Classification:

BCC

Certifying Authority

Certificate Policy

Version: 1.0.0

Bangladesh Computer Council

Information and Communication Technology Division

Table of Contents

Document Control

Field	Details
Document Name	Bangladesh Computer Council CA Certificate Policy (BCC CA CP)
Version	1.0
Classification	Public
Document OID	2.16.50.1.5.2
Document Location	https://bcc-ca.gov.bd/content/downloads
Maintenance Owner	BCC CA Document Manager
Approval Owner	BCC CA Document Manager
Release Date	07 March 2026
Associated CPS	BCC CA CPS V1.0.5
Governing Law	ICT Act 2006; IT (CA) Rules 2010

Revision History

Version	Date	Rev #	Description of Changes
1.0	07 March 2026	—	Initial release of BCC CA Certificate Policy

1. Introduction

1.1 Overview

This Certificate Policy (CP) outlines the policies governing the issuance, management, and use of digital certificates by the Bangladesh Computer Council Certifying Authority (BCC CA). It is aligned with the framework provided in RFC 3647, which establishes a standard structure for Certificate Policies and Certification Practice Statements. This document defines the rules and assurance levels for certificates issued by BCC CA, ensuring security, reliability, and compliance with national and international standards for public key infrastructure (PKI).

This CP provides the rules for the issuance and management of X.509 public key certificates by BCC CA. It supports various assurance levels (low, medium, and high) for applications such as digital signatures, authentication, and encryption in government, business, and public services within Bangladesh. The PKI operated by BCC CA aims to facilitate secure electronic transactions in alignment with the Digital Security Act of Bangladesh and international best practices.

This CP defines the policy framework governing the issuance, management, renewal, re-keying, and revocation of digital certificates within the BCC CA Public Key Infrastructure (PKI). The BCC CA is an autonomous organisation of the Government of Bangladesh and a licensed Certifying Authority of the Office of the Controller of Certifying Authorities (CCA), Information and Communication Technology Division.

The Office of the CCA has accredited BCC as a licensed CA under the CCA hierarchical PKI Trust chain, resulting in a BCC CA certificate being signed under the CCA Root CA. Subscriber certificates issued from BCC CA Managed PKI services chain up to the BCC.

1.2 Document Name and Identification

Document Name	Bangladesh Computer Council CA Certificate Policy (BCC CA CP)
Document Location	http://repo.bcc-ca.gov.bd/CP
Document X.500 OID	2.16.50.1.5.2
Associated CPS OID	2.16.50.1.5.1

1.3 Policy Scope and Applicability

This CP is applicable to:

- BCC CA hosted and controlled CA infrastructure.
- BCC CA Infrastructure CAs and BCC CA Administrative CAs supporting the BCC CA Certificate Lifecycle Platform.
- All Subordinate CAs hosted and controlled by BCC CA within the BCC CA certificate hierarchy.
- All classes of certificates issued under the BCC CA hierarchy, including Class 0, Class 1, Class 2, Class 3, and e-Sign Certificates.
- All PKI participants: Certification Authorities, Verification Authorities, Registration Authorities, Subscribers, Validation Authorities, e-Sign Service Providers, and Relying Parties.

1.4 PKI Participants

1.4.1 Certification Authorities (CA)

Certification Authorities are entities licensed by the Office of the CCA to sign and issue certificates under the CCA PKI Trust chain. For the purpose of this CP:

- The Office of the CCA acts as the Root CA.
- BCC CA is an Intermediate CA that issues certificates to BCC CA internal and external Subordinate CAs and end-user Subscribers.
- BCC CA Managed PKI customers may operate their own CAs as external Subordinate CAs to the BCC CA.
- BCC CA will also operate a BCC CA Internal Administrator CA hierarchy limited to BCC CA internal service administration activities.

1.4.2 Verification Authorities

Verification Authorities are entities authorised by BCC CA to:

- Perform identification and authentication of certificate applicants requesting the issuance of end-user certificates.
- Verify whether the payment process has been completed for a certificate request.
- Approve or deny certificate requests and notify applicants accordingly.

1.4.3 Registration Authorities (RA)

Registration Authorities perform the following functions:

- Review and verify certificate requests approved by Verification Authorities for final approval.
- Forward approved certificate requests to the CA for generation of a digital certificate.
- Initiate certificate revocation or suspension under certain circumstances.
- Process subscriber requests to revoke, suspend, renew, or re-key certificates.

1.4.4 Subscribers

Subscribers are applicants approved by the Verification Authorities and RA to receive an end-entity certificate signed by BCC CA. All Subscribers must agree to be bound by the terms of the applicable Subscriber Agreement.

1.4.5 Validation Authority (VA)

The Validation Authority (VA) is an entity that provides a service used to verify the validity of a digital certificate issued by subordinate CA of BCC CA using Certificate Revocation Lists (CRLs) and Online Certificate Status Protocol (OCSP).

1.4.6 e-Sign Service Provider (ESP)

The e-Sign Service Provider (ESP) is an entity of BCC CA with a subordinate CA role to provide remote signing service to subscribers. ESP:

- Maintains an automated enrolment process for subscriber certificate requests.
- Provides an interface to accept document signing requests through business applications.
- Creates subscribers' signatures in a secure manner ensuring sole control assurance level.

1.4.7 Relying Parties

Relying Parties rely on the binding of the Public Key to the identity of a subject in a certificate. All Relying Parties agree to be bound by the terms of a Relying Party Agreement. The act of relying on a BCC CA issued certificate constitutes acceptance of any applicable Certificate Policy and Relying Party Agreement.

1.5 Certificate Usage

1.5.1 Appropriate Certificate Uses

Certificates issued under the BCC CA hierarchy are provisioned to end-entities for:

- Digital signing of electronic documents and transactions.
- Encryption and decryption of data.
- Authentication to Relying Party applications and services.
- Remote electronic signing (e-Sign) operations.

1.5.2 Certificate Classes and Assurance Levels

There are four levels of assurance for certificates issued under the BCC CA hierarchy:

Certificate Class	Assurance Level	Signing	Encryption	Client Auth
Class 0	No Assurance	Yes	Yes	Yes
Class 1	Low Assurance	Yes	Yes	Yes
Class 2	Medium Assurance	Yes	Yes	Yes
Class 3	High Assurance	Yes	Yes	Yes
e-Sign	High Assurance	Yes	No	No

1.5.3 Certificate Assurance Level Descriptions

- Class 0: Test certificates only — no identity authentication required.
- Class 1: Low assurance — limited confirmation of Subscriber's email address only; not suitable for non-repudiation.
- Class 2: Medium assurance — identity verified against government-approved identity database and business records.
- Class 3: High assurance — physical presence verification required; highest level of identity assurance.
- e-Sign Certificates: High assurance — biometric face-matching against government-approved identity database.

1.5.4 Prohibited Certificate Uses

BCC CA certificates SHALL NOT be used for:

- Control equipment in hazardous circumstances requiring fail-safe performance (e.g., nuclear facilities, aircraft navigation, weapons control systems).
- Any functions other than those specified in the certificate's KeyUsage extension.
- CA functions by end-user Subscriber certificates.
- Any purpose prohibited under ICT Act 2006, IT (CA) Rules 2010, Digital Certificate Interoperability Guideline, or directives of Office of the CCA.

1.6 Policy Administration

1.6.1 Organisation Administering the Document

Bangladesh Computer Council
ICT Tower, E-14/X Agargaon, Sher-e-Bangla Nagar
Dhaka-1207, Bangladesh

1.6.2 Contact Person

Director (CA Operation & Security), BCC
Telephone: 88-02-55006840 | Fax: 88-02-55006791 | Email: cps@bcc-ca.gov.bd

1.6.3 CP Approval Procedures

Approval of this CP and subsequent amendments shall be made by BCC CA and the Office of the CCA. All proposed changes must be approved by the Office of the CCA, Bangladesh before implementation. Amendments shall be published to the BCC CA Managed PKI Repository.

2. Publication and Repository Responsibilities

2.1 Repositories

An authoritative repository for all PKI-related information is located at: https://repo.bcc-ca.gov.bd

Certificate Revocation Lists (CRLs) are hosted at: http://crl.bcc-ca.gov.bd

2.2 Publication of Certification Information

The following information is published and publicly accessible:

- This Certificate Policy (CP).
- The Certification Practice Statement (CPS).
- CA certificates.
- Certificate status information (CRLs and OCSP responses).

2.3 Time or Frequency of Publication

Changes to the CP shall be published to the Repository in accordance with the notification requirements. Certificate status information shall be made available in accordance with Section 5 of this CP (Certificate Revocation). CRLs for end-entity certificates are issued at least once per day; for CA certificates, at least annually and upon each revocation.

2.4 Access Controls on Repositories

Information published in the BCC CA Managed PKI Repository is publicly accessible on a read-only basis. BCC CA requires persons to agree to a Relying Party Agreement as a condition of accessing certificates, certificate status information, or CRLs.

3. Identification and Authentication

3.1 Naming

3.1.1 Types of Names

BCC CA hierarchy certificates contain an X.500 Distinguished Name (DN) in the Issuer and Subject fields. Naming conventions comply with the Office of the CCA issued Digital Certificate Interoperability Guideline.

3.1.2 Name Requirements

- Distinguished Names (DNs) shall be interpreted according to the X.501 standard.
- Each DN assigned to a Subscriber under this CP shall be unique.
- Certificates shall not be issued for anonymous or pseudonymous Subscribers (excluding Class 0 certificates, role-based certificates, and device certificates).
- Certificate applicants are prohibited from using names that infringe upon Intellectual Property Rights of others.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

Where the Subscriber generates the Private Key, proof of possession shall be performed by provision of a PKCS #10 Certificate Signing Request (CSR) or equivalent method. If the Subscriber does not generate the Private Key, the delivery process shall be auditable.

3.2.2 Authentication Standards by Certificate Class

Certificate Class	Identity Authentication Standard
Class 0	No identity authentication required — test purpose only.
Class 1	No identity authentication. Limited confirmation of the Subscriber's email address only.
Class 2	Identity verified by matching to government-approved identity database (e.g., National Identity Database) with address verification; or business records for organisational certificates.
Class 3	Physical (in-person) presence of the Certificate Applicant before an authorised agent of the CA or RA, or notary public. Government-issued photographic identification required.
e-Sign	Face-matching of the individual against a government-approved identity database. Authentication per the prescribed guideline of the Office of the CCA.

3.2.3 Authentication of Organisation Identity

Whenever a CA certificate is to contain an organisation name, the CA shall:

- Confirm the organisation's existence using at least one identity proofing service or database, or government-issued documentation.

- Confirm by telephone, postal mail, or comparable procedure that the organisation has authorised the BCC CA Managed PKI Service application.

3.3 Identification and Authentication for Re-key Requests

Prior to expiration of a certificate, a Subscriber must generate a new key pair (re-key) to maintain continuity. Procedures to authenticate the Subscriber for re-key include:

- Challenge Phrase submission matching enrolment information on record.
- Proof of possession of the existing private key.
- Re-key requests received 30 or more days after certificate expiration require full re-authentication equivalent to an original Certificate Application.

3.4 Identification and Authentication for Re-key After Revocation

Re-key/renewal after revocation is NOT permitted if the revocation occurred because the certificate was:

- Issued to a person other than the one named as Subject.
- Issued without the authorisation of the named Subject.
- Issued on the basis of false material fact in the Certificate Application.
- Revoked for any reason deemed necessary by the RA to protect the BCC CA PKI Trust chain.

3.5 Identification and Authentication for Revocation Requests

Acceptable procedures for authenticating revocation requests include:

- Submission of the Subscriber's Challenge Phrase.
- A digitally signed revocation request verifiable with the certificate to be revoked.
- Communication with the Subscriber providing reasonable assurances (telephone, facsimile, email, mail, or courier).

4. Certificate Life-Cycle Operational Requirements

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application

The following may initiate certificate applications:

- Any individual who is the subject of the certificate.
- Any authorised representative of an Organisation or entity.
- Any authorised representative of a CA or RA.

4.1.2 Enrolment Process and Responsibilities

All end-entity certificate Subscribers shall:

- Complete a certificate application providing true and correct information.
- Generate, or arrange to have generated, a key pair.
- Deliver their public key to the RA.
- Demonstrate possession and/or sole control of the private key corresponding to the public key.
- Agree to the applicable Subscriber Agreement.

4.2 Certificate Application Processing

4.2.1 Approval Criteria

A certificate application SHALL be approved if:

- Successful identification and authentication of all required Subscriber information is completed.
- All applicable departmental and financial requirements are met.

A certificate application SHALL be rejected if:

- Identification and authentication cannot be completed.
- The Subscriber fails to furnish supporting documentation upon request.
- The Subscriber fails to respond to notices within the specified time.
- Issuing a certificate may bring the BCC CA hierarchy and/or CCA PKI Trust chain into disrepute.
- Issuing a certificate may lead to any infringement of law and order.

4.2.2 e-Sign Certificate Applications

e-Sign Certificate applications are approved automatically upon successful enrolment of a subscriber via BCC CA's eKYC application system. Upon successful enrolment, the certificate is issued instantaneously.

4.3 Certificate Issuance

A Certificate is created and issued following approval of a Certificate Application by the RA. BCC CA shall notify Subscribers of certificate availability via the BCC CA portal or a notification message.

4.4 Certificate Acceptance

Certificate acceptance is constituted by:

- Downloading or installing a Certificate from the BCC CA portal.
- Failure of the Subscriber to object to the certificate or its content within the specified period.
- e-Sign certificates are considered accepted upon issuance.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

Subscribers shall:

- Use the Private Key only after accepting the certificate and agreeing to the Subscriber Agreement.
- Protect their private keys from unauthorised use.
- Discontinue use of the private key following expiration or revocation of the certificate.
- Not use the certificate for purposes inconsistent with the KeyUsage field extensions.

For e-Sign certificates, BCC CA protects the private keys of the subscriber according to the e-Sign Guideline and directives of the Office of the CCA, ensuring sole control by the subscriber.

4.6 Certificate Renewal and Re-key

Certificate rekey is performed for each certificate renewal in accordance with the Information Technology (Certifying Authorities) Rules, 2010. Prior to expiration, a Subscriber must re-key the certificate to maintain continuity. Re-keyed certificates are subject to the same authentication requirements as the original certificate application.

4.7 Certificate Revocation and Suspension

4.7.1 Circumstances for Revocation

An end-user Subscriber certificate SHALL be revoked if:

- There is reason to believe or strongly suspect a compromise of the Subscriber's private key.
- The Subscriber has materially breached obligations under the Subscriber Agreement.
- The Subscriber Agreement has been terminated.
- The affiliation between BCC CA and the Subscriber has ended.
- The certificate was issued in a manner not materially in accordance with the applicable CP/CPS.
- A material fact in the certificate application is false.
- The information within the certificate has changed.
- The Subscriber has not submitted payment when due.
- The continued use of the certificate is harmful to BCC CA and/or the CCA PKI Trust chain.
- Certificate usage may lead to infringement of law and order.

4.7.2 Circumstances for Suspension

A certificate may be suspended if:

- The subscriber requests suspension of their Digital Certificate.
- Non-payment of certificate fees within the stipulated time.
- Any circumstance which may jeopardise the trust of the BCC CA hierarchy and/or CCA PKI Trust chain.
- Any circumstance which may breach law and order.
- If BCC CA is of the opinion that suspension is in the public interest.

Suspended certificates will be revoked if an activation request is not received within 15 days of the date of suspension.

4.7.3 CRL Issuance Frequency

- CRLs for end-entity Subscriber certificates are issued at least once per day.
- CRLs for CA-certificates are issued at least annually, and whenever a CA-certificate is revoked.
- In the event of key compromise, a new CRL must be published within 24 hours of revocation.

4.8 Certificate Status Services

Certificate status information is available through:

- Certificate Revocation Lists (CRLs) available at https://crl.bcc-ca.gov.bd.
- Online Certificate Status Protocol (OCSP) where available.
- Web-based query functions in the BCC CA Repository.

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

5. Facility, Management, and Operational Controls

5.1 Physical Controls

BCC CA systems are protected by a minimum of four tiers of physical security. Access to each tier requires a proximity card employee badge and is automatically logged and video recorded. Additional tiers enforce two-factor authentication including biometrics.

Physical security requirements include:

- Site Location and Construction: Physically protected environment that deters, prevents, and detects unauthorised use.
- Physical Access: Progressively restrictive physical access privileges control access to each tier.
- Power and Air Conditioning: Primary and backup power systems ensuring continuous, uninterrupted access.
- Fire Prevention and Protection: Measures designed to comply with local fire safety regulations.
- Media Storage: All media stored with appropriate physical and logical access controls.
- Waste Disposal: Sensitive documents shredded; media rendered unreadable before disposal.
- Off-Site Backup: Routine backups stored at a physically secure disaster recovery facility.

5.2 Procedural Controls

5.2.1 Trusted Roles

Trusted Persons include all employees, contractors, and consultants with access to or control over authentication or cryptographic operations that may materially affect the validation, acceptance, rejection, issuance, or revocation of certificates. At a minimum, two trusted personnel are required for sensitive tasks.

5.2.2 Separation of Duties

Roles requiring separation of duties shall include, but are not limited to, the following:

a) Validation of information contained in certificate applications;

b) Acceptance, rejection, or other processing of certificate applications, revocation requests, renewal requests, or enrolment information;

c) Issuance or revocation of certificates, including access to restricted portions of the repository;

d) Handling of Subscriber information or requests;

e) Generation, issuance, or destruction of CA certificates; and

f) Loading of a CA into the production environment.

5.3 Personnel Controls

Prior to commencement of employment in a Trusted Role, BCC CA conducts background checks including:

- Confirmation of previous employment and professional references.
- Confirmation of highest educational degree obtained.
- Search of criminal records (state and national).
- Check of credit/financial/insolvency records.

BCC CA provides training upon hire covering PKI concepts, job responsibilities, security policies, hardware/software operation, incident reporting, and disaster recovery procedures.

5.4 Audit Logging

BCC CA logs significant events including:

- CA key lifecycle management events (key generation, backup, storage, recovery, archival, destruction).
- CA and Subscriber certificate lifecycle management events.
- Security-related events (access attempts, system actions, security profile changes, network activity).
- e-Sign Service Provider events (signing key generation, CSR generation, signing operations, OTP generation/verification, subscriber enrolment).

Audit logs are retained onsite for at least two months after processing, then archived for seven years.

5.5 Records Archival

BCC CA archives all audit data, certificate application information, documentation supporting certificate applications, and certificate lifecycle information. Archives are retained for 7 (seven) years and protected against unauthorised viewing, modification, or deletion.

5.6 Compromise and Disaster Recovery

BCC CA has implemented a disaster recovery site physically separate from the primary facility. The BCC CA has the capability to restore or recover essential operations within 72 hours following a disaster, supporting:

- Certificate issuance.
- Certificate revocation.
- Publication of revocation information.
- Key recovery information provision.

6. Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

CA key pairs are generated using Trustworthy Systems by multiple pre-selected, trained, and trusted individuals. Cryptographic modules meet the requirements of at least FIPS 140-2 Level 3. Key Generation Ceremonies are conducted in accordance with the BCC CA Key Ceremony Reference Guide.

6.1.2 Key Sizes

Entity	Key Size	Standard
CA / Sub-CA	4096-bit RSA	Directive of Office of the CCA
End-Entity Subscribers	2048-bit RSA (minimum)	Digital Certificate Interoperability Guideline
e-Sign Certificates	2048-bit RSA (minimum)	e-Sign Guideline, Office of the CCA

6.1.3 Key Usage Purposes

Key usage purposes are set based on RFC 5280 and the BCC CA Digital Certificate Interoperability Guideline:

- Authentication certificates: digitalSignature bit.
- Key encryption certificates: keyEncipherment bit.
- Data encryption certificates: dataEncipherment bit.
- Digital signature certificates: digitalSignature and nonRepudiation bits.
- CA certificates: cRLSign and keyCertSign bits.
- Key agreement certificates: keyAgreement bit.

6.2 Private Key Protection

6.2.1 Cryptographic Module Standards

For CA key pair generation and CA private key storage, BCC CA uses hardware cryptographic modules certified at FIPS 140-2 Level 3 or higher.

6.2.2 Multi-Person Control

BCC CA uses Secret Sharing to split activation data for CA private keys into Secret Shares held by multiple trusted individuals. A threshold of 3 Secret Shares (out of n distributed) is required to activate a CA private key.

6.2.3 Private Key Escrow

CA private keys are NOT escrowed. BCC CA does not provide key escrow service for any signing keys.

6.2.4 Private Key Backup

BCC CA creates backup copies of CA private keys for routine recovery and disaster recovery purposes. Keys are stored in encrypted form within hardware cryptographic modules. Upon expiration of a BCC CA certificate, the key pair is securely retained for at least 5 years.

6.2.5 Private Key Activation Standards by Class

Class	Private Key Activation Standard
Class 0-1	Reasonable physical protection of workstation. Password recommended.
Class 2	Password-based authentication required before activation. Encrypted storage when deactivated.
Class 3	Smart card, biometric device, or equivalent required. Encrypted storage when deactivated.
e-Sign	Keys generated in FIPS 140-2 Level 2 module; stored encrypted with key encryption key; subscriber has sole control and required authorization. Always encrypted.

6.3 Certificate Operational Periods

Operational periods and key pair usage periods for all BCC CA hierarchy certificates shall be in accordance with the Digital Certificate Interoperability Guideline document issued by the Office of the CCA.

6.4 Computer Security Controls

BCC CA ensures that systems maintaining CA software and data files are Trustworthy Systems secured from unauthorised access. Controls include:

- Logical separation of the production network from other components.
- Firewalls and Intrusion Prevention Systems (IPS) protecting production networks.
- Password policies requiring minimum character length, alphanumeric and special characters, and periodic changes.
- Network time synchronisation with National NTP Servers.

6.5 Network Security Controls

BCC CA performs all CA and RA functions using networks secured to prevent unauthorised access and malicious activity. Communications of sensitive information are protected through encryption and digital signatures.

7. Certificate, CRL, and OCSP Profiles

7.1 Certificate Profile

Certificates shall conform to:

- IETF PKIX RFC 5280.
- The BCC CA Digital Certificate Interoperability Guideline document.

7.2 CRL Profile

Certificate Revocation Lists shall conform to:

- IETF PKIX RFC 5280.
- The BCC CA Digital Certificate Interoperability Guideline document.

7.3 OCSP Profile

Online Certificate Status Protocol shall conform to:

- IETF PKIX RFC 6960.
- The BCC CA Digital Certificate Interoperability Guideline document.

8. Compliance Audit and Other Assessments

8.1 Frequency of Assessments

- Annual External Audit: Performed by empanelled auditors under the Office of the CCA per IT (CA) Rules 2010.
- Internal Audit: Performed twice per year; reports submitted to the Office of the CCA.
- Exigent Audit/Investigation: May be performed at any time BCC CA has reason to believe an entity has failed to meet BCC CA Managed PKI Standards.
- Supplemental Risk Management Reviews: Following incomplete or exceptional findings in a Compliance Audit.

8.2 Assessor Qualifications

- External auditors must be Office of the CCA empanelled auditors in accordance with IT (CA) Rules 2010.
- Internal auditors must not hold any Trusted Roles within BCC CA PKI.
- External auditing firms must be independent of the audited entity.

8.3 Topics Covered by Assessment

The scope of BCC CA's annual audit includes:

- CA environmental controls.
- Key management operations.
- Infrastructure and Administrative CA controls.
- Certificate lifecycle management.
- CA business practices disclosure.
- Compliance with Bangladesh ICT Act 2006, IT (CA) Rules 2010, and PKI Audit Guidelines.

8.4 Actions Taken as a Result of Deficiency

Significant exceptions or deficiencies identified during a Compliance Audit will result in:

- Determination of corrective actions by BCC CA management with input from the auditor.
- Immediate corrective action plan if deficiencies pose an immediate threat to BCC CA PKI security or integrity.
- Audit reports submitted to the Office of the CCA identifying corrective measures.

9. Other Business and Legal Matters

9.1 Fees

Fees may be payable by Subscribers for the issue or renewal of Certificates. Fee schedules are provided in accordance with the notification requirements. Key fee provisions:

- Certificate Issuance/Renewal Fees: Applicable as per the current fee schedule.
- e-Sign Service Fees: Applicable per the approved and current fee schedule.
- Certificate Access Fees: BCC CA does not charge a fee for making Certificates available in a repository to Relying Parties.
- Revocation/Status Information: BCC CA does not charge a fee for making CRLs available to Relying Parties.

9.2 Financial Responsibility

Each BCC CA Managed PKI Participant is solely responsible for determining appropriate insurance coverage. BCC CA does not provide any insurance coverage or warranty for loss or damage resulting from participation in the Certificate application process or use of Certificates.

9.3 Confidentiality

The following records shall be kept confidential:

- CA application records (approved or disapproved).
- Certificate Application records.
- Private keys held by enterprise Customers using BCC CA Managed PKI Key Manager.
- Transactional records and audit trails.
- Contingency planning and disaster recovery plans.
- Security measures controlling BCC CA operations.

Information not within the scope of confidential information includes: certificate content, revocation/suspension status, and information lawfully received from third parties not bound by confidentiality.

9.4 Privacy of Personal Information

Any information about Subscribers not publicly available through the issued certificate, certificate directory, and online CRLs is treated as private. BCC CA Managed PKI participants receiving private information shall secure it and comply with all applicable privacy laws.

9.5 Representations and Warranties

9.5.1 CA Representations and Warranties

BCC CA warrants that there are no material misrepresentations in certificates, no errors introduced through failure to exercise reasonable care, all certificates meet material requirements of this CP, and revocation services conform to the applicable CP.

9.5.2 Subscriber Representations and Warranties

Subscribers warrant that:

- Each digital signature is the Subscriber's own and the certificate is operational at the time of signing.
- The private key is protected and no unauthorised person has had access to it.
- All information supplied in the Certificate Application is true.
- The Certificate is used exclusively for authorised and legal purposes consistent with this CP.
- The Subscriber is an end-user Subscriber and not acting as a CA.

9.5.3 Relying Party Representations and Warranties

Relying Parties acknowledge that they are solely responsible for deciding whether to rely on certificate information, must verify certificate status before reliance, and bear the legal consequences of failing to perform their obligations under this CP.

9.6 Dispute Resolution

Disputes among BCC CA and Managed PKI participants shall be resolved pursuant to provisions in applicable agreements. Disputes involving BCC CA require an initial negotiation period of 60 days followed by litigation in court or, for other claimants, arbitration administered by the International Chamber of Commerce (ICC) in accordance with ICC Rules.

9.7 Governing Law

The laws of the People's Republic of Bangladesh govern the enforceability, construction, interpretation, and validity of this CP, irrespective of contract or other choice of law provisions. This CP is also subject to applicable national, state, local, and foreign laws, rules, regulations, and orders.

9.8 CP Amendments

BCC CA shall review this CP at least annually. Material amendments are subject to a 30-day comment period after publication. All proposed changes must be approved by the Office of the CCA, Bangladesh before implementation. Non-material amendments (e.g., typographical corrections, URL changes, contact information updates) may be made without prior notification.

10. Policy Object Identifiers (OIDs)

The OIDs registered by BCC CA under the BCC CA arc are as follows:

Policy	OID	Certificate Class
BCC CA CP (this document)	2.16.50.1.5.6	All Classes
BCC CA CPS	2.16.50.1.5.1	All Classes
BCC CA Class 0 Policy	2.16.50.1.2.0	Class 0
BCC CA Class 1 Policy	2.16.50.1.2.1	Class 1
BCC CA Class 2 Policy	2.16.50.1.2.2	Class 2
BCC CA Class 3 Policy	2.16.50.1.2.3	Class 3
BCC CA e-Sign Policy	2.16.50.1.5.4	e-Sign

OID Arc: joint-iso-itu-t(2) country(16) bd(50) root-ca-bangladesh(1) bcc-ca(5)

Appendix A: Key Definitions and Acronyms

Term / Acronym	Definition
BCC CA	Bangladesh Computer Council Certifying Authority — the issuing CA under the CCA PKI Trust chain.
CA	Certification Authority — an entity authorised to issue, manage, revoke, and renew Certificates.
CCA	Controller of Certifying Authorities — the regulatory authority overseeing PKI in Bangladesh.
CP	Certificate Policy — a named set of rules indicating the applicability of a certificate to a particular community or class of application.
CPS	Certification Practice Statement — a statement of the practices a CA employs in issuing, managing, revoking, and renewing certificates.
CRL	Certificate Revocation List — a signed, time-stamped list of revoked certificate serial numbers.
CSR	Certificate Signing Request (PKCS #10) — a message conveying a request to have a certificate issued.
DN	Distinguished Name — a unique identifier assigned to each certificate applicant, structured per X.500.
e-Sign	Electronic Signing — remote signing service provided by the e-Sign Service Provider (ESP) under BCC CA.
ESP	e-Sign Service Provider — entity with subordinate CA role providing remote signing services.
FIPS 140-2	Federal Information Processing Standard — US standard for cryptographic module validation.
HSM	Hardware Security Module — tamper-protected hardware device for secure key generation and storage.
OCSP	Online Certificate Status Protocol — a protocol for providing real-time certificate status information.
PKI	Public Key Infrastructure — the architecture, organisation, and procedures supporting certificate-based public key cryptographic systems.
RA	Registration Authority — an entity performing identification, authentication, and approval functions on behalf of a CA.

RFC 5280	IETF standard defining the X.509 certificate and CRL profile for the Internet PKI.
RSA	Public key cryptographic system (Rivest, Shamir, Adleman) — used for digital signatures and key exchange.
Sub-CA	Subordinate Certification Authority — a CA whose certificate is certified by another CA (e.g., BCC CA).
VA	Validation Authority — an entity providing certificate validity verification via CRLs and OCSP.
X.509	International standard defining the format of public key certificates used in PKI systems.