Certificate Policy
(Version 1.0.01)

Document Control

Title	Relief Validation Limited Certificate Policy (RVL CP)
Document Type	Public
Version	1.0.01
Approve Date	
Previous Version	1.0.00
Previous Version Revised Date	
Pages	
Status	Final for CCA's Approval

Revision History

Sl.	Version	Section Affected	Modification
01			
02			

Table of Contents

1. Introduction

Relief Validation Limited (hereinafter referred to as the “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, Government of Bangladesh. Below Bangladesh Root CA there are Certifying Authorities (CAs) licensed by CCA to issue Digital Signature Certificates under the provisions of IT Act 2006. These are also called Licensed CAs. RVL CA is a Licensed CA under Bangladesh Root CA.

1.1. Overview

This CP is the foundation for the CPS, which asserts the operational procedures for issuance of certificate(s).

This CP states what assurance can be placed in a certificate issued under this policy. A Certification Practice Statement (CPS) for PKI component(s) states how the PKI component(s) meet the assurance requirements.

Certificates contain one or more registered certificate policy OID, which may be used by a Relying Party to decide whether a certificate is trusted for a particular purpose. The party that registers the OIDs also publishes the CP, for examination by Relying Parties.

1.2. Document Name and Identification

This Certificate Policy is published by the Relief Validation Limited Certifying Authority (hereinafter referred to as the “RVL CA” or “RVL-CA” or “RVLCA”) and is approved by the Office of the Controller of Certifying Authority (CCA) and specifies the baseline set of security controls and practices that RVLCA employ in issuing, revoking or suspending and publishing certificates.

Internet Numbers Assigned Authorities (IANA) has assigned the country OID 2.16.50 to Bangladesh. For identification purpose, this Certificate Policy bears an Object Identifier (OID) “2.16.50.1.12.”

Document Title: Relief Validation Limited Certificate Policy (RVL CP)
Document Version: RVL CP v 1.0.01
Document OID: 2.16.50.1.12
Document Date: 01.01.2024

1.3. PKI Participants

1.3.1. PKI Authorities

1.3.1.1. Controller of Certifying Authorities (CCA)

The CCA is responsible for:

1. Approval of the Relief Validation Limited Certifying Authority CP or RVLCA CP.
2. Commissioning compliance analysis and approval of the RVL CA's CPS.
3. Accepting and processing applications from entities desiring to become Licensed CA; and
4. Ensuring continued conformance of Licensed CAs with this CP by examining compliance and audit results.

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.

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.

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 CAs:
    a. Client Applicant based e-Sign.

1.3.3. Registration Authority (RA)

A Registration Authority (RA) is an entity and/or an automated system, as the case maybe, is responsible for identification and authentication of certificate applicants 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

A Subscriber is the entity whose name appears as the subject in a certificate, who asserts that it uses its key and certificate in accordance with the certificate policy asserted in the certificate, and who does not itself issue certificates. CAs are sometimes technically considered "subscribers" in a PKI. However, the term "Subscriber" as used in this document refers only to those who request certificates for uses other than signing and issuing certificates or certificate status information.

1.3.5. Relying Parties

A Relying Party is the entity that relies on the validity of the binding of the Subscriber's name to a public key. 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, or to identify the creator of a message. 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.

1.4. Certificate Usage

1.4.1. Appropriate Certificate Uses

Certificate usage shall be governed by the ICT Act 2006, IT (CA) Rules 2010 and all relevant Guidelines from CCA that is updated by CCA time to time.

1.4.2. Prohibited Certificate Uses

Certificate usage shall be governed by the ICT Act 2006, IT (CA) Rules 2010 and all relevant Guidelines from CCA that is updated by CCA time to time.

1.5. Policy Administration

1.5.1. Organization administering the document.

The RVLCA is responsible for all aspects of this CP.

1.5.2. Contact Person

Any questions or clarification request regarding this CP can be directed to the concerned official(s) of the RVLCA via established communication channel.

1.5.3. Person Determining CPS Suitability for the Policy

A person duly mandated by the Board of Directors of RVL is responsible for administering and determining CPS suitability for the policy.

1.5.4. CPS Approval Procedures

RVLCA CPS shall be submitted to CCA, Bangladesh for approval before commencing operations under the said CPS. The approved CPS shall be made available in 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

PKI Repository related requirement shall be governed by the ICT Act 2006, IT (CA) Rules 2010 and all relevant Guidelines from CCA that is updated by CCA time to time.

2.2. Publication of Certificate Information

Please refer to Section 2.1.

2.3. Time or Frequency of Publication

Please refer to Section 2.1.

2.4. Access Controls on PKI Repositories

Any PKI Repository information not intended for public dissemination or modification shall be protected.

3. Identification & Authentication

3.1. Naming

3.1.1. Types of Names

RVLCA will generate and sign certificates containing an X.500 Distinguished Name (DN) in the Issuer and in Subject fields; and requirements for name forms are specified in the relevant guideline(s) published by CCA.

3.1.2. Need for Names to be Meaningful

The names contained in a certificate must be in English alphabet with commonly understood semantics permitting the determination of the identity of the individual or organization that is the subject of the certificate.

When DNs are used, it is preferable that the common name represents the subscriber in a way that is readable to humans. For a person or organization, this will typically be a legal name. For equipment, this may be a model name and/or serial number, and/or an application process.

3.1.3. Anonymity or Pseudonymity of Subscribers

Subscriber certificates issued by RVLCA shall not contain anonymous or pseudonymous identities.

3.1.4. Rules for Interpreting Various Name Forms

RVLCA will comply to rules for interpreting distinguished name forms as specified in X.501. Rules for interpreting e-mail addresses will be followed as per the RFC 2822.

3.1.5. Uniqueness of Names

RVLCA will issue certificates under this CP must ensure that the subject name assigned to a subscriber must identify that subscriber uniquely and unambiguously.

3.1.6. Recognition, Authentication & Role of Trademarks

The CA that issues certificates under this CP reserves no liability to any certificate applicant on the usage of Distinguished Names appearing in a certificate. The right to use the name is the responsibility of the applicant and must be in accordance with the relevant laws, regulations, legal obligations, or announcements.

3.2. Initial Identity Validation

3.2.1. Method to Prove Possession of Private Key

In all cases where the party named in a certificate generates its own keys, that party shall be required to prove possession of the private key, which corresponds to the public key in the certificate request. The CA shall state in its CPS the method to prove possession of private key.

3.2.2. Authentication of Organization user Identity

Requests for certificates in the name of an organizational user shall include the Username, Organization Name, Address, and documentation of the existence of the organization. The CA shall verify the information relating to the authenticity of the requesting representative.

3.2.3. Authentication of Individual Identity

Public key certificates bind public keys to identities. However, the entity to be identified depends on the application for which the public keys are used. Identifying different types of entity requires different evidence and procedures. RVLCA that issues certificates under this CP have stated in its CPS the types of entity that the RVLCA will support and details the required evidence and procedures.

3.2.4. Device Certificates

Device certification procedure will be encompassed in the RVLCA CPS in compliance with the relevant international standards and CCA guidelines.

3.2.5. Non-verified Subscriber Information

Information that is not verified shall not be included in certificates.

3.2.6. Validation of Authority

Certificates that contain explicit or implicit organizational affiliation shall be issued only after ascertaining the applicant has the authorization to act on behalf of the organization in the asserted capacity.

3.2.7. Criteria for Interoperation

Certificates shall be issued in accordance with relevant guideline(s) published by CCA to ensure interoperability.

3.3. Identification and Authentication for Re-Key Requests

3.3.1. Identification and Authentication for Routine Re-key

Identification and authentication requirements are specified in Section 3.2.

3.3.2. Identification and Authentication for Re-key after Revocation

Identification and authentication requirements are specified in Section 3.2.

3.4. Identification and Authentication for Revocation Request

Identification and authentication requirements are specified in Section 3.2.

4. Certificate Life-Cycle Operational Requirements

4.1. Certificate Application

4.1.1. Who Can Submit a Certificate Application

Certificate applications may be submitted to RVLCA that issues certificates under this CP by the Subscribers listed in Section 1.3.4, or an RA on behalf of the Subscriber.

4.1.2. Enrollment Process and Responsibilities

Applicants for public key certificates shall be responsible for providing accurate information in their applications for certification.

4.2. Certificate Application Processing

It is the responsibility of the RVLCA to verify that the information in certificate applications is accurate. RVL CPS shall specify procedures to verify information in certificate applications.

4.2.1. Performing Identification and Authentication Functions

See Section 3.2 and subsections thereof.

4.2.2. Approval or Rejection of Certificate Applications

A Certification Authority (CA) may approve or reject a certificate application.

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

Upon receiving a request for a certificate, a Certification Authority (CA) shall respond in accordance with the requirements set forth in applicable laws/regulations/guidelines in place.

4.3.1. CA Actions during Certificate Issuance

A Certification Authority (CA) shall verify the source of a certificate request before issuance. Certificates shall be checked to ensure that all fields and extensions are properly populated. After generation, verification, and acceptance, a Certification Authority (CA) shall post the certificate as set forth in the RVLCA's CPS.

4.3.2. Notification to Subscriber of Certificate Issuance

A Certification Authority (CA) will notify the subscriber of the creation of a certificate and make the certificate available to the subscriber.

4.4. Certificate Acceptance

4.4.1. Conduct Constituting Certificate Acceptance

The customer must confirm acceptance of the certificate upon notification of issuance by RVLCA.

4.4.2. Publication of the Certificate by the CA

All certificates shall be published in repositories. Publication arrangements of subscriber certificate are specified in the CPS of the RVLCA.

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

A Certification Authority (CA) does not follow any other means of notification or publication of information pertaining to issuing certificate for an entity.

4.5. Key Pair and Certificate Usage

4.5.1. Subscriber Private Key and Certificate Usage

Subscribers and RVLCA shall protect their private keys from access by any other party. Subscribers shall use their private keys for the purposes as constrained by the extensions (such as key usage, extended key usage, certificate policies, etc.) in the certificates issued to them.

4.5.2. Relying Party Public Key and Certificate Usage

Relying parties shall use public key certificates and associated public keys for the purposes as constrained by the extensions (such as key usage, extended key usage, certificate policies, etc.) in the certificates.

4.6. Certificate Renewal

RVLCA does not support renewal of certificates in any circumstances.

4.6.1. Circumstance for Certificate Renewal

Refer to Section 4.6

4.6.2. Who may Request Renewal

Refer to Section 4.6

4.6.3. Processing Certificate Renewal Requests

Refer to Section 4.6

4.6.4. Notification of New Certificate Issuance to Subscriber

Refer to Section 4.6

4.6.5. Conduct Constituting Acceptance of a Renewal Certificate

Refer to Section 4.6

4.6.6. Publication of the Renewal Certificate by the CA

Refer to Section 4.6

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

Refer to Section 4.6

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.

4.7.1. Circumstance for Certificate Re-key

RVLCA may issue a new certificate to the Subject when the Subject has generated a new key pair and is entitled to a 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

A certificate re-key shall be achieved using one of the following processes:

1. Initial registration process as described in Section 3.2; or
2. Identification & Authentication for Re-key as described in Section 3.3.2.

4.7.4. Notification of New Certificate Issuance to Subscriber

See Section 4.3.2.

4.7.5. Conduct Constituting Acceptance of a Re-keyed Certificate

See Section 4.4.1.

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

See Section 4.4.2.

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

See Section 4.4.3.

4.8. Certificate Modification

4.8.1. Circumstance for Certificate Modification

Certificate modification refers to the application for the issuance of a new certificate.

4.8.2. Who May Request Certificate Modification

See Section 4.1.1

4.8.3. Processing Certificate Modification Requests

See Section 3.2

4.8.4. Notification of New Certificate Issuance to Subscriber

See Section 4.3.2

4.8.5. Conduct Constituting Acceptance of a Modified Certificate

See Section 4.4.1

4.8.6. Publication of the Modified Certificate by the CA

See Section 4.4.2

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

See Section 4.4.3

4.9. Certificate Revocation and Suspension

Revocation requests must be authenticated.

4.9.1. Circumstance for Revocation of a Certificate

A certificate shall be revoked when the binding between the subject and the subject's public key defined within a certificate is no longer considered valid.

Whenever any circumstances occur, the associated certificate shall be revoked and placed on the CRL. Revoked certificates shall be included on all new publications of the certificate status information until the certificates expire. A revoked certificate shall appear on at least one CRL.

4.9.2. Who Can Request Revocation of a Certificate

a) User/Subject of the certificate for both the individual and organizational users
b) Human supervisor of a human subject for organizational user
c) Human Resources (HR) person for the human subject for organizational user
d) For CA certificates, authorized individuals representing the RVLCA may request revocation of certificates.

4.9.3. Procedure for Revocation Request

A request to revoke a certificate shall identify the certificate to be revoked, explain the reason for revocation, and allow the request to be authenticated (e.g., digitally, or manually signed by the subject).
Upon receipt of a revocation request, RVLCA shall authenticate the request and then revoke the certificate.

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 CA shall make its best efforts to process revocation requests so that it is posted in the next CRL.

4.9.6. Revocation Checking Requirements for Relying Parties

Use of revoked certificates may result in catastrophic consequences in certain applications. The Relying Party will determine the frequency of retrieving the revocation data from RVL CA URL. If the revocation information is temporarily unavailable for whatsoever reason, the Relying Party must reject use of the certificate; however, in the event of urgent operational requirement, the Relying Party may make an informed decision to accept the risk, responsibility, and consequences for using a certificate whose authenticity cannot be guaranteed to the standards of this policy.

4.9.7. CRL Issuance Frequency

CRL will be updated once in every 24 hours.

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.

4.9.9. Online Revocation Checking Availability

In addition to CRLs, CAs and Relying Party client software may optionally support on- line status checking. Client software using on-line status checking need not obtain or process CRLs.
If on-line revocation/status checking is supported by a CA, the latency of certificate status information distributed on-line by the CA or its delegated status responders shall meet or exceed the requirements for CRL issuance stated in 4.9.7.

4.9.10. Online Revocation Checking Requirements

RVLCA will recommend relying parties 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-line revocation status will be provided.

4.9.12. Special Requirements Related to Key Compromise

RVLCA uses reasonable efforts to notify potential Relying Parties if it discovers.

4.9.13. Circumstances for Suspension

Suspension shall be permitted if a user’s Key is temporarily unavailable to them.

4.9.14. Who can Request Suspension

A human subscriber, human supervisor of a human subscriber (organizational user), Human Resources (HR) person for the human subscriber (organizational user), issuing CA, may request suspension of a certificate.

4.9.15. Procedure for Suspension Request

A request to suspend a certificate shall identify the certificate to be suspended, explain the reason for suspension, and allow the request to be authenticated (e.g., digitally, or manually signed).

The reason code CRL entry extension shall be populated with “certificate Hold”. The Hold Instruction Code CRL entry extension shall be absent.

4.9.16. Limits on Suspension Period

A certificate may only be suspended for up to 15 days. If the subscriber has not removed their certificate from hold (suspension) within that period, the certificate shall be revoked for the reason of “Key Compromise”.

4.9.17. Who Can Request for Activation of a Suspended Certificate

CA may initiate the request for activation for any suspended certificate.

4.9.18. Procedure for Activation Request

The suspended certificates shall be re-activated upon approval by the RVLCA or when the same party that had the certificate suspended initiates the request.

4.10. Certificate Status Services

4.10.1. Operational Characteristics

The Status of public certificates is available via CRL at RVLCA’s website.

4.10.2. Service Availability

Certificate Status Services are available 24 x 7.

4.10.3. Optional Features

OCSP is an optional status service feature that is not available for all products.

4.11. End of Subscription

Certificates that have expired prior to or upon end of subscription are not required to be revoked.

4.12. Key Escrow and Recovery

4.12.1. Key Escrow and Recovery Policy and Practices

No Stipulation.

4.12.2. Session Key Encapsulation and Recovery Policy and Practices

No Stipulation.

5. Facility Management & Operational Controls

5.1. Physical Controls

Physical security controls shall be in accordance with the Information Security Policies and Standards and guidelines from CCA.

5.1.1. Site Location & Construction

The location and construction of the facility of RVLCA equipment shall be consistent with facilities used to house high value, sensitive information. The site location and construction, when combined with other physical security protection mechanisms such as guards and intrusion sensors, shall provide robust protection against unauthorized access to the RVLCA equipment and records.

5.1.2. Physical Access

RVLCA equipment shall always be protected from unauthorized access. A remote security check of the facility housing the RVLCA equipment shall occur if the facility is left unattended. A person or group of people shall be made explicitly responsible for making such checks. A log identifying access to the facility, at each instance, shall be maintained.

5.1.3. Power and Air Conditioning

RVLCA shall have backup power sufficient to automatically lockout input, finish any pending actions, and record the state of the equipment before lack of power or air conditioning causes a shutdown. PKI Repositories are provided with sufficient uninterrupted power for continuous CA operations.

5.1.4. Water Exposures

RVLCA has a standard water exposures system.

5.1.5. Fire Prevention & Protection

RVLCA has a compliant fire prevention and protection system.

5.1.6. Media Storage

CA media shall be stored to protect it from accidental damage (water, fire, electromagnetic). Media that contains audit, archive, or backup information shall be duplicated and stored in a location separate from the CA location.

5.1.7. Waste Disposal

Sensitive waste material shall be disposed of in a secure manner.

5.1.8. Off-Site backup

Off-Site backup will be taken place as per laws/regulations/guidelines.

5.2. Procedural Controls

5.2.1. Trusted Roles

A trusted role is an individual performing distinguished tasks that requires access to confidential and sensitive data in the PKI. The functions performed in these roles form the basis of trust for all uses of the CA. Trustworthiness of the person(s) concerned must be ensured as per CCA guidelines (if any) and properly be trained for their respective roles.

5.2.2. Number of Persons Required per Task

Two or more people (to establish n out of m rule) shall be assigned to perform each specific task.

5.2.3. Identification and Authentication for Each Role

An individual shall identify and authenticate him/herself before being permitted to perform any actions set forth above for that role or identity.

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 for these roles.

5.3. Personnel Controls

5.3.1. Qualifications, Experience, and Clearance Requirements

A group of individuals responsible and accountable for the operation of RVLCA shall be identified. The trusted roles of these individuals per Section 5.2.1 shall be identified.
All persons filling trusted roles shall be selected based on loyalty, trustworthiness, and integrity, and shall be subject to background investigation.

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.

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.

5.3.4. Retraining Frequency and Requirements

Individuals responsible for trusted roles shall be aware of changes in the CA or RA operations, as applicable. Any significant change to the operations shall have a training (awareness) plan, and the execution of such plan shall be documented. Examples of such changes are CA software or hardware upgrade, RA software upgrades, changes in automated security systems, and relocation of equipment.

5.3.5. Job Rotation Frequency and Sequence

RVLCA personnel will undergo job rotation practices as per the HR Policy.

5.3.6. Sanctions for Unauthorized Actions

Appropriate administrative and disciplinary actions shall be taken against personnel who violate this policy.

5.3.7. Documentation Supplied to Personnel

RVLCA shall make available to its personnel this certificate policy, the applicable CPS, and any relevant statutes, policies, or contracts. Other technical, operations, and administrative documents (e.g., Administrator Manual, User Manual, etc.) shall be provided for the trusted personnel to perform their duties.

Documentation shall be maintained identifying all personnel who received training and the level of training completed.

5.4. Audit Logging Procedures

Audit log files shall be generated for all events relating to the security of the CAs and RAs. Where possible, the security audit logs shall be automatically collected. Where this is not possible, a logbook, paper form, or other physical mechanism shall be used. All security audit logs, both electronic and non-electronic, shall be retained and made 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

All security auditing capabilities of the CA and RA operating system and the CA and RA applications required by this CP shall be enabled. As a result, most of the events identified in the table shall be automatically recorded. At a minimum, each audit record shall include the following (either recorded automatically or manually for each auditable event):

1. The type of event,
2. The date and time the event occurred,
3. Success or failure where appropriate, and
4. The identity of the entity and/or operator that caused the event.

5.4.2. Frequency of Processing Audit Logs

Audit logs shall be reviewed according to the relevant guidelines of CCA.

5.4.3. Retention Period for Audit Logs

See Section 5.5.2.

5.4.4. Protection of Audit Logs

System configuration and procedures shall be implemented together to ensure that:

1. Only authorized people have access to the logs.
2. Only authorized people may archive audit logs; and,
3. Audit logs are not modified.

5.4.5. Audit Log Backup Procedures

Audit logs and audit summaries shall be archived per Section 5.5.1.

5.4.6. Audit Collection System (internal vs. external)

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

5.4.7. Notification to Event-Causing Subject

This CP 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 a half yearly basis. Such vulnerability assessments focused on internal and external threats that could result in unauthorized access, tampering, modification, alteration, or destruction of the Certificate issuance process.

5.5. Records Archival

5.5.1. Types of Records Archived

CA and RA archive records shall be sufficiently detailed to establish the proper operation of the component or the validity of any certificate (including those revoked or expired) issued by the RVLCA.

5.5.2. Retention Period for Archive

The minimum retention periods for archive data are according to the relevant guidelines of CCA.

5.5.3. Protection of Archive

RVLCA protects the archive so that only authorized Trusted Persons can obtain access to the archive.

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 shall be time stamped such that order of events can be determined.

5.5.6. Archive Collection System (internal or external)

This system is internal to RVLCA.

5.5.7. Procedures to Obtain & Verify Archive Information

Procedures detailing how to create, verify, package, and transmit archive information shall be published in the RVL CPS.

5.6. Key Changeover

To minimize risk from compromising RVLCA's private signing key, that key may be changed often; from that time on, only the new key shall be used for certificate signing purposes. The older, but still valid, certificate will be available to verify old signatures until all the certificates signed using the associated private key have also expired. If the old private key is used to sign CRLs, then the old key shall be retained and protected.

5.7. Compromise and Disaster Recovery

5.7.1. Incident and Compromise Handling Procedures

If RVLCA detects a potential hacking attempt or other form of compromise, it shall perform an investigation to determine the nature and the degree of damage. If the RVLCA 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 to determine if the RVLCA needs to be rebuilt, only some certificates need to be revoked, and/or the RVLCA key needs to be declared compromised.

The CCA shall be notified if any of the following cases occur:

1. Suspected or detected compromise of a licensed CA system.

2. Physical or electronic attempts to penetrate a licensed CA system.
3. Denial of service attacks on a licensed CA system; or
4. Any incident preventing the licensed CA from issuing a CRL within 24 hours of the time specified in the next update field of its currently valid CRL. A CA shall reestablish capability to 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.

5.7.3. Entity Private Key Compromise Procedures

If RVLCA signature keys are compromised, lost, or suspected to be compromised, CCA shall be notified at the earliest feasible time so that CCA can revoke the CA certificate.

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.

5.8. CA, RA and Sub-CA Termination

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.

6. Technical Security Controls

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.

6.1.2. Private Key Delivery to Subscriber

A subscriber shall generate the key pairs and there is no need to deliver private keys.

6.1.3. Public Key Delivery to Certificate Issuer

End-entity Subscribers and RAs submit their public key for certification electronically through the use of a PKCS #10 Certificate Signing Request (CSR).

6.1.4. CA Public Key Delivery to Relying Parties

The public key of a trust anchor shall be provided to the subscribers acting as relying parties in a secure manner so that the trust anchor is not vulnerable to modification or substitution.

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.

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.

6.2. Private Key Protection and Cryptographic Module Engineering Controls

6.2.1. Cryptographic Module Standards and Controls

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

Use of RVLCA private signing key shall require action by at least two persons.

6.2.3. Private Key Escrow

CA private keys are not escrowed. Subscriber Private Key Escrow shall be in accordance with Section 4.12.1.

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.

6.2.5. Private Key Archival

Subscriber private signature keys shall not be archived by the CA.

6.2.6. Private Key Transfer into or from a Cryptographic Module

RVLCA private keys shall be generated by and remain in a cryptographic module. The RVLCA private keys shall be backed up in a secure manner.

6.2.7. Private Key Storage on Cryptographic Module

The cryptographic module may store Private Keys in any form if the keys are not accessible without authentication mechanism that follows FIPS 140-2 rating of the cryptographic module.

6.2.8. Method of Activating Private Key

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. Entry of activation data shall be protected from disclosure (i.e., the data should not be displayed while it is entered).

6.2.9. Methods of Deactivating Private Key

The cryptographic modules that have been activated shall not be left unattended or otherwise available for unauthorized access. After use, the cryptographic module shall be deactivated, e.g., via a manual logout procedure, or automatically after a period of inactivity as per laws/regulations/guidelines.

6.2.10. Method of Destroying Private Key

Private signature keys shall be destroyed when they are no longer needed, or when the certificates to which they correspond expire or are revoked. For software cryptographic modules, this can be overwriting the data. For hardware cryptographic modules, this will likely be executing a “zeroize” command. Physical destruction of hardware is required in the case of Root CA

6.2.11. Cryptographic Module Rating

See Section 6.2.1.

6.3. Other Aspects of Key Management

6.3.1. Public Key Archival

The public key is archived as part of the certificate archival.

6.3.2. Certificate Operational Periods/Key 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.

6.4. Activation Data

6.4.1. Activation Data Generation and Installation

The activation data used to unlock private keys, in conjunction with any other access control, shall have an appropriate level of strength for the keys or data to be protected and shall meet the applicable security policy requirements of the cryptographic module used to store the keys.

Activation data may be user selected. If the activation data must be transmitted, it shall be via an appropriately protected channel, and distinct in time and place from the associated cryptographic module.

6.4.2. Activation Data Protection

Data used to unlock private keys shall be protected from disclosure. After a predetermined number of failed login attempts, a facility to temporarily lock the account shall be provided.

6.4.3. Other Aspects of Activation Data

RVLCA shall change the activation data whenever the token is re-keyed or returned from maintenance.

6.5. Computer Security Controls

6.5.1. Specific Computer Security Technical Requirements

The following computer security functions may be provided by the operating system, or through a combination of operating system, software, and physical safeguards. The RVLCA shall include the following functionality:

1. Require authenticated logins
2. Provide Discretionary Access Control
3. Provide a security audit capability
4. Require a trusted path for identification and authentication
5. Provide domain isolation for process
6. Provide self-protection for the operating system

The computer system shall be configured with the minimum of the required accounts and network services.

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 RVLCA are as follows:

1. Hardware and software procured shall be purchased in a fashion to reduce the likelihood that any component was tampered with.

2. 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

3. The hardware and software shall be dedicated to performing the PKI activities. There shall be no other applications; hardware devices, network connections, or component software installed which are not part of the PKI operation.

4. Proper care shall be taken to prevent malicious software from being loaded onto the equipment. Only applications required to perform the PKI operations shall be obtained from sources authorized by local policy.

5. RVLCA hardware and software shall be scanned for malicious code on first use and periodically thereafter.

6.6.2. Security Management Controls

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

6.6.3. Life Cycle Security Controls

No stipulation.

6.7. Network Security Controls

RVLCA shall employ appropriate security measures to ensure they are guarded against denial of service and intrusion attacks. Such measures shall include the use of hardware firewalls, hardware filtering routers, and intrusion detection systems. Unused network ports and services shall be turned off.

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).

7. Certificate, CRL and OCSP Profiles

7.1. Certificate Profile

Certificate profiles are detailed in the CCA's Interoperability Guidelines document.

7.2. CRL Profile

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

7.3. OCSP Profile

OCSP requests and responses shall be in accordance with RFC 6960.

8. Compliance Audit and Other Assessments

8.1. Frequency or Circumstances of Assessments

RVLCA shall be subject to a periodic compliance audit at least once per year.

8.2. Identity and Qualifications of Assessor

The annual audit will be performed by the empaneled external auditor, who is recognized by the Controller of Certifying Authorities.

8.3. Assessor's Relationship to Assessed Entity

The auditor shall be a firm which is independent from the entity being audited. The office of CCA shall determine whether an auditor meets this requirement.

8.4. Topics Covered by Assessment

RVLCA shall have a compliance audit mechanism in place to ensure that the requirements of the relevant guidelines of CCA.

8.5. Actions Taken as a Result of Deficiency

RVLCA management is 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.

8.6. Communication of Results

An Audit Report, including identification of corrective measures taken or being taken by the CA, shall be provided to the office of CCA and the audited CA.

9. Other Business and Legal Matters

9.1. Fees

9.1.1. Certificate Issuance and Renewal Fees

RVLCA may set any reasonable certificate issuance and renewal fees.

9.1.2. Certificate Access Fees

RVLCA may not charge for access to any certificates.

9.1.3. Revocation Status Information Access Fees

RVLCA may not charge for access to any revocation status information.

9.1.4. Fees for Other Services

RVLCA may set any reasonable fees for any other services such as access to archive records or key recovery.

9.1.5. Refund Policy

RVLCA may follow the Subscriber's agreement for refund process.

9.2. Financial Responsibility

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 CP.

9.2.3. Insurance or Warranty Coverage for End-Entities

RVLCA does not offer protection to end entities that extend beyond the protections provided in this CP.

9.3. Confidentiality of Business Information

RVLCA shall maintain the confidentiality of confidential business information that is clearly marked or labeled as confidential, or by its nature should reasonably be understood to be confidential and shall treat such information with the same degree of care and security as the RVLCA treats its own most confidential information.

9.4. Privacy of Personal Information

RVLCA shall implement a privacy policy, which complies with this CP.

9.5. Intellectual Property Rights

RVLCA shall not knowingly violate any intellectual property rights held by others.

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 the right to modify such representations as it sees fit or required by law.

9.6.2. RA Representations and Warranties

RVLCA RA operates under the policies and practices detailed in its CPS and the associated Web Host Reseller agreement and Enterprise PKI Manager Account agreement.

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 or infringe 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.

9.6.4. Relying Party Representations and Warranties

Parties who rely upon the certificates issued under a policy defined in this document shall:

1. Use the certificate for the purpose for which it was issued, as indicated in the certificate information (e.g., the key usage extension).
2. Check each certificate for validity, using procedures described in RFC 5280, prior to reliance.
3. Preserve original signed data, the applications necessary to read and process that data, and the cryptographic applications needed to verify the digital signatures on that data for as long as it may be necessary to verify the signature on that data. Note: data format changes associated with application upgrades will often invalidate digital signatures and shall be avoided.

9.6.5. Representations and Warranties of Other Participants

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

9.7. Disclaimers of Warranties

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

9.8. Limitations of Liabilities

RVLCA may limit liabilities if they meet the liability requirements stated in ICT Act 2006 (amended 2013) and IT (CA) Rules 2000 made there under.

9.9. Indemnities

RVLCA includes indemnification clauses if the clauses are consistent with the ICT Act 2006 (amended 2013) and IT (CA) Rules 2000 made there under.

9.10. Term and Termination

9.10.1. Term

The CP becomes effective upon ratification by the Office of CCA. Amendments to this CP become effective upon ratification by the Office of CCA.

9.10.2. Termination

While this CP may be amended from time to time, it shall remain in force until replaced by a newer version or explicitly terminated by the Office of CCA.

9.10.3. Effect of Termination and Survival

Upon termination of this CP, RVLCA is 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 shall use commercially reasonable methods to communicate, considering the criticality and subject matter of the communication.

9.12. Amendments

9.12.1. Procedure for Amendment

Amendments to this CP shall be made by RVLCA and approved by Controller of Certifying Authorities, Bangladesh.

9.12.2. Notification Mechanism and Period

RVLCA reserves the right to amend the CP without notification for amendments that are not material, including without limitation corrections of typographical errors, changes to URLs, and changes to contact information.

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 CP, the amendment shall contain new object identifiers for the Certificate Policies.

9.13. Dispute Resolution Provisions

9.13.1. Disputes among RVLCA and Customers

Provisions for resolving disputes between RVLCA and its customers shall be set forth in the applicable agreements between the parties.

Dispute resolution procedures shall be consistent with the ICT Act 2006.

9.13.2. Disputes with End-User Subscribers or Relying Parties

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 CP.

9.15. Compliance with Applicable Law

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

9.16. Miscellaneous Provisions

9.16.1. Entire Agreement

This CP 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.

9.16.2. Assignment

Requirements of the assignment must be in accordance with the laws/regulations/guidelines.

9.16.3. Severability

If any provision of this CP is held to be invalid by a court of competent jurisdiction, then the remaining provisions will nevertheless remain in full force and effect.

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

No waiver of any breach or default or any failure to exercise any right hereunder shall be construed as a waiver of any subsequent breach or default or relinquishment of any future

right to exercise such right. The headings in this CP are for convenience only and cannot be used in interpreting this CP.

9.16.5. Force Majeure

RVLCA shall not be liable for any failure or delay in its performance under this CP due to causes that are beyond their reasonable control, including, but not limited to, an act of God, act of civil or military authority, fire, epidemic, flood, earthquake, riot, war, failure of equipment, failure of telecommunications lines, lack of Internet access, sabotage, and governmental action.

9.17. Other Provisions

Not being considered currently.

Appendix A: Definitions and Acronyms

Term	Description
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.
Authorized Party	(Certificate purpose) An Individual or Device with authority to conduct certain actions or make certain assertions.
Authorization	The granting of rights, including the ability to access specific information or resources.
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.
Certificate Chain	An ordered list of Certificates containing an end-user Subscriber Certificate and CAcertificates, which terminates in a root Certificate.
Certificate Management Control Objectives	Criteria that an entity must meet in order to satisfy compliance audit.

Term	Description
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.
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.
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 Authority Owner (CAO)	The legal entity responsible for the Certification Authority.
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.

Term	Description
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 the message 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.
Encryption Certificate	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 name is, in fact, the named entity.
User	(Certificate purpose)
(Certificate)	A person.
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 enduser 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 Generation Ceremony	A procedure whereby a CA's or RA's key pair is generated, its private key is transferred into a cryptographic module, its private key is backed up, and/or its public key is certified.

Term	Description
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 ecommerce applications.
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-byone by an Administrator using a web-based interface.
Non-repudiation	An attribute of a communication that provides protection against a party to a communication falsely denying its origin, denying that it was submitted, or denying its delivery. Denial of origin includes the denial that a communication originated from the same source as a sequence of one or more prior messages, even if the identity associated with the sender is unknown. Note: only 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.
No verified Subscriber Information	Information submitted by a Certificate Applicant to a CA or RA, and included within a Certificate, that has not been confirmed by the CA or RA and for which the applicable CA and RA provide no assurances other than that the information was submitted by the Certificate Applicant.
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.

Term	Description
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.
RVLCA Managed PKI 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 Managed PKI Standards	The business, legal, and technical requirements for issuing, managing, revoking, renewing, and using Certificates within the RVLCAPKI.
RVLCA Repository	RVLCA database of Certificates and other relevant RVLCA Managed PKI information accessible online.
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 which an 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.
Secret Share	A portion of a CA private key or a portion of the activation data needed to operate a CA private key under a Secret Sharing arrangement.
Secret Sharing	The practice of splitting a CA private key or the activation data to operate a CA private key in order to enforce multi-person control over CA private key operations under 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.

Term	Description
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 under which 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 necessarily a “trusted system” as recognized in classified government nomenclature.
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” 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
PIN	Personal Identification Number
OCSP	Online Certificate Status Protocol
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