Classification: Public

BCC

Certifying Authority

Certification Practice Statement (CPS)

Version: 1.0.3

Bangladesh Computer Council
Information and Communication Technology Division

Contents

Revision History

Version	Date	Revision Number	Updates
1.0	19 April 2016		
1.0.1	02 June 2016	1	As per recommendation of CCA
1.0.2	19 December 2016	2	To comply with the changes made in Digital Certificate Interoperability Guideline,2016
1.0.3	11 April 2019	3	License Renewal Purpose

Document Control

Document Name	Bangladesh Computer Council Certification Practice Statement (BCC CPS)
Classification	Public
Document Location	http://repo.bcc-ca.gov.bd/CPS
Maintenance Owner	BCC CA Document Manager
Approval owner	BCC CA Document Manager
Release Date	11/04/2019
Next Review Date	As when necessary

1 Introduction

1.1 Overview

1. This document is the Certification Practice Statement (CPS) of Bangladesh Computer Council (BCC) Certifying Authority. This CPS governs the use of Public Key Infrastructure (PKI) services within the BCC Certification Authority (CA) which is an autonomous organization of the Government of Bangladeshand licensed Certifying Authority ofOffice of the Controller of Certifying Authorities (CCA),Information & Communication Technology Division.
2. CCA has accredited BCC as a licensed CA under the CCA hierarchical PKI Trust Network resulting in a BCC CA certificate being signed under the CCA Root CA.
3. Subscriber certificates issued from BCC Managed PKI services chain up to the BCC CA (collectively known as the BCC Sub-Domain participants of the CCA PKI Trust Network) with the BCC CA signed under the CCA RootCA (The top level trust point of the CCA PKI Trust Network)
4. The BCC CPS states the practices that the BCC CA employ in providing certification services to BCC Sub-Domain participants in accordance with the regulations and Guidelines of the CCA.
5. This CPS is applicable to:
   a) BCC hosted and controlled CA;
   b) BCC Infrastructure CAs and BCC Administrative CA'ssupporting the BCC Certificate Lifecycle Platform;
   c) All Sub-ordinate CA's hosted and controlled by BCC within the CCA and BCC certificate hierarchy.
6. Disclosure of the CPS is detailed in the Subscriber and/or Relying Party Agreements.
7. This CPS and any subordinate CPS', where used, shall be approved by BCCand the CCA.
8. In some instances, this CPS refers to ancillary confidential security and operational documents for specific detailed practices, where including the specifics in this CPS could compromise the security of the BCCPKI.

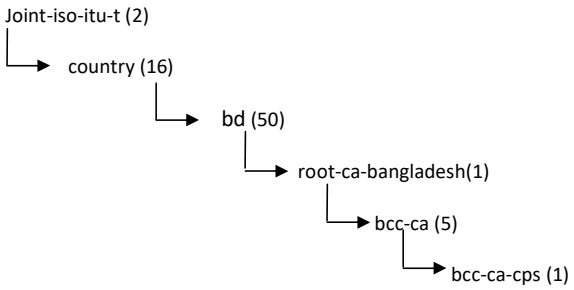
1.2 Document Name and Identification

Document Name:	**Bangladesh Computer CouncilCertification Practice Statement (BCC CPS)**
Document Public Location:	**http://repo.bcc-ca.gov.bd/CPS**
Document X.500 OID:	**2.16.50.1.5.1**

Comment [U1]: BCC-CA.GOV.BD is the new CA domain registered under .BD

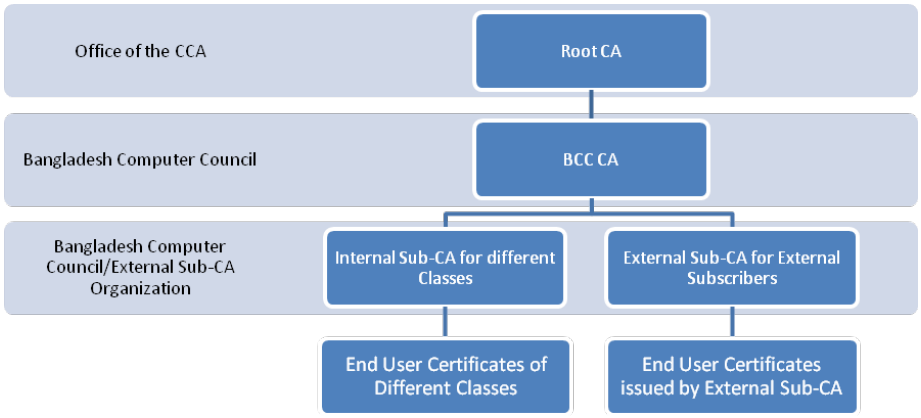
1. Policy Object Identification

1. The OIDs registered by BCCfor the Certification Practice Statement policy is shown below. These OIDs are registered under the BCCarc as:



1.3 PKI Participants

BCC follows the following hierarchy for issuing certificates to the subscribers:



1.3.1 Certification Authorities

1. Certification Authorities (CA) are entities licensed by CCA to sign and issue certificates under the CCA PKI Trust Network. For the purpose of this CPS, CCA acts as the Root CA and BCC is a Sub-Domain CA that issues certificates to BCC Subordinate CAs and end-user Subscribers.
2. BCC Managed PKI customers may operate their own CA's as Subordinate CA's to the BCC CA. The Subordinate CA's are part of the CCA PKI Trust Network and are contracted to abide by this CPS.
3. BCC will also operate a BCC Internal Administrator CA hierarchy that is limited to BCC internal Managed PKI service administration activities.

1.3.2 Registration Authorities

1. Registration Authorities (RA) are entities authorised by BCC to perform identification and authentication of certificate applicants requesting the issuance of end-user certificates.
2. Certificate requests are either denied and the applicant is notified or approved by the RA with the certificate requestsent to the CA for generation of a digital certificate.

1.3.3 Subscribers

1. Subscribers are the applicants that have been approved by the RA to receive an end-entity certificate signed by the CA.
2. All Subscribers agree to be bound by the terms of the applicable Subscriber Agreement in order to be issued certificates.
3. Where a Subscriber delegates responsibility for initiating applications for certificates to a system, the Subscriber agrees to ensure that the system meets the terms and conditions of the Subscriber Agreement.

1.3.4 Relying Parties

1. Relying Parties rely on the binding of the Public Key to the identity of a subject in a certificate to the stated level of certification assurance.
2. All Relying Parties agree to be bound by the terms of a Relying Party Agreement. The act of relying on BCCissued CCA Trust Network certificate constitutes acceptance of any applicable Certificate Policy and Relying Party Agreement.

1.3.5 Other Participants

1.3.5.1 Auditors and Assessors

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

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

1. Certificates issued under the BCC CA hierarchy are provisioned to end-entitiesfor the purpose of digital signing, encryption/decryption of data and/or authentication to Relying Party applications and services. While the most common usages for end-entity certificates are included in Table 1 below, an end-entity certificate may be used for other purposes, provided that a Relying Party is able to reasonably rely on that certificate and the usage is not otherwise prohibited by law, a CP, the CPS under which the certificate has been issued and any agreements with Subscribers.

2.

Certificate Class	Assurance Level				Usage		
	No Assurance	Low Assurance	Medium Assurance	High Assurance	Signing	Encryption	Client Auth
Class 1 Certificates		✓			✓	✓	✓
Class 2 Certificates			✓		✓	✓	✓
Class 3 Certificates				✓	✓	✓	✓

Table 1 – End-Entity Certificate Usage

Apart from the above BCC CA issues Class 0 Certificate for Test Purposes without any assurance given to the Subscribers.

1.4.2 Certificate Assurance Levels

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

1. **Class 0 Certificate**: Certificates used and branded for test purposes ONLY.
2. **Class 1 Certificate**: Certificates that should not be used for authentication purposes or to support Non-repudiation. The digital signature provides modest assurances that the e-mail originated from a sender with a certain e-mail address. The Certificate, however, provides no proof of the identity of the Subscriber. The encryption application enables a Relying Party to use the Subscriber's Certificate to encrypt messages to the Subscriber, although the sending Relying Party cannot be sure that the recipient is in fact the person named in the Certificate.
3. **Class 2 Certificate**: Certificates that are suitable for digital signing, authenticating, secure email, and/or data encryption for inter- and intra-organisational, commercial, and personal requiring medium level of assurances of the Subscriber's identity.
4. **Class 3 Certificate**: Certificates that are issued to individuals and Organisations that provide a high level of assurance of the identity of the Subscriber in comparison with Class 1 and 2.

1.4.3 Prohibited Certificate Uses

1. BCCcertificates are not designed, intended, or authorised for use or resale as control equipment in hazardous circumstances or for uses requiring fail-safe performance such as the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control systems, or weapons control systems, where failure could lead directly to death, personal injury, or severe environmental damage.
2. CA-certificates may not be used for any functions except CA functions. In addition, end-user Subscriber certificates shall not be used as CA-certificates.
3. Refer to the ICT Act 2006, IT-CA-Rules-2010 and the Subscriber and/or Relying Party Agreements.

1.5 Policy Administration

1.5.1 Organisation Administering the Document

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

1.5.2 Contact Person

1. The registration and maintenance of this CPS is the responsibility of the BCC Managed PKI Certification Authority Manager (CAM).

2. The contact details for the BCCManaged PKI CAM are:

Bangladesh Computer Council Certification Authority Manager
Bangladesh Computer Council
ICT Tower, E-14/X Agargaon, Sher-e-Bangla Nagar
Dhaka-1207, BANGLADESH
Telephone: 88-02-55006840
Fax: 88-02-9124626
Email: cps@bcc-ca.gov.bd

1.5.3 Person Determining CPS Suitability for the Policy

1. The BCC Certifying Authority Manager is the person who would determine the suitability of the CPS for the policy in accordance with the guidelines provided by the CCA, Bangladesh.

1.5.4 CPS Approval Procedures

1. Approval of this CPS and subsequent amendments shall be made by the BCCCAM, BCC Legal Department, and CCA.

2. Amendments shall either be in the form of a document containing an amended form of the CPS or an update notice. Amended versions or updates shall be available from the BCCManaged PKI Repository located at **https://repo.bcc-ca.gov.bd/CPS**.

3. Updates supersede any designated or conflicting provisions of the referenced version of the CPS.

1.6 Definitions and Acronyms

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

2 Publication and Repository Responsibilities

2.1 Repositories

1. An authoritative repository for all PKI-related information issued by any CA using this CPS is located under the URL https://repo.bcc-ca.gov.bd and made available to all Subscribers and Relying Parties of those certificates as detailed in the respective Subscriber and Relying Party Agreements.

2. Certificate revocation lists using this CPS will be hosted in a separate repository located under the URLhttp://crl.bcc-ca.gov.bd

2.2 Publication of Certification Information

1. The Certification Practice Statement, CA-certificate, and certificate status information are available from the repository.

2.3 Time or Frequency of Publication

1. Any changes made to the CPS shall be published to the Repository in accordance with the notification requirements in Section 9.11.

2. Certificate Status shall be made available in accordance with Section 4.10.

2.4 Access Controls on Repositories

1. Information published in the BCCManaged PKI Repository is publicly-accessible information. Read only access to such information is unrestricted. BCCrequires persons to agree to a Relying Party Agreement as a condition of accessing certificates, certificate status information, or CRLs.

3 Identification and Authentication

3.1 Naming

3.1.1 Types of Names

1. BCC CA hierarchy Certificates contain an X.500 Distinguished Name (DN) in the Issuer and Subject fields. BCC CA, Sub-CA and Subscriber End-Entity certificate naming conventions are in compliance with the CCA Digital Certificate Interoperability Guideline v1.5 (19 July 2016) as specified in the Tables below.

BCC CA (SUBJECT Specifications)	
Attribute	***Value***
Common Name (CN) =	Bangladesh Computer Council CA YYYY[-Gn][1]
House Identifier (2.5.4.51) =	ICT Tower
Street Address (STREET) =	E-14/X Agargaon, Sher-e-Bangla Nagar
Locality	Dhaka
Post Code (PostalCode) =	1207
Organisational Unit (OU) =	Certifying Authority
Organisation (O) =	Bangladesh Computer Council
Country (C) =	BD

Comment [U2]: As per Interop Guideline of CCA

(Internal) Sub-CA (SUBJECT Specifications)	
Common Name (CN) =	BCC Sub-CA for Class “n” Certificates
Organisational Unit (OU) =	Sub-CA
Organisation (O) =	Bangladesh Computer Council
Country (C) =	BD

[1] In BCC CA Certificate **YYYY** is replaced with current Year and **-Gn** is optionally used if there are multiple Key Generation on the same year (e.g. 2016-G2)

(External) Sub-CA (SUBJECT Specifications)	
Attribute	***Value***
Common Name (CN) =	<External Org Name> Sub-CA for Class "n" Certificates or <External Org Name> Sub-CA for<Branding Name>
House Identifier (2.5.4.51) =	Max Length: 60 Characters Flat number, Apartment name and Plot number. OR House Name/Number and Plot Number of the External Sub-CA's Head Office or Registered Office Address
Street Address (STREET) =	Max Length: 60 Characters This attribute value MUST contain the External Sub-CA's Head Office or Registered Office Address
Locality (L) =	Name of City/District where Sub-CA's Head Office or Registered Office is.
Post Code (PostalCode) =	Postal Code of the External Sub-CA's Head Office or Registered Office Address
Organisation (O) =	Legal Name of the Organisation operating the Sub-CA
Country (C) =	Max Length: 2 Characters Country Code as per the verified residential/office address

Comment [U3]: As Per Interop Guideline of CCA

Comment [U4]: As per Interop Guideline it is an mandatory field

(Internal & External) Subscriber End-Entity Certificate	
Common Name (CN) =	Name string of maximum 64 characters constructed in the following manner: (Person) "Surname" "Given Name" "Initials" (Device) "Fully Qualified Domain Name" (System) "IP Address" or "MAC Address" or "System Serial Number"
Serial Number (SN) =	Serial Number will be generated by the Sub-CAs complying uniqueness.In case of person, Serial Number will be generated as per Interoperability Guideline of CCA i.e. 3 letter prefix of type of Identity (NID/Passport/Birth Registration Number)along with 160 bit SHA1 digest of the Identity value provided.
Unique Identifier =	This is a reserved attribute for future use and shall be used in the future for SHA 256 hash of National ID or any other Unique ID for individuals.
State or Province (S) =	Max Length: 60 Characters This attribute value MUST be populated with the name of the State / Province of Subject's residential or office address (if any).
Locality (L) =	City/District of Subjects residential or Office Address
Postal Code (PostalCode) =	Post Code for the for Subject's residential or office address

Comment [U5]: As per Interop Guideline of CCA

Organisational Unit (OU) =	Max Length: 64 Characters This attribute MUST either contain the name of the department or sub-division of the organisation the Subscriber belongs to if the certificate is being issued for official purposes OR must not be used. The Organisational unit must not be present when the organisation has been marked as "personal"
Organisation (O) =	Max Length: 64 Characters This attribute MUST contain either Name of the organisation the Subscriber belongs to – if such information has been verified by the CA OR Contain string "Personal"
Country (C) =	Max Length: 2 Characters;For Bangladesh Country code is BD

3.1.2 Need for Names to be Meaningful

1. Class 1, 2 and 3 end-entity Subscriber Certificates contain names with commonly understood semantics permitting the determination of the identity of the individual or organisation that is the Subject of the Certificate.
2. CA certificates contain names with commonly understood semantics permitting the determination of the identity of the CA that is the Subject of the Certificate.

3.1.3 Anonymity or Pseudonymity of Subscribers

1. Certificates shall not be issued for anonymous Subscribers under the BCC CA hierarchy.
2. CA-certificates shall not be issued for anonymous or pseudonymous Subscribers under the BCC CA hierarchy.
3. This does not include role-based certificates, as long as the role is correctly identified.
4. This does not include certificates issued for an officially recorded identifier, such as a device identifier.
5. This does not include certificates issued under a Class 0 CA.

3.1.4 Rules for Interpreting Various Name Forms

1. DNs shall be interpreted according to the X.501 standard:
    a) Country [countryName] (C) – This attribute contains a two-letter ISO 3166 country code.
    b) Organisation [organisationName] (O) – This attribute contains the name of an organisation.
    c) Organisational Unit Name [organisationalUnitName] (OU) – This attribute contains the name of an organisational unit.
    d) Common Name [commonName] (CN) – This attribute contains a name of an object.

3.1.5 Uniqueness of Names

1. Each DN assigned to a Subscriber under this CPS shall be unique.

Comment [U6]: What will happen for two persons with same name from same organization?

3.1.6 Recognition, Authentication, and Role of Trademarks

1. Certificate applicants are prohibited from using names in their certificate applications that infringe upon the Intellectual Property Rights of others. BCC, however, does not verify whether a certificate applicant has Intellectual Property Rights in the name appearing in a certificate application or arbitrates, mediate, or otherwise resolve any dispute concerning the ownership of any domain name, trade name, trademark, or

service mark. BCCis entitled, without liability to any certificate applicant, to reject or suspend any certificate application because of such dispute.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

1. Where the Subscriber does generate the Private Key, proof of possession shall be performed by provision of PKCS #10 Certificate Signing Request (CSR) or equivalent methods.

2. If the Subscriber does not generate the Private Key, then the delivery process by which the Private Key is transferred to the Subscriber shall be auditable. Refer to Section 6.1 and 6.2.

3.2.2 Authentication of Organisation Identity

1. Whenever a CA certificate is to contain an organisation name, the identity of the organisation and other enrolment information is confirmed by the Registration Authority of the Issuer of the CA.

2. For Organisations using BCC's Managed PKI service, BCC, as the Issuing CA hosting provider will perform the following:

   a) Determines that the organisation exists by using at least one identity proofing service or database or, alternatively, organisational documentation issued by or filed with the applicable government agency or competent authority that confirms the existence of the organisation, and

   b) Confirms with the organisation by telephone, postal mail, or comparable procedure certain information about the organisation, that the organisation has authorised the BCCManaged PKI Service application, and that the person submitting the BCCManaged PKI Service application is authorised to do so.

3.2.3 Authentication of Individual Identity

1. Authentication of individual identity differs according to the Class of Certificate. The minimum authentication standard for each class of certificate is explained in the table below.

Certificate Class	**Authentication of Identity**
Class 0	This intended for test purpose use only and no identity authentication required.
Class 1	No identity authentication. There is a limited confirmation of the Subscriber's e-mail address by requiring the Subscriber to be able to answer an e-mail to that address.
Class 2	Authenticate identity by matching the identity provided by the Subscriber to: • information residing in the database of a BCC-approved identity proofing service, such as a National Identity Verification along with Address Verification using copy of any utility bills or other reliable source of information providing, or • information contained in the business records or databases of business information (employee or customer directories) of an RA approving certificates to its own affiliated individuals
Class 3	The authentication of Class 3 individual Certificates is based on the personal (physical) presence of the Certificate Applicant before an agent of the CA or RA, or before a notary public or other official with comparable authority within the Certificate Applicant's jurisdiction. The agent, notary or other official shall check the identity of the Certificate Applicant against a well-recognised form of

Comment [B7]: NID verification is available for Certificate Identity verification

	government-issued photographic identification, such as a National Identity Card, Passport or Driver's license and one other identification credential.

3.2.4 Device Certificates

1. The CA RA validates certificate applications for Device Certificates by determining the ownership of the FQDN domain name through third party domain registration database and validating legality of the applicant company against the government issued proof of right to do business certificate.

3.2.5 Non-verified Subscriber Information

1. Non-verified subscriber information includes:

   a) Organisation Unit (OU)

   b) Subscriber's name in Class 0 and 1 certificates

   c) Any other information designated as non-verified in the certificate.

3.2.6 Validation of Authority

1. Whenever an individual's name is associated with an Organisation name in a certificate in such a way to indicate the individual's affiliation or authorisation to act on behalf of the Organisation, the RA:

   a) Determines that the Organisation exists by using at least one third party identity proofing service or database, or alternatively, organisational documentation issued by or filed with the applicable government that confirms the existence of the organisation, and

   b) Uses information contained in the business records or databases of business information (employee or customer directories) of an RA approving certificates to its own affiliated individuals or confirms by telephone, confirmatory postal mail, or comparable procedure to the organisation, the employment with the Organisation of the individual submitting the Certificate Application and, when appropriate, his/her authority to act on behalf of the Organisation.

3.2.7 Criteria for Interoperation

1. Digital Certificates issued under the BCC CA hierarchy will be in accordance with the CCA's Digital Certificate Interoperability Guidelines.

3.3 Identification and Authentication for Re-key Requests

1. Prior to the expiration of an existing Subscribers Certificate, it is necessary for the Subscriber to obtain a new certificate to maintain continuity of Certificate usage. BCC requires that the Subscriber generate a new key pair to replace the expiring key pair. (technically defined as "rekey")

2. In general, both "Rekey" and "Renewal" is commonly described as "Certificate Renewal", focusing on the fact that the old Certificate is being replaced with a new Certificate and not emphasising whether or not a new key pair is generated. For all Classes and Types of Certificates, this distinction is not important as a new key pair is always generated as part of BCC CA hierarchy end-entity Subscriber Certificate replacement process.

3. Depending on the assurance level of the certificateRA may ask any of the proof of identity or authenticity as given by the subscriber during certificate issuance to cross check the identity and authenticity of the subscriber with previously given information.

Comment [B8]: We think this point may require in certain cases.

3.3.1 Identification and Authentication for Routine Re-Key

1. Re-key procedures ensure that the person or organisation seeking to rekey an end-user Subscriber Certificate is in fact the Subscriber of the Certificate.

2. One acceptable procedure is through the use of a Challenge Phrase (or the equivalent thereof), or proof of possession of the private key. Subscribers choose and submit with their enrolment information a Challenge Phrase. Upon renewal of a Certificate, if a Subscriber correctly submits the Subscriber's Challenge Phrase (or the equivalent thereof) with the Subscriber's reenrolment information, and the enrolment information

(including Corporate and Technical contact information) has not changed, a new key pair is generated and a renewal Certificate is automatically issued. As an alternative to using a challenge phrase (or equivalent) the RA may send an e-mail message to the e-mail address associated with the verified corporate contact for the certificate being renewed, requesting confirmation of the Certificate renewal order and authorisation to issue the Certificate. Upon receipt of confirmation authorising issuance of the Certificate, the RA will issue the Certificate if the enrolment information (including Corporate and Technical contact information) has not changed.

3. After rekeying/renewal in this fashion, and on at least alternative instances of subsequent rekeying/renewal thereafter, The RA reconfirms the identity of the Subscriber in accordance with the identification and authentication requirements of an original CertificateApplication.

4. The RA will not have to reconfirm by telephone, confirmatory postal mail, or comparable procedure to the Certificate Applicant certain information about the organisation, that the organisation has authorised the Certificate Application and that the person submitting the Certificate Application on behalf of the Certificate Applicant is authorised to do so."

5. Rekey after 30-days from expiration of the Certificate are re-authenticated as an original Certificate Application and are not automatically issued.

3.4 Identification and Authentication for Re-Key After Revocation

1. Re-key/renewal after revocation is not permitted if the revocation occurred because:

   a) The Certificate (other than a Class 0 or 1 Certificate) was issued to a person other than the one named as the Subject of the Certificate, or

   b) The Certificate (other than a Class 0 or 1 Certificate) was issued without the authorisation of the person or entity named as the Subject of such Certificate, or

   c) The entity approving the Subscriber's Certificate Application discovers or has reason to believe that a material fact in the Certificate Application is false. or

   d) For any other reason deemed necessary by the RA to protect the BCC PKI, CCA PKI Trust Network and to comply with the CCA regulations andcountry lawsuits.

2. Subject to the foregoing paragraph, renewal of an Organisational or CA Certificate following revocation of the Certificate is permissible as long as renewal procedures ensure that the Organisation or CA seeking renewal is in fact the Subscriber of the Certificate. Renewed Organisational Certificates shall contain the same Subject DN as the Subject DN of the Organisational Certificate being renewed.

3. Renewal of an individual Certificate following revocation must ensure that the person seeking renewal is, in fact, the Subscriber. One acceptable procedure is the use of a Challenge Phrase (or the equivalent thereof). Other than this procedure or another BCC-approved procedure, the requirements for the identification and authentication of an original Certificate Application shall be used for renewing a Certificate following revocation.

3.5 Identification and Authentication for Revocation Requests

1. Prior to the revocation of a CA certificate, the RAverifies that the revocation has been requested by an authorised entity.

2. For revocation of end-entity subscriber certificates issued from a BCCManaged PKI Service, the acceptable procedures for authenticating the revocation requests of a Subscriber include:

   a) Having the Subscriber for certain certificate types submit the Subscriber's Challenge Phrase (or the equivalent thereof), and revoking the certificate automatically if it matches the Challenge Phrase (or the equivalent thereof) on record.

   b) The authorised BCC Managed PKI RA receiving a message from the Subscriber that requests revocation and contains a digital signature verifiable with reference to the certificate to be revoked.

   c) Communication with the Subscriber providing reasonable assurances in light of the Assurance Level of certificate that the person or organisation requesting revocation is in fact the Subscriber. Such communication, depending on the circumstances, may include one or more of the following: telephone, facsimile, e-mail, mail, or courier service.

3. RAs using an Automated Administration Software Module may submit bulk revocation requests. Such requests shall be authenticated via a digitally signed request signed with the private key in the RA's Automated Administration hardware token.

4. Any request to revoke a CA-certificate shall be authenticated by BCCto ensure that the revocation has in fact been requested by an appropriately authorised party.

4 Certificate Life-Cycle Operational Requirements

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application

1. Certificate applications are initiated by Subscribers to a RA.

2. The following may initiate certificate applications:

   a) Any individual who is the subject of the certificate.

   b) Any authorised representative of an Organisation or entity.

   c) Any authorised representative of a CA.

   d) Any authorised representative of an RA.

4.1.2 Enrolment Process and Responsibilities

4.1.2.1 End-Entity Certificate Subscribers

1. All end-entity certificate Subscribers shall agree to the relevant Subscriber Agreement that contains representations and warranties described in Section 9.6.3 and undergo an enrolment process consisting of:

   a) Completing a certificate application and providing true and correct information;

   b) Generating, or arranging to have generated, a key pair;

   c) Delivering his, her, or its public key to the RA; and

   d) Demonstrating possession and/or exclusive control of the private key correspondingto thepublic key.

4.1.2.2 CA and RA Certificates

1. Subscribers of CA (Subordinate CA of BCC CA)and RA certificates enter into a contract with the BCC. CA and RA Applicants shall provide their credentials to demonstrate their identity and provide contact information during the contracting process.

2. During this contracting process or, at the latest, prior to the Key Generation Ceremony to create a CA or RA key pair, the applicant shall cooperate with BCC to determine the appropriate distinguished name and the content of the Certificates to be issued by the applicant.

Comment [B9]: To clarify or distinguish Sub-CA of BCC and BCC CA itself

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

1. The RA shall perform identification and authentication of all required Subscriber information in terms of Section 3.2.

4.2.2 Approval or Rejection of Certificate Applications

1. The RA shall approve an application for a certificate if:

   a) Successful identification and authentication of all required Subscriber information in terms of Section 3.2, and

   b) Applicable departmental and financial requirements have been met.

2. The RA shall reject a certificate application if:

   a) Identification and authentication of all required Subscriber information in terms of Section 3.2 cannot be completed, or

   b) The Subscriber fails to furnish supporting documentation upon request, or

   c) The Subscriber fails to respond to notices within a specified time, or

   d) The RA believes that issuing a certificate to the Subscriber may bring the BCCCA hierarchy and/or CCA PKI Trust Networkinto disrepute, or

   e) The RA believes that issuing a certificate to the Subscriber may leads to any infringe of the law and order.

4.2.3 Time to Process Certificate Applications

1. The RA begins processing certificate applications within a reasonable time of receipt. There is no time stipulation to complete the processing of an application unless otherwise indicated in the relevant Subscriber Agreement, CPS or other Agreement between participants. A certificate application remains active until rejected.However applicantshall be notified time-to-time with status of his/her application if the processes take longer than 5 working days.

Comment [B10]: Need this in respect of our country

4.3 Certificate Issuance

4.3.1 CA Actions during Certificate Issuance

1. A Certificate is created and issued following the approval of a Certificate Application by RA or following receipt of an RA's request to issue the Certificate. The RA creates and issues a Certificate to a Certificate Applicant based on the information in a Certificate Application following approval of such Certificate Application.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

1. BCC shall, either directly or through an RA, notify Subscribers that they have created such Certificates, and provide Subscribers with access to the Certificates by notifying them that their Certificates are available. Certificates shall be made available to end-entity Subscribers, either by allowing them to download them from a web site or via a message sent to the Subscriber containing the Certificate.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

1. The following conduct constitutes certificate acceptance:

   a) Downloading a Certificate or installing a Certificate from a message attaching it constitutes the Subscriber's acceptance of the Certificate.

   b) Failure of the Subscriber to object to the certificate or its content constitutes certificate acceptance.

4.4.2 Publication of the Certificate by the CA

1. BCC publishes the Certificates as soon as it issues in a publicly accessible repository.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

1. RAs may receive notification of the issuance of certificates they approve.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

1. 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 BCC's Subscriber Agreement and the terms of this CPS. Certificate use

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).

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

4.5.2 Relying Party Public Key and Certificate Usage

1. Relying parties shall assent to the terms of the applicable Relying Party Agreement as a condition of relying on the certificate.

2. Reliance on a certificate must be reasonable under the circumstances. If the circumstances indicate a need for additional assurances, the Relying Party must obtain such assurances for such reliance to be deemed reasonable.

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

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

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

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

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

4.6 Certificate Renewal

1. In accordance to the "Information Technology (Certifying Authorities) Rules, 2010" and Section 3.3 of this CPS, certificate rekey will be performed for each certificate "renewal".

4.6.1 Circumstance for Certificate Renewal

1. Refer to Section 4.7.1

4.6.2 Who May Request Renewal

1. Refer to Section 4.7.2

4.6.3 Processing Certificate Renewal Requests

1. Refer to Section 4.7.3

4.6.4 Notification of New Certificate Issuance to Subscriber

1. Refer to Section 4.7.4

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

1. Refer to Section 4.7.5

4.6.6 Publication of the Renewal Certificate by the CA

1. Refer to Section 4.7.6

4.6.7 Notification of Certificate Issuance by the CA to other Entities

1. Refer to Section 4.7.7

4.7 Certificate Re-key

4.7.1 Circumstance for Certificate Re-key

1. Prior to the expiration of an existing Subscriber's Certificate, it is necessary for the Subscriber to re-key the certificate to maintain continuity of Certificate usage. A certificate may also be re-keyed after expiration.

4.7.2 Who May Request Certification of a New Public Key

1. Only the subscriber for an individual certificate or an authorised representative for an Organisational certificate may request certificate renewal.

4.7.3 Processing Certificate Re-keying Requests

1. The person or organisation seeking to re-key an end-user Subscriber certificate shall be authenticated as the Subscriber (or authorised by the Subscriber) of the certificate by one of the following procedures:

    a) Proof of possession of the private key.

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

2. Other than this procedure or another RA-approved procedure, the requirements for the authentication of an original certificate application shall be used for re-keying an end-user Subscriber certificate.

4.7.4 Notification of New Certificate Issuance to Subscriber

1. Notification of issuance of a re-keyed certificate to the Subscriber is in accordance with Section 4.3.2.

4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate

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

4.7.6 Publication of the Re-keyed Certificate by the CA

1. The re-keyed certificate is published in BCC's publicly accessible repository.

4.7.7 Notification of Certificate Issuance by the CA to other Entities

1. RAs may receive notification of the issuance of certificates they approve.

4.8 Certificate Modification

4.8.1 Circumstance for Certificate Modification

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

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

4.8.2 Who May Request Certificate Modification

1. Refer to Section 4.1.1.

4.8.3 Processing Certificate Modification Requests

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

4.8.4 Notification of New Certificate Issuance to Subscriber

1. Refer to Section 4.3.2.

4.8.5 Conduct Constituting Acceptance of a Modified Certificate

1. Refer to Section 4.4.1.

4.8.6 Publication of the Modified Certificate by the CA

1. Refer to Section 4.4.2.

4.8.7 Notification of Certificate Issuance by the CA to other Entities

1. Refer to Section 4.4.3.

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for Revocation

1. In the circumstances listed below an end-user Subscriber certificate will be revoked by BCC(or by the Subscriber) and published on a CRL.

2. An end-user Subscriber certificate is revoked if:

    a) BCC, a BCC Managed PKI Customeror a Subscriber has reason to believe or strongly suspects that there has been a Compromise of a Subscriber's private key.

    b) BCCor a BCC Managed PKI Customer has reason to believe that the Subscriber has materially breached a material obligation, representation, or warranty under the applicable Subscriber Agreement.

    c) The Subscriber Agreement with the Subscriber has been terminated.

    d) The affiliation between the BCCor a BCC Managed PKI Customer and a Subscriber is terminated or has otherwise ended.

    e) The affiliation between an entity that is a Subscriber of a Device, User, or Organisation certificate and the organisational representative controlling the Subscriber's private key is terminated or has otherwise ended.

    f) BCCor a BCC Managed PKI Customer has reason to believe that the certificate was issued in a manner not materially in accordance with the procedures required by the applicable CP/CPS, the certificate was issued to an entity other than the one named as the Subject of the certificate, or the certificate was issued without the authorisation of the entity named as the Subject of such certificate.

    g) BCCor a BCC Managed PKI Customer has reason to believe that a material fact in the certificate application is false.

    h) BCCor a BCC Managed PKI Customer determines that a material prerequisite to certificate issuance was neither satisfied nor waived.

    i) In the case of Class 3 High Assurance certificates, the Subscriber's organisation name changes.

    j) The information within the certificate, other than non-verified Subscriber Information, is incorrect or has changed.

    k) The Subscriber identity has not been re-verified in accordance with Section 6.3.2.

    l) The Subscriber has not submitted payment when due.

    m)The continued use of that certificate is harmful to BCC and/or the CCA PKI Trust Network.

    n) Usage of the certificate may lead to any infringe of the law and order.

3. When considering whether certificate usage is harmful, BCCconsiders, among other things, the following:

    a) The nature and number of complaints received.

    b) The identity of the complainant(s).

c) Relevant legislation in force.

d) Responses to the alleged harmful use from the Subscriber.

4. BCCSubscriber Agreements require each end-user Subscriber to immediately notify BCCof a known or suspected compromise of its private key.

5. BCC may also revoke an Administrator Certificate if the Administrator's authority to act asAdministrator has been terminated or otherwise has ended.

4.9.2 Who Can Request Revocation

4.9.2.1 CA Certificates

1. A request to revoke a CA (Sub-CA issued by BCC CA) Certificate must be made by one of the following:

a) An authorised CA Manager of the CA whose certificate is to be revoked

b) An authorised representative of BCC

4.9.2.2 RA Certificates

1. A request to revoke a RA Certificate must be made by one of the following:

a) an authorised RA Manager of the RA whose certificate is to be revoked

b) an authorised CA Manager of the CA that issued the certificate

c) an authorised representative of BCC

4.9.2.3 Subscriber Certificates

1. A request to revoke a Subscriber certificate may be made by one of the following:

a) the individual Subscriber identified in the Subject Name field of the certificate

b) the OIC / Section Head of the individual Subscriber identified in the Subject Name field of the certificate

c) the Manager, HR or his/her delegate when the period of employment of a staff member or contractor is terminated

d) the custodian of a device or service

e) a RA Manager on behalf of BCC or the BCC Managed PKI Customer

f) the CA Manager of the CA that issued the certificate

g) an authorised representative of BCC

4.9.3 Procedure for Revocation Requests

4.9.3.1 Procedure for Requesting the Revocation of an End-User Subscriber Certificate

1. An end-user Subscriber requesting revocation is required to communicate the request to BCC or the BCC Managed PKI Customer approving the Subscriber's Certificate Application, who in turn will initiate revocation of the certificate promptly.

2. For BCC Managed PKI Customers, the Subscriber is required to communicate the request to the BCC Managed PKI Customer Administrator who will communicate the revocation request to BCC for processing.

3. Communication of such revocation request shall be in accordance with Section 3.4.

4. Where a BCC Managed PKI Customer initiates revocation of an end-user Subscriber Certificate upon its own initiative, the BCC Managed PKI Customer instructs BCC to revoke the Certificate.

4.9.3.2 Procedure for Requesting the Revocation of a CA or RA Certificate

1. A CA or RA requesting revocation of its CA or RA Certificate is required to communicate the request to BCC. BCC will then revoke the Certificate. BCC may also initiate CA or RA Certificate revocation.

4.9.4 Revocation Request Grace Period

1. Revocation requests shall be submitted as promptly as possible within a reasonable time.

4.9.5 Time within which CA must Process the Revocation Request

1. BCCtakes reasonable steps to process revocation requests without delay.

4.9.6 Revocation Checking Requirement for Relying Parties

1. Relying Parties shall check the status of Certificates on which they wish to rely. One method by which Relying Parties may check Certificate status is by consulting the most recent CRL from the CA that issued the Certificate on which the Relying Party wishes to rely. Alternatively, Relying Parties may meet this requirement either by checking Certificate status using the applicable web-based repository or by using OCSP (if available). CAs shall provide Relying Parties with information on how to find the appropriate CRL, web-based repository, or OCSP responder (where available) to check for revocation status.

4.9.7 CRL Issuance Frequency

1. CRLs for end-entity Subscriber certificates are issued at least once per day. CRLs for CA-certificates shall be issued at least annually, but also whenever a CA-certificate is revoked.
2. If a certificate listed in a CRL expires, it may be removed from later-issued CRLs after the certificate's expiration.

4.9.8 Maximum Latency for CRLs

1. The BCChosted CA CRLs are posted to the repository within a reasonable time after generation.

4.9.9 On-Line Revocation/Status Checking Availability

1. Online revocation and other Certificate status information are available via a web-based repository and, where offered, OCSP. In addition to publishing CRLs, BCC provides Certificate status information through query functions in the BCC Repository.
2. Certificate status information is available through web-based query functions accessible through the BCC Repository.
3. BCC also provides OCSP Certificate status information. BCC Managed PKI Customers who contract for OCSP services may check Certificate status through the use of OCSP.
4. If the Certificate Status Services include online CRLs, the location of the CRL shall be encoded in the appropriate Certificate extension.
5. If the Certificate Status Services include Online Certificate Status Protocol (OCSP), the location of the OCSP responder shall be encoded in the appropriate Certificate extension.

4.9.10 On-Line Revocation Checking Requirements

1. A relying party must check the status of a certificate on which he/she/it wishes to rely. If a Relying Party does not check the status of a Certificate on which the Relying Party wishes to rely by consulting the most recent relevant CRL, the Relying Party shall check Certificate status by consulting the applicable repository or by requesting Certificate status using the applicable OCSP responder (where OCSP services are available).

4.9.11 Other Forms of Revocation Advertisements Available

1. Not Applicable

4.9.12 Special Requirements Related to Key Compromise

1. If a certificate is lost or it is suspected that the private key is compromised, a new CRL containing the revoked certificate must be published within 24 hours of revocation. If a CA is compromised, the CA's certificate must be revoked and the CRL updated at the soonest possible time.
2. BCCuses reasonable efforts to notify potential Relying Parties if it discovers, or has reason to believe, that there has been a compromise of the private key of one of its hosted CAs.

3. This CPS makes no stipulation as to the total time elapsed from notification of a Private Key compromise to revocation of the certificate.

4.9.13 Circumstances for Suspension

1. BCC, the BCC Managed PKI Customer RA or the certificate subscriber may suspend a certificate that has OCSP enabled in the following circumstances:
    a) The subscriber requests for suspension of his/her Digital Certificate
    b) Non-payment of certificate fees from the RA or Subscriber within the stipulated time
    c) Any circumstance which leads BCC to believe that the trust of the BCC CA hierarchy and/or CCA PKI Trust Network may be jeopardised
    d) Any circumstance which leads BCC to believe that the law and order situation may breached
    e) If it is of opinion that the Digital Certificate should be suspended in public interest by BCC

4.9.14 Who can Request Suspension

1. BCC, RA or the subscriber may request for suspension.
2. BCC, RA or the subscriber may only request for the suspension of the certificate if there is reason to believe that circumstances exist that require the certificate to be suspended.

4.9.15 Procedure for Suspension Request

1. The subscribers and the RAs will request for the certificate suspension using the same procedures as for the certificate revocation specified in Section 4.8.3.

4.9.16 Limits on Suspension Period

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

4.9.17 Who Can Request Activation of a Suspended Certificate

1. A subscriber can initiate a request for activation of his/her suspended certificate within 15 days of suspension.
2. RAs may only initiate the request for activation for those certificates for which they had initiated the suspension. CA may initiate the request for activation for any suspended certificate. A certificate shall be activated only if the BCC is satisfied that the reason for suspension is no longer valid.

4.9.18 Procedure for Activation Request

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

4.10 Certificate Status Services

4.10.1 Operational Characteristics

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

4.10.2 Service Availability

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

4.10.3 Optional Features

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

4.11 End of Subscription

1. A Subscriber may end a subscription for a BCCcertificate by:

   a) Allowing his/her/its certificate to expire without renewing or re-keying that certificate, or

   b) Revoking his/her/its certificate before certificate expiration without replacing thecertificate.

4.12 Key Escrow and Recovery

Comment [B11]: Requires consultation with CCA Bangladesh to provide the Key Escrow service. BCC shall consult after submitting CPS to CCA Office

4.12.1 Key Escrow and Recovery Policy and Practices

1. Escrowed private keys shall be stored in encrypted form using the BCC Managed PKI Key Manager software.

2. End-user Subscriber private keys shall only be recovered under the circumstances permitted within the BCC Managed PKI Key Management Service Administrator's Guide, under which:

   a) CAs using BCC Managed PKI Key Manager shall confirm the identity of any person purporting to be the Subscriber to ensure that a purported Subscriber request for the Subscriber's private key is, in fact, from the Subscriber and not an impostor,

   b) CAs shall recover a Subscriber's private key without the Subscriber's authority only for legitimate and lawful purposes, such as to comply with judicial or administrative process or a search warrant, and not for any illegal, fraudulent, or other wrongful purpose, and

   c) Such CAs shall have personnel controls in place to prevent Key Management Service Administrators and other persons from obtaining unauthorised access to private keys.

3. It is recommended that CAs using the BCC Managed PKI Key Management Service:

   a) Notify the Subscribers that their private keys are escrowed.

   b) Protect Subscribers' escrowed keys from unauthorised disclosure.

   c) Protect all information, including the administrator's own key(s) that could be used to recover Subscribers' escrowed keys.

   d) Release Subscribers' escrowed keys only for properly authenticated and authorised requests for recovery.

   e) Revoke the Subscriber's key pair prior to recovering the encryption key.

   f) Not be required to communicate any information concerning a key recovery to the Subscriber except when the Subscriber him/herself has requested recovery.

   g) Not disclose or allow to be disclosed escrowed keys or escrowed key-related information to any third party unless required by the law, government rule, or regulation; by the enterprise's organisation policy; or by order of a court of competent jurisdiction.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

1. Session key recovery is not supported under this CPS.

5 Facility, Management, and Operational Controls

5.1 Physical Controls

1. BCChas implemented a set of Information Security Policies and Standards which support the security requirements of this CPS. Compliance with these policies and standards is included in BCC's independent audit requirements described in Section 8. An overview of the requirements is given below.

5.1.1 Site Location and Construction

1. BCCCA and RA operations are conducted within a physically protected environment that deters, prevents, and detects unauthorised use of, access to, or disclosure of sensitive information and systems whether covert or overt.
2. BCCalso maintains disaster recovery facilities for its CA operations. The BCCdisaster recovery facilities are protected by multiple tiers of physical security comparable to those of the primary facility used by BCC.

5.1.2 Physical Access

1. BCCCA systems are protected by a minimum of four tiers of physical security, with access to the lower tier required before gaining access to the higher tier.
2. Progressively restrictive physical access privileges control access to each tier. Sensitive CA operational activity—any activity related to the lifecycle of the certification process such as authentication, verification, and issuance—occurs within very restrictive physical tiers. Access to each tier requires the use of a proximity card employee badge. Physical access is automatically logged and video recorded. Additional tiers enforce individual access control through the use of two factor authentication including biometrics. Unescorted personnel, including untrusted employees or visitors, are not allowed into such secured areas.
3. The physical security system includes additional tiers for key management security, which serves to protect both online and offline storage of CA cryptographic hardware (cryptographic signing units or CSU) and keying material. Areas used to create and store cryptographic material enforce dual control, each through the use of two factor authentication including biometrics. Online CSUs are protected through the use of locked cabinets. Offline CSUs are protected through the use of locked safes, cabinets, and containers. Access to CSUs and keying material is restricted in accordance with BCC's segregation of duty requirements. The opening and closing of cabinets or containers in these tiers is logged for audit purposes.

5.1.3 Power and Air Conditioning

1. All critical components shall be equipped with primary and backup power systems to ensure continuous, uninterrupted access to electric power. Also, these secure facilities shall be equipped with primary and backup heating/ventilation/air conditioning systems to control temperature and relative humidity.

5.1.4 Water Exposures

1. BCChas taken reasonable precautions to minimise the impact of water exposure to BCCsystems.

5.1.5 Fire Prevention and Protection

1. BCChas taken reasonable precautions to prevent and extinguish fires or other damaging exposure to flame or smoke. The BCCfire prevention and protection measures have been designed to comply with local fire safety regulations.

5.1.6 Media Storage

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

5.1.7 Waste Disposal

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

5.1.8 Off-Site Backup

1. BCCperforms routine backups of critical system data, audit log data, and other sensitive information. Offsite backup media are stored in a physically secure manner using a BCCdisaster recovery facility.

5.2 Procedural Controls

5.2.1 Trusted Roles

1. Trusted Persons include all employees, contractors, and consultants that have access to or control authentication or cryptographic operations that may materially affect:
    a) The validation of information in certificate applications.
    b) The acceptance, rejection, or other processing of certificate applications, revocation requests, renewal requests, or enrolment information.
    c) The issuance or revocation of certificates, including personnel having access to restricted portions of its repository.
    d) The handling of Subscriber information or requests.
2. Trusted Persons include, but are not limited to:
    a) Customer service personnel.
    b) Cryptographic business operations personnel.
    c) Security personnel.
    d) System administration personnel.
    e) Designated engineering personnel.
    f) Executives that are designated to manage infrastructural trustworthiness.
3. BCCconsiders the categories of personnel identified in this section as Trusted Persons having a Trusted Position. Persons seeking to become Trusted Persons by obtaining a Trusted Position must successfully complete the screening requirements set out in this CPS.

5.2.2 Number of Persons Required for Task

1. BCChas established, maintains, and enforces rigorous control procedures to ensure the segregation of duties based on job responsibility and to ensure that multiple Trusted Persons are required to perform sensitive tasks.
2. Policy and control procedures are in place to ensure segregation of duties based on job responsibilities. The most sensitive tasks, such as access to and management of CA cryptographic hardware (cryptographic signing unit or CSU) and associated key material, require multiple Trusted Persons.
3. These internal control procedures are designed to ensure that at a minimum, two trusted personnel are required to have either physical or logical access to the device. Access to CA cryptographic hardware is strictly enforced by multiple Trusted Persons throughout its lifecycle, from incoming receipt and inspection to final logical and/or physical destruction. Once a module is activated with operational keys, further access controls are invoked to maintain split control over both physical and logical access to the device. Persons with physical access to modules do not hold "Secret Shares" and vice versa.

5.2.3 Identification and Authentication for Each Role

1. For all personnel seeking to become Trusted Persons, verification of identity is performed through the personal (physical) presence of such personnel before Trusted Persons performing BCCHR or security functions and a check of well-recognised forms of identification (e.g., passports and driver's licences). Identity is further confirmed through the background checking procedures in Section 5.3.2.

2. BCCensures that personnel have achieved Trusted Status and departmental approval has been given before such personnel are:

   a) Issued access devices and granted access to the required facilities; or

   b) Issued electronic credentials to access and perform specific functions on BCCCA, RA, or other IT systems.

5.2.4 Roles Requiring Separation of Duties

1. Roles requiring Separation of duties include but are not limited to:

   a) The validation of information in certificate applications.

   b) The acceptance, rejection, or other processing of certificate applications, revocation requests, renewal requests, or enrolment information.

   c) The issuance or revocation of certificates, including personnel having access to restricted portions of the repository.

   d) The handling of Subscriber information or requests.

   e) The generation, issuing or destruction of a CA-certificate.

   f) The loading of a CA on production.

5.3 Personnel Controls

5.3.1 Qualifications, Experience, and Clearance Requirements

1. BCCrequires that personnel seeking to become Trusted Persons present proof of the requisite background, qualifications, and experience needed to perform their prospective job responsibilities competently and satisfactorily, as well as proof of any government clearances, if any, necessary to perform certification services under government contracts.

5.3.2 Background Check Procedures

1. Prior to commencement of employment in a Trusted Role, BCCconducts background checks which include the following:

   a) Confirmation of previous employment.

   b) Check of professional reference.

   c) Confirmation of the highest or most relevant educational degree obtained.

   d) Search of criminal records (state and national).

   e) Check of credit/financial/insolvency records.

2. To the extent that any of the requirements imposed by this section cannot be met due to a prohibition or limitation in local law or other circumstances, BCCwill utilise a substitute investigative technique permitted by law that provides substantially similar information, including but not limited to obtaining a background check performed by the applicable governmental agency.

3. The factors revealed in a background check that may be considered grounds for rejecting candidates for Trusted Positions or for taking action against an existing Trusted Person generally include (but are not limited to) the following:

   a) Misrepresentations made by the candidate or Trusted Person.

   b) Highly unfavourable or unreliable professional references.

   c) Certain criminal convictions.

   d) Breach of BCC Code of Conduct.

4. Reports containing such information are evaluated by human resources and security personnel, who then determine the appropriate course of action in light of the type, magnitude, and frequency of the behaviour uncovered by the background check. Such actions may include measures up to and including the

cancellation of offers of employment made to candidates for Trusted Positions or the termination of existing Trusted Persons.

5. The use of information revealed in a background check to take such actions is subject to the applicable federal, state, and local laws.

5.3.3 Training Requirements

1. BCCprovides its personnel with training upon hire as well as the requisite on-the-job training needed for them to perform their job responsibilities competently and satisfactorily. BCCmaintains records of such training. BCCperiodically reviews and enhances its training programs as necessary.

2. BCCtraining programs are tailored to the individual's responsibilities and include the following as relevant:

   a) Basic PKI concepts.

   b) Job responsibilities.

   c) BCCsecurity and operational policies and procedures.

   d) Use and operation of deployed hardware and software.

   e) Incident and Compromise reporting and handling.

   f) Disaster recovery and business continuity procedures.

5.3.4 Retraining Frequency and Requirements

1. BCCprovides refresher training and updates to their personnel to the extent and frequency required to ensure that such personnel maintain the required level of proficiency to perform their job responsibilities competently and satisfactorily.

5.3.5 Job Rotation Frequency and Sequence

1. No stipulation.

5.3.6 Sanctions for Unauthorised Actions

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

5.3.7 Independent Contractor Requirements

1. No independent contractors shall be used to fill any of the trusted positions of BCC CA, however solutions or hardware vendors (herein after Independent Contractors and Consultants) may be used time to time for only maintenance purpose and theirbackground and authenticity shall be checked by BCC approved procedures. After passing the background check Independent contractors and consultants are permitted to access to BCCsecure facilities only to the extent they are escorted and directly supervised by Trusted Persons at all times.

Comment [B12]: Trusted positions shall not be transferred to anyone other than BCC officials

5.3.8 Documentation Supplied to Personnel

1. BCCprovides its employees with the requisite training and other documentation needed to perform their job responsibilities competently and satisfactorily.

5.4 Audit Logging Procedures

5.4.1 Types of Events Recorded

1. BCClogs the following significant events:

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

   b) CA and Subscriber certificate life cycle management events, including:
      - Certificate applications, renewal, re-key, and revocation.

- Successful or unsuccessful processing of requests.
- Generation and issuance of certificates and CRLs.

c) Security-related events including:

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

2. Log entries include the following elements:

a) Date and time of the entry.

b) Serial or sequence number of entry, for automatic journal entries.

c) Identity of the entity making the journal entry.

d) Type of entry.

3. BCCRAs log certificate application information including:

a) Type of identification document(s) presented by the certificate applicant.

b) Record of unique identification data, numbers, or a combination thereof (e.g. certificate applicant's drivers licence number) of identification documents, if applicable.

c) Storage location of copies of applications and identification documents.

d) Identity of entity accepting the application.

e) Method used to validate identification documents, if any.

f) Name of receiving CA or submitting RA, if applicable.

5.4.2 Frequency of Processing Log

1. BCCreviews its audit logs for suspicious or unusual activity in response to alerts generated based on irregularities and incidents within BCCCA and RA systems.

5.4.3 Retention Period of Audit Log

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

5.4.4 Protection of Audit Log

1. Audit logs are protected with an electronic audit log system that includes mechanisms to protect the log files from unauthorised viewing, modification, deletion, or other tampering.

5.4.5 Audit Log Backup Procedures

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

5.4.6 Audit Collection System (Internal vs. External)

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

5.4.7 Notification to Event-Causing Subject

1. Where an event is logged by the audit collection system, no notice is required to be given to the individual, organisation, device, or application that caused the event.

5.4.8 Vulnerability Assessments

1. Events in the audit process are logged, in part, to monitor system vulnerabilities. Logical security vulnerability assessments (LSVAs) are performed, reviewed, and revised following an examination of these

monitored events. LSVAs are based on real-time automated logging data and are performed on a weekly basis. An LSVA will be performed every six months.

5.5 Records Archival

5.5.1 Types of Records Archived

1. BCCarchives:

    a) All audit data collected in terms of Section 5.4.

    b) Certificate application information.

    c) Documentation supporting certificate applications.

    d) Certificate lifecycle information, e.g. revocation, re-key and renewal application information.

5.5.2 Retention Period of Archive

1. Audit logs will be retained for 7 (seven) years.

5.5.3 Protection of Archive

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

5.5.4 Archive Backup Procedures

1. BCCincrementally backs up electronic archives of its issued certificate information on a daily basis and performs full backups on a weekly basis. Copies of paper-based records shall be maintained in an off-site secure facility.

5.5.5 Requirements for Time-Stamping of Records

1. Certificates, CRLs, and other revocation database entries shall contain time and date information. Such time information need not be cryptographic-based.

5.5.6 Archive Collection System (Internal vs. External)

1. BCCarchive collection systems are internal.

5.5.7 Procedures to Obtain and Verify Archive Information

1. Only authorised Trusted Personnel are able to obtain access to the archive. The integrity of the information is verified when it is restored.

5.6 Key Changeover

1. The BCCCA key pairs are retired from service at the end of their respective maximum lifetimes as defined in this CPS. New CA key pairs will be generated as necessary, for example to replace CA key pairs that are being retired, to supplement existing, active key pairs and to support new services.

2. Prior to the expiration of the CA-certificate for a Superior CA, key changeover procedures are enacted to facilitate a smooth transition for entities within the Superior CA's hierarchy from the old Superior CA key pair to new CA key pair(s). The BCCCA key changeover process requires that:

    a) A Superior CA ceases to issue new Subordinate CA-certificates no later than 60 days before the point in time ("Stop Issuance Date") where the remaining lifetime of the Superior CA key pair equals the approved certificate Validity Period for the specific type(s) of certificates issued by Subordinate CAs in the Superior CA's hierarchy.

    b) Upon successful validation of Subordinate CA (or end-user Subscriber) certificate requests received after the "Stop Issuance Date," certificates will be signed with a new CA key pair.

c) The Superior CA continues to issue CRLs signed with the original Superior CA private key until the expiration date of the last certificate issued using the original key pair has been reached.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

1. Backups of the following CA information shall be kept in off-site storage and made available in the event of a Compromise or disaster: certificate application data, audit data, and database records for all certificates issued. Back-ups of CA private keys shall be generated and maintained in accordance with Section 6.2.4. BCCmaintains backups of the foregoing CA information for its own CAs, as well as the CAs of BCC Managed PKI Customers within its domain.

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

1. In the event of the corruption of computing resources, software, and/or data, the BCCincident handling procedures are enacted. Such procedures require appropriate escalation, incident investigation, and incident response. If necessary, BCCkey compromise or disaster recovery procedures will be enacted.

5.7.3 Entity Private Key Compromise Procedures

1. Upon the suspected or known Compromise of a BCCCA, BCCinfrastructure, or CA private key, BCCKey Compromise Response procedures are enacted by BCC security incident management processes. These processes will engage Information, Security, Cryptographic Business Operations, Production Services personnel, and other management representatives as necessary to assess the situation, develop an action plan, and implement the action plan with approval from the BCC.
2. If CAcertificate revocation is required, the following procedures are performed:
    a) The certificate's revoked status is communicated to Relying Parties through the BCCrepository in accordance with Section 4.9.9,
    b) Reasonable efforts will be made to provide additional notice of the revocation to all affected participants, and
    c) The CA will generate a new key pair in accordance with Section 4.7, except where the CA is being terminated in accordance with Section 4.9.

5.7.4 Business Continuity Capabilities after a Disaster

1. BCChas implemented a disaster recovery site, which is physically separate from the BCCprincipal secure facilities. BCChas developed, implemented and tested a disaster recovery plan to mitigate the effects of any kind of natural or man-made disaster. This plan is regularly tested, verified, and updated to be operational in the event of a disaster.
2. Detailed disaster recovery plans are in place to address the restoration of information systems services and key business functions. BCC's disaster recovery site has implemented the physical security protections and operational controls required by the BCCSecurity and Audit Requirements Guide to provide for a secure and sound backup operational setup.
3. In the event of a natural or man-made disaster requiring temporary or permanent cessation of operations from the BCCprimary facility, the BCCdisaster recovery process is initiated by the BCCEmergency Response Team.
4. BCChas the capability to restore or recover essential operations within twenty four (24) hours following a disaster with, at a minimum, support for the following functions:
    a) Certificate issuance,
    b) Certificate revocation,
    c) Publication of revocation information, and
    d) Provision of key recovery information for Enterprise Customers using BCC Managed PKI Key Manager.

5. The BCCdisaster recovery database is synchronised regularly with the production database within the time limits set forth in the BCCSecurity and Audit Requirements Guide. BCCdisaster recovery equipment is protected by physical security protections comparable to the physical security tiers specified in Section 5.1.1.

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

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

8. BCCmaintains offsite backups of important CA information for BCCCA's. Such information includes, but is not limited to: certificate application data, audit data (per Section 5.4), and database records for all certificates issued.

5.8 CA, RA and Sub-CA Termination

1. In the event that it is necessary for BCCCA to cease operation, BCCmakes a reasonable effort to notify Subscribers, Relying Parties, and other affected entities of such termination in advance of the CA termination. Where CA termination is required, BCCwill develop a termination plan to minimise disruption to Subscribers and Relying Parties. Such termination plans may address the following, as applicable:

    a) Provision of notice to parties affected by the termination, such as Subscribers and Relying Parties, informing them of the status of the CA,

    b) Handling the cost of such notice,

    c) The revocation of the certificate issued to the CA,

    d) The preservation of the CA's archives and records for the time periods required in this CPS,

    e) The continuation of Subscriber and customer support services,

    f) The continuation of revocation services, such as the issuance of CRLs or the maintenance of online status checking services,

    g) The revocation of unexpired unrevoked certificates of end-user Subscribers and subordinate CAs, if necessary,

    h) Refunding (if necessary) Subscribers whose unexpired unrevoked certificates are revoked under the termination plan or provision, or alternatively, the issuance of replacement certificates by a successor CA,

    i) Disposition of the CA's private key and the hardware tokens containing such private key, and

    j) Provisions needed for the transition of the CA's services to a successor CA.

2. In the event that it is necessary for BCCCA to terminate the operation of its RA, BCCmakes a reasonable effort to notify Subscribers, Relying Parties, and other affected entities of such termination in advance of the RA termination. Where RA termination is required, BCCwill develop a termination plan to minimise disruption to Subscribers and Relying Parties. Such termination plans may address the following, as applicable:

    a) Provision of notice to parties affected by the termination, such as Subscribers and Relying Parties, informing them of the status of the RA,

    b) Handling the cost of such notice,

    c) The continuation of Subscriber and customer support services,

    d) Continuation of Registration service by other means which will be notified to the customer,

    e) Publish Notification in the BCC CA website;

    f) Pending Registration Process will be handled by BCC CA;

    g) Notify Office of the CCA about the termination stating reasons along with.

3. In the event that it is necessary for BCCCA to terminate the operation of its Internal or External Sub-CA, BCCmakes a reasonable effort to notify Subscribers, Relying Parties, and other affected entities of such termination in advance of the termination. Where Sub-CA termination is required, BCCwill develop a termination plan to minimise disruption to Subscribers and Relying Parties. Such termination plans may address the following, as applicable:

   a) Provision of notice to parties affected by the termination, such as Subscribers and Relying Parties, informing them of the status of the Sub-CA,

   b) Handling the cost of such notice,

   c) Notify Office of the CCA about the termination of the Sub-CA with reasons for such termination,

   d) The revocation of the certificate issued to the Sub-CA,

   e) The preservation of the Sub-CA's archives and records for the time periods required in this CPS,

   f) The continuation of Subscriber and customer support services,

   g) The continuation of revocation services, such as the issuance of CRLs or the maintenance of online status checking services,

   h) The revocation of unexpired unrevoked certificates of end-user Subscribers, if necessary,

   i) Refunding (if necessary) Subscribers whose unexpired unrevoked certificates are revoked under the termination plan or provision, or alternatively, the issuance of replacement certificates by a successor CA,

   j) Disposition of the Sub-CA's private key and the hardware tokens containing such private key, and

   k) Provisions needed for the transition of the Sub-CA's services to a successor CA.

6 Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

1. CA key pair generation is performed by multiple pre-selected, trained and trusted individuals using Trustworthy Systems and processes that provide for the security and required cryptographic strength for the generated keys. The cryptographic modules used for CA key generation meet the requirements of at least FIPS 140-2 level 3.
2. All CA key pairs are generated in pre-planned Key Generation Ceremonies in accordance with the requirements of the BCC Key Ceremony Reference Guide, the BCC CA Key Management Tool User's Guide, and the standards specified in the Bangladesh ICT Act 2006, IT (CA) Rules 2010 and the CCA Digital Certificate Interoperability Guideline document. The activities performed in each key generation ceremony is recorded, dated and signed by all individuals involved. These records are kept for audit and tracking purposes.
3. Generation of RA key pairs is generally performed by the RA using a FIPS 140-2 level 2 certified cryptographic modules provided with their browser software.
4. BCCgenerates the key pairs used by their BCCAutomated Administration servers. BCCrecommends that Automated Administration server key pair generation be performed using a FIPS 140-2 level 2 certified cryptographic module.
5. Generation of end-entity Subscriber key pairs is generally performed by the Subscriber.

6.1.2 Private Key Delivery to Subscriber

1. When end-entity Subscriber key pairs are generated by the end-user Subscriber, private key delivery to a Subscriber is not applicable.
2. Where RA or end-entity Subscriber key pairs are pre-generated on hardware tokens or smart cards, such devices are distributed to the RA or end-user Subscriber using a commercial delivery service and tamper evident packaging. The data required to activate the device is communicated to the RA or end-user Subscriber using an out of band process. The distribution of such devices is logged.

6.1.3 Public Key Delivery to Certificate Issuer

1. End-entity Subscribers and RAs submit their public key for certification electronically through the use of a PKCS #10 Certificate Signing Request (CSR) or other digitally signed package in a session secured by Secure Sockets Layer (SSL). Where CA key pairs are generated by BCC, this requirement is not applicable.

6.1.4 Public Key Delivery to Relying Parties

1. BCC issued End-entity Public Keys shall be delivered in signed certificates and validated by the Relying Party.
2. BCC issued Root and Subordinate CAs are made available to Relying Parties at http://www.bcc-ca.gov.bd/

6.1.5 Key Sizes

3. Key pairs shall be of sufficient length to prevent others from determining the key pair's private key using cryptanalysis during the period of expected utilisation of such key pairs. The current CCA Interoperability GuidelinesStandard for minimum key sizes is the use of key pair's equivalent in strength to 2048 bit RSA for all certificates.

6.1.6 Public Key Parameters Generation and Quality Checking

1. Not applicable.

Comment [SYMC-LH13]: Duplication deleted

Comment [B14]: Need this paragraph

Comment [SYMC-LH15]: Added content to 6.1.4

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

1. Key Usage purposes will be set based on RFC 5280 and the BCC Digital Certificate Interoperability Guideline.
2. The use of a specific key is constrained by the key usage extension in the X.509 certificate. All certificates shall include a critical key usage extension.
3. In particular:
    a) Certificates used for authentication set the digitalSignature bit
    b) Certificates used for key encryption set the keyEncipherment bit
    c) Certificates used for data encryption set the dataEncipherment bit
    d) Certificates used for digital signatures set the digitalSignature, nonRepudiation bit
    e) CA certificates set cRLSign and keyCertSign bits
    f) Certificates used for key agreement set the keyAgreement bit.

6.2 Private Key protection and Cryptographic Module Engineering Controls

1. BCChas implemented a combination of physical, logical, and procedural controls to ensure the security of CA private keys. Subscribers are required to take necessary precautions to prevent the loss, disclosure, modification, or unauthorised use of private keys.

6.2.1 Cryptographic Module Standards and Controls

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

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

1. BCChas implemented technical and procedural mechanisms that require the participation of multiple trusted individuals to perform sensitive CA cryptographic operations. BCCuses “Secret Sharing” to split the activation data needed to make use of a CA private key into separate parts called “Secret Shares” which are held by trained and trusted individuals called “Shareholders.” A threshold number of Secret Shares (m) out of the total number of Secret Shares created and distributed for a particular hardware cryptographic module (n) is required to activate a CA private key stored on the module.
2. The threshold number of shares needed to sign a CA certificate is 3. It should be noted that the number of shares distributed for disaster recovery tokens may be less than the number distributed for operational tokens, while the threshold number of required shares remains the same. Secret Shares are protected in accordance with this CPS.

6.2.3 Private Key Escrow

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

6.2.4 Private Key Backup

1. BCCcreates backup copies of CA private keys for routine recovery and disaster recovery purposes. Such keys are stored in encrypted form within hardware cryptographic modules and associated key storage devices. Cryptographic modules used for CA private key storage meet the requirements of this CPS. CA private keys are copied to backup hardware cryptographic modules in accordance with this CPS.
2. Modules containing onsite backup copies of CA private keys are subject to the requirements of this CPS. Modules containing disaster recovery copies of CA private keys are subject to the requirements of this CPS.
3. BCCdoes not store copies of RA private keys. For the backup of end-user Subscriber private keys, see Section 6.2.3 and Section 4.12.

6.2.5 Private Key Archival

1. Upon expiration of a BCCCA certificate, the key pair associated with the certificate will be securely retained for a period of at least 5 years using hardware cryptographic modules that meet the requirements of this

CPS. These CA key pairs shall not be used for any signing events after their expiration date, unless the CA certificate has been renewed in terms of this CPS.

2. The BCCdoes not archive copies of RA and Subscriber private keys.

6.2.6 Private Key Transfer Into or From a Cryptographic Module

1. BCCgenerates CA key pairs on the hardware cryptographic modules in which the keys will be used. In addition, BCCmakes copies of such CA key pairs for routine recovery and disaster recovery purposes. Where CA key pairs are backed up to another hardware cryptographic module, such key pairs are transported between modules in encrypted form.

6.2.7 Private Key Storage on Cryptographic Module

1. CA or RA private keys held on hardware cryptographic modules shall be stored in encrypted form.

6.2.8 Method of Activating Private Key

1. All participants shall protect the activation data for their private keys against loss, theft, modification, unauthorised disclosure, or unauthorised use.

6.2.8.1 Class 0-1 Certificates

1. The Standard for Class 0 and Class 1 private key protection is for Subscribers to take reasonable measures for the physical protection of the Subscriber's workstation to prevent use of the workstation and its associated private key without the Subscriber's authorisation. In addition, the BCCrecommends that Subscribers use a password in accordance with Section 6.3.3 or security of equivalent strength to authenticate the Subscriber before the activation of the private key, which includes, for instance, a password to operate the private key, a Windows logon or screen saver password, or a network logon password.

6.2.8.2 Class 2 Certificates

1. The Standard for Class 2 Private Key protection is for Subscribers to:

    a) Use a password in accordance with Section 6.3.3 or security of equivalent strength to authenticate the Subscriber before the activation of the private key, which includes, for instance, a password to operate the private key, a Windows logon or screen saver password, a network logon password; and

    b) Take reasonable measures for the physical protection of the Subscriber's workstation to prevent use of the workstation and its associated private key without the Subscriber's authorisation.

2. When deactivated, private keys shall be kept in encrypted form only.

6.2.8.3 Class 3 Certificates

1. The Standard for private key protection (other than Administrators) is for Subscribers to:

    a) Use a smart card, biometric access device, password or security of equivalent strength to authenticate the Subscriber before the activation of the private key; and

    b) Take reasonable measures for the physical protection of the Subscriber's workstation to prevent use of the workstation and its associated private key without the Subscriber's authorisation.

2. Use of a password along with a smart card or biometric access device in accordance with Section 6.1.1 is recommended. When deactivated, private keys shall be kept in encrypted form only.

6.2.8.4 Administrators' Private Keys

1. The Standard for Administrators' private key protection requires them to:

    a) Use a smart card, biometric access device, password in accordance with Section 6.3.3, or security of equivalent strength to authenticate the Administrator before the activation of the private key, which includes, for instance, a password to operate the private key, a Windows logon or screen saver password, or a network logon password; and

b) Take reasonable measures for the physical protection of the Administrator's workstation to prevent use of the workstation and its associated private key without the Administrator's authorisation.

2. BCCrecommends that Administrators use a smart card, biometric access device, or security of equivalent strength along with the use of a password in accordance with Section 6.3.3 to authenticate the Administrator before the activation of the private key.

3. When deactivated, private keys shall be kept in encrypted form only.

6.2.9 Method of Deactivating Private Key

1. BCCCA private keys are deactivated upon removal from the token reader. BCCRA private keys (used for authentication to the RA application) are deactivated upon system log off. BCCRAs are required to log off their workstations when leaving their work area.

2. Client Administrators, RA, and end-user Subscriber private keys may be deactivated after each operation, upon logging off their system, or upon removal of a smart card from the smart card reader depending upon the authentication mechanism employed by the user. In all cases, end-user Subscribers has an obligation to adequately protect their private key(s) in accordance with this CPS. The private key associated with an application is deleted immediately after it has been used for code signing.

6.2.10 Method of Destroying Private Key

1. Where required, BCCdestroys CA private keys in a manner that reasonably ensures that there are no residual remains of the key that could lead to the reconstruction of the key. BCCutilises the zeroing function of its hardware cryptographic modules and other appropriate means to ensure the complete destruction of CA private keys. CA key destruction activities are logged.

6.2.11 Cryptographic Module Rating

1. See Section 6.2.1.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

1. BCCCA, RA, and end-user Subscriber certificates are backed up and archived as part of BCCroutine backup procedures.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

1. Operational periods and key pair usage period for all BCC hierarchy certificates will be in accordance to the CCA Digital Certificate Interoperability Guideline document.

6.3.3 Activation Data Generation and Installation

1. Activation data (Secret Shares) used to protect tokens containing BCCCA private keys is generated in accordance with the requirements of Section 6.2.2. The creation and distribution of Secret Shares is logged.

2. Activation data may be Subscriber selected for Subscriber private keys.

3. A pass-phrase, PIN, biometric data, or other mechanisms of equivalent authentication robustness shall be used to protect access to use of a Subscriber or RA Private Keys.

6.3.4 Activation Data Protection

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

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

3. Activation data for Private Keys associated with certificates asserting organisational identities shall be restricted to those in the organisation authorised to use the Private Keys.

6.3.5 Other Aspects of Activation Data

6.3.5.1 Activation Data Transmission

1. To the extent activation data for private keys are transmitted, BCCCA hierarchy Participants shall protect the transmission using methods that protect against the loss, theft, modification, unauthorised disclosure, or unauthorised use of such private keys. To the extent System or network logon user name/password combination is used as activation data for an end-user Subscriber, the passwords transferred across a network shall be protected against access by unauthorised users.

6.3.5.2 Activation Data Destruction

1. Activation data for CA private keys shall be decommissioned using methods that protect against the loss, theft, modification, unauthorised disclosure, or unauthorised use of the private keys protected by such activation data. After the record retention periods in Section 5.5.2 lapse, BCCshall decommission activation data by overwriting and/or physical destruction.

6.4 Computer Security Controls

6.4.1 Specific Computer Security Technical Requirements

1. BCCensures that the systems maintaining CA software and data files are Trustworthy Systems secure from unauthorised access. In addition, BCClimits access to production servers to those individuals with a valid business reason for such access. General application users do not have accounts on production servers.
2. The BCCproduction network is logically separated from other components. This separation prevents network access except through defined application processes. BCCuses firewalls, IPS to protect the production network from internal and external intrusion and limit the nature and source of network activities that may access production systems.
3. BCCrequires the use of passwords that have a minimum character length and a combination of alphanumeric and special characters. BCCrequires that passwords be changed on a periodic basis.
4. Direct access to BCCdatabases supporting BCCCA Operations is limited to Trusted Persons in the hosted Production Operations group having a valid business reason for such access.

6.4.2 Computer Security Rating

1. No stipulation.

Comment [SYMC-LH16]: Updated to No Stipulation

6.5 Life Cycle Technical Controls

6.5.1 System Development Controls

1. Applications are developed and implemented by BCCin accordance with BCCsystems development and change management standards.
2. Such developed software, when first loaded, provides a method to verify that the software on the system originated from BCC, has not been modified prior to installation, and is the version intended for use.

Comment [B17]: Please clarify what applications you meant here? Since we are having the PKI management application from Symantec.

Comment [SYMC-LH18]: This will be the Symantec provided PKI Applications and (optionally) any additional Applications BCC may decide to introduce to perform certificate lifecycle management

6.5.2 Security Management Controls

1. BCChas mechanisms and/or policies in place to control and monitor the configuration of its CA systems.
2. The configuration, including modifications and upgrades of BCCManaged PKI components shall be documented.
3. There shall be a mechanism for detecting unauthorised modification to the software or configuration of BCCManaged PKI components.
4. The BCCIssuing Certification Authorities must only have applications or component software or hardware installed that are directly related to the operation of the BCCPKI.

6.5.3 Life Cycle Security Controls

1. Equipment (hardware and software), including modifications and upgrades, procured for the BCCManaged PKI shall be:

    a) purchased through a mechanism that will reduce the likelihood that any particular component was tampered with

    b) shipped or delivered via controlled methods that provide a continuous chain of accountability from its origin to its destination and handover to BCC

    c) deployed using BCCauthorised personnel

6.6 Network Security Controls

1. BCCperforms all its CA and RA functions using networks secured in accordance with the BCCSecurity and Audit Requirements to prevent unauthorised access and other malicious activity. BCCprotects its communications of sensitive information through the use of encryption and digital signatures.

6.7 Time Stamping

1. Certificates, CRLs, and other revocation database entries shall contain time and date information. Such time information need not be cryptographic-based.

2. A trusted source of network time shall be used. In BCC CA synchronization of CA system is done with the National NTP Servers.

7 Certificate, Certificate Revocation List (CRL), and Online Certificate Status Protocol (OCSP) Profiles

7.1 Certificate Profile

1. Certificates shall conform to the IETF PKIX, RFC 5280 and the CCA Digital Certificate Interoperability Guideline document.

7.2 CRL Profiles

1. Certificate Revocation Lists shall conform to the IETF PKIX, RFC 5280 and the CCA Digital Certificate Interoperability Guideline document.

7.3 OCSP Profiles

2. Online Certificate Status Protocol shall conform to the IETF PKIX, RFC 6960and the CCA Digital Certificate Interoperability Guideline document.

Comment [B19]: RFC 2560 is obsolete by RFC 6960 for OCSP; We guess we can add this new RFC as reference of OCSP

Comment [SYMC-LH20]: Yes, RFC ref updated to 6960

8 Compliance Audit and Other Assessments

1. An annual External Audit for Certification Authorities examination is performed as per the IT(CA) Rules 2010by empanelled auditor under CCA for BCCCA data centre operations and key management operations supporting BCCManaged PKI services.

2. In addition to external audits, BCC shall perform internal audit twice in a year and submit audit reports to Office of the CCA to comply with the IT (CA) Rules 2010.

3. In addition to compliance audits, the BCCshall be entitled to perform other reviews and investigations to ensure the trustworthiness of the BCCPKI, which include, but are not limited to:

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

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

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

Comment [B21]: Reference of CCA Rules

Comment [B22]: Requirement of IT (CA) Rules 2010

8.1 Frequency or Circumstances of Assessment

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

8.2 Identity/Qualifications of Assessor

1. The external auditors must be CCA empanelledauditors in accordance to the IT (CA) Rules 2010.

2. The internal auditors must not hold any Trusted Roles within BCC PKI.

8.3 Assessor's Relationship to Assessed Entity

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

8.4 Topics Covered by Assessment

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

8.5 Actions Taken as a Result of Deficiency

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

9 Other Business and Legal Matters

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

1. Fees may be payable by Subscribers for the issue or Renewal of Certificates. Where fees are payable, an up to date fee schedule shall be provided to Subscribers by way of a Notice in accordance with Section 9.11.

9.1.2 Certificate Access Fees

1. BCC does not charge a fee as a condition of making a Certificate available in a repository or otherwise making Certificates available to Relying Parties.

9.1.3 Revocation or Status Information Access Fees

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

9.1.4 Fees for Other Services

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

9.1.5 Refund Policy.

1. No stipulation.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

1. It is the sole responsibility of each BCC Managed PKI Participant to determine the appropriate insurance coverage in regard to any loss or damage that may be suffered as a result of using a Certificate or associated Keys issued under this CPS.

9.2.2 Insurance or Warranty Coverage for End Entities

1. Each BCC Managed PKI Participant acknowledges that BCC does not provide any insurance coverage or warranty for the benefit of BCC Managed PKI Participants in relation to any loss or damage that they may suffer as a result of participating in the Certificate application process or using a Certificate or associated Keys issued under this CPS.

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

1. The following records of Subscribers shall, subject to Section 9.3.2, be kept confidential and private ("Confidential/Private Information"):

    a) CA application records, whether approved or disapproved,
    b) Certificate Application records,
    c) Private keys held by enterprise Customers using BCC Managed PKI Key Manager and information needed to recover such Private Keys,
    d) Transactional records (both full records and the audit trail of transactions),
    e) Audit trail records created or retained by BCC or a Customer,

f) Audit reports created by BCC or a Customer (to the extent such reports are maintained), or their respective auditors (whether internal or public),
g) Contingency planning and disaster recovery plans
h) Security measures controlling the operations of BCC hardware and software and the administration of Certificate services and designated enrolment services, and
i) Any other information classified as Confidential as per the information classification guideline of BCC.

9.3.2 Information Not Within the Scope of Confidential Information

1. Notwithstanding Section 9.3.1, Confidential Information does not include information which:

a) was already lawfully disclosed by BCC prior to BCC being required to treat the information as confidential;

b) is lawfully received from a third party who is not bound by a duty of confidentiality;

c) has become public knowledge, other than through a breach of an obligation of confidence under this CPS;

d) was independently developed or released by BCC without reference to the Confidential Information;

e) is information that the BCC Managed PKI Participant provides for inclusion within a Certificate;

f) is information indicating that a Certificate has been Revoked or Suspended, though not including the reason behind this Certificate Status; or

g) includes any information relating to the BCC Managed PKI Participant's use of the Repository

9.3.3 Responsibility to Protect Confidential Information

Comment [B23]: Requires Legal Vetting

1. Subject to Section 9.3.3 paragraph 2, BCC shall protect any Confidential Information provided by a BCC Managed PKI Participant in accordance with any relevant contractual undertakings and any applicable law, and shall not, without the prior written approval of the relevant BCC Managed PKI Participant (which approval shall not be withheld unreasonably), make public or disclose to any person, the BCC Managed PKI Participant's Confidential Information.

2. Nothing within Section 9.3.3 paragraph 1 shall be construed to prevent BCC from disclosing any information provided by a BCC Managed PKI Participant:

a) to Bangladesh Government or anyone in connection with the carrying out of any functions, duties, powers and discretions conferred on BCC;

b) to such legal advisors, financial advisers, auditors or insurers of BCC as may be necessary for any proceedings or investigation involving BCC, or for the purposes of facilitating BCC's performance of its functions under this CPS; or

c) to the extent required by law

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

1. No Stipulation.

9.4.2 Information Treated as Private

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

9.4.3 Information Not Treated as Private

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

9.4.4 Responsibility to Protect Private Information

1. BCCManaged PKI participants receiving private information shall secure it from compromise and disclosure to third parties and shall comply with all local privacy laws in their jurisdiction.

9.4.5 Notice and Consent to Use Private Information

1. Each BCC Managed PKI Participant consents to the collection, use, storage, transfer, and disposal of Personal Information by BCC for the purposes of fulfilling its functions under this CPS.

2. This section is subject to applicable privacy laws.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

1. BCCshall be entitled to disclose Confidential/Private Information if, in good faith, BCCbelieves that:

   a) Disclosure is necessary in response to subpoenas and search warrants.

   b) Disclosure is necessary in response to judicial, administrative, or other legal process during the discovery process in a civil or administrative action, such as subpoenas, interrogatories, requests for admission, and requests for production of documents.

2. This section is subject to applicable privacy laws.

9.4.7 Other Information Disclosure Circumstances

1. No stipulation.

9.5 Intellectual Property Rights

1. The allocation of Intellectual Property Rights among BCCManaged PKI Participants other than Subscribers and Relying Parties is governed by the applicable agreements among such BCCManaged PKI Participants. The following subsections of Section 9.5 apply to the Intellectual Property Rights in relation to Subscribers and Relying Parties.

9.5.1 Property Rights in Certificates and Revocation Information

1. CA's retain all Intellectual Property Rights in and to the certificates and revocation information that they issue. BCCgrants permission to reproduce and distribute certificates on a nonexclusive royalty-free basis, provided that they are reproduced in full and that use of certificates is subject to the Relying Party Agreement referenced in the certificate. BCCshall grant permission to use revocation information to perform Relying Party functions subject to the applicable CRL Usage Agreement, Relying Party Agreement, or any other applicable agreements.

9.5.2 Property Rights in the CPS

1. BCCManaged PKI Participants acknowledge that BCCretains all Intellectual Property Rights in and to this CPS.

9.5.3 Property Rights in Names

1. A certificate applicant retains all rights it has (if any) in any trademark, service mark, or trade name contained in any certificate application and distinguished name within any certificate issued to such certificate applicant.

9.5.4 Property Rights in Keys and Key Material

1. Key pairs corresponding to certificates of CAs and end-entity Subscribers are the property of the CAs and end-entity Subscribers that are the respective Subjects of these certificates, subject to the rights of enterprise Customers using BCC Managed PKI Key Manager, regardless of the physical medium within which they are stored and protected, and such persons retain all Intellectual Property Rights in and to these key pairs. Without limiting the generality of the foregoing, BCCroot public keys and the root certificates containing them, including all CA public keys and self-signed certificates, are the property of BCC. BCClicenses software and hardware manufacturers to reproduce such root certificates to place copies in trustworthy hardware devices or software. Finally, Secret Shares of a CA's private key are the property of the CA, and the CA retains all Intellectual Property Rights in and to such Secret Shares even though they cannot obtain physical possession of those shares from BCC.

9.6 Representations and Warranties

1. BCC makes no representations or warranties in regard to any part of the BCC Managed PKI, or any Key or Certificate, other than as specifically provided in this CPS.

2. This CPS is not a contract and cannot be used for warranty purposes.

9.6.1 CA Representations and Warranties

1. BCC warrants that:
   a) There are no material misrepresentations of fact in the Certificate known to or originating from the entities approving the Certificate Application or issuing the Certificate,
   b) There are no errors in the information in the Certificate that were introduced by the entities approving the Certificate Application or issuing the Certificate as a result of a failure to exercise reasonable care in managing the Certificate Application or creating the Certificate,
   c) Their Certificates meet all material requirements of this CPS, and
   d) Revocation services and use of a repository conform to the applicable CPS in all material aspects.

2. Subscriber Agreements may include additional representations and warranties..

9.6.2 RA Representations and Warranties

1. RAs warrant that:
   a) There are no material misrepresentations of fact in the Certificate known to or originating from the entities approving the Certificate Application or issuing the Certificate,
   b) There are no errors in the information in the Certificate that were introduced by the entities approving the Certificate Application as a result of a failure to exercise reasonable care in managing the Certificate Application,
   c) Their Certificates meet all material requirements of this CPS, and
   d) Revocation services (when applicable) and use of a repository conform to the applicable CPS in all material aspects.

2. Subscriber Agreements may include additional representations and warranties.

9.6.3 Subscriber Representations and Warranties

1. Subscribers warrant that:
   a) Each digital signature created using the private key corresponding to the public key listed in the Certificate is the digital signature of the Subscriber and the Certificate has been accepted and is operational (not expired or revoked) at the time the digital signature is created,
   b) Their private key is protected and that no unauthorised person has ever had access to the Subscriber's private key,
   c) All representations made by the Subscriber in the Certificate Application the Subscriber submitted are true,
   d) All information supplied by the Subscriber and contained in the Certificate is true,
   e) The Certificate is being used exclusively for authorised and legal purposes, consistent with this CPS, and
   f) The Subscriber is an end-user Subscriber and not a CA, and is not using the private key corresponding to any public key listed in the Certificate for purposes of digitally signing any Certificate (or any other format of certified public key) or CRL, as a CA or otherwise.

2. Subscriber Agreements may include additional representations and warranties.

9.6.4 Relying Party Representations and Warranties

1. Relying Party Agreements require Relying Parties to acknowledge that they have sufficient information to make an informed decision as to the extent to which they choose to rely on the information in a Certificate, that they are solely responsible for deciding whether or not to rely on such information, and that they shall bear the legal consequences of their failure to perform the Relying Party obligations in terms of this CPS.

2. Relying Party Agreements may include additional representations and warranties.

9.6.5 Representations and Warranties of Other Participants

1. No stipulation.

9.7 Disclaimer of Warranties

1. To the extent permitted by applicable law, Subscriber Agreements and Relying Party Agreements shall disclaim BCC's possible warranties, including any warranty of merchantability or digital transaction.

9.8 Limitation of Liability

1. The liability (and/or limitation thereof) of Subscribers shall be as set forth in the applicable Subscriber agreements.
2. The liability (and/or limitation thereof) of enterprise RAs and the applicable CA shall be set out in the agreement(s) between them.
3. The liability (and/or limitation thereof) of Relying Parties shall be as set forth in the applicable Relying Party Agreements.

9.9 Indemnities

9.9.1 Indemnification by Subscribers

1. To the extent permitted by applicable law, Subscribers are required to indemnify BCC for:
    a) Falsehood or misrepresentation of fact by the Subscriber on the Subscriber's Certificate Application,
    b) Failure by the Subscriber to disclose a material fact on the Certificate Application, if the misrepresentation or omission was made negligently or with intent to deceive any party,
    c) The Subscriber's failure to protect the Subscriber's private key, to use a Trustworthy System, or to otherwise take the precautions necessary to prevent the compromise, loss, disclosure, modification, or unauthorised use of the Subscriber's private key, or
    d) The Subscriber's use of a name (including without limitation within a common name, domain name, or e-mail address) that infringes upon the Intellectual Property Rights of a third party.
2. The applicable Subscriber Agreement may include additional indemnity obligations.

9.9.2 Indemnification by Relying Parties

1. To the extent permitted by applicable law, Relying Party Agreements shall require Relying Parties to indemnify BCC for:
    a) The Relying Party's failure to perform the obligations of a Relying Party,
    b) The Relying Party's reliance on a Certificate that is not reasonable under the circumstances, or
    c) The Relying Party's failure to check the status of such Certificate to determine if the Certificate is expired or revoked.
2. The applicable Relying Party Agreement may include additional indemnity obligations.

9.10 Term and Termination

9.10.1 Term

1. The CPS becomes effective upon publication in the BCCrepository. Amendments to this CPS become effective upon publication in the BCCrepository.

9.10.2 Termination

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

9.10.3 Effect of Termination and Survival

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

9.11 Individual Notices and Communications with Participants

1. Unless otherwise specified by agreement between the parties, BCCManaged PKI participants shall use reasonable methods to communicate with each other, taking into account the criticality and subject matter of the communication.

9.12 Amendments

9.12.1 Procedure for Amendment

1. BCC shall review this CPS at least annually. Corrections, updates, or changes to this CPS shall be publicly available.
2. Proposals for change to this CPS shall be provided in Section 1.5.2. The proposals must include:
    a) detailed description of the change
    b) change justification
    c) contact information for the person requesting the change
3. BCC may consider any proposals for change.
4. CCA, Bangladesh must approve all proposed changes to this CPS before they are included in this CPS.
5. BCC must forward all modifications to this CPS to CCA, Bangladesh for consideration and approval before any change is made to the BCC Managed PKI.

9.12.2 Notification Mechanisms and Period

1. BCCreserve the right to amend the CPS without notification for amendments that are not material, including without limitation corrections of typographical errors, changes to URLs, and changes to contact information. The BCCdecision to designate amendments as material or non-material shall be within the BCCsole discretion.
2. BCCsolicits proposed amendments to the CPS from other BCCManaged PKI participants. If BCCconsiders such an amendment desirable and proposes to implement the amendment, BCC shall provide notice of such amendment in accordance with this section.
3. Notwithstanding anything in this CPS to the contrary, if BCCbelieves that material amendments to the CPS are necessary immediately to stop or prevent a breach of the security of the BCCManaged PKI or any portion of it, BCCshall be entitled to make such amendments by publication in the BCCRepository. Such amendments will be effective immediately upon publication. Within a reasonable time after publication, BCCshall provide notice to CA customers of such amendments.

9.12.2.1 Comment Period

1. Except as otherwise stated, the comment period for any material amendments to the CPS shall be thirty (30) days, starting on the date on which the amendments are posted on the BCCRepository. Any BCCManaged PKI participant shall be entitled to file comments BCC up until the end of the comment period.

9.12.2.2 Mechanism to Handle Comments

1. BCCshall consider any comments on the proposed amendments. BCCshall either (a) allow the proposed amendments to become effective without amendment, (b) amend the proposed amendments and republish them as a new amendment when required, or (c) withdraw the proposed amendments. BCCis entitled to withdraw proposed amendments by notifying Sub-CA's and providing notice in the Practices Updates and Notices section of the BCCRepository. Unless proposed amendments are amended or withdrawn, they shall become effective upon the expiration of the comment period.

9.12.3 Circumstances under Which OID Must Be Changed

1. If BCCdetermines that a change is necessary in the object identifier corresponding to Certificate Policy orCPS, the amendment shall contain new object identifiers for the Certificate Policies. Otherwise, amendments shall not require a change in Certificate Policy object identifier.

9.13 Dispute Resolution Procedures

9.13.1 Disputes among BCCand Customers

1. Disputes among BCCManaged PKI participants shall be resolved pursuant to provisions in the applicable agreements among the parties.

9.13.2 Disputes with End-User Subscribers or Relying Parties

1. To the extent permitted by applicable law, Subscriber Agreements and Relying Party Agreements shall contain a dispute resolution clause. Disputes involving BCCrequire an initial negotiation period of sixty (60) days followed by litigation in the court or, in the case of all other claimants, arbitration administered by the International Chamber of Commerce ("ICC") in accordance with the ICC Rules of Conciliation and Arbitration, unless otherwise approved by BCC.

9.14 Governing Law

1. Subject to any limits appearing in applicable law, the laws of the Peoples Republic of Bangladesh shall govern the enforceability, construction, interpretation, and validity of this CPS, irrespective of contract or other choice of law provisions and without the requirement to establish a commercial nexus. This choice of law is made to ensure uniform procedures and interpretation for all BCCManaged PKI Participants, no matter where they are located.
2. This governing law provision applies only to this CPS. Agreements incorporating the CPS by reference may have their own governing law provisions, provided that this Section 9.14 governs the enforceability, construction, interpretation, and validity of the terms of the CPS separate and apart from the remaining provisions of any such agreements, subject to any limitations appearing in applicable law.
3. This CPS is subject to applicable national, state, local and foreign laws, rules, regulations, ordinances, decrees, and orders including, but not limited to, restrictions on exporting or importing software, hardware, or technical information.

9.15 Compliance with Applicable Law

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

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

1. Not applicable.

9.16.2 Assignment

1. Not applicable.

9.16.3 Severability

1. In the event that a clause or provision of this CPS is held to be unenforceable by a court of law or other tribunal having authority, the remainder of the CPS shall remain valid.

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

1. Not applicable.

9.16.5 Force Majeure

1. To the extent permitted by applicable law, Subscriber Agreements and Relying Party Agreements shall include a force majeure clause protecting BCC.

9.17 Other Provisions

1. Not applicable.

Appendix A: Definitions and Acronyms

Abstract Syntax Notation (ASN.1)	An abstract notation for structuring complex data objects.
Activation Data	Data values, other than keys, that are required to operate cryptographic modules and that need to be protected (e.g., a PIN, a passphrase, or a manually held key share).
Administrator (PKI)	A Trusted Person within the organisation of a Processing Centre that performs validation and other CA or RA functions.
Administrator Certificate	A Certificate issued to an Administrator that may only be used to perform CA or RA functions.
Application Software Vendor	A developer of Internet browser software or other software that displays or uses certificates and distributes root certificates, such as KDE, Microsoft Corporation, Mozilla Corporation, Opera Software ASA, and Red Hat, Inc.
Assurance Level	A specified level of assurances as defined within this CPS.
Asymmetric Cryptography	A class of Cryptography in which a Key Pair is used – a Private Key to create signatures and to decrypt messages, and a Public Key to encrypt messages and verify signatures. It has two main advantages: For n users, only n Key Pairs are needed; and Public Keys can be widely distributed with no requirement for confidentiality;but most methods which can achieve good security require significant computing resources. (see Symmetric Cryptography)
Audit	Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures.
Authorised Party	(Certificate purpose) An Individual or Device with authority to conduct certain actions or make certain assertions.
Authorisation	The granting of rights, including the ability to access specific information or resources.
Automated Administration	A procedure whereby Certificate Applications are approved automatically if enrolment information matches information contained in a database.
Automated Administration Software Module	Software provided by BCCthat performs Automated Administration.
Backup	Copy of files and programs made to facilitate recovery if necessary.
Binding	Process of associating two related elements of information.
Business Day	Any day other than a Saturday, Sunday or public holiday (including public service holidays) for the whole of BCC.
CA-certificate	A certificate for a CA's public key.
Certificate	See X.509 Certificate.
Certificate Applicant	An individual or organisation that requests the issuance of a Certificate by a CA.

Certificate Application	A request from a Certificate Applicant (or authorised agent of the Certificate Applicant) to a CA for the issuance of a Certificate.
Certificate Chain	An ordered list of Certificates containing an end-user Subscriber Certificate and CA-certificates, which terminates in a root Certificate.
Certificate Management Control Objectives	Criteria that an entity must meet in order to satisfy compliance audit.
Certificate Policy (CP)	A named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements.
Certificate Profile	The specification of the fields to be included in a Certificate and the contents of each, as set in the relevant Certificate Policy.
Certificate Re-key	Within the BCCPKI, Certificate Re-key is defined as the issuance of a new certificate to replace an existing valid certificate, with a new serial number, validity, and public key, but with no other Subscriber information changed.
Certificate Renewal	Within the BCCPKI, Certificate Renewal is defined as the issuance of a new certificate to replace an existing valid certificate, with a new serial number and extended validity but with no other Subscriber information changed
Certificate Revocation List (CRL)	A signed, time-stamped list of serial numbers of the Public Key Certificates of Subscribers (other than Certification Authorities) that have been revoked prior to their scheduled Expiry.
Certificate Signing Request (CSR)	A message conveying a request to have a Certificate issued.
Certification Authority (CA)	An entity authorised to issue, manage, revoke, and renew Certificates in the BCCPKI.
Certification Authority Manager (CAM)	The CA individual who is responsible for overseeing the management of the CA.
Certification Authority Owner (CAO)	The legal entity responsible for the Certification Authority.
Certification Path	An ordered sequence of certificates that, together with the public key of the initial object in the path, can be processed to obtain that of the final object in the path.
Certification Practice Statement (CPS)	A statement of the practices that a CA employs in issuing, managing, revoking, and renewing or re-keying certificates.
Challenge Phrase	A secret phrase chosen by a Certificate Applicant during enrolment for a Certificate. When issued a Certificate, the Certificate Applicant becomes a Subscriber and a CA or RA can use the Challenge Phrase to authenticate the Subscriber when the Subscriber seeks to revoke or renew the Subscriber's Certificate.
Ciphertext	Information that has been encrypted into seemingly meaningless code. (see Plaintext)

Compromise	A violation (or suspected violation) of a security policy, in which an unauthorised disclosure of, or loss of control over, sensitive information may have occurred. With respect to private keys, a Compromise is a loss, theft, disclosure, modification, unauthorised use, or other compromise of the security of such private key.
CRL Usage Agreement	An agreement setting forth the terms and conditions under which a CRL or the information in it can be used.
Cross Certification	The process undertaken by Certification Authorities to establish a trust relationship. When two Certification Authorities are cross-certified, they agree to trust and rely upon each other's public key certificates and keys as if they had issued them themselves. The two Certification Authorities exchange cross-certificates, enabling their respective users to interact securely.
Cryptographic Module	The set of hardware, software, firmware, or some combination thereof that implements cryptographic logic or processes, including cryptographic algorithms, and is contained within the cryptographic boundary of the module.
Device (Certificate)	(Certificate purpose) A device, host, service, or process. For example, a network device, firewall, server, personal computer, handheld digital device, Smartphone, access point, website, service, process, socket, interface, or the like.
Digital Signature	A method of using Cryptography to link an exclusive identity to an electronic document or transaction to accomplish what a written signature accomplishes in a paper document. A digital signature also verifies that the contents of the message or document have not been altered.
Distinguished Encoding Rules (DER)	Rules for encoding ASN.1 objects which give a consistent encoding for each ASN.1 value using a binary format.
Distinguished Name (DN)	A unique identifier assigned to each Certificate Applicant, having the structure required by the Certificate Profile.
Dual Use Certificate	A Certificate that is intended for use with both digital signature and data encryption services.
Encryption Certificate	A Certificate containing a Public Key that is used to encrypt electronic messages, files, documents, or data transmissions, or to establish or exchange a session key for these same purposes.
EndEntity	A Relying Party or a Subscriber.
Evidence Of Identity (EOI)	The process implemented to determine the identity of an entity using documents or other information identifying the entity.
Hardware Security Module	A hardware device incorporating tamper protection, used to securely generate and store cryptographic keys.
Hashing	The process of subjecting a set of data to a sequence of mathematical operations to compute a numeric value that will later be compared to ensure the original data has not been altered.
Identification	The process of establishing the identity of an entity, by: • Establishing that a given name of an entity corresponds to a real-world identity of an entity, and • Establishing that an entity applying for or seeking access under that name is, in fact, the named entity.
User	(Certificate purpose)

(Certificate)	A person.
Intellectual Property Rights	Rights under one or more of the following: any copyright, patent, trade secret, trademark, and any other intellectual property rights.
Intermediate Certification Authority (Intermediate CA)	A Certification Authority whose Certificate is located within a Certificate Chain between the Certificate of the root CA and the Certificate of the Certification Authority that issued the end-user Subscriber's Certificate.
Issuing Certification Authority (Issuing CA)	In the context of a particular certificate, or when the phrase "the issuing CA" is used, the issuing CA is the CA that issued the certificate. In the context of the BCCPKI hierarchy of CAs, or when the phrase "an Issuing CA" is used, an Issuing CA is a CA that issues End-Entity Certificates, and does not issue CA-certificates.
Key	A sequence of symbols that controls the operation of a cryptographic transformation.
Key Escrow	The process of entrusting a Private Key to a third party (an Escrow Agent such as an Organisation or government) and providing another third party with a legal right to obtain the Key from the Escrow Agent in certain circumstances.
Key Exchange	The process of exchanging public keys in order to establish secure communications.
Key Generation Ceremony	A procedure whereby a CA's or RA's key pair is generated, its private key is transferred into a cryptographic module, its private key is backed up, and/or its public key is certified.
Key Pair	A matching Private Key and Public Key which are mathematically linked such that one will decrypt Ciphertext produced with the other. In many cryptosystems, including those used here, the converse is also true, i.e. either key can be used to decrypt Ciphertext produced with the other.
Managed PKI	BCCfully integrated managed PKI service that allows enterprise Customers of BCCand its Partners to distribute certificates to individuals, such as employees, partners, suppliers, and customers, as well as devices, such as servers, routers, and firewalls. BCC Managed PKI permits enterprises to secure messaging, intranet, extranet, virtual private network, and e-commerce applications.
Managed PKI Administrator	An Administrator that performs validation or other RA functions for BCC Managed PKI Customer.
Managed PKI Control Centre	A web-based interface that permits BCC Managed PKI Administrators to perform Manual Authentication of Certificate Applications
BCC Managed PKI Key Manager	A key recovery solution for those BCC Managed PKI Customers choosing to implement key recovery under a special BCC Managed PKI Agreement.
BCC Managed PKI Key Management Service Administrator's Guide	A document setting forth the operational requirements and practices for BCC Managed PKI Customers using BCC Managed PKI Key Manager.
Manual Authentication	A procedure whereby Certificate Applications are reviewed and approved manually one-by-one by an Administrator using a web-based interface.

Non-repudiation	An attribute of a communication that provides protection against a party to a communication falsely denying its origin, denying that it was submitted, or denying its delivery. Denial of origin includes the denial that a communication originated from the same source as a sequence of one or more prior messages, even if the identity associated with the sender is unknown. Note: only adjudication by a court, arbitration panel, or other tribunal can ultimately prevent repudiation. For example, a digital signature verified with reference to a BCCManaged PKI Certificate may provide proof in support of a determination of Non-repudiation by a tribunal, but does not by itself constitute Non-repudiation.
No verified Subscriber Information	Information submitted by a Certificate Applicant to a CA or RA, and included within a Certificate, that has not been confirmed by the CA or RA and for which the applicable CA and RA provide no assurances other than that the information was submitted by the Certificate Applicant.
Offline CA	BCCPCAs, Root CAs and other designated intermediate CAs that are maintained offline for security reasons in order to protect them from possible attacks by intruders by way of the network. These CAs do not directly sign end user Subscriber Certificates.
Online CA	CAs that sign end user Subscriber Certificates are maintained online so as to provide continuous signing services.
Online Certificate Status Protocol (OCSP)	A protocol for providing Relying Parties with real-time Certificate status information.
Operational Period	The period starting with the date and time a Certificate is issued (or on a later date and time certain if stated in the Certificate) and ending with the date and time on which the Certificate expires or is earlier revoked.
PKCS #10	Public-Key Cryptography Standard #10, developed by RSA Security Inc., which defines a structure for a Certificate Signing Request.
PKCS #12	Public-Key Cryptography Standard #12, developed by RSA Security Inc., which defines a secure means for the transfer of private keys.
Plaintext	Information in a directly-usable, unencrypted form. (see Ciphertext)
Policy Authority (PA)	The entity responsible for the approval of a Certificate Policy and the associated Certification Practice Statement, Subscriber Agreement and Relying Party Agreement.
Policy Management Authority (PMA)	The organisation within BCCresponsible for promulgating this policy throughout the BCCPKI.
Private Key	That Key of an entity's Key Pair which should only be used by that entity, and should not be disclosed to any other entity.
Private Signing Key	See Private Authentication Key.
Processing Centre	An organisation (BCCor certain other entities) that creates a secure facility housing, among other things, the cryptographic modules used for the issuance of Certificates.
Public Key	That Key of an entity's Key Pair which can be made public.
Public Key Infrastructure (PKI)	The architecture, organisation, techniques, practices, and procedures that collectively support the implementation and operation of a Certificate-based public key cryptographic system.
Public-Key Cryptography Standards (PKCS)	A series of cryptographic standards dealing with public-key issues, published by RSA Laboratories.
BCCManaged PKI Participant	An individual or organisation that is one or more of the following within the BCCManaged PKI CA hierarchy: BCC, a Subscriber, or a Relying Party.
BCCManaged PKI Standards	The business, legal, and technical requirements for issuing, managing, revoking, renewing, and using Certificates within the BCCPKI.
BCC Repository	BCCdatabase of Certificates and other relevant BCCManaged PKI information accessible on-line.

Registration Authority (RA)	An entity which carries out a number of functions on behalf of a Certification Authority (CA), including one or more of the following functions: The identification and authentication of certificate applicants, the approval or rejection of certificate applications and requesting generation of certificates from the CA, initiating certificate revocations or suspensions under certain circumstances, processing subscriber requests to revoke or suspend their certificates, and approving or rejecting requests by subscribers to renew or rekey their certificates. RAs do not sign or issue certificates.
Registration Authority Manager (RAM)	The RA individual who is responsible for overseeing the management of the RA.
Registration Information	Information that an applicant is required to disclose for the purpose of obtaining keys and certificates.
Relying Party	A recipient of a certificate which relies on that certificate for authentication or confidentiality and/or any digital signatures verified using that certificate.
Relying Party Agreement	An agreement used by a CA setting forth the terms and conditions under which an individual or organisation acts as a Relying Party.
Repudiation	The denial or attempted denial of involvement by a party in all or part of an electronic Transaction.
Revoke	The process undertaken by the CA, generally in response to a request by an RA, to invalidate a certificate. A subscriber may request revocation through the RA.
Root Certification Authority (Root CA)	The CA which is the highest trusted element in the PKI.
Secret Share	A portion of a CA private key or a portion of the activation data needed to operate a CA private key under a Secret Sharing arrangement.
Secret Sharing	The practice of splitting a CA private key or the activation data to operate a CA private key in order to enforce multi-person control over CA private key operations under Section 6.2 of the CP and CPS
Secure Sockets Layer (SSL)	The industry-standard method for protecting Web communications developed by Netscape Communications Corporation. The SSL security protocol provides data encryption, server authentication, message integrity, and optional client authentication for a Transmission Control Protocol/Internet Protocol connection.
Session Key	A Symmetric Cryptography Key generated specifically for use within a single transaction or session.
Subject	The holder of a private key corresponding to a public key. The term "Subject" can, in the case of an organisational Certificate, refer to the equipment or device that holds a private key. A Subject is assigned an unambiguous name, which is bound to the public key contained in the Subject's Certificate.
Subordinate CA	In a hierarchical PKI, a CA whose certificate signature key is certified by another CA, and whose activities are constrained by that other CA. (see Superior CA)
Subscriber	In the case of an individual Certificate, a person who is the Subject of, and has been issued, a Certificate. In the case of an organisational Certificate, an organisation that owns the equipment or device that is the Subject of, and that has been issued, a Certificate. A Subscriber is capable of using, and is authorised to use, the private key that corresponds to the public key listed in the Certificate.
Subscriber Agreement	An agreement used by a CA or RA setting forth the terms and conditions under which an individual or organisation acts as a Subscriber.
Superior CA	In a hierarchical PKI, a CA who has certified the certificate signature key of another CA, and who constrains the activities of that CA. (see Subordinate CA)
Symmetric Cryptography	A class of cryptography in which a single Key is used to both encrypt and decrypt a message. It has two main disadvantages: • for n users, approximately n2 Keys are required; and

	• confidentiality must be ensured when distributing Keys. (see Asymmetric Cryptography)
System Administrator	An individual who maintains the CA's or RA's hardware and software.
Token	Media capable of storing the Private Key of a Subscriber. Tokens include secure tokens and other devices such as smart cards.
Trusted Person	An employee, contractor, or consultant of an entity within the BCCManaged PKI responsible for managing infrastructural trustworthiness of the entity, its products, its services, its facilities, and/or its practices as further defined in CP.
Trusted Position	The positions within a BCCManaged PKI entity that must be held by a Trusted Person.
Trustworthy System	Computer hardware, software, and procedures that are reasonably secure from intrusion and misuse; provide a reasonable level of availability, reliability, and correct operation; are reasonably suited to performing their intended functions; and enforce the applicable security policy. A trustworthy system is not necessarily a "trusted system" as recognised in classified government nomenclature.
Valid Certificate	A Certificate issued by a CA and accepted by the Subscriber listed in it that has not been revoked or suspended and remains operational.
X.509	The International Telegraph and Telephone Consultative Committee (CCITT1) recommendation X.509 "Information technology - Open Systems Interconnection - The directory: Authentication framework" was published in 1988 to authenticate access to modify parts of the X.500 directory. The certificates used the X.208 "Abstract Syntax Notation One (ASN.1)" according to a unique subset of the X.209 "Basic Encoding Rules (BER)", called the "Distinguished Encoding Rules (DER)".
X.509 Certificate	Binds an entity's identity, such as a person's name, an asset number, or a position title, to a cryptographic Public Key. The entity (person, asset or role) is the "subject" or "subscriber" of the certificate. The identity (name, number or title) forms the X.500 Distinguished Name (DN) of the certificate. The certificate is evidence that the Certification Authority (CA) has verified that the cryptographic public key in the certificate belongs to the entity identified by the DN of the certificate.

Acronyms and Abbreviations

AAL	Authentication Assurance Level
ANSI	The American National Standards Institute
AO	Authorising Officer
ASN.1	Abstract Syntax Notation
CA	Certification Authority
CAM	Certification Authority Manager
CAO	Certification Authority Owner
CC	Common Criteria
CO	Certifying Officer
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSR	Certificate Signing Request
DER	Distinguished Encoding Rules
DN	Distinguished Name
EOI	Evidence Of Identity
FIPS	United States Federal Information Processing Standards
HSM	Hardware Security Module
IETF	The Internet Engineering Task Force
LDAP	Lightweight Directory Access Protocol
OCSP	Online Certificate Status Protocol
PA	Policy Authority
PIN	Personal identification number

PKCS	Public-Key Cryptography Standard
PKIX	IETF “Public-Key Infrastructure (X.509)” Working Group standards
PMA	Policy Management Authority
RA	Registration Authority
RFC	Request for comment
RO	Registration Officer
RSA	A public key cryptographic system invented by Rivest, Shamir, and Adelman.
S/MIME	Secure multipurpose Internet mail extensions
SSL	Secure Sockets Layer