[Draft]

Bangladesh Bank Certification Authority (BBCA)

Certification Practice Statement (CPS)

Version: 1.00
August, 2015

Bangladesh Bank

Document Reference

Title	**Bangladesh Bank CA CPS**
Document Type	**Public**
Version	**1.00**
Publishing Date	
Last Update	
Pages	
Status	**Draft**

Contents

1 Introduction

1.1 *Overview*

This document is structured according to CPS Guideline issued by Office of the Controller of Certifying Authorities and in accordance with RFC 3647. This document describes the set of rules and procedures established by Bangladesh Bank CA for the operations of the CA services as government CA licensed under ICT Act 2006 by Office of the Controller of Certifying Authorities.

This document will include the Certification Practice Statement for the BBCA CPS. The general architecture is a subordinate CA under Root CA according to the hierarchical PKI model of Bangladesh as shown below:

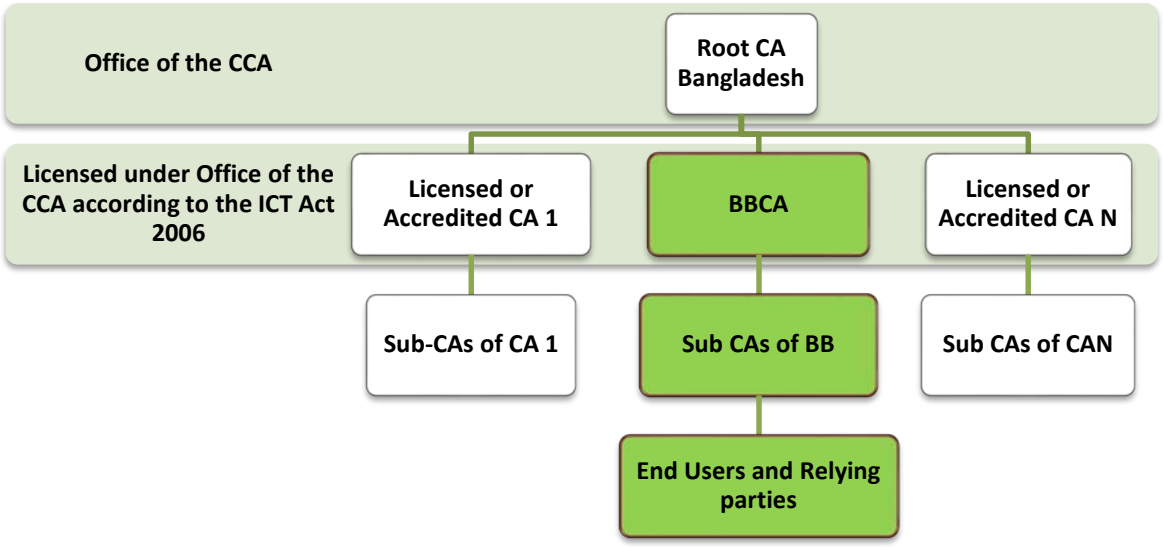


Figure 1: BBCA in Bangladesh PKI

The CA of BB is one of the licensed CAs whose public key is signed by the Root CA of Bangladesh operated by Office of the CCA. As one of the licensed CAs under Office of the CCA, BBCA maintains 4 classes of certificates for end users as per the CPS Guideline issued by Office of the CCA. Those are:

Class 0	Test certificates are issued for one month with no assurance at all.
Class 1	Class 1 certificates are issued to individuals/private subscribers. These certificates will confirm that user's name (or alias) and E-mail address form an unambiguous subject within the Certifying Authorities database. The assurance level of this type of certificate is low.
Class 2	Class 2 certificates have two categories namely individual and organization. These certificates are issued for both business personnel and private individuals use. The assurance level of this kind of certificate is medium and appropriate for e-governance and other electronic transactions. These certificates will confirm that the information in the

	application provided by the subscriber does not conflict with the information in well-recognized consumer databases such as national id database, passport database etc. BBCA primarily checks with national id database and collects appropriate documents before issuing this kind of certificates to individuals. BBCA verifies appropriate documents such as TIN/VAT certificate, trade certificate, certificate of incorporation, AoA & MoA of the company in case of organization certificate. In case of GoB organizations, letter from appropriate authorities is required before request for an organization certificate.
Class 3	Class 3 certificates are issued to individuals as well as organizations. As these are high assurance certificates, primarily intended for e-commerce applications, these shall be issued to individuals only (nominated by organization) on their personal (physical) appearance before the Certifying Authorities with appropriate documents. Examples of Class 3 certificates are SSL certificate, device certificate, VPN certificates, code signing certificates etc.

1.2 *Document Name and Identification*

Document title:

BBCA CPS

Document version:

1.00

Document Date:

September, 2015

OID: *[OID will be assigned after OID registration from country RA]*

1.3 *PKI Participants*

1.3.1 Root CA

Office of the CCA manages and operates the Root CA of Bangladesh PKI. Root CA Bangladesh is at the top of the PKI hierarchy in Bangladesh and the only self-signed CA in Bangladesh. Root CA Bangladesh signs licensed CAs in Bangladesh to act as recognized Certification Authority.

1.3.2 Certification Authority

Certification Authority in Bangladesh is designated to issue certificates to end users and maintain certificate lifecycle within its PKI. Certification Authorities can start issuing certificates after its' Public Key is signed by Root CA Bangladesh. BBCA, as one of the licensed CAs in Bangladesh, will issue certificates signed with its' private key. The private key of BBCA is managed by a FIPS 140 level 3 compliant Hardware Security Module. BBCA may assign sub CA within its organization or may issue sub CA certificates to any other organization upon approved request from competent authority.

1.3.3 **Registration Authority**

Registration Authority establishes enrollment procedures for end-user certificate applicants, perform identification and authentication of certificate applicants, initiate or pass along revocation requests for certificates, and approve applications for renewal or re-keying certificates on behalf of a CA. Subordinate organizations within a larger organization can act as RA for the CA serving the entire organization, but RA may also be external to the CA. In case of BBCA, primarily there will be a RA within its Head Office.

1.3.4 **Subscriber**

The user of the digital certificates is the subscriber. Subscriber may be individual or organization or any device or applications running within or by an organization. Subscriber is required to submit his/her certificate request in form of CSR and in prescribed manner to BBCA to get the certificate issued to him/her.

1.3.5 **Relying Parties**

Relying parties are those who trust the PKI or rely on the PKI. Relying parties may or may not be the subscriber of BBCA, e.g. when an email recipient having no digital certificate is trusting on an email since it is signed with digital signature certificate issued by BBCA, then that email recipient is acting as relying party for BBCA.

1.4 ***Certificate Usage***

BBCA issues certificates for digital signature, non-repudiation, authentication, encryption etc. These certificate are four types as follows:

Class 0	Test certificates are issued for one month with no assurance at all. Anyone can enroll online for this certificate. The certificate can only be used for digital signature with no assurance ensured by BBCA.
Class 1	The assurance level of class 1 certificate is low; this type of certificate can be used by any entity or subscriber for digital signature, non-repudiation and encryption. This kind of certificate has two categories namely organization and personal. These certificates are appropriate to use in email and document for signing.
Class 2	These certificates have two categories namely individual and organization. The assurance level of this kind of certificate is medium and appropriate for e-governance and other electronic transactions. These certificates will confirm that the information in the application provided by the subscriber does not conflict with the information in well-recognized consumer databases such as national id database, passport database, company registration database etc. The usage of this type of certificate is digital signature, non-repudiation and encryption.
Class 3	These certificates are issued to individuals as well as organizations. These are high assurance certificates, and shall be issued to individuals only on their physical appearance before the CA or RAs with appropriate documents. Examples of Class 3 certificates are SSL certificate, device certificate, VPN certificates, code signing certificates etc.

1.5 *Policy Administration*

The BBCA is operated and managed by Bangladesh Bank under Ministry of Finance.

1.5.1 Contact Details of the Organization

Name: Bangladesh Bank
Address: Bangladesh Bank, Head Office, Dhaka, Bangladesh
Email: ca.bb@bb.org.bd
Web: www.bb.org.bd
Phone: 88029530165

1.5.2 Contact Details of the Persons

The following persons are responsible for drafting, registering, maintaining, and updating of this CPS. They are also responsible answering any query about this CPS.

Sl.	Name	Email
1.	Mohammed Ishaque Miah Senior Systems Analyst Address: IT Operation and Communication Department Head Office, Bangladesh Bank Motijheel Dhaka 1000, Bangladesh Phone: 029530165, 01799384759	ishaque.miah@bb.org.bd, ca.bb@bb.org.bd

1.6 *Definitions and Acronyms*

1.6.1 Definitions

Activation 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).

Authentication The process of establishing that individuals, organizations, or things are who or what they claim to be. In the context of a PKI, authentication can be the process of establishing that an individual or organization applying for or seeking access to something under a certain name is, in fact, the proper individual or organization. This corresponds to the identification. Authentication can also refer to a security service that provides assurances that individuals, organizations, or things are who or what they claim to be or that a message or other data originated from a specific individual, organization, or device. Thus, it is said that a digital signature of a message authenticates the message's sender.

Certification Authority (CA) The entity/system that issues X.509 identity certificates (places a subject name and public key in a document and then digitally signs that document using the private key of the CA.

CA Certificate A certificate for one CA's public key issued by the Root CA.

Certificate Chain (CC) A hierarchical list certificates containing an end-user certificate, Sub-CA certificate (if any), CA certificate and Root Certificate.

Certificate Hierarchy (CH) A level based sequence of certificates of one Root CA and subordinate entities that include, Certification Authorities and subscriber.

Certificate Policy (CP) A named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements. For example, a particular CP might indicate applicability of a type of certificate to the authentication of parties engaging in business-to-business transactions for the trading of goods or services within a given price range.

Certification Path An ordered sequence of certificates that, together with the public key of the initial object in the path, can be processed to obtain that of the final object in the path.

Certification Practice Statement A statement of the practices that a certification authority employs in issuing, managing, revoking, and renewing or re-keying certificates.

CPS Summary A subset of the provisions of a complete CPS that is made public by a CA.

Certificate Revocation List (CRL) A list issued and digitally signed by CA that includes revoked and suspended certificates.

Identification The process of establishing the identity of an individual or organization, i.e., to show that an individual or organization is a specific individual or organization.

Issuing Certification Authority In the context of a particular certificate, the issuing CA is the CA that issued the certificate

Participant An individual or organization that plays a role within a given PKI as a subscriber, relying party, CA, RA, certificate manufacturing authority, repository service provider, or similar entity.

PKI Disclosure Statement (PDS) An instrument that supplements a CP or CPS by disclosing critical information about the policies and practices of a CA/PKI. A PDS is a vehicle for disclosing and emphasizing information normally covered in detail by associated CP and/or CPS documents. Consequently, a PDS is not intended to replace a CP or CPS.

Policy Qualifier The Policy-dependent information that accompanies a certificate policy identifier in an X.509 certificate.

Registration Authority (RA) An entity that is responsible for one or more of the following functions:

- The identification and authentication of certificate applicants
- The approval or rejection of certificate applications
- Initiating certificate revocations or suspensions under certain circumstances
- Processing subscriber requests to revoke or suspend their certificates

- Approving or rejecting requests by subscribers to renew or re-key their certificates. RAs, however, do not sign or issue certificates

Relying Party A recipient of a certificate who acts in reliance on that certificate and/or any digital signatures verified using that certificate. In this document, the terms "certificate user" and "relying party" are used interchangeably.

Relying Party Agreement (RPA) An agreement between a certification authority and relying party that typically establishes the rights and responsibilities between those parties regarding the verification of digital signatures or other uses of certificates.

Set of provisions A collection of practice and/or policy statements, spanning a range of standard topics, for use in expressing a certificate policy definition or CPS and employing the approach described in this framework.

Subject CA In the context of a particular CA-certificate, the subject CA is the CA whose public key is certified in the certificate (see also Issuing certification authority)

Subscriber The user of the digital certificates is the subscriber. Subscriber may be individual or organization or any device or applications running within or by an organization. Subscriber is required to submit his/her certificate request in form of CSR and in prescribed manner to BBCA to get the certificate issued to him/her.

Subscriber Agreement An agreement between a CA and a subscriber that establishes the right and responsibilities of the parties regarding the issuance and management of certificates.

Validation The process of identification of certificate applicants. "Validation" is a subset of "identification" and refers to identification in the context of establishing the identity of certificate applicants.

1.6.2 **Acronyms**

AoA	Article of Association
BB	Bangladesh Bank
CA	Certifying Authority
CC	Certificate Chain
CCA	Controller of Certifying Authorities
CH	Certificate Hierarchy
CN	Common Name
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSP	Cryptographic Service Provider
CSR	Certificate Signing Request
DN	Distinguished Name
DPDT	Department of Patents, Designs and Trademarks
DVD	Digital Versatile Disc
EAL	Evaluation Assurance Level
FIPS	Federal Information Processing Standard
GoB	Government of Bangladesh
HSM	Hardware Security Module
ICT	Information and Communication Technology
KGC	Key Generation Ceremony
LDAP	Lightweight Directory Access Protocol
MoA	Memorandum of Association
NID	National Identity Registration
NIST	National Institute of Standards and Technology
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OU	Organizational Unit
PAC	Powdered Activated Carbon
PDS	PKI Disclosure Statement
PIN	Personal Identification Number
PKD	Public Key Directory
PKI	Public Key Infrastructure
RA	Registration Authority
RFC	Request For Comment
RPA	Relying Party Agreement
RSA	The Rivest Shamir Adleman Cryptographic Algorithm
SSL	Secure Socket Layer
SUB-CA	Subordinate Certifying Authority
TIN	Taxpayer's Identification Number
URL	Uniform Resource Locator
VAT	Value Added Tax
VPN	Virtual Private Network
WWW	World Wide Web
X.500	The ITU-T standard for electronic directory services
X.509	The ITU-T standard for Certificates and CRLs

2 Publication and Repository Responsibilities

2.1.1 Repositories

BBCA itself provides the repository service apart from the central repository services of Office of the CCA. BBCA publishes its certification practices, certificates, and the current status of such certificates to its repository. Repository of certificates and CRLs can be found at: **ldap.bb.org.bd** or **crl.bb.org.bd**. The status of a certificate is also available from **www.bb.org.bd** website.

2.1.2 Publication of Certification information

BBCA operates a secure online repository for its subscriber and relying parties that contains:

- CA certificate signed by the Root CA Bangladesh;
- Certificates issued by BBCA;
- A Certificate Revocation List issued by BBCA;
- An online certificate status responder in a form of OCSP;
- A copy of this CPS;
- Other information deemed relevant to the BBCA.

2.1.3 Time or Frequency of Publication

- Certificates will be published to the BBCA repository as soon as it is been issued.
- CRLs will be published as soon as there is any revocation done by BBCA. Apart from that CRL repository will be refreshed once in every 30 days.

2.1.4 Access Control on Repositories

The online repository is available on a substantially 24/7 basis from anywhere, subject to reasonable scheduled maintenance. The BBCA service does not impose any access control on its Policy, its' signing Certificate and issued certificates, and its' CRLs but ensures reasonable security measures to protect those information from unauthorized modification.

3 Identification and Authentication

BBCA ensures proper verification method for verifying the identity and authenticity of its end users prior to the issuance of certificates. The verification method for identity and authenticity differs in different classes of certificates. BBCA follows the Interoperability Guideline issued by Office of the CCA for naming and identification.

3.1 *Naming*

3.1.1 Types of names

The type of name assigned to the subject of BBCA, its' Sub-CA and end users are in the form of X.500 DN format. As per the Interoperability Guideline BBCA uses the following attribute for its' subject specification:

Sl. No	Attribute Type
1.	Country
2.	Organization
3.	Organization Unit
4.	Postal Code
5.	Street Address
6.	House Identifier
7.	Common Name
8.	Locality

For sub-CA within BBCA (i.e. the sub-CA for distinguishing different classes of certificate), the following parameters are used by BBCA for subject specification:

Sl. No	Attribute Type
1.	Country
2.	Organization
3.	Organization Unit
4.	Common Name

For external sub-CA, the following parameters are used by BBCA for subject specification:

Sl. No	Attribute Type
1.	Country
2.	Organization
3.	Post Code
4.	Organization Unit
5.	Street Address
6.	House Identifier
7.	Common Name
8.	Locality

The following parameters are used by BBCA for end user subject specification:

Sl. No	Attribute Type
1.	Country
2.	Organization
3.	Organization Unit
4.	Post Code
5.	Locality
6.	State/Province
7.	Unique Identifier
8.	Serial Number
9.	Common Name

3.1.2 Name Meanings

BBCA certificate uses name in a meaningful way as per the Interoperability Guideline issued by Office of the CCA. The subject DN of BBCA is as below:

CN=	BBCA
O (Organization) =	Bangladesh Bank
OU=	Certification Authority
HouseIdentifier=	Head Office
StreetAddress=	Motijheel
Locality=	Dhaka
PostalCode=	1000
C (Country) =	BD

For both external and internal Sub-CA certificate BBCA practices the guidance of Interoperability Guideline. For end user certificate, the following naming convention is used for subject specification:

CN =	"Surname" "Given Name" "Initials"
Serial Number=	(NID/PPN/BRN/TIN) (Digest of the corresponding id value)
UniqueIdentifier=	Not Used
State/Province=	(Division Name of the end user is used here)
Locality=	(City/District Name)
Postal Code=	(The postal code of the end user)
OU=	(name of the department or sub-division of the organization the end user belongs to OR does not used if the Organization value is Personal)
O (Organization) =	(name of the organization the end user belongs to OR Personal)
C (country) =	BD OR Country Code if certificate is issued outside Bangladesh

3.1.3 Anonymity or Pseudonymity of Subscribers

BBCA does not process any anonymous or pseudonymous certificate request from the end users.

3.1.4 Rules for interpreting various name forms

Various name forms in sub-CA and end user certificate is interpreted in accordance with the Digital Certificate Interoperability Guideline and IT (CA) Rules 2010 and other orders or guidelines issued by Office of the CCA for naming purpose.

3.1.5 Uniqueness of names

BBCA ensures the uniqueness of certificate subject specification for both sub CA and end users. For end users whether it is organization or personal, BBCA maintains a method of uniqueness by using serial number field in the subject DN of the certificate user as well as the serial number field of the certificate. The name conforms to X.500 standards for name uniqueness. There may be multiple certificate requests from a single user which is uniquely distinguishable using the certificate serial number field. Moreover there is no chance of having any ambiguity between two or more end users even though they may have same name since their identification value (e.g. NID, Passport Number, TIN or Birth Registration Number) is different which is used as digest in the serial number field of the subject DN.

3.1.6 Recognition, authentication, and role of trademarks

End users requesting for a certificate to BBCA are prohibited from using names in their certificate request form that infringe upon the Intellectual Property Rights of others. However, BBCA does not verify whether a certificate applicant has Intellectual Property Rights in the name appearing in a certificate request form. Any such disputes shall be resolved as per the rules and guideline of Office of the CCA and/or by the Copyright Office of Bangladesh and/or by the Department of Patents, Designs and Trademarks (DPDT), Bangladesh. BBCA does not responsible and engaged in any dispute resolution.

BBCA has the rights to reject any certificate request and revoke or suspend any existing certificate because of such dispute, without explaining any reason whatsoever to the end user.

3.2 *Initial Identity Validation*

3.2.1 Method to Prove Possession of Private Key

BBCA accepts two methods for processing subscribers' certificate request; one of the methods is that the subscriber can generate its own key pair and request to BBCA for certificate by sending the public key along with CSR and another method is BBCA, on behalf of its subscriber, generates the key pair centrally in a secured and trustworthy manner so that any tamper to that system or to the private key is not possible. For the first method, the subscriber requesting for the certificate must have to ensure and demonstrate to BBCA that he/she is rightfully holds the private key corresponding to the public key requested for certificate, and for the second method BBCA does deliver the certificate along with the private key in a secured and trustworthy manner to the subscriber after identity verification. BBCA does not keep or store private key of any subscriber.

3.2.2 Authentication of Organization Identity

If the certificate is an organization type of certificate, i.e. if the certificate subject is an

organization, then an authorized representative of that organization shall have to request for the certificate on behalf of the organization, in such case the proof of that authorization shall have to be submitted to BBCA which is different from organization to organization.

In case of government organization, the head of the organization can directly apply for the certificate or his authorized representative can request for the certificate along with the authorization letter signed by the head of the organization.

In case of any private limited company, the Chairman or the Board of Directors or Chief Executing Officer or Managing Director or equivalent of that company may apply directly for the certificate or any person authorized by the Board of Director or Chairman or equivalent may apply for the certificate.

In case of Sub-CA and RA certificate issuance, BBCA will rigorously and physically verify the information given by the Sub-CA or RA applicant before issuing certificate and approving such service.

In all cases BBCA will verify the identity of the authorized person and the organization depending on the certificate type and class.

3.2.3 Authentication of Individual Identity

BBCA verification team verifies the authenticity of the subscriber requesting for personal certificate. The verification process depends on the class of certificate.

3.2.4 Non-Verified Subscriber Information

BBCA does not include any non-verified subscriber information for any class of certificates though for Class 0 and Class 1 certificate BBCA will collect and preserve certain information which will not be verified by the validation team of BBCA. Information that will not be verified for Class 0 and Class 1 certificates are:

- Identity Value (NID/Passport/TIN/Birth Registration Number);
- Address of the Subscriber

3.2.5 Validation of Authority

BBCA shall validate by its validation team to determine whether a person has specific rights, entitlements, or permissions, including the permission to act on behalf of an organization to obtain a certificate.

3.2.6 Criteria for Interoperation

No Stipulation.

3.3 *Identification and Authentication for re-key Requests*

3.3.1 Routine re-key

BBCA maintains the identification and authentication process of routine re-key which is similar to the identification and authentication process of certificate renewal of a subscriber or RA or Sub-CA.

3.3.2 Re-key After Revocation

BBCA does not allow any re-key after the revocation of the certificate. In such case, subscriber or RA or sub-CA must go through initial identity validation process to get a new certificate.

3.4 *Identification and Authentication for Revocation Request*

BBCA verifies the identity and authenticity of the requestors for revocation. BBCA ensures that the revocation request is generated from the authorized entity before processing the revocation. See section 4.9.1 and 4.9.2 for details on what circumstance who can request a certificate revocation.

4 Certificate Life-Cycle Operational Requirements

4.1 *Certificate Application*

This CPS section describes the followings regarding subject certificate application:

- Who can submit a certificate application;
- Enrollment process used by subjects to submit certificate applications;
- Responsibilities of different entities in connection with the application process.

4.1.1 Certificate Application Submission

The end user entity, i.e. Sub-CA, RA or Subscriber (personal/organization/device) can apply to BBCA for digital certificate. The subscriber entity is required to apply through prescribed application form and other application procedure. The verification team of BBCA will verify the identity and authenticity of the entity applying for digital certificate prior to certificate issuance. RA of BBCA can also apply on behalf of a subscriber entity for digital certificate.

4.1.2 Enrollment Process and Responsibilities

Enrollment process is used by subjects to submit certificate applications and responsibilities in connection with this process. The subject may generate the key pair and sends a certificate request to the RA. The RA validates and signs the request and sends it to the BBCA. BBCA has the responsibility of establishing an enrollment process in order to receive certificate applications. Likewise, certificate applicants have the responsibility of providing accurate information on their certificate applications.

4.2 *Certificate Application Processing*

4.2.1 Performing Identification and Authentication Functions

After a Certificate Applicant submits a Certificate Application, BBCA attempts to confirm the information in the Certificate Application (other than Non-Verified Subscriber Information) pursuant to 3.2.2.

4.2.2 Approval or Rejection of Certificate Applications

Upon successful performance of all required authentication procedures pursuant to 3.1.1 and 3.2.2, BBCA approves the Certificate Application and issues a Certificate based on the

information in the Certificate Application. If authentication is unsuccessful, BBCA rejects the Certificate Application.

4.2.3 Time to Process Certificate Applications

BBCA makes reasonable efforts to confirm certificate application information and issue a digital certificate within a reasonable time frame. The time frame is greatly dependent on the applicant providing the necessary details and documentation in a timely manner. Upon the receipt of the necessary details and documentation, BBCA aims to confirm submitted application data and to complete the validation process and issue or reject a certificate application within fifteen (15) working days.

4.3 *Certificate Issuance*

4.3.1 CA Actions during Certificate Issuance

Upon issuance, Certificates are made available to end-user Subscribers, either by allowing them to download from a website (such as their Certificate Status Page) or via a message sent to the Subscriber containing the Certificate. For example, BBCA may send the Subscriber a PIN, which the Subscriber enters into an enrollment web page to obtain the Certificate. The Certificate may also be sent to the Subscriber in an e-mail message.

4.3.2 Notification to Subscriber about Issuance of Certificate

Upon Certificate generation, BBCA notifies Subscribers that their Certificates are available and notifies them of the means for obtaining such Certificates.

4.4 *Certificate Acceptance*

4.4.1 Conduct Constituting Certificate Acceptance

Downloading a Certificate or installing a Certificate from a message attaching it constitutes the Subscribers acceptance of the Certificate.

4.4.2 Publication of the Certificate by the CA

BBCA will publish the public key of the subscriber into its public key repository as soon it's been issued and accepted by the subscriber.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.5 *Key Pair and Certificate Usage*

4.5.1 Subscriber Private Key and Certificate Usage

Use of the Private key corresponding to the public key in the certificate shall only be permitted once the Subscriber has agreed to the Subscriber Agreement and accepted the certificate. The certificate shall be used lawfully in accordance with BBCA's Subscriber Agreement, ICT Act 2006, IT (CA) Rules 2010 and Subscriber obligations set forth in section 9.6.3 of this CPS.

Certificate usage must be consistent with the KeyUsage field extensions included in the certificate (e.g., if Digital Signature is not enabled then the certificate must not be used for signing). Subscribers shall protect their private keys from unauthorized use and shall discontinue use of the private key following expiration or revocation of the certificate. Parties other than the Subscriber including BBCA shall not archive the Subscriber Private Key.

4.5.2 Relying Party Public Key and Certificate Usage

See section 9.6.4.

4.6 *Certificate Renewal*

Certificate renewal is the issuance of a new certificate without changing the public key or any other information in the certificate. Certificate renewal is not supported for BBCA issued certificates. For renewal purposes, subscriber shall follow re-key procedure section 4.7.

4.7 *Certificate Re-key*

Re-keying a certificate (key update) refers to the issuance of new certificate with a different key pair and serial number while retaining other subject information from old certificate. The new Certificate may be assigned a different validity period and/or signed using a different issuing CA private key.

4.7.1 Circumstances for Certificate Re-Key

Manual Certificate re-key may take place after a certificate is revoked and the subscriber information is still accountable. Manual Certificate re-key may also be performed within one-month of certificate expiry, or after certificate expiry. Automatic updates of managed digital IDs and any or all the certificates constituting the digital ID may be performed on or after reaching 80% of the certificate lifetime.

4.7.2 Who Can Request a Certificate Re-Key

Certificate re-key may be requested by:

- the Sub-CAs for its Sub-CA certificate,
- a subscriber for his/her individual certificate,
- a manufacturer/organization for a device certificate, or
- an authorized representative for an Organizational Certificate.

4.7.3 Processing certificate re-key request

See Section 3.3

4.7.4 Notification of re-keyed certificate issuance to subscriber

No Stipulation

4.7.5 Conduct constituting acceptance of a re-keyed certificate

No Stipulation

4.7.6 **Publication of the re-keyed certificate by the CA**

No Stipulation

4.7.7 **Notification of re-keyed certificate issuance by the CA to other entities**

No Stipulation

4.8 ***Certificate Modification***

Certificate modification for all applicants will be accomplished through Certificate re-key. No other form of certificate modification is supported by BBCA.

4.9 ***Certificate Revocation and Suspension***

4.9.1 **Circumstances for Revocation**

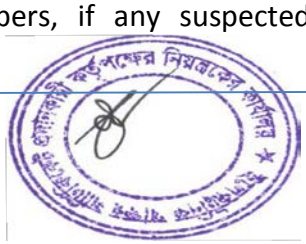
A certificate will be revoked when the information it contains is suspected to be incorrect or compromised. This includes situations where:

- CCA suspend or revoke the license as per Section of the ICT Act 2006 (amended in 2009);
- Contravened any provisions of the ICT Act 2006 and Rules made there under;
- The Subject has failed to meet its obligations under this CPS or any other applicable Agreements, regulations, or laws;
- BBCA determines that a Certificate was not issued correctly in accordance with this CPS;
- The Subscriber's private key is suspected to be compromised;
- The cryptographic storage device of the Subscriber is lost or stolen; or If he/she no longer wishes to use the certificate.
- If Subscribers, Relying Parties and other third parties suspect Secure Site Certificate misuse, or other types of fraud, compromise, misuse, inappropriate conduct, or any other matter related to Certificates. The CA shall do the appropriate investigation before taking any action on the request through respective CSP.
- Subscriber or other authorized agent asks for his/her Certificate to be revoked.
- Any other reason deems required revocation of the certificate of the licensee by BBCA.

4.9.2 **Who Can Request Revocation**

A request to revoke an end user certificate can be done by the following entities:

- BBCA can request the revocation of any certificates issued by any CA participating in the National PKI,
- BBCA can request the revocation of any certificates issued under its authority,
- BBCA can request the revocation of any RA or LRA certificates,
- RA can request the revocation of any of their Subscribers Certificate,
- The RA for their own certificate, if any suspected misuse has been attributed to their given Certificates.
- Subscribers, if any suspected misuse has been attributed to their given



Certificates, can request a revocation.

- A legal, judicial or regulatory agency can request certificate revocation, within applicable laws.
- Office of the CCA can also initiate revocation request for certificate with a valid reason;

4.9.3 Procedure for Revocation Request

A request to revoke a certificate shall identify the certificate to be revoked, explain the reason for revocation, and allow the request to be authenticated (e.g., digitally or manually signed). The CA or RA shall authenticate the request as well as the authorization of the requester in accordance with the applicable agreements.

4.9.4 Time within which Root CA must process the revocation request

Root CA shall process authorized revocation requests within 24 hours or as per Root CA CPS.

4.9.5 CRL Issuance Frequency

After the revocation request is received by BBCA, the concerned certificate will be revoked as per the procedure of certificate revocation, at the earliest. The revoked certificate will be added to the CRL immediately as part of this revocation procedure. The latest CRL will be available round the clock for downloading. In unforeseen circumstances the certificate will be revoked in not more than three working days after receiving the certificate revocation request. On detection of serious key compromise, the corresponding digital certificate is revoked, CRL generated and published immediately.

4.9.6 Maximum latency for CRLs

The Root CA will publish its CRLs at least once every 24 hours or as per Root CA CPS, and at the time of any Certificate revocation of its subscribers.

4.9.7 Online Revocation/status checking availability

BBCA may provide access to an OCSP Responder covering the issued certificates.

4.9.8 Online Revocation checking requirements

BBCA may make its Certificate status information available through an OCSP responder.

4.9.9 Other forms of revocation advertisement available

No stipulation.

4.9.10 Circumstances for Suspension

Same as 4.9.1

4.10 *Certificate Status Services*

The relying parties can check the status of a certificate online from the repository of CCA.

4.11 *End of Subscription*

Revocation of certificates will not be required if the certificate is expired prior to or upon end of subscription.

4.12 *Key Escrow and Recovery*

No Stipulation.

4.13 *Security Audit Procedures*

Security audit will be performed at least once a year.

5 Facility, Management and Operational Controls

5.1 *Physical Security Controls*

5.1.1 Site Location and construction

BBCA is operated by Bangladesh Bank and the construction of BBCA infrastructure complies with the best practices and proper security controls. BBCA follows the physical security requirements specified as below:

- Denies unauthorized access to the CA hardware and other related infrastructures,
- Store all removable media and paper containing sensitive plain-text information in data safe;
- Monitor, either manually or electronically, for unauthorized intrusion at all times,
- Maintain and periodically inspect access logs.

5.1.2 Physical Access

BBCA Data center is situated in the Bangladesh Bank Data Center operated by BB. It maintains Tier-3 data center features for physical access. The CA infrastructure is isolated from other infrastructure in the data center using glass cage.

5.1.3 Power and Air Conditioning

BBCA 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 PAC system.

5.1.5 Fire prevention and protection

BBCA data center is protected by central Fire prevention system. Fire alarm and gas extinguisher (ceiling mounted) is deployed as part of the fire prevention system. Also, hand fire extinguishers are mounted at the entrance of the data center.

5.1.6 Media Storage

Cryptography token is used for primary storage media of Root CA key pairs. It is preserved inside a Safe kept into the Root CA Strong Room. Other medias are DVD, Hard Disk, Tapes to store LDAP, certificate, CRLs, Root CA documents and other relevant software.

5.1.7 Waste Disposal

The Data center is cleaned once in every 7 days. Destruction of cryptographic devices is performed as per manufacturer's guideline before disposal. Media and documents not needed will be destroyed using appropriate disposal process.

5.1.8 Off-site Backup

System and Data are backed up into tape and stored in Strong Room. The backup is taken whenever any new certificate or CRL issued or in every 6 months.

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. The people selected to fill these roles must be extraordinarily responsible. The functions performed in these roles form the basis of trust for all uses of BBCA. The following are the trusted roles for BBCA:

- Director
- Security Manager
- CA Manager
- RA Manager
- Application Manager
- Application Developer
- Web Administrator
- RA
- Assistant Engineer
- Assistant Programmer
- Operator

5.2.2 Number of Persons required per Task

BBCA ensures separation of duties for critical CA functions to prevent one person from maliciously using the PKI systems without detection. Each user's system access is limited to those actions for which they are required to perform in fulfilling their responsibilities. Separate individuals shall fill each of the roles specified in Section 5.2.1. This provides the maximum security and affords the opportunity for the greatest degree of checks and balances over the system operation. Activation of the CA certificate signing Private Key shall require actions by at least two individuals.

5.2.3 Identification and authentication for each role

An individual must be identified and authenticated for any action to be performed that is beyond to his/her role.

5.2.4 Roles requiring separation of duties

No individual will be assigned more than one trusted Role.

5.3 *Personnel Security Controls*

5.3.1 Qualification, Experience and Clearance requirements

Qualification, Experience and clearance of the CA operations personnel are verified as per

standard recruitment rules and regulations of the Bangladesh Bank.

5.3.2 Background Check Procedures

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

5.3.3 Training Requirements

BBCA ensures that all personnel have appropriate training. Such training addresses relevant topics such as PKI, Cryptography, CA Operation Procedure, CA HSM administration, Security requirements, operational responsibilities and associated procedures.

5.3.4 Retraining Frequency and Requirements

Any significant change in CA operations, such as changes/upgrades in CA software, requires some sort of training. This type of training is delivered through as per documented training plan.

5.3.5 Job Rotation frequency and sequence

Job rotation frequency for every role is 12 months as on when necessary.

5.3.6 Sanctions for unauthorized actions

BBCA 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

No Stipulation.

5.3.8 Documentation Supplied to personnel

BBCA will make all the guidelines issued by BBCA, BBCA CPS, Operational Procedure and other relevant documents available to its personnel required to perform their jobs.

5.4 *Audit Logging Procedure*

5.4.1 Types of Events Recorded

BBCA ensures recording of all events in audit log files related to the security of the BBCA system. All security audit capabilities of the BBCA operating system and BBCA applications are enabled. Such events include, but are not limited to:

- System start-up and shutdown;
- BBCA application start-up and shutdown;
- Attempts to create, remove, set passwords or change the system privileges of the PKI users and Administrators;
- Changes to BBCA details and/or keys;
- Changes to certificate creation policies (e.g. validity period);

- Login and logout attempts;
- Unauthorized attempts at network access to the BBCA system;
- Unauthorized attempts to access system files;
- Generation of BBCA keys;
- Creation and revocation of certificates;
- Attempts to initialize, remove, enable, and disable Subscribers or Designated
- Certificate Holders, as well as attempts to update and recover their keys;

5.4.2 Frequency of Processing Data

Audit log is processed and archived whenever the audit log is 60% full.

5.4.3 Retention period for Security Audit Data

Frequency of processing log will be maintained as per CCA determined.

5.4.4 Protection of Security Audit Data

BBCA protects audit information and log from unauthorized viewing, modification, deletion or destruction. Only the designated personnel of BBCA can have access to the audit logs.

5.4.5 Security Audit Data Backup Procedure

BBCA does backup all audit data as per section 5.5 of this document.

5.4.6 Audit Collection System (Internal or External)

Audit collection system is internal to BBCA. Auditable events are generated from both automated and manual processes. Control measures of both automated and manual processes are audited.

5.4.7 Notification to Event-Causing Subject

Event–causing subjects are not notified.

5.4.8 Vulnerability Assessment

No Stipulation.

5.5 *Records Archival*

5.5.1 Types of Event Recorded

The following events are recorded and archived

- Certification requests;
- Issued certificates;
- Issued CRLs;
- All e-mail correspondence;

5.5.2 Retention Period for Archives

Minimum retention period for archives log will be maintained as per CCA determined.

5.5.3 Protection of Archive

Only authorized personnel are permitted to review the archive. The contents of the archive are not released except as determined by BBCA or as required by law.

5.5.4 Archive Backup Procedure

Archives are written to tape/DVD, at least 2 copies. 1 copy is stored into the strong room of BBCA and another copy in CA's Safe.

5.5.5 Requirements for time-stamping of Records

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

5.5.6 Archive Collection System (Internal or External)

Only authorized and authenticated personnel are allowed to handle archive.

5.5.7 Procedures to obtain and verify archive information

Backup media is verified just after taking backup operation. Off-site back up is also verified once in 6 months for integrity.

5.6 *Key Changeover*

BBCA supports key changeover to minimize risk to the integrity of the BBCA keys. Once changed, the new key will be made available. The unexpired older keys are used to sign CRL's until all certificates signed by the unexpired older private key have expired.

5.7 *Compromise and Disaster Recovery*

5.7.1 Incident and Compromise Handling Procedures

If the BBCA or other CA detects a potential hacking attempt or other form of compromise to PKI, it shall perform an investigation in order to determine the nature and the degree of damage. If the BBCA key is suspected of compromise, it'll revoke its key pair and generate new key pair.

5.7.2 Computing Resources, Software and/or Data are corrupted

Backup copies of hardware, system, databases, and private keys are used in order to rebuild the BBCA capability in case of software and/or data corruption.

5.7.3 BBCA private key Compromise Recovery Procedure

If BBCA private key is compromised or is suspected to be compromised, it will:

1. Inform all subscribers about that;
2. It'll publish a public notice through web and newspapers (at least 2 national)
3. Terminate the certificates and CRL distribution services for certificates and CRLs issued using the compromised key.
4. Inform Office of the CCA

5.7.4 Business Continuity Capabilities after a Disaster

In the case of a disaster whereby BBCA installation is physically damaged and all copies of the CA Signing Key are destroyed as a result, BBCA shall request that certificates need to be revoked, and to take to re-establish of BBCA, and will follow whatever processes have been set forth in the respective Agreement for that purpose.

5.8 *BBCA Termination*

If BBCA terminates its operation by the government policy or acts or whatsoever, BBCA 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 BBCA, and other third parties or relying parties.

In such case, BBCAs shall stop their operation within the period noticed by CCA. BBCA shall revoke all the issued certificates within that noticed period and shall issue any new certificate after such notification.

6 Technical Security Controls

6.1 *Key Pair Generation and Installation*

6.1.1 Key Pair Generation

BBCA will generate its own key pair with a ceremony known as Key Generation Ceremony (KGC). The Key Generation Ceremony is a formal procedure, and will be done maintaining multi person control. The CA Key Pair will be generated inside a FIPS 140-2 Level 3 validated Hardware Security Module.

6.1.2 Private Key Delivery to Subscriber

If key pairs are generated by the Subscriber, then delivery is not required, otherwise, the private keys shall be delivered to the Subscriber electronically using industry standard secure protocols. In case the Signing Private keys are generated by the CA or RA, then the CA or RA shall not retain any copy of the Signing Private Keys after delivery to the Subscriber. In addition, the Subscriber shall acknowledge receipt of the private key(s).

6.1.3 Public Key Delivery to Certificate Issuer

Applicant public keys must be delivered for certificate issuance using industry standard secure protocol.
In respect of Server certificate, the Applicant's Public Key which will be generated by the Applicant must be transferred to BBCA using a method designed to ensure that:

- The Public Key is not changed during transit; and
- The sender possesses the Private Key that corresponds to the transferred Public Key.

6.1.4 CA Public Key Delivery to relying parties

BBCA will ensure that its subscribers and relying parties receive and maintain the trust anchor

in a trustworthy fashion. Methods for trust anchor delivery may include:

- A trusted role loading the trust anchor onto Tokens delivered to Subscribers via secure mechanisms,
- Distribution of trust anchor through secure out-of-band mechanisms,
- Calculation and comparison of trust anchor hash or fingerprint against the hash made available via authenticated out-of-band sources, or
- Downloading trust anchor from web sites secured with a currently valid certificate of equal or greater assurance level than the Certificate being downloaded and the site trust anchor already on the Subscriber system via secure means.

6.1.5 Key Sizes

BBCA and subscriber key size is 2048 bits.

6.1.6 Public Key Parameters Generation

The HSM pseudo-random number generator is validated by NIST. Public key parameters prescribed are generated in accordance with industry best practices.

6.1.7 Parameter Quality Checking

No stipulation.

6.1.8 Key usage Purposes

Public keys that are bound into certificates shall be certified for use in authenticating, signing or encrypting, as specified by BBCA. The use of a specific key is determined by the key usage extension in the X.509 certificate. BBCA key is used for certificate and CRL signing.

6.2 *Private Key Protection and Cryptographic Module Engineering Controls*

6.2.1 Cryptographic Module Standards & Controls

BBCA uses a FIPS 140-2 Level 3 validated Hardware Security Module. The HSM is control by multiple persons. The cryptographic module is kept in a data safe and when necessary (e.g to sign any CSR), it is taken out with access of multiple persons.

6.2.2 Private Key multi person control

The private key is stored in the cryptographic module and accessibility to the private key is controlled complying *n out of m* rule. The operation using the private key is also controlled with *n out of m* rule.

6.2.3 Private Key escrow

No Stipulation.

6.2.4 Private Key backup

BBCA private key is backed up in backup token of the cryptographic module ensuring multi person control.

6.2.5 Private Key archival

BBCA private key is not archived after it is expired.

6.2.6 Private Key Storage on cryptographic Module

BBCA private key stored only on a cryptographic module which is FIPS 140-2 Level 3 validated.

6.2.7 Method of Activating Private Key

The private key is activated after it's been generated using multi person control. The detail methods are defined in "BBCA Operation Manual" & "Handbook for Key Generation Ceremony".

6.2.8 Method of Deactivating Private Key

The private key is deactivated after it's been expired using multi person control.

6.2.9 Method of Destroying Private Key

The private key is destroyed after it's been deactivated using multi person control.

6.3 *Other Aspects of Key Pair Management*

6.3.1 Public Key Archival

BBCA public key will be archived and will be kept secure. And in case of subscriber the Public Key is archived as part of the certificate archive process.

6.3.2 Certificate operational periods and key pair usage period

Once BBCA certificate is generated, it is valid for 5 years. Subscriber certificates are valid for either 1 or 2 years depending on the subscribers requirement.

6.4 *Activation Data*

BBCA private key is protected by a FIPS 140-2 Level 3 compliant device. Access is multi person controlled. Access procedures are confidential.

6.5 *Computer Security Controls*

6.5.1 Specific Computer Security Technical Requirements

The server, hosting BBCA product, is built from a vendor CD with reasonable provenance. No other services or software are loaded or operated on the CA servers. The server will receive occasional patches and other adjustments if the security risk warrants, in the judgment of BBCA.

6.5.2 Computer Security Rating

The CA software shall be certified under the Common Criteria or a level equivalent to Common Criteria EAL 4.

6.6 *Life-Cycle Security Controls*

6.6.1 System Development Controls

The BBCA design, installation, and operation will be documented by qualified personnel. BB operations personnel, will develop and produce appropriate qualification documentation establishing that BBCA components are properly installed and configured, and operate in accordance with the technical specifications.

6.6.2 Security Management Controls

The configuration of the BBCA systems as well as any modifications and upgrades shall be documented and controlled. In such case Bangladesh Bank ICT Policy, ISMS and ISO 27002 guidelines shall be followed by BBCA. There shall be a mechanism for detecting unauthorized modification to software or configuration. A formal configuration management methodology shall be used for installation and on-going maintenance of the system.

6.6.3 LIFE CYCLE SECURITY RATINGS

No stipulations.

6.7 *Network Security Controls*

BBCA shall employ appropriate security measures to ensure they are guarded against denial of service and intrusion attacks. Also it shall employ network security and firewall management, including port restrictions and IP address filtering. Any boundary control devices used to protect the network on which PKI equipment is hosted shall deny all but the necessary services to the PKI equipment.

6.8 *Time Stamping*

Time stamping shall be supported for the Certificates, CRLs, and other revocation database entries containing time and date information.

7 Certificate, CRL and OCSP Profiles

7.1 *Certificate Profile*

7.1.1 Version number

X.509 v3.

7.1.2 Certificate Extensions

authorityKeyIdentifier: Hash value of CA public key
subjectKeyIdentifier: Hash value of CA public key
Key Usage: Certificate Signing, Off-line CRL Signing, CRL Signing
Certificate Policy: OID Specific
subjectAltName: Not Used by Root CA
Basic Constraints: CA
cRLDistributionPoints: crl.bb.org.bd

7.1.3 Algorithm Object identifiers

Signature Algorithm is 1.2.840.113549.1.1.11 SHA256 with RSA Encryption

7.1.4 Name Forms

CCA prefers that organizations use domain component naming. For Root CA, the DN is:

CN=	BBCA
O (Organization) =	Bangladesh Bank
OU=	Certification Authority
HouseIdentifier=	Head Office
StreetAddress=	Motijheel
Locality=	Dhaka
PostalCode=	1000
C (Country) =	BD

7.1.5 Name Constraints

Not used by BBCA.

7.1.6 Certificate Policy Object Identifier

No Stipulation

7.1.7 Usage of Policy Constraints Extensions

No Stipulation

7.1.8 Policy qualifier syntax and semantics

Not supported.

7.2 *CRL Profile*

7.2.1 Version

X.509 v2.

7.2.2 CRL and CRL Entry Extensions

ReasonCode (Mandatory, non-critical): Values of this field may be:

keyCompromise (1), cACompromise (2), affiliationChanged (3), superseded (4), cessationOfOperation (5), certificateHold (6), removeFromCRL (8), privilegeWithdrawn (9) or aACompromise (10)

invalidityDate : GeneralizedTime

7.3 *OCSP Profile*

In accordance with RFC 2560.

8 Compliance Audit & Other Assessments

The CA operation may be reviewed by any cross certifying organization or potential relying organization or internally whichever approved by the CCA.

8.1 *Frequency or circumstances of assessment*

BBCA infrastructure and its operations are audited once a year as per the audit checklist of Office of the CCA. Apart from that BBCA maintains internal audit at least once a year.

8.2 *Identity/qualification of assessor*

The auditor need to be competent in the field of compliance audits for security and PKIs, and shall be thoroughly familiar with requirements that the Office of the CCA imposes on the issuance and management of certificates. The compliance auditor shall perform such compliance audits as a primary responsibility.

8.3 *Assessor's relationship to assessed entity*

To provide an unbiased and independent evaluation, the auditor and audited party shall not have any current or planned financial, legal or other relationship that could result in a conflict of interest.

8.4 *Topics covered by assessment*

The audit verifies if the BBCA is in compliance with requirements specified in the BBCA CPS, SOP and any documents referenced in them, and any relevant Operating Policies and Procedures.

8.5 *Actions taken as a result of deficiency*

If irregularities are found by the auditor, BBCA informed in writing to Office of the CCA about the findings. BBCA submits a report to the auditor as to any remedial action to be taken in response to the identified deficiencies. This report includes a timeline for completion in consultation with the auditor.

8.6 *Communication of results*

An Audit Compliance Report, including identification of corrective measures taken or being taken by the BBCA, is provided to the CCA.

9 Other Business and Legal Matter

9.1 *Fees*

9.1.1 Certificate issuance and renewal fees

BBCA follows the rate limit for certificate fee issued by Office of the CCA.

9.1.2 Certificate Access fees

BBCA follows the rate limit for certificate fee issued by Office of the CCA.

9.1.3 Revocation or status information access fees

BBCA follows the rate limit for certificate fee issued by Office of the CCA.

9.1.4 Fees for other service

BBCA follows the rate limit for certificate fee issued by Office of the CCA.

9.1.5 Refund Policy

Refunds are not applicable for the Digital Certificates for which no fees are charged.

9.2 *Financial Responsibility*

No Financial responsibility is involved with BBCA.

9.2.1 Insurance Coverage

No insurance coverage is provided by BBCA.

9.2.2 Other assets

The BBCA maintains sufficient financial resources to maintain its operations and fulfill other duties.

9.2.3 Insurance or Warranty coverage for end entities

BBCA 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

Any corporate or personal information held by the BBCA related to the application and issuance of CA Certificates is considered confidential and will not be released without the prior consent of the relevant holder, unless required otherwise by law or to fulfill the requirements of this CPS, and in accordance with the Privacy policy.

9.3.2 Information not within the scope of confidential information

BBCA service collects information about the licensed CA. Information included in issued certificates and CRLs is not considered confidential.

9.3.3 Responsibility 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

BBCA will prevent subscriber and relying parties information from disclosure.

9.4.2 Information treated as private

Information collected from CAs under a confidentiality agreement are treated as private.

9.4.3 Information not deemed as private

Information made available public by BBCA is not private.

9.4.4 Responsibility to protect private information

Any sensitive information shall be explicitly identified in the agreement with the contracting party. Access to this information shall be restricted to those with an official need-to-know in order to perform their official duties.

9.4.5 Notice and consent to use private information

Any use of private information by BBCA will be subjected to consent from the party.

9.4.6 Disclosure pursuant to judicial or administrative process

Any disclosure shall be handled in accordance with the Privacy policy of Bangladesh government.

9.4.7 Other information disclosure circumstances

No Stipulation.

9.5 *Intellectual Property Rights*

No Stipulation.

9.6 *Representation and Warranties*

9.6.1 BBCA representation & warranties

BBCA will:

- Accept certification requests from licensed CAs only;
- Issue certificates based on the requests from authenticated CAs;
- Publish the issued certificates;
- Accept revocation requests according to the procedures outlined in this document;
- Authenticate CAs requesting the revocation of a certificate;
- Issue a Certificate Revocation List (CRL);
- Publish the CRL issued;

Keep audit logs of the certificate issuance and revocation process.

9.6.2 **Relying Party representation & warranties**

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, it's 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 BBCA.

Relying parties may:

- Check that the Licensed CA certificate and Subscriber certificate is not on the CCA root CRL and BB CRL.

9.6.3 **Repository representation & warranties**

BBCA will provide access to BBCA information, as outlined in section 2.6.1, on its web site or other participating web sites. The BBCA Repository can be found at:

www.bb.org.bd

The following pages deal with individual items from 2.6.1:

CA information: http://www.bb.org.bd

CRL information PEM:

http://crl.bb.org.bd

9.7 ***Disclaimers of Warranties***

BBCA only signs sub-CA, RA and subscribers certificates according to the practices described in this document. No liability, implicit or explicit, is accepted.

BBCA and its agents make no guarantee about the security or suitability of a Sub-CA that is signed by the BBCA. The BBCA 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. BBCA denies any financial or any other kind of responsibility for damages or impairments resulting from its operation.

9.8 ***Limitations of Liability***

BBCA denies any financial or any other kind of responsibility for damages or impairments resulting from its CA operation.

The BBCA will not incur any liability to Subscribers or any person to the extent that such liability results from their negligence, fraud or willful misconduct.

9.9 *Indemnities*

The subscribers, CAs and Relying Partiers shall indemnify, defend and hold harmless the BBCA, 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.

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 BBCA policy and CPS. It is expected that, over time, a set of standard policies profiles will emerge, and BBCA may adapt if deemed so. BBCA is responsible for the CPS. All changes must be approved by BB authority.

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*

The document is available at: http://www.bb.org.bd

9.12 *Amendments*

9.12.1 **Procedure for amendment**

The BBCA shall review this CPS at least once per year. Errors, updates, or suggested changes to this CPS shall be notified through website of BBCA. After 30 days of notification the CPS will automatically be effected. For critical changes BBCA may communicate to the PKI participants.

9.12.2 **Notification mechanism and period**

BBCA will publish necessary updates, changes in the form of notice/press release in its web site.

9.12.3 **Circumstances under which OID must be changed**

The policy OID shall only change if the change in the CPS results in a material change to the trust by the relying parties, as determined by the BBCA, in its sole discretion informing Office of the CCA.

9.13 *Dispute Resolution Procedure*

The use of certificates issued by BBCA is governed by contracts, agreements, and standards set forth by BB. Those contracts, agreements and standards include dispute resolution policy

and procedures that shall be employed in any dispute arising from the issuance or use of a certificate governed by this CPS. Dispute Resolution mechanism is described in BB Dispute Resolution Policy.

9.14 *Governing Law*

This policy is subordinate to all applicable Bangladesh government laws and statutes including ICT Act 2006 and rules there under.

9.15 *Compliance with Applicable Law*

This policy is subordinate to all applicable Bangladesh government laws and statutes including ICT Act 2006 and rules there under.

9.16 *Miscellaneous Provisions*

No Stipulation.

9.17 *Other Provisions*

No Stipulation.