Bangladesh Root CA Certificate Practice Statement (CPS)

Office of the Controller of Certifying Authorities

Ministry of Information & Communication Technology

Government of the Peoples Republic of Bangladesh

Document Reference

Title	Bangladesh Root CA Certificate Practice Statement (CPS)
Document Type	Public
Version	3.00
Approve Date	15 February 2020
Previous Version	2.00
Previous Version Revised Date	18 November 2013
Pages	57
Status	Approved

24.03.2020

Signature:

(The Controller of Certifying Authorities)

List of Abbreviations/Acronyms

ICT	Information & Communication Technology
CA	Certificate authority
CCA	Controller of Certifying Authority
CRL	Certificate Revocation List
RA	Registration Authority
VA	Verification Authorities
CPS	Certification Practice Statement
CP	Certificate Policy
RM	Registration Manager
PKI	Public Key Infrastructure
CRL	Certificate Revocation List
PAG	PKI Assessment Guidelines

Changes History

This section contains the summary of changes made to the CP. Please check the archived document versions for detailed comparative differences.

Term	Release Date	Changes Log
Version 3.0	15 February 2020	• The entire CP/CPS has been revised to comply with RFC 3647.
Version 2.0	18 November 2013	• Office of the CCA has been allocated with Object Identifier (OID) from the Country RA for OID of Bangladesh. The OID assigned to Office of the CCA is 2.16.50.1. OID assigned to Office of the CCA is for the PKI of Bangladesh. All Licensed CAs, Certification Practice Statement (CPS), Certificate Policy (CP), and other PKI components will be using OID. The revision to this CPS is to identify the CPS document with an OID. This revision is made in 1.2. • The contact details for this Policy Administration has also been modified which is available in 1.5.1.
Version 1.0	17 April 2012	• Base Version

Table of Contents

24.02.2020

24.03.2021

24.03.2020

24.03.2020

29.03.2020

Table of Tables

1 Introduction

1.1 Overview

The Office of the Controller of Certifying Authorities (CCA) is established under the Information and Communication Technology (Amended) Act, 2006 on May in 2011. The controller is appointed by the Government to supervise and control all Certifying Authorities of Electronic Signature in 2009. Since it is plausible and necessary to provide legal recognition & security of Information and Communication Technology, the Government has passed the Information and Communication Technology (Amended) Act, 2006 by which Digital Signature is being introduced among the people of Bangladesh and Electronic Signatures, Records have been given legal recognition. National Information & Communication Technology Policy, 2018 provides directions to introduce Digital Signature. Digital Signature is introduced in 2009 under the ICT Act, 2006 and it will gradually spread over the whole country. Under Section-8 of the ICT Act, 2006, the usage of Digital/ Electronic Signature and Records is recognized in all Government offices.

In 2011, the Controller of Certifying Authorities (CCA) provides licenses to be Certifying Authorities to 6(six) organizations. One important step for introduction of Digital Signature has been completed through the Root Key Generation Ceremony on April 18, 2012.

Objective of the CCA office is:

- Help to make a secure cyber space in the country.
- Running Public Key Infrastructure (PKI) program within legal framework.
- Building Public Awareness in secure e-transaction

The general architecture is a single certificate authority. The certificate authority is a standalone self-signed CA. It is the intent of the Bangladesh Root CA to sign only licensed CAs certificate and CRL.

Bangladesh Root conforms to SSL, EV SSL, Code Signing, EV Code Signing guidelines; application trust stores requirements; the current version of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates published at http://www.cabforum.org. In the event of any inconsistency between this document and those requirements, those requirements take precedence over this document.

Bangladesh Root CA Certificate Policy Statement (CPS) is the principal statement of policy governing the Bangladesh Root CA. The CP applies to all subordinate certification authorities under Bangladesh Root CA and thereby provides assurances of uniform trust throughout the Bangladesh Root CA. The CP sets forth requirements that subordinate certification authorities under CCA must meet.

This CPS also sets out the certification service scope and procedures of Bangladesh Root CA, as well as to specify duties, functions, legal obligations and potential liabilities of participants in the systems used by CCA. The document structure and topics conform to ICT Act. 2006, Digital Security Act. 2018, the Internet Engineering Task Force (IETF) RFC 3647 for Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework.

1.2 Document Name and Identification

This document is the Bangladesh Root Certification Authority Certification Practice Statement (CPS). This CPS is published for public knowledge on the CCA Website (http://www.cca.gov.bd).

1.3 PKI Participants

1.3.1 Certification Authority

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

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

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

1.3.2 Registration Authority

The designated officers of CCA acts as the RA and process all licensed CA signing requests including verification of their signing request. The RA performs its function in accordance with the CPS and is responsible for:

- The registration processes.
- The identification and authentication process.

1.3.3 Subscribers

A Subscriber is a person or legal entity whose name appears as the subject in a certificate. The Subscriber asserts the use of the key and certificate in accordance with the Certificate Policy asserted in the certificate. CAs are sometimes technically considered "Subscribers" in a PKI. However, the term "Subscribers" as used in this CPS refers only to "CA Subscribers" who request certificates for signing and issuing certificates or certificate status information. CAs who want to apply for a certificate from Bangladesh Root CA for signing and issuing certificates or certificate status information, and so become a subordinate CA of Bangladesh Root CA and will be qualified as CA Subscriber.

1.3.4 Relying Parties

A Relying Party is a person or legal entity that acts in reliance on the validity of the binding of the subscriber's name to a public key. The Relying Party uses the subscriber's certificate to verify a digital signature that is generated using the private key corresponding to the public key listed in a certificate. The Relying Party may or may not be a subscriber within Bangladesh Root CA.

24.03.2020

1.3.5 Other Participants

1.3.5.1 Policy Authority

A Policy Authority (PA) is a committee setup by the Office of Certifying Authority (CCA). The duty of the PA is to decide a set of requirements for certificate issuance and use is sufficient for a given application. The PA has roles and responsibilities as follows:

- Establishing certificate policy and certification practice statement of Bangladesh Root CA and other certification authorities under the Bangladesh Root CA trust model;
- Arranging for a review of certificate policy and certification practice statement of Bangladesh Root CA and other certification authorities under the Bangladesh Root CA trust model on a regular basis; and
- Promoting trust relationship of Bangladesh Root CA with other domestic or overseas certification authorities.

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

The usage of a certificate issued by Bangladesh Root CA is limited to support the following core security needs:

- Certificate signing – verify the certificate of Subordinate CAs;
- Certificate revocation list (CRL) signing / Online Certificate Status Protocol (OCSP) responder – signs and publishes CRLs.

1.4.2 Prohibited Certificate Uses

A certificate issued by Bangladesh Root CA shall be used only for the purpose as specified in Section 1.4.1, and in particular shall be used only to the extent the use consistent with applicable laws.

1.5 Policy Administration

1.5.1 Organization Administering the Document

This document is administered by Bangladesh Root CA. This document is publicly available with approval from PA.

1.5.2 Contact Person

Office Name	:	Office of the Controller of Certifying Authority
Contact Person	:	Deputy Controller (Deputy Secretary), ICT
Address	:	E-14/X, ICT Tower, Sher-E-Bangla Nagar, Agargaon Dhaka-1207, Bangladesh.
Email	:	dc.ict@cca.gov.bd
Phone	:	+880-2-8181709
Fax	:	+880-2-8181711

1.5.3 Person Determining CPS Suitability for the Policy

The PA shall determine the CPS of each CA that issues certificates under this CP.

1.5.4 CPS Approval Procedures

The CPS approval procedures are as follows:

- CCA proposes CPS changes and submits to the PA.
  - In case the PA has no further comments, the PA approves the CPS.
  - In case the PA has comments, the PA returns the CPS to CCA for proper modification or correction before resubmission.
- CCA announces and publishes the CPS to the channel as listed in Section 2.2.

1.6 Definitions and Acronyms

1.6.1 Definitions

A list of definitions are as below.

Term	*Definition*
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 pass phrase, or a manually-held key share).
Certificate	A form of electronic documents used for verifying the relationship between entities and public key. A certificate is issued in compliance with ITU-T Recommendation X.509 (10/12): Information technology - Open systems interconnection - The Directory: Public-key and attribute certificate frameworks and ISO/IEC 9594-8:2012 Information technology -- Open Systems Interconnection -- The Directory: Public-key and attribute certificate frameworks.
Certificate Policy (CP)	The document, which is entitled "Bangladesh Root CA Certificate Policy", describes the principal statement and applications of certificates.
Certificate Repository	A source for storage and publication of certificates and certificate revocation lists.
Certificate Revocation	A certificate may be revoked prior to its expiration date. Once revoked, it can no longer be used.
Certification Authority (CA)	An entity authorized to issue, manage, revoke, and renew certificates.
Certification Practice Statement (CPS)	The document, which is entitled "Bangladesh Root CA Certification Practice Statement", describes the procedures and scope of the certification authority, duties and obligations of the parties that act in reliance of a certificate.

24.03.2020

Cryptographic Module	The specialized equipment used to maintain, manage and operate the key pair.
Digital Signature	A digital signature is a mathematical scheme for demonstrating the authenticity and integrity of a digital message or document.
Directory Service	A storage for publication of certificates and certificate revocation lists following the X.500 Standard or LDAP.
Entity	An individual or server, operating unit / site, or any device that is under the control of the individual.
Key Pair	A key pair refers to two separate keys of the asymmetric cryptographic system, one of which is secret (Private Key) and another is public (Public Key). The two parts of the key pair are mathematically linked in the ways that one key lock or encrypts the plaintext, and the other unlocks or decrypts the cipher text. Neither key can perform both functions by itself. The key pair can be used to authenticate the digital signature as well as maintain the confidentiality of information.
OCSP (Online Certificate Status Protocol)	A protocol used for verifying status of a certificate.
Private Key	The key used to create a digital signature and can be used to decrypt the message that is encrypted with its pair of public key to obtain the original message.
Public Key	The key used to verify a digital signature to ensure the integrity of electronic message and also to encrypt a message to maintain its confidentiality.

Table 1: Terms and Definitions

24.03.2020

1.6.2 Acronyms

A list of definitions are as below.

Acronym	*Term*
CA	Certification Authority
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DN	Distinguished Name
CCA	Controller of the Certification Authority
PA	Policy Authority
PIN	Personal Identification Number
PKI	Public Key Infrastructure
RA	Registration Authority

Table 2: Acronyms

2 Publication and Repository Responsibilities

2.1 Repositories

CCA posts all issued certificates on the publicly accessible website at the URL http://www.cca.gov.bd. Bangladesh Root CA's publicly trusted root Certificates and its CRLs (http://crl.cca.gov.bd)and OCSP responses are available through online resources 24 hours a day, 7 days a week with systems described in Section 5 to minimize downtime.

2.2 Publication of Certificate Information

CCA shall make information publicly available on their website (www.cca.gov.bd) such as CPs, CPSs, Certificates and CRLs in repositories. For public services, they are available 24 hours per day and 7 days per week. It shall ensure that its repository or repositories are implemented through trustworthy systems.

2.3 Time or Frequency of Publication

CCA shall publish their certificates and CRLs as soon as possible after issuance. CAs shall review CP and CPS at least annually and make appropriate changes. The latest versions of CP and/or CPS are published within three days after updating and of their approval.

2.4 Access Controls on Repositories

CCA has implemented physical access control as well as network security measures to authenticate and restrict modification or deletion to the repository. The adding, deleting, or modifying repository entries can be performed only by authorized personnel of CCA. CCA website is used as repositories to access the published documents.

24.03.2020

3 Identification and Authentication

3.1 Naming

3.1.1 Types of Names

Bangladesh Root CA Certificates contain a Distinguished Name (DN) in the Issuer and Subject fields, following the X.501 Information technology – Open Systems Interconnection – The Directory: Models. The Distinguished Names consist of the components specified in Table 3 below.

Attribute Name	*Value*
Common Name (CN) =	Bangladesh Root CA or <certification authority name>
Organization (O) =	Office of the CCA or <organization name>
OU =	Root CA
Country (C) =	BD

Table 3: Distinguished Name Attributes in certificates

3.1.2 Need for Names to be Meaningful

The names contained in a certificate must be in English with commonly understood semantics permitting the determination of the identity of the individual or organization that is the subject of the certificate, for example, through the verification of Jurisdiction of Incorporation and/or Certificate of Registration issued by the Registrar of Joint Stock Companies and Firms (RJSC).

3.1.3 Anonymity or Pseudonymity of Subscribers

The Bangladesh Root CA that issues certificates under this CP shall not issue anonymous or pseudonymous certificates.

3.1.4 Rules for Interpreting Various Name Forms

Rules for interpreting distinguished name forms are specified in X.501. Rules for interpreting e-mail addresses are specified in RFC 2822.

3.1.5 Uniqueness of Names

The Bangladesh Root CA shall ensure that the set of names is unambiguous. The CCA shall reject a License application or certificate signing request in the case where the name cannot sufficiently distinguish the new CA Applicant from an existing CA's Distinguished Name. The name shall conform to X.500 standards for name uniqueness.

3.1.6 Recognition, Authentication, and Role of Trademarks

The Bangladesh Root CA that issues certificates under this CPS 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 to the relevant laws, regulations, legal obligations or announcements.

24.03.2020

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

The CA Authorized person should submit letter of authorization to CCA in this regard and the digital signature in their certificate request message is required as well to proof their possession of the private key.

3.2.2 Authentication of Organization and Domain Identity

The Licensed CAs, while request for certificate signing to CCA, requires to show the following documents:

- Original CA License document;
- Attested copy of Incorporation Certificate (in case of Limited company)/Attested copy of any other form of company registration;
- Approved copy of CPS;
- Report submitted by the empaneled auditor of CCA; and
- Any other document ask by CCA in this regard.

3.2.3 Authentication of Individual Identity

CCA does not issue certificates to individual entity.

3.2.4 Non-verified Subscriber Information

All CA Subscriber's information contained in a certificate is verified.

3.2.5 Validation of Authority

CCA follows Section 3.2.5 of CA/B Forum Baseline Requirements.

3.2.6 Criteria for Interoperation

The PA promotes interoperation between CAs issuing certificates under the Bangladesh Root CA trust model and other CAs which may or may not issue certificates under the Bangladesh Root CA trust model (for example, overseas CA(s)). CCA will interoperate with other Certification Authorities after signing the agreement or Memorandum of Understanding (MOU) on behalf of all CAs.

3.3 Identification and Authentication for Re-key Requests

3.3.1 Identification and Authentication for Routine Re-key

Identification and authentication procedure are specified in Section 3.2.

3.3.2 Identification and Authentication for Re-key after Revocation

Identification and authentication procedure are specified in Section 3.2.

3.4 Identification and Authentication for Revocation Request

Identification and authentication procedure 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

Only the licensee (as certifying authority) under Office of the CCA, who has completed their initial audit with fair score and completed their Key Generation, can submit certificate application to CCA.

4.1.2 Enrollment Process and Responsibilities

CAs must complete Digital Signature Certificate Application Form and submit it to CCA as per Bangladesh ICT Act 2006 (Amendment 2009) and applicable laws including the required documenting evidences. By submitting a certificate application, the CA authorizes the publication of the certificate to the CCA repository and thus accepts the certificate to be issued to the CA. This section is to list all the necessary documents required to be submitted by the applicant to CCA. Example:

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

After receiving a certificate application, CCA verifies the application information and other information in accordance with Section 3.2.

CCA does not perform any CAA record checking as there are no FQDNS certificate issuance.

If an RA assists in the verification, the RA must create and maintain records sufficient to establish that it has performed its required verification tasks and communicate the completion of such performance to CCA. After verification is complete, CCA evaluates the corpus of information and decides whether or not to issue the Certificate. As part of this evaluation, CCA checks the Certificate against an internal database of previously revoked Certificates and rejected certificate requests to identify suspicious certificate requests. If some or all of the documentation used to support an application is in a language other than English, an CCA employee, RA, or agent skilled in the language performs the final cross-correlation and due diligence.

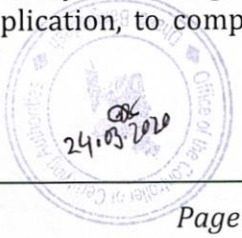
CCA considers a source's availability, purpose, and reputation when determining whether a third party source is reasonably reliable. CCA does not consider a database, source, or form of identification reasonably reliable if CCA or the RA is the sole source of the information.

4.2.2 Approval or Rejection of Certificate Applications

Any certificate application that is received by CCA for which the identity and authorization of the applicant has been validated, will be duly processed. However, CCA will reject any application for which such validation cannot be completed.

4.2.3 Time to Process Certificate Applications

Certificate applications must be processed within 10 business days, counting from the date that CA or RA endorses the receipt of a certificate application, to complete the processing of the application.



4.3 Certificate Issuance

4.3.1 CA Actions during Certificate Issuance

Following the identity verification process, CCA will notify the CA Subscriber the approval of application. Hence, the certificate issuance process is as follows:

1. CA Subscriber generates a key pair on its own device and a Certificate Signing Request (CSR) that conforms to PKCS # 10: Certificate Request Syntax Standard. The CSR contains the identity of CA Subscriber organization and the public key. The private key must be secured in the hardware security module.
2. Upon receipt of the CSR, CCA will verify that the applicant is in possession of the corresponding Private Key by checking the digital signature on the CSR structure containing the public key material and CAO must verify and ensure that information in CSR must conform in Section 6. If not conform in Section 6, CAO should reject. CCA will not have possession of the applicants' Private Keys.
3. Upon verifying the applicant's possession of its Private Key, CCA will generate the certificate in which the applicant's public key will be included.
4. The certificate will be delivered to the authorized representative in a secure manner such as by hand or by registered mail.
5. Upon CCA acknowledgement of certificate acceptance by the authorized representative, the issued certificate will be published in the CCA Repository together with its thumbprint for verifying the Subordinate CA authenticity on CCA website.
6. Applicants can either verify the information on the certificate by browsing the certificate file or through CCA Repository. Applicants should notify CCA immediately of any incorrect information of the certificate.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

CCA will notify the CA Subscriber the creation of a certificate and make the certificate available to the CA Subscribers.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

Upon the receipt of a certificate, the CA Subscriber must verify the information contained in the certificate and determine whether to accept or reject the certificate. The CA Subscriber may notify CCA if it accepts the certificate or rejects the certificate for some reasons. If the CA Subscriber fails to notify CCA the rejection of the issued certificate within ten business days, the certificate will be revoked.

4.4.2 Publication of the Certificate by the CA

CCA will publish the issued certificates to Publication Channel of Certification Information within one business day after being notified by the CA Subscriber.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

Bangladesh Root CA will notify the PA whenever a certificate is issued to a CA.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

CA Subscriber can use the Private Key corresponding to the Public Key in the certificate, which issued by CCA, in order to issue subscriber certificates signing with its digital signature to other subscribers or sign the certificate revocation list in relation to those subscriber certificates. Subscriber certificates shall be used lawfully in accordance with the CP, CPS and Terms of Service of CCA.

4.5.2 Relying Party Public Key and Certificate Usage

Before any act of reliance, Relying Parties shall assess the certificate as follows:

- The accuracy of the digital signature in the CA's certificate and subscriber hierarchy (e.g.: path validation).
- The validity period of the certificates of CAs and subscribers, e.g.: the certificates should not expire by the time of use.
- The status of the certificate and all the CAs and their parent in every level of the hierarchy involved, e.g.: the certificate should not be revoked or suspended.
- Certificate usage shall be in accordance with Section 1.4.

4.6 Certificate Renewal

4.6.1 Circumstance for Certificate Renewal

Bangladesh Root CA may renew a Certificate if:

1. The associated public key has not reached the end of its validity period
2. The associated private key has not been compromised
3. The subscriber and attributes remain consistent
4. No new or additional validation is required

4.6.2 Who May Request Renewal

Certificate Renewal means the issuance of a new Certificate without changing the Public Key or any other information in the Certificate, except the validity period.

Bangladesh Root CA may accept a renewal request provided that it is authorized by the original subscriber using a passphrase or any kind of shared secret or any other form of subscriber authentication mechanism. A Certificate Signing request is not mandatory, however if one is used, then it must contain the same public key.

4.6.3 Processing Certificate Renewal Requests

Bangladesh Root CA may request additional information before processing a renewal request.

4.6.4 Notification of New Certificate Issuance to Subscriber

The notification to subscriber for renewal certificate shall be same as the process defined in this CPS for new certificate issuance notification to Certificate Holder.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

The conduct constituting the certificate acceptance for renewal shall be same as the process defined in this CPS for new certificate acceptance.

24.03.2020

4.6.6 Publication of the Renewal Certificate by the CA

The publication of certificate in case of renewal shall be same as the process defined in this CPS for new certificate publication.

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

The notification to other entities for renewal certificate shall be same as the process defined in this CPS for new certificate issuance notification to other entities.

4.7 Certificate Re-key

Re-keying a certificate consists of creating new certificates with a different public key (and serial number) while retaining the remaining contents of the old certificate that describe the subject. The new certificate may be assigned a different validity period, key identifiers, specify a different CRL distribution point, and/or be signed with a different key. Re-key of a certificate does not require a change to the subject name and does not violate the requirement for name uniqueness. The old certificate may or may not be revoked, but must not be further re-keyed, renewed, or modified.

4.7.1 Circumstance for Certificate Re-key

CCA requires its CA Subscribers to re-key the certificate in the following cases:

- CA Subscriber's certificate has less than 5 years before expiration or has already expired.
- CA Subscriber's certificate has been revoked.
- CA Subscriber needs to modify information in the certificate.

4.7.2 Who May Request Certification of a New Public Key

Only the Licensed CAs may request a new certificate.

4.7.3 Processing Certificate Re-keying Requests

CA Subscribers must follow the procedures of certificate re-keying requests as specified in Section 4.1.2.

4.7.4 Notification of New Certificate Issuance to Subscriber

CCA notifies the result of new certificate issuance to its CA Subscriber according to the procedures specified in Section 4.3.2.

4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate

After CA Subscribers receive re-keyed certificate, they must follow the procedure in Section 4.4.1 to accept the re-keyed certificate.

4.7.6 Publication of the Re-keyed Certificate by the CA

CCA publishes the re-keyed according to the procedure in Section 4.4.2.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

CCA notifies the result of certificate issuance to other entities according to the procedure in Section 4.4.3.

4.8 Certificate Modification

Modifying a certificate means creating a new certificate that has the same or a different key and a different serial number, and that differs in one or more other fields from the old certificate. The old certificate may or may not be revoked, but must not be further re-keyed, renewed, or modified.

4.8.1 Circumstance for Certificate Modification

Since the interpretation of modifying certificate contents are sometimes complex, CCA does not offer certificate modification. If a circumstance for certificate modification is deemed to arise, re-certification will be followed, that means the initial registration process as described in section 3.2 will be gone through again. The new certificate shall have a different subject public key.

4.8.2 Who May Request Certificate Modification

Not Applicable.

4.8.3 Processing Certificate Modification Requests

Not Applicable.

4.8.4 Notification of New Certificate Issuance to Subscriber

Not Applicable.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

Not Applicable.

4.8.6 Publication of the Modified Certificate by the CA

Not Applicable.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

Not Applicable.

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for Revocation

4.9.1.1 Reasons for Revoking a Subscriber Certificate

Not Applicable.

4.9.1.2 Reasons for Revoking a Subordinate CA Certificate

CCA SHALL revoke a Subordinate CA Certificate within seven (7) days if one or more of the following occurs:

1. CCA suspend or revoke the license as per Section 26 (1) of the ICT Act 2006 (amended in 2009);
2. The licensee breach any direction made upon as per the ICT Act 2006 (amended in 2009), IT (CA) Rules 2010, License Document and other guidelines issued by CCA;
3. The information in the licensed CA certificate is suspected to be inaccurate;
4. The Subordinate CA requests revocation in writing;
5. The Subordinate CA notifies CCA that the original certificate request was not authorized and does not retroactively grant authorization;
6. CCA obtains evidence that the Subordinate CA's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise or no longer complies with the requirements of section 6.1.5 and 6.1.6 in CA/Browser Forum Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates;
7. The Issuing CA obtains evidence that the Certificate was misused;
8. CCA is made aware that the Certificate was not issued in accordance with or that Subordinate CA has not complied with this CP or the applicable Certificate Policy or Certification Practice Statement;
9. CCA determines that any of the information appearing in the Certificate is inaccurate or misleading;
10. CCA or Subordinate CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate;
11. CCA's or Subordinate CA's right to issue Certificates under these Requirements expires or is revoked or terminated, unless the Issuing CA has made arrangements to continue maintaining the CRL/OCSP Repository;
12. Revocation is required by the Issuing CA's Certificate Policy and/or Certification Practice Statement; or
13. The technical content or format of the Certificate presents an unacceptable risk to Application Software Suppliers or Relying Parties (e.g. the CA/Browser Forum might determine that a deprecated cryptographic/signature algorithm or key size presents an unacceptable risk and that such Certificates should be revoked and replaced by CAs within a given period of time).
14. Any other reason deems required revocation of the certificate of the licensee by CCA.

4.9.2 Who Can Request Revocation

A request to revoke a licensed CA certificate can be done by the following entities:

- The licensee or any other official signatory of the licensed CA organization can request for revocation with proper reason.
- CCA can also initiate revocation of certificate of the licensed if any reason found as per 4.9.1

4.9.3 Procedure for Revocation Request

CA Subscriber requesting revocation is required to follow the procedures such as:

1. The CA Subscriber submits the revocation request and related documents to CCA, or a RA of the CA, providing that the information is genuine, correct and complete.
2. CCA verifies and endorses the revocation requests and the related documents.
3. The RA is responsible for verifying and authenticating an authorized representative of a juristic person by following the procedures as specified in Section 3.2.
4. CCA, if necessary with the assistance of the RA, will approve and process the revocation request.
5. CCA, if necessary with the assistance of the RA, will inform the revocation result to the CA Subscriber and the PA.

4.9.4 Revocation Request Grace Period

There is no grace period for revocation under this CPS.

4.9.5 Time within Which CA Must Process the Revocation Request

CCA shall revoke certificates as quickly as practical, or within one business day after the revocation request is endorsed.

4.9.6 Revocation Checking Requirement for Relying Parties

Relying Parties are responsible for checking the validity of each certificate in the certificate path, including checks for certificate validity, issuer-to-subject name chaining, certificate policy and key usage constraints, and the status of the certificate through the Certificate Revocation List (CRL).

4.9.7 CRL Issuance Frequency

CRL will be issued as soon as CCA revokes any certificate or will be refreshed every six months.

4.9.8 Maximum Latency for CRLs

CRLs are published to repository within 30 minutes of generation.

4.9.9 On-line Revocation/Status Checking Availability

On-line status checking is provided by CCA, where on-line status checking is supported, status information is updated and available to relying parties within 30 minutes of CRL publication.

4.9.10 On-line Revocation Checking Requirements

Relying Parties shall check the validity of a certificate via CRL or OCSP before relying on the Certificate.

Failure to do so negates the ability of the Relying Party to claim that it acted on the Digital Certificate with reasonable reliance.

The OCSP URL is provided as part of the Digital Certificate, wherever applicable. The OCSP requests supports both GET and POST requests. The OCSP responder does not respond 'good' response, in case the certificate has not been issued.

Licensed CA certificates, the updates are made once in every 6 (six) months, or within 30 minutes of a revocation of Subordinate CA.

4.9.11 Other Forms of Revocation Advertisements Available

Not Applicable.

4.9.12 Special Requirements Regarding Key Compromise

CCA, the CA Subscriber and subscribers must notify Relying Parties as soon as practical regarding its key compromise.

4.9.13 Circumstances for Suspension

Under no circumstances a certificate would be suspended. If a certificate is no longer considered as valid, it will be revoked.

4.9.14 Who Can Request Suspension

Not Applicable.

4.9.15 Procedure for Suspension Request

Not Applicable.

4.9.16 Limits on Suspension Period

Not Applicable.

4.10 Certificate Status Services

4.10.1 Operational Characteristics

The status of certificates is available through the CCA's website.

4.10.2 Service Availability

CCA has implemented backup systems for providing certificate status services and put the best efforts to make such services available 24x7.

4.10.3 Optional Features

Not Applicable.

4.11 End of Subscription

The CA Subscriber may end a subscription by allowing its certificate to expire or revoking its certificate without requesting a new certificate.

4.12 Key Escrow and Recovery

4.12.1 Key Escrow and Recovery Policy and Practices

Not Applicable.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

Private Keys of a CA that issues certificates under the CCA are never escrowed.

5 Facility, Management, and Operational Controls

5.1 Physical Controls

5.1.1 Site Location and Construction

Bangladesh Root CA located at two secure facilities i.e. the main site is located at Office of the CCA, ICT Tower, Agargaon, Dhaka and the disaster recovery site in a geographic location reasonably apart from the main site. The Root CA construction is made complying best practices and proper security controls. The Root CA system is designed to have isolated collocation trust center in order to maintain utmost security.

- Zone 1 is the highest security trust zone as isolated offline data zone.
- Zone 2 is the secured data center (tier-3 certified) for publicly available Publishing zone.

Zone 1, the Key Generation and Signing Room is an offline zone inside a secure strong room with 6 tier of physical security layer.

Both secure facilities are equipped with physical access controls as follows:

- Six layers of physical access controls.
- Two-factor authentication for accessing the server rooms.
- CCTVs (Closed Circuit Televisions) record the activity in the server room at all times.
- Smoke detector and fire extinguisher (using electronic equipment safe agent) systems.

The server rooms are accessible by the CCA authorized personnel only. If a visitor required to access the room, authorization from CCA must be provided in order to allow that person to enter the server room. At all time, such a person accompanied by the CCA authorized person. Certificate issuing servers and Cryptographic Module are stored in a separate rack where physically accessing to such systems requires a user to perform a two-factor authentication.

5.1.2 Physical Access

The CCA Data center maintains a restricted access procedure for authorized personnel only. In case that a third party who need to access the service area of CCA, prior authorization must be obtained. All visits to the CCA premise recorded in the access log. At all time, third parties accompanied by the CCA officer during the whole visit. Certificate issuing servers and Cryptographic Module are stored in a secure rack where physical access to such systems requires dual control and two-factor authentication. Six tiers of access control is present –

- 1st tier: Main entrance, it is controlled with biometric and card based access control.
- 2nd tier: Door with manual lock.
- 3rd tier: 1st Iron door of strong room.
- 4th tier: 2nd door of strong room.
- 5th tier: 3rd Iron door of strong room.
- 6th tier: 4th Iron door of strong room.

The servers are kept inside a Rack which is also protected.

5.1.3 Power and Air Conditioning

An online UPS is located to ensure power supply for Root CA Offline Zone. The UPS is connected with main power supply. The entire site is equipped with central A/C of ICT Tower. Inside the strong room, a separate A/C is mounted, as central A/C is not reachable inside strong room.

The publishing zone has power supply and air conditioning as required by a tier-3 certified data center.

5.1.4 Water Exposures

Water exposure is controlled by central A/C system. A water disposal pipe is mounted for the A/C inside the strong room. Water from the dehumidifier is disposed.

5.1.5 Fire Prevention and Protection

The certificate issuing area is equipped with a smoke detector where the fire extinguisher will be automatically activated when the smoke is detected. The certificate issuing area is equipped with fire extinguishing system that operates quickly and effectively without causing damage to electrical equipment.

5.1.6 Media Storage

All magnetic media holding back ups of critical system data or any other sensitive information are protected from water, fire, or other environmental hazards, and protective measures are in place to deter, detect, and prevent the unauthorized use of, access to, or disclosure of such media.

5.1.7 Waste Disposal

CCA has implemented procedures for the disposal of waste (paper, media, or any other waste) to prevent the unauthorized use of, access to, or disclosure of waste containing Confidential/Private Information.

5.1.8 Off-site Backup

A backup media is stored at the secure disaster recovery facility.

5.2 Procedural Controls

5.2.1 Trusted Roles

A trusted role is one whose incumbent performs functions that can introduce security problems if not carried out properly, whether accidentally or maliciously. It is essential that the people selected to fill these roles shall be held accountable to perform designated actions correctly or the integrity of the CA is weakened. The functions performed in these roles form the basis of trust in the CA. CCA takes two approaches to increase the likelihood that these roles can be successfully carried out:

- The first approach is to minimize the number of trusted roles and ensure that the people filling those roles are trustworthy and properly trained.
- The second is to enforce the concept of least privilege and distribute the functions of the roles among several people, so that any malicious activity requires collusion.

Trusted role operations include:

- The validation, authentication, and handling of information in Certificate Applications.
- The acceptance, rejection, or other processing of Certificate Applications, revocation requests renewal requests, or enrollment information.
- The issuance, or revocation of Certificates, including personnel having access to restricted portions of its repository.
- Access to safe combinations and/or keys to security containers that contain materials supporting production services.
- Access to hardware security modules (HSMs), their associated keying material, and the secret share splits of the PINS that protect access to the HSMs.
- Providing enterprise customer support.
- Access to any source code for the digital certificate applications or systems.
- Access to restricted portions of the certificate repository.
- The ability to grant physical and/or logical access to the CA equipment.
- The ability to administer the background investigation policy processes.

Multiple people may hold the same trusted role, with collective privileges sufficient to fill the role. Other trusted roles may be defined in other documents, which describe or impose requirements on the CA operation.

CA defines trusted roles and rights as follows:

- Policy Authority (PA)
- Certification Authority Manager (CAM)
- Certification Authority Officer (CAO)
- Registration Authority Officer (RAO)
- Security Officer (SO)
- System Administrator (SA)
- Network Administrator (NA)
- Software Developer (SD)
- Internal Auditor (IA)

Below table 4 shows the Position, Roles and Rights mapping for CCA.

Position	*Trusted Roles*	*Rights*
Committee	Policy Authority (PA)	• Issue and approve the policy and the CP/CPS of the Bangladesh Root CA and other certification authorities.
	Certification Authority Manager (CAM)	• Access to the certificate issuing facilities. • Access to the Cryptographic Module and give authorization to who can access the Cryptographic Module
	Certification Authority Officer (CAO)	• Access to the list of CA Subscribers • Access to the personal information of CA subscribers.
	Registration Authority Officer (RAO)	• Access to the list of CA Subscribers. • Access to the personal information of CA subscribers.
	Security Officer (SO)	• Access to audit logs • Access to the certificate issuing and supporting facilities. • Hold all privilege account passwords for all systems.
	System Administrator (SA)	• Access to the certificate issuing facilities • Hold the multi-person control token for managing the Cryptographic Module
	Network Administrator (NA)	• Access to the facilities in relation to certificate issuance; • Access to the configuration of equipment such as network, firewall, antivirus, backup, etc.
	Software Developer (SD)	• Access to the facilities in relation to software development
	Internal Auditor (IA)	• Access to information in relation with audit matters on a need to know basis

Table 4: Position, Roles and Rights Mapping

5.2.2 Number of Persons Required per Task

Where multi-party control is required, all participants shall hold a trusted role. Multi-party control shall not be achieved using personnel that serve in a Security Auditor role with the exception of audit functions. The following tasks shall require two or more persons:

- Generation, activation, and backup of CA keys.
- Performance of CA administration or maintenance tasks.
- Archiving or deleting CA audit logs. At least one of the participants shall serve in a Security Auditor role.
- Physical access to CA equipment.
- Access to any copy of the CA cryptographic module.
- Processing of third party key recovery requests.

For the tasks that require access to the CCA's private key, issuing a certificate, and revoking a certificate, such tasks require at least two authorized officers from the trusted roles.

5.2.3 Identification and Authentication for Each Role

CCA have confirmed the identity and authorization of all personnel seeking to become Trusted before such personnel are:

- issued with their access devices and granted access to the required facilities.
- given electronic credentials to access and perform specific functions on Information Systems and CCA.

Individuals holding trusted roles identify themselves and be authenticated by CCA before being permitted to perform any actions set forth above for that role or identity. CCA Operations Staff have authenticated using a credential that is distinct from any credential they use to perform non-trusted role functions. This credential is generated and stored in a system that is protected to the same level as the CA system.

CCA equipment are under strong authenticated access control for remote access using multi-factor authentication. CCA equipment required, at a minimum, authenticated access control (e.g., strong passwords) for local multi-party access. Individuals holding trusted roles appointed to the trusted role by an appropriate approving authority. The approvals are recorded in a secure and auditable fashion.

Individuals holding trusted roles accept the responsibilities of the trusted role, and this acceptance is recorded in a secure and auditable fashion. Users authenticated themselves to all aspects of the network (servers, operating systems, applications, databases, processes, and so on) before they can access that resource.

5.2.4 Roles Requiring Separation of Duties

No individual will be assigned more than one trusted Role.

5.3 Personnel Controls

5.3.1 Qualifications, Experience and Clearance Requirements

Qualification, Experience and clearance of the CA operations personnel are verified as per standard recruitment rules and regulations of the Government of Bangladesh.

5.3.2 Background Check Procedures

Background check is performed as per standard recruitment rules and regulations of the Government of Bangladesh.

5.3.3 Training Requirements

CCA provides its officers with appropriate training as well as the requisite on-the-job training needed to perform their job responsibilities related to Root CA operations with competency and satisfaction. The training programs include the following as relevant:

- Basic cryptography and Public Key Infrastructure (PKI) concepts
- This CP/CPS
- Cryptography
- Documented Root PKI security and operational policies and procedures
- Information Security Awareness
- Use and operation of deployed hardware and software related to Root CA operations
- Common threats to the validation process including phishing and other social engineering Tactics
- Security Risk Management
- CA/Browser forum guidelines
- Disaster recovery and Business continuity procedures

5.3.4 Retraining Frequency and Requirements

CCA provides its officers with appropriate training at least once a year on the related topics and Information Security Awareness. Whenever there is any change in the Issuer CA's or RA's operations appropriate training is provided to the individuals acting in trusted roles so that they are aware of the changes.

5.3.5 Job Rotation Frequency and Sequence

Job rotation frequency for every role is 6 months.

5.3.6 Sanction for Unauthorized Actions

CCA will take administrative and disciplinary action against personnel who perform unauthorized actions involving CA or its repository or anything subversive to the trust of Bangladesh PKI as per ICT Act 2006 (amended in 2009) and government policy.

5.3.7 Independent Contractor Requirements

In case that independent contractors or consultants is employed and is obliged to pass the background check procedures specified in Section 5.3.2. Any such contractor or consultant are only permitted to access to CCA's secure facilities if they are escorted and directly supervised by trusted CCA officers at all times.

For system maintenance purposes, operating staffs must present their employee identification card to Trusted Persons of CCA for verification and record. They are also escorted and directly supervised by trusted CCA officers at all times.

5.3.8 Documentation Supplied to Personnel

All the policies, guidelines, CP, CPS and any relevant documents issued by CCA will make available to its personnel required to perform their job responsibilities competently and satisfactorily.

24/03/2020

5.4 Audit Logging Procedures

5.4.1 Types of Events Recorded

CCA logs the following significant events:

- CA Key Life Cycle Management, including:
  - Key generation, backup, storage, recovery, archival, and destruction
  - Cryptographic Module life cycle management events
- CA and Subscriber certificate life cycle management events, including:
  - Certificate Applications, rekey, and revocation
  - Approval or rejection of requests
  - Generation and issuance of certificates and CRL
- Security-related events including:
  - Successful and unsuccessful access attempts to Root CA systems
  - Security system actions performed by CA officers
  - Security profile changes
  - System crashes, hardware failures and other anomalies
  - Firewall, Router and Switches activities
  - Root CA facility visitor's entry/exit
  - System startup and shutdown
  - CA Application startup and shutdown

Log entries include the following elements:

- Date and time of entry;
- Identity of the person making the journal entry; and
- Description of the entry.

5.4.2 Frequency of Processing Log

Audit logs for security-related events and for Key Life Cycle Management & CA certificate life cycle management events are examined at least every six months. CRL/OCSP logs are examined monthly basis.

5.4.3 Retention Period for Audit Log

Logs of aforementioned events are preserved for 7 years. Root CA does backup all audit logs and audit results.

5.4.4 Protection of Audit Log

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

5.4.5 Audit Log Backup Procedures

CCA performs backup all audit data as per section 5.5

24.03.2020

5.4.6 Audit Log Accumulation System (Internal vs. External)

The audit data is generated and recorded at the machine that the event has occurred and at the audit log system.

5.4.7 Notification to Event-Causing Subject

Not Applicable.

5.4.8 Vulnerability Assessments

CCA performs vulnerability assessments quarterly. 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.

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

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

5.4.9 Penetration Test Assessments

CCA assess security Penetration Test assessment annually.

5.5 Records Archival

5.5.1 Types of Records Archived

CCA archives:

- CA systems
  - All audit data specified in 5.4.1
  - System configuration
  - Website
- Documentation supporting certificate applications
  - Certificates, CRLs, and expired or revoked certificates
  - CP and CPS
  - Email Correspondences
- Certificate lifecycle information
  - Forms such as Application Form, Revocation Request Form, Re-key Request Form, and Certificate Acceptance Form
  - Required documents for application
  - Internal documents such as procedure manuals and system access approval request
  - Letters or memos used for communication between CA and external parties such as, CCA, Subscriber and other CAs.

5.5.2 Retention Period for Archive

Records retains for at least 7 years, unless there are specific requirements.

5.5.3 Protection of Archive

Records archival are stored in secure facilities and are accessed only by authorized persons.

5.5.4 Archive Backup Procedure

Records archival are backed up in every six months as below procedures:

- Paper-based event records are converted into electronic format before being stored and backed up.
- CCA backups event records specified in Section 5.5.1.

5.5.5 Requirements for Time Stamping of Records

Certificates, CRLs and other revocation database entries contain time and date information. Also all the system log are time-stamped.

5.5.6 Archive Collection System (Internal or External)

Archive Collection System is internal to CCA only.

5.5.7 Procedures to Obtain and Verify Archive Information

Procedures to obtain and verify archive information are as follows:

1. CCA submits access request to archive information to PA specifying reasons and necessity of obtaining such information as well as identifying the type of information needed.
2. The PA justifies the appropriateness and necessity of the request and notifies the decision result to the requester.
3. An authorized CCA officer obtains the archive information, defines access rights, and forwards to the requester.
4. The requester verifies the integrity of information.

5.6 Key Changeover

To minimize risk from compromise of Bangladesh Root CA's private signing key, that key may be changed often. From that time on, only the new key will be used to sign subscriber certificates.

CCA's signing keys shall have a validity period as described in section 6.3.2.

When Bangladesh Root CA updates its private signature key and thus generates a new public key, CCA shall notify all CAs, RAs, and subscribers that rely on the CA's certificate that it has been changed.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

If compromise of Bangladesh Root CA is suspected, an independent third-party investigation shall be performed in order to determine the nature and the degree of damage. Certificates issuance shall be stopped immediately upon detection of a compromise. If a Bangladesh Root CA private signing key is suspected of compromise, the procedure outlined in section 5.7.3 shall be followed. Otherwise, the scope of potential damage shall be assessed in order to determine if Bangladesh Root CA needs to be rebuilt,

24.03.2020

only some certificates need to be revoked, and/or the Bangladesh Root CA private key needs to be declared compromised.

In case that there is an event that affects the security of Bangladesh Root CA system, the corresponding CCA officers shall notify the PA if any of the following occur:

- Suspected or detected compromise of any Bangladesh Root CA system or subsystem.
- Physical or electronic penetration of any Bangladesh Root CA system or subsystem.
- Successful denial of service attacks on any Bangladesh Root CA system or subsystem.
- Any incident preventing Bangladesh Root CA from issuing and publishing a CRL or on-line status checking prior to the time indicated in the nextUpdate field in the currently published CRL, or the certificate for on-line status checking suspected or detected compromise.

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

In case of software, hardware or data failure, CCA officers will report such incidents to the upper authorities in order to make decisions and deal with the incident properly. If it is necessary, a disaster recovery plan may be used to restore Bangladesh Root CA services.

5.7.3 Entity Private Key Compromise Procedures

In the case of Bangladesh Root CA compromise, CCA shall notify the PA and relying parties via public announcement of the Bangladesh Root CA compromise so that they can revoke any Subordinate CAs and notify all CA Subscribers and Relying Parties to remove the trusted self-signed certificate from their trust stores. Notification shall be made in an authenticated and trusted manner. Initiation of notification to the PA and any Sub CAs shall be made at the earliest feasible time and shall not exceed 24 hours beyond determination of compromise or loss unless otherwise required by law enforcement. Initiation of notification to relying parties and CA subscribers will be made after mediations are in place to ensure continued operation of applications and services. If the cause of the compromise can be adequately addressed, and it is determined that the PKI can be securely re-established, Bangladesh Root CA shall then generate a new root certificate, solicit requests and issue new certificates, securely distribute the new root certificate, and re-establish any CA certificates.

In case of a subordinate CA key compromise, the subordinate CA shall notify the PA and CCA. CCA shall revoke that subordinate CA's certificate, and the revocation information shall be published immediately in the most expedient, authenticated, and trusted manner but within 24 hours after the notification. The compromised subordinate CA shall also investigate and report to the PA and CCA what caused the compromise or loss, and what measures have been taken to preclude recurrence. If the cause of the compromise can be adequately addressed and it is determined that the subordinate CA can be securely re-established, then the subordinate CA shall be re-established. Upon re-establishment of the subordinate CA, new subscriber certificates shall be requested and issued again. When a certificate of the subordinate CA is revoked because of compromise, suspected compromise, or loss of the private key, a CRL shall be published at the earliest feasible time by the subordinate CA, but in no case more than 6 hours after notification.

In case of an RA compromise, CA will disable the RA. In the case that the RA's key is compromised, CA will revoke it, and the revocation information shall be published within 24 hours in the most expedient, authenticated, and trusted manner. The compromise will be investigated by CA in order to determine the actual or potential date and scope of RA compromise. All certificates approved by that RA since the date of actual or potential RA compromise shall be revoked. In the event that the scope is indeterminate, then the CA compromise procedures as specified in above shall be followed.

5.7.4 Business Continuity Capabilities after a Disaster

CCA has prepared a disaster recovery plan which have been tested, verified and continually updated. A full restoration of services will be done within 24 hours in case of disaster.

5.8 CA or RA Termination

If Root CA terminates its operation by the government policy or acts or whatsoever, CCA shall set forth what actions are to be taken to ensure continued support for certificates previously issued. At a minimum, such actions shall include preservation of the components Bangladesh PKI for at least 7 years as per the IT (CA) Rules 2010. The responsibility for such preservation is on CCA, licensed CAs and other third parties or relying parties.

If there is any circumstance to terminate the services of CCA with the approval of the PA, CCA will notify the subordinate CAs, RAs, the subscribers and all relying parties. The action plan is as follow:

- Notify status of the service to affected users.
- Revoke all certificates.
- Long-term store information of Bangladesh Root CA, its Subordinate CA and subscribers according to the period herein specified.
- Provide ongoing support and answer questions.
- Properly handle key pair and associated hardware.

6 Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

Cryptographic keying material used by Bangladesh Root CA to sign certificates, CRLs or status information are generated in FIPS 140-2 Level 3 or equivalent standard validated cryptographic modules. Multi-party control is required for Bangladesh Root CA key pair generation, as specified in section 6.2.2.

Bangladesh Root CA will generate its own key pair with a ceremony known as Root Key Generation Ceremony (RKGC). The Root Key Generation Ceremony (RKGC) is a formal procedure, and will be done maintaining multi person control. The documentation of the procedure has shown that appropriate role separation was used. An independent third party has validated the execution of the key generation procedures by witnessing the key generation, as well as by examining the signed and documented record of the key generation.

CA Subscriber key pair generation shall be performed by the CA subscriber. The CA subscriber is required to generate the signature key pairs for the purpose of digital signature by FIPS 140 validated hardware cryptographic modules to support source authentication.

6.1.2 Private Key Delivery to Subscriber

CA Subscribers must generate the key pair by themselves. CCA has no policy to generate a key pair for CA subscribers.

6.1.3 Public Key Delivery to Certificate Issuer

CA Subscribers are required to submit Certificate Signing Request in the form of PKCS # 10 standard with the application by themselves.

6.1.4 CA Public Key Delivery to Relying Parties

Relying parties can access Bangladesh Root CA public key in the certificate by the published channel.

6.1.5 Key Sizes

Currently, Bangladesh Root CA has one root certificate and this root certificate contains a public key of RSA 2,048 bits key length and is signed with the corresponding private key by using SHA-512 signature algorithm. . For Code Signing and EV Code Signing minimum key sizes of 4096 bits. Find table 5 for the key requirements.

Key sizes shall be assessed by the PA at least once a year or as necessary especially in an incident that is believed to significantly impact trustworthiness of Bangladesh Root CA.

Subordinate CAs of Bangladesh Root CA will also use the same signature algorithm of Bangladesh Root CA and a key size no larger than that of Bangladesh Root CA.

Bangladesh Root CA root certificate and CAs that issues certificates and CRLs under this CP should use the SHA256, or SHA-384, or SHA-512 hash algorithm when generating digital signatures. CAs that issue certificates signed with SHA-256, or SHA-384, or SHA-512 must not issue certificates signed with SHA-1.

24.03.2020

Algorithm	All Uses Except for Code Signing and Time Stamping	Code Signing and Time Stamping Use
Digest Algorithms	SHA1 may submit until January 1, 2016 SHA2 (SHA256, SHA384, SHA512)	SHA1 may submit until January 1, 2016 SHA2 (SHA256, SHA384, SHA512)
RSA	2048	4096 (New roots only)
ECC / ECDSA	NIST P-256, P-384, P-521	NIST P-256, P-384, P-521

Table 5: Key requirement

6.1.6 Public Key Parameters Generation and Quality Checking

Not Applicable.

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

The use of a specific key is constrained by the key usage extension in the X.509 certificate. All certificates include a critical key usage extension.

Bangladesh Root CA allows using its key pair for digital signature verification, signing certificate to other certification providers (Certificate Signing) and certificate revocation (CRL Signing).

The Public key that is bound into issued certificates is used only for signing certificates and status information such as CRLs. Only Bangladesh Root CA shall issue certificates to CAs located in Bangladesh.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

Bangladesh Root CA uses a FIPS 140-2 Level 3 validated hardware cryptographic module for signing operations. The Subordinate CA of Bangladesh Root CA shall use a FIPS 140-2 Level 3 or higher validated hardware cryptographic module for signing operations.

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

Accessing the private key of Bangladesh Root CA performs by at least two persons with Trusted Role.

6.2.3 Private Key Escrow

Bangladesh Root CA does not allow to keep the private key with other parties or keep its subscribers' private key.

6.2.4 Private Key Backup

Bangladesh Root CA's private signature key is backed up under the same multiparty control as the original signature key. More than one copy of the private signature key are stored off-site. All copies of the CA private signature key are accounted for and protected in the same manner as the original. Bangladesh Root CA backup its private signature key in FIPS 140-2 Level 3 validated hardware cryptographic module.

6.2.5 Private Key Archival

Bangladesh Root CA private key beyond the validity period will be kept at least 10 years and stored in Cryptographic Module with FIPS 140-2 Level 3 standards.

6.2.6 Private Key Transfer into or from a Cryptographic Module

The backup of the Bangladesh Root CA private key must perform through the Cryptographic Module with FIPS 140-2 Level 3 standards. Importing and exporting process of the private key requires at least two persons with Trusted Role.

6.2.7 Private Key Storage on Cryptographic Module

Bangladesh Root CA private key stored in a Cryptographic Module and back up the private key in another Cryptographic Module.

6.2.8 Method of Activating Private Key

Activation of Bangladesh Root CA's private key operations performs by the authorized person and requires two factor authentication process.

6.2.9 Method of Deactivating Private Key

After working with the private key of Bangladesh Root CA, all certificate authority officers must leave the system (Log Out) to prevent unauthorized access.

6.2.10 Method of Destroying Private Key

Bangladesh Root CA will delete the private keys from the Cryptographic Module and its backup by overwriting the private key or initialize the module with zeroization function. The event of destroying Bangladesh Root CA must be recorded into evidence under section 5.4.

6.2.11 Cryptographic Module Rating

Cryptographic Module Rating complies with FIPS 140-2 Level 3 standard.

24.03.2016

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

A public key will be archived and kept securely. The archival period is 7 years.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

The certificate validity period and key pair associated with the certificate can be used up to the expiry date specified in the certificate. The public key can be used to verify the digital signature even if the certificate is expired but the digital signature to be verified must be created before expiry date of the certificate. For the private key, it can be used to decrypt even if the certificate is expired.

The validity period of Bangladesh Root CA root certificate is 10 years and the validity period of CA Subscriber certificates is not more than 10 years. Certificate operational periods and key pair usage periods shall be assessed by the PA at least once a year or as necessary especially in an incident that is believed to significantly impact trustworthiness of Bangladesh Root CA.

Subscriber certificates issued after 1 March 2018 must have a Validity Period no greater than 825 days. Subscriber certificates issued after 1 July 2016 but prior to 1 March 2018 must have a Validity Period no greater than 39 months.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

Bangladesh Root CA activation data such as Personal Identification Number (PIN) and passwords for accessing the CA systems are user-selected and protected under multi-person control by each of whom holding that activation data. Subordinate CAs use the same data generation mechanism.

6.4.2 Activation Data Protection

Data used to unlock private keys is protected from disclosure by storing in safe and allow only the authorized person to access.

6.4.3 Other Aspects of Activation Data

Not Applicable.

6.5 Computer Security Controls

CCA implemented multi-person control access to information such as sensitive details about customer accounts and passwords. Ultimately CA-related private keys are carefully guarded, along with the machines housing such information. Security procedures are in place to prevent and detect unauthorized access, modification, malicious code or compromise of the Bangladesh Root CA systems such as firmware and software. Such security controls are subject to compliance assessment as specified in section 8.

6.5.1 Specific Computer Security Technical Requirements

The server hosting the Root CA product is built from a vendor CD with reasonable provenance. No other services or software are loaded or operated on the Root CA servers. The server will receive occasional patches and other adjustments if the security risk warrants, in the judgment of CCA. In addition, installed applications are regularly reviewed for security updates to ensure that no vulnerability is exposed.

6.5.2 Computer Security Rating

No stipulation.

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

For both readymade software and in-house developed software by Bangladesh Root CA that are used in certificate management, they shall be checked to ensure the software is genuine and fully tested in nonproduction environment before deployment in production environment. Any change to Bangladesh Root CA systems or components must go through the Change Management Control review and approval process.

6.6.2 Security Management Controls

CCA has procedures to monitor and control variables of the certificate system. Changes of variables are processed through security management control.

6.6.3 Life Cycle Security Controls

Not Applicable.

6.7 Network Security Controls

Bangladesh Root CA servers are kept offline and will never be connected to a computer networks under any circumstances. The public servers have sufficient network security controls with firewall and other network security rules.

6.8 Time-stamping

The system clock will be set in the time setting device (NTP Server) which shall be accurate to within three minutes. Any recording time in the system will refer to the same time setting device.

7 Certificate, CRL and OCSP Profiles

7.1 Certificate Profile

The certificate issued by Bangladesh Root CA is complied with ITU-T Recommendation X.509 (11/08): Information technology - Open systems interconnection - The Directory: Public-key and attribute certificate frameworks in which the certificate contains the information shown in Table 6.

Field	Value or Value Constraint
Version	Version of certificate, the details are described in section 7.1.1
Serial Number	Reference number of each Certificate Authority is unique. This shall be minimum 64 bits, value greater than 0 and generated through a CSPRNG.
Signature	The method of digitally sign consists of Asymmetric cryptographic algorithms (Public Key Algorithm) and data digestion (Hash Function) which Certificate Authority is used to sign the certificate in form of Object Identifier (OID)
Issuer	The name of the Certificate Authority in the certificate must be in the format of Distinguished Name (DN) in accordance with ISO / IEC 9594- 2.
Validity	Period of certificate usage is specified by the begin date (notBefore) and expiration date (notAfter)
Subject	Specify the entity name of Certificate Authority or Subscriber as the owner of public key in the certificate
Subject Public Key Info	Specify the type of public key and subject value of public key

Table 6: Fields in the Certificate

7.1.1 Version Number

The certificate issued by Bangladesh Root CA is in accordance with X.509 version 3.

7.1.2 Certificate Content and Extensions; Application of RFC 5280

This section specifies the additional requirements for Certificate content and extensions for Certificates generated after the Effective Date.

7.1.2.1 Root CA Certificate

Bangladesh Root CA follows Section 7.1.2.1 of CA/B Forum Baseline Requirements.

7.1.2.2 Subordinate CA Certificate

Bangladesh Root CA follows Section 7.1.2.2 of CA/B Forum Baseline Requirements.

7.1.2.3 Subscriber Certificate

Bangladesh Root CA follows Section 7.1.2.3 of CA/B Forum Baseline Requirements. In addition, certificatePolicies:policyQualifiers:qualifier:cPSuri must be mandatory.

7.1.2.4 All Certificate

Bangladesh Root CA follows Section 7.1.2.4 of CA/B Forum Baseline Requirements.

7.1.2.5 Application of RFC 5280

Bangladesh Root CA follows Section 7.1.2.5 of CA/B Forum Baseline Requirements.

7.1.3 Algorithm Object Identifiers

The OID of digital signature and encryption of certificate is in Table 7.

Algorithm	Object Identifier
RSAEncryption	1.2.840.113549.1.1.1
SHA512withRSAEncryption	1.2.840.113549.1.1.13
SHA512	2.16.840.1.101.3.4.2.3

Table 7: Method of Digital Signature and Encryption with Object Identifier

7.1.4 Name Forms

The name format of Issuer and Subject are specified in the certificate as reference to the section 3.1.1.

7.1.5 Name Constraints

Bangladesh Root CA follows Section 7.1.5 of CA/B Forum Baseline Requirements. The Bangladesh Root CA Root Certificate does not assert Name Constraints. It may be asserted in Bangladesh Root CA Subordinate certificates if required.

7.1.6 Certificate Policy Object Identifier

Bangladesh Root CA follows Section 7.1.6 of CA/B Forum Baseline Requirements and the Subordinate CAs MUST define the Certificate Policy OID provided by Bangladesh Root CA's OID Structure.

7.1.7 Usage of Policy Constraints Extension

Not Applicable.

7.1.8 Policy Qualifiers Syntax and Semantics

CAs may issue Certificates with a policy qualifier and suitable text to aid Relying Parties in determining applicability.

24.03.2020

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

Not Applicable.

7.2 CRL Profile

Bangladesh Root CA's certificate revocation list must comply with RFC5280 as the following details as in Table 8.

Field	Value or Value Constraint
version	Version of the certificate revocation list will be version number 2 as provided in section 7.2.1.
signature	The method of digitally sign consists of Asymmetric cryptographic algorithms (Public Key Algorithm) and data digestion (Hash Function) which is used by Certificate Authority to sign the certificate in form of Object Identifier (OID).
issuer	The name of the Certificate Authority in the certificate must be in the format of Distinguished Name (DN) in accordance with ISO / IEC 9594- 2.
thisUpdate	The date and time of the revocation list.
nextUpdate	The specified date and time to the next update of certificate revocation list. If necessary, Bangladesh Root CA will issue the certificate revocation list before the scheduled date and time.
revokedCertificates	A list of the serialNumber of the certificate has been revoked with the specified date and time of revocation.

Table 8: Item List in Certificate Revocation

7.2.1 Version Number(s)

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

7.2.2 CRL and CRL Entry Extensions

The information on certificate revocation lists issued by the Certification Authority is complied with ISO / IEC 9594-8:2012 standard and contains at least the following:

7.2.2.1 Authority Key Identifier

This attribute indicates information associated with the public key of the certificate which is digitally signed by subscribers. The signing uses SHA-256, or SHA-384 or SHA-512 hashing algorithm of the public key of the Certificate Authority.

7.2.2.2 BaseCRLNumber

This attribute indicates the sequence number that the Certificate Authority assigns to each revoked certificate to order the certificate revocation list.

7.2.2.3 ReasonCode

This attribute indicates the Reason Code (0-9) of the revoked certificate.

7.2.2.4 InvalidityDate

This attribution indicates start time when using the pair of private key and the revoked certificate is insecure.

7.2.2.5 Issuing DistributionPoint

This attribution is used to locate the certificate revocation list (Distribution Point) and indicates that the certificate revocation list is for a Certification Authority or subscribers including the reasons of revocation (Reason Code).

7.3 OCSP Profile

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

7.3.1 Version Number(s)

CAs shall issue Version 1 OCSP responses.

7.3.2 Fields in OCSP Responses

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

7.3.3 OCSP Extensions

No Stipulation.

8 Assessments Compliance Audit and Other Assessments

Bangladesh Root CA has a compliance audit mechanism in place to ensure that the requirements of its CPS are being implemented and audited for complying with the following standards:

- WebTrust - Principles and Criteria for Certification Authorities latest version
- WebTrust Principles and Criteria for Certification Authorities - SSL Baseline with Network Security – latest version
- CA/Browser Forum Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates with the latest version
- SSL and EV SSL Certificate Guidelines – Latest Version
- Code Singing and EV Code Signing Certificate Guidelines – Latest Version
- ICT Act 2006 (amended in 2009), IT (CA) Rules 2010
- Relevant laws and regulations

8.1 Frequency or Circumstances of Assessment

Bangladesh Root CA follows Section 8.1 of CA/B Forum Baseline Requirements.

8.2 Identity/Qualifications of Assessor

WebTrust auditors must meet the requirements of Section 8.2 of the Baseline Requirements.

8.3 Assessor's Relationship to Assessed Entity

Auditors are independent from the Bangladesh Root CA, or it shall be sufficiently organizationally separated from Bangladesh Root CA and shall provide an unbiased, independent evaluation. To insure independence and objectivity, the compliance auditor may not have served the entity in developing or maintaining Bangladesh Root CA's facility or certification practice statement. The CAM shall determine whether a compliance auditor meets this requirement. There must not be conflict of interest to the CAs.

8.4 Topics Covered by Assessment

The purpose of compliance audit is to verify that a CA and its RAs comply with all the requirements of the current version of this CP and the CA's CPS. The audit meets the requirements of the audit schemes highlighted in Section 8 under which the assessment is being made. These requirements may vary as audit schemes are updated. An audit scheme is applicable to CAs in the year following the adoption of the updated scheme.

8.5 Actions Taken As a Result of Deficiency

CCA's officers must plan to improve the deficiencies (Non-conformity) based on the assessment results with an explicit operating time. The plan will be submitted to auditors to ensure that the sufficient security of the system is still in place.

8.6 Communication of Results

After the assessment is completed, the audit compliance report and identification of corrective measures will be sent to the PA within 30 days of completion.

8.7 Self-Audits

During the period in which the CA issues Certificates, the CA SHALL monitor adherence to its Certificate Policy, Certification Practice Statement and these Requirements and strictly control its service quality by performing self-audits on at least a quarterly basis against a randomly selected sample of the greater of one certificate or at least three percent of the Certificates issued by it during the period commencing immediately after the previous self-audit sample was taken.

9 Other Business and Legal Matters

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

No fees charged.

9.1.2 Certificate Access Fees

No fees charged.

9.1.3 Revocation or Status Information Access Fees

No fees charged.

9.1.4 Fees for Other Services

No fees charged.

9.1.5 Refund Policy

The relevant contractual document will prevail for refunding.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

The Root CA maintains sufficient financial resources to ensure respective performance and obligations.

9.2.2 Other Assets

The Root CA maintains sufficient financial resources to maintain its operations and fulfill duties.

9.2.3 Insurance or Warranty Coverage for End-entities

Root CA does not issue certificate to end entities, hence no Insurance or Warranty coverage for end entities is acceptable.

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

Bangladesh Root CA keeps following information in the scope of confidential information:

- Private key of Bangladesh Root CA and required information to access the private key including password to access Bangladesh Root CA's hardware and software
- Registration application of subscribers for both approved and rejected application
- Audit Trail record
- Contingency Plan or Disaster Recovery Plan
- Security controls of Bangladesh Root CA's hardware and software
- Sensitive information with potential to have an impact on security and reliable of Bangladesh Root CA's system

9.3.2 Information Not within the Scope of Confidential Information

The following information is not within the scope of confidential information:

- Certificate Practice Policy of Certification Authority
- Certificate uses policy
- Information inside certificate
- Certificate revocation
- Information without impact on security and reliable of Bangladesh Root CA's system such as articles and news

9.3.3 Responsibility to Protect Confidential Information

Bangladesh Root CA has security measure in place to protect confidential information. All Bangladesh PKI participants shall be responsible for protecting the confidential information they possess in accordance with the Privacy policy and applicable laws and Agreements.

The CA key pairs are generated and managed by the requesting CA and are the sole responsibility of the licensed CA.

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

Bangladesh Root CA developed, implemented and maintained a privacy plan. The privacy plan documented what personally identifiable information is collected, how it is stored and processed, and under what conditions the information may be disclosed.

9.4.2 Information Treated As Private

Private information in this document means related information of subscribers that does not include in the certificate or directory.

9.4.3 Information Not Deemed Private

Not deemed private information in this document means related information of subscribers that include in the certificate or directory.

9.4.4 Responsibility to Protect Private Information

Bangladesh Root CA has implemented security measure to protect private information.

9.4.5 Notice and Consent to Use Private Information

Bangladesh Root CA will use private information only if subscribers are noticed and consent to use private information in compliance with the privacy policy.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

In the event of court order or administrative order, Bangladesh Root CA needs to disclose personal information with required by law or officers under the law.

9.4.7 Other Information Disclosure Circumstances

Not Applicable.

9.5 Intellectual Property Rights

Bangladesh Root CA is the only owner of intellectual property rights associated with the certificate, certificate revocation information and this certificate practice statement.

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

Bangladesh Root CA assures that

- Procedures are implemented in accordance with this CP of Bangladesh Root CA.
- Any certificates issued that assert the policy OIDs identified in this CPS were issued in accordance with the stipulations of this CPS.
- The Certification Practice Statement (CPS) will be provided, as well as any subsequent changes, for conformance assessment.
- The CA operation is maintained in conformance to the stipulations of the CPS.
- The registration information is accepted only from approved RAs operating under an approved CPS.
- All information regarding certificate issuance and certificate revocation are processed through the procedures specified in the CPS of the Bangladesh Root CA.

9.6.2 RA Representations and Warranties

An RA shall assure that

- Its RA registration operation is performed in conformance to the stipulations of the approved CPS of the Bangladesh Root CA and related regulations.
- All information contained in the certificate issued by Bangladesh Root CA is valid and appropriate. The evidence that due diligence was exercised in validating the information contained in the certificates is maintained.
- The obligations are imposed on subscribers in accordance with section 9.6.3, and subscribers are informed of the consequences of not complying with those obligations.

9.6.3 Subscriber Representations and Warranties

By using the certificate, the CA subscriber assures that

- He/She accurately represents itself in all communications with the Bangladesh Root CA.
- The private key is properly protected at all times and inaccessible without authorization.
- Bangladesh Root CA is promptly notified when the private key is suspected loss or compromise.
- All information displays in the certificate is complete and accurate.
- The certificate will be used legitimately under laws, related regulations, terms, conditions and other related service announcements of the Bangladesh Root CA by authorized persons.

9.6.4 Relying Party Representations and Warranties

In case of relying party representations use the certificate, the relying party shall properly verify information inside the certificate before using and accepting the fault of single side verification.

Relying parties must:

- Read the procedures published in this document.
- Must read and comply with provisions of licensed CA's CP/CPS.
- Verify the purpose of a certificate, its validity period, key usage, class of certificate and path to trust anchor.

Relying parties must not:

- Assume any attributes or policies based solely on the licensed CA being signed by the CCA Root CA.

Relying parties may:

- The relying party should check that the Licensed CA certificate is not on the CCA root CRL.

9.6.5 Representations and Warranties of Other Participants

Not Applicable.

9.7 Disclaimers of Warranties

Bangladesh Root CA only signs CA certificates according to the practices described in this document. No liability, implicit or explicit, is accepted.

CCA and its agents make no guarantee about the security or suitability of a CA that is signed by the Bangladesh Root CA. The CCA certification service is run with a reasonable level of security, but it is provided on a best effort only basis. It does not warrant its procedures and it will take no responsibility for problems arising from its operation, or for the use made of the certificates it provides. CCA denies any financial or any other kind of responsibility for damages or impairments resulting from its operation.

9.8 Limitations of Liability

Root CA denies any financial or any other kind of responsibility for damages or impairments resulting from its CA operation. The Root CA will not incur any liability to CA Subscribers or any person to the extent that such liability results from their negligence, fraud or willful misconduct.

The CA is responsible for any damage incurred in the event of damage caused by the use of the service systems from the willful act or gross negligence of the corresponding CA. The response to the damage is under determination of the CA.

9.9 Indemnities

The subscribers, CAs and Relying Partiers shall indemnify, defend and hold harmless the Root CA, its directors, officers, employees, agents, consultants, and subsidiaries from any and all claims, damages, costs (including, without limitation, attorney's fees), judgments, awards or liability.

24.03.2020

9.10 Term and Termination

9.10.1 Term

The CPS becomes effective upon its publication in the repository.

9.10.2 Termination

Users will not be warned in advance of changes to CCA policy and CPS. It is expected that, over time, a set of standard policies profiles will emerge, and CCA may adapt if deemed so. The CCA is responsible for the CPS. All changes must be approved by the PA.

9.10.3 Effect of Termination and Survival

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

9.11 Individual Notices and Communications with Participants

CCA will communicate to those participants using the reliable channel as soon as possible in accordance with the importance of information. The information is available at http://www.cca.gov.bd.

9.12 Amendments

9.12.1 Procedure for Amendment

Amendment of CPS is subject to Bangladesh Root CA and it needs to be approved by the PA before announcement. However, all amendments are performed pursuant to laws, regulation or other related service announcements of Bangladesh Root CA.

9.12.2 Notification Mechanism and Period

Bangladesh Root CA reserves the right to revise this document. In case there are any significant changes, CCA will announce on the website before the date of enforcement. After 30 days of notification the CPS will automatically be effect. For critical changes CCA may communicate to the PKI participant.

9.12.3 Circumstances under Which OID Must Be Changed

In case the PA has the view that it is necessary to change the involved OID numbers, Bangladesh Root CA will change the OID and enforce the new policy using the new OID.

9.13 Dispute Resolution Provisions

Any dispute between CAs and CCA will be resolved as per Act, Rules and Guidelines.

9.13.1 Disputes between Issuer and Subscriber

The decisions of Bangladesh Root CA pertaining to matters within the scope of this CPS are final. Any claims should be submitted to CCA at the following address:

Office of the Controller of Certifying Authorities (CCA)

E-14/X, ICT Tower (1st Floor)

Agargaon, Sher-e-Bangla Nagar

Dhaka-1207.

In the event of undefined, PA has jurisdiction over the dispute.

9.13.2 Disputes between Issuer and Relying Parties

The same procedure as stated in section 9.13.1. In the event of undefined, the PA has jurisdiction over the dispute.

9.14 Governing Law

The laws of the People Republic of Bangladesh shall govern this CP.

9.15 Compliance with Applicable Law

All CAs operating under this CP are required to comply with the laws of the People Republic of Bangladesh.

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

This CPS shall be considered as part of the agreement between Bangladesh Root CA and its subscribers.

9.16.2 Assignment

Requirements of the assignment must be in accordance with laws, regulations, or announcements relating to Bangladesh Root CA.

9.16.3 Severability

It should be determined that one section of this CPS is incorrect or invalid, the other sections of this CPS shall remain in effect until the CPS is updated.

9.16.4 Enforcement

It should be determined that any section of this CPS is illegal, unenforceable, or void, then any offending words in it will be deleted to the extent necessary to make it legal and enforceable while preserving its intent.

9.16.5 Force Majeure

The provided Bangladesh Root CA and subordinate CAs have exercised a reasonable degree of skill and care to avoid and/or mitigate the effects of matters beyond its control, neither Bangladesh Root CA, the subordinate CA nor any RA is liable for the adverse effects to Subscribers or Relying Parties of any matters outside our control whatsoever, including (without limitation) the availability of the Internet, or telecommunications or other infrastructure systems or the adverse effects of the acts of God, war, military operations, national emergency, epidemic, fire, flood, earthquake, strike or riots or the negligence or deliberate wrongful conduct of other Subscribers or other third parties.

9.17 Other Provisions

Not Applicable.