must be held by a Trusted Person.
Trustworthy System	Computer hardware, software, and procedures that are reasonably secure from intrusion and misuse; provide a reasonable level of availability, reliability, and correct operation; are reasonably suited to performing their intended functions; and enforce the applicable security policy. A trustworthy system is not necessarilya “trusted system” as recognized in classified government nomenclature.
User	(Certificate purpose)
Valid Certificate	A Certificate issued by a CA and accepted by the Subscriber listed in it that has not been revoked or suspended and remains operational.
X.509	The International Telegraph and Telephone Consultative Committee (CCITT1) recommendation X.509 “Information technology - Open Systems Interconnection - The directory: Authentication framework” was published in 1988 to authenticate access to modify parts of the X.500 directory. The certificates used the X.208 “Abstract Syntax Notation One (ASN.1)” according to a unique subset of the X.209 “Basic Encoding Rules (BER)”, called the “Distinguished Encoding Rules (DER)”.
X.509 Certificate	Binds an entity’s identity, such as a person’s name, an asset number, or a position title, to a cryptographic Public Key. The entity (person, asset or role) is the “subject”

Term	Description
	or “subscriber” of the certificate. The identity (name, number or title) forms the X.500 Distinguished Name (DN) of the certificate. The certificate is evidence that the Certification Authority (CA) has verified that the cryptographic public key in the certificate belongs to the entity identified by the DN of the certificate.

Acronyms and Abbreviations

Acronym	Meaning
CA	Certificate Authority
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSP	Certificate Status Provider
CSR	Certificate Signing Request
DN	Distinguished Name
FIPS	Federal Information Processing Standard
HSM	Hardware Security Module
IETF	The Internet Engineering Task Force
LDAP	Lightweight Directory Access Protocol
OCSP	Online Certificate Status Protocol
PIN	Personal Identification Number
PKCS	Public-Key Cryptography Standard
PKI	Public Key Infrastructure
RA	Registration Authority
RFC	Request for comment
RSA	A public key cryptographic system invented by Rivest, Shamir, and Adelman.
RVL	Relief Validation Limited
SSL	Secure Sockets Layer