

# Bangladesh Root CA CPS

Title	
Document Code	
Version	
Publication Date	
Last Update	
Author	
Editor	

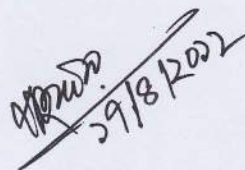


**Office of the Controller of Certifying Authorities**  
**Ministry of Information & Communication Technology**  
**Government of the Peoples Republic of Bangladesh**

## Document Reference

Title	Bangladesh Root CA CPS
Document Type	Public
Version	1.00
Publishing Date	17 April 2012
Last Update	17 April 2012
Pages	31
Status	Approved

Signature:

  
29/8/2012

---

(Md. Zahangir Alam, ndc)  
Controller of Certifying Authorities

## List of Abbreviations/Acronyms

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

## Table of Contents

Root CA CPS	1
1 Introduction	8
1.1 Overview	8
1.2 Document Name and Identification	8
1.3 PKI Participants	8
1.3.1 Root CA	8
1.3.2 Registration Authority	8
1.3.3 End Entities	8
1.4 Certificate Usage	8
1.5 Policy Administration	9
1.5.1 Contact Details	9
1.6 General Definitions	9
2 Publication and Repository Responsibilities	10
2.1.1 Repositories	10
2.1.2 Publication of CA information	10
2.1.3 Frequency of Publication	10
2.1.4 Access Control on Repositories	10
3 Identification and Authentication	11
3.1 Naming	11
3.1.1 Types of names	11
3.1.2 Name Meanings	11
3.1.3 Uniqueness of names	11
3.1.4 Anonymity or Pseudonymity of Subscribers	11
3.1.5 Rules for interpreting various name forms	11
3.1.6 Name claim Dispute resolution procedure	11
3.2 Initial Identity Validation	11
3.2.1 Method to Prove Possession of Private Key	11
3.2.2 Authentication of Organization Identity	11
3.2.3 Authentication of Individual Identity	12
3.2.4 Criteria for Interoperation	12
3.3 Identification and Authentication for Re-key Requests	12
3.3.1 Routine Rekey	12
3.3.2 Rekey After Revocation	12
3.4 Identification and Authentication for Revocation Request	12
4 Certificate Life-Cycle Operational Requirements	12
4.1 Certificate Application	12
4.1.1 Who can submit Certificate Application	12
4.1.2 Enrollment Process and Responsibilities	12
4.2 Certificate Application Processing	13
4.3 Certificate Issuance	13
4.4 Certificate Acceptance	13
4.5 Key Pair and Certificate Usage	13
4.6 Certificate Renewal	13
4.7 Certificate Re-key	13
4.8 Certificate Modification	13
4.9 Certificate Revocation and Suspension	13
4.9.1 Circumstances for Revocation	13
4.9.2 Who Can Request Revocation	14
4.9.3 Procedure for Revocation Request	14
4.9.4 Time within which Root CA must process the revocation request	14
4.9.5 CRL Issuance Frequency	14
4.9.6 Maximum latency for CRLs	14
4.9.7 Online Revocation/status checking availability	14
4.9.8 Online Revocation checking requirements	14
4.9.9 Other forms of revocation advertisement available	14
4.9.10 Circumstances for Suspension	15

4.10	Certificate Status Services	15
4.11	End of Subscription	15
4.12	Key Escrow and Recovery	15
4.13	Security Audit Procedures	15
5	Facility, Management and Operational Controls	15
5.1	Physical Security Controls	15
5.1.1	Site Location and construction	15
5.1.2	Physical Access	15
5.1.3	Power and Air Conditioning	16
5.1.4	Water Exposures	16
5.1.5	Fire prevention and protection	16
5.1.6	Media Storage	16
5.1.7	Waste Disposal	16
5.1.8	Off-site Backup	16
5.2	Procedural Controls	16
5.2.1	Trusted Roles	16
5.2.2	Number of Persons required per Task	17
5.2.3	Identification and authentication for each role	17
5.2.4	Roles requiring separation of duties	17
5.3	Personnel Security Controls	17
5.3.1	Qualification, Experience and Clearance requirements	17
5.3.2	Background Check Procedures	17
5.3.3	Training Requirements	17
5.3.4	Retraining Frequency and Requirements	17
5.3.5	Job Rotation frequency and sequence	17
5.3.6	Sanctions for unauthorized actions	18
5.3.7	Independent contractor requirements	18
5.3.8	Documentation Supplied to personnel	18
5.4	Audit Logging Procedure	18
5.4.1	Types of Events Recorded	18
5.4.2	Frequency of Processing Data	18
5.4.3	Retention period for Security Audit Data	18
5.4.4	Protection of Security Audit Data	18
5.4.5	Security Audit Data Backup Procedure	19
5.4.6	Audit Collection System (Internal or External)	19
5.4.7	Notification to Event-Causing Subject	19
5.4.8	Vulnerability Assessment	19
5.5	Records Archival	19
5.5.1	Types of Event Recorded	19
5.5.2	Retention Period for Archives	19
5.5.3	Protection of Archive	19
5.5.4	Archive Backup Procedure	19
5.5.5	Requirements for time-stamping of Records	19
5.5.6	Archive Collection System (Internal or External)	19
5.5.7	Procedures to obtain and verify archive information	19
5.6	Key Changeover	20
5.7	Compromise and Disaster Recovery	20
5.7.1	Incident and Compromise Handling Procedures	20
5.7.2	Computing Resources, Software and/or Data are corrupted	20
5.7.3	Root CA private key Compromise Recovery Procedure	20
5.7.4	Business Continuity Capabilities after a Disaster	20
5.8	Root CA Termination	20
6	Technical Security Controls	21
6.1	Key Pair Generation and Installation	21
6.1.1	Key Pair Generation	21
6.1.2	Private Key Delivery to Subscriber	21
6.1.3	Public Key Delivery to Certificate Issuer	21

6.1.4	CA Public Key Delivery to relying parties	21
6.1.5	Key Sizes	21
6.1.6	Public Key Parameters Generation	21
6.1.7	Parameter Quality Checking	21
6.1.8	Key usage Purposes	21
6.2	Private Key Protection and Cryptographic Module Engineering Controls	21
6.2.1	Cryptographic Module Standards & Controls	21
6.2.2	Private Key multi person control	22
6.2.3	Private Key escrow	22
6.2.4	Private Key backup	22
6.2.5	Private Key archival	22
6.2.6	Private Key archival	22
6.2.7	Private Key Storage on cryptographic Module	22
6.2.8	Method of Activating Private Key	22
6.2.9	Method of Deactivating Private Key	22
6.2.10	Method of Destroying Private Key	22
6.3	Other Aspects of Key Pair Management	22
6.3.1	Public Key Archival	22
6.3.2	Certificate operational periods and key pair usage period	23
6.4	Activation Data	23
6.5	Computer Security Controls	23
6.5.1	Specific Computer Security Technical Requirements	23
6.5.2	Computer Security Rating	23
6.6	Life-Cycle Security Controls	23
6.7	Network Security Controls	23
6.8	Time Stamping	23
7	Certificate, CRL and OCSP Profiles	23
7.1	Certificate Profile	23
7.1.1	Version number	23
7.1.2	Certificate Extensions	23
7.1.3	Algorithm Object identifiers	24
7.1.4	Name Forms	24
7.1.5	Name Constraints	24
7.1.6	Certificate Policy Object Identifier	24
7.1.7	Usage of Policy Constraints Extensions	24
7.1.8	Policy qualifier syntax and semantics	24
7.2	CRL Profile	24
7.2.1	Version	24
7.2.2	CRL and CRL Entry Extensions	24
7.3	OCSP Profile	24
8	Compliance Audit & Other Assessments	24
8.1	Frequency or circumstances of assessment	24
8.2	Identity/qualification of assessor	25
8.3	Assessor's relationship to assessed entity	25
8.4	Topics covered by assessment	25
8.5	Actions taken as a result of deficiency	25
8.6	Communication of results	25
9	Other Business and Legal Matter	25
9.1	Fees	25
9.1.1	Certificate issuance and renewal fees	25
9.1.2	Certificate Access fees	25
9.1.3	Revocation or status information access fees	25
9.1.4	Fees for other service	25
9.1.5	Refund Policy	26
9.2	Financial Responsibility	26
9.2.1	Insurance Coverage	26
9.2.2	Other assets	26

9.2.3	Insurance or Warranty coverage for end entities	26
9.3	Confidentiality of Business Information	26
9.3.1	Scope of Confidential Information	26
9.3.2	Information not within the scope of confidential information	26
9.3.3	Responsibility to protect confidential information	26
9.4	Privacy of Personal Information	26
9.4.1	Privacy Plan	26
9.4.2	Information treated as private	26
9.4.3	Information not deemed as private	27
9.4.4	Responsibility to protect private information	27
9.4.5	Notice and consent to use private information	27
9.4.6	Disclosure pursuant to judicial or administrative process	27
9.4.7	Other information disclosure circumstances	27
9.5	Intellectual Property Rights	27
9.6	Representation and Warranties	27
9.6.1	Root CA representation & warranties	27
9.6.2	CA representation & warranties	27
9.6.3	Relying Party representation & warranties	28
9.6.4	Repository representation & warranties	28
9.7	Disclaimers of Warranties	28
9.8	Limitations of Liability	28
9.9	Indemnities	29
9.10	Term and Termination	29
9.10.1	Term	29
9.10.2	Termination	29
9.10.3	Effect of termination and survival	29
9.11	Individual Notices and communications with participants	29
9.12	Amendments	29
9.12.1	Procedure for amendment	29
9.12.2	Notification mechanism and period	29
9.12.3	Circumstances under which OID must be changed	29
9.13	Dispute Resolution Procedure	29
9.14	Governing Law	30
9.15	Compliance with Applicable Law	30
9.16	Miscellaneous Provisions	30
9.17	Other Provisions	30
	Bibliography	31

# 1 Introduction

## 1.1 Overview

This document is structured according to CPS Guideline issued by CCA and in accordance with RFC 3647. This document describes the set of rules and procedures established by Bangladesh Root CA for the operations of the Bangladesh National PKI service.

This document will include the Certification Practice Statement for the Bangladesh Root CA. The general architecture is a single certificate authority. The certificate authority is a stand-alone self signed CA. It is the intent of the Root CA Bangladesh to sign only licensed CAs certificate and CRL.

## 1.2 Document Name and Identification

Document title:  
Bangladesh Root CA CPS  
Document version:  
1.00  
Document Date:  
April 17, 2012  
OID: -

## 1.3 PKI Participants

### 1.3.1 Root CA

CCA will manage and operate the Root CA of Bangladesh PKI. This CA is never on a computer network. When not in use to sign certificates or CRL's, the CA is offline, with components stored in a highly secured location. Access to CA services is controlled in a highly secured manner with N out of M control mechanism. All data transferred to or from the CA hosting server will be done by secure removable media. The private key of the CA is managed by a FIPS 140 level 3 compliant Hardware Security Module.

### 1.3.2 Registration Authority

The designated officers of Office of the CCA will act as the RA and process all licensed CA signing requests including verification of their signing request.

### 1.3.3 End Entities

Root CA is the issuer of the CA certificates only. No end entity certificate is issued by Root CA.

## 1.4 Certificate Usage

The Root CA certificate is only applicable to sign certificate and CRLs of the licensed CA certificates.



## 1.5 *Policy Administration*

### 1.5.1 *Contact Details*

The Root CA is operated and managed by Office of the CCA under Ministry of ICT. Contact person for questions related to this document is:

Name: Md. Zahangir Alam, ndc

Designation: Controller

Address: Office of the CCA, BCC Bhaban, Agargaon, Dhaka, Bangladesh

Email: controller@cca.gov.bd

Phone: 028144042

## 1.6 *General Definitions*

### **Activation Data**

Data values, other than keys, that are required to operate cryptographic modules and that need to be protected (e.g., a PIN, a pass phrase, or a manually-held key share).

### **Certification Authority (CA)**

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

### **Certificate Policy (CP)**

A named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements. For example, a particular certificate policy might indicate applicability of a type of certificate to the authentication of electronic data interchange transactions for the trading of goods within a given price range.

### **Certification Practice Statement (CPS)**

A statement of the practices, which a certification authority employs in issuing certificates.

### **Host Certificate**

A Certificate for server certification and encryption of communications (SSL/TLS). It will represent a single machine. Host Certificates are used internally by the PKI service and are not issued to other sites.

### **Person Certificate**

A certificate used for authentication to establish a Person Identity. It will represent an individual person.

### **Policy Qualifier**

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

### **Registration Authority (RA)**

An entity that is responsible for identification and authentication of certificate subjects, but that does not sign or issue certificates (i.e., an RA is delegated certain tasks on behalf of a CA)

**Relying Party**

A recipient of a certificate who acts in reliance on that certificate and/or digital signatures verified using that certificate.

**Service Certificate**

A certificate for a particular service running on a host. It will represent a single service on a single host.

**Set of provisions**

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

**Subscriber**

Or sometimes called End Entity is the person who applied for and was issued a certificate.

## 2 Publication and Repository Responsibilities

### 2.1.1 Repositories

Repository of certificates and CRLs can be found at: [pub.cca.gov.bd](http://pub.cca.gov.bd) or [ldap.cca.gov.bd](http://ldap.cca.gov.bd) or [crl.cca.gov.bd](http://crl.cca.gov.bd)

### 2.1.2 Publication of CA information

Root CA Bangladesh will operate a secure online repository that contains:

- Root CA certificate;
- Certificates issued by CCA;
- A Certificate Revocation List issued by CCA;
- A copy of this document;
- Other information deemed relevant to the CCA.

### 2.1.3 Frequency of Publication

- Certificates will be published to the Root CA repository as soon as it is issued.
- CRLs will be published as soon as it is issued or refreshed once every six months if there are no changes.

### 2.1.4 Access Control on Repositories

The online repository is available on a substantially 24/7 basis, subject to reasonable scheduled maintenance. The CCA Root CA service does not impose any access control on its Policy, its signing Certificate and issued certificates, and its CRLs.

### **3 Identification and Authentication**

#### **3.1 Naming**

##### **3.1.1 Types of names**

See section 7.1.4 for more details.

##### **3.1.2 Name Meanings**

The Root CA signs licensed CA certificates and it is the only self signed certificate in Bangladesh PKI. Root CA certificate uses name in a meaningful way and as per the Interoperability Guideline. The subject DN of Root CA is as below:

CN= Root CA Bangladesh, O=Office of the CCA, C=BD

Licensed Certifying Authorities are required to use name in accordance with Interoperability Guideline.

##### **3.1.3 Uniqueness of names**

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

##### **3.1.4 Anonymity or Pseudonymity of Subscribers**

No Stipulation.

##### **3.1.5 Rules for interpreting various name forms**

No Stipulation.

##### **3.1.6 Name claim Dispute resolution procedure**

No Stipulation.

#### **3.2 Initial Identity Validation**

##### **3.2.1 Method to Prove Possession of Private Key**

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

##### **3.2.2 Authentication of Organization Identity**

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

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

### **3.2.3 Authentication of Individual Identity**

No Stipulation.

### **3.2.4 Criteria for Interoperation**

No Stipulation.

## **3.3 Identification and Authentication for Re-key Requests**

### **3.3.1 Routine Rekey**

No Stipulation.

### **3.3.2 Rekey After Revocation**

Rekey after revocation follows the same rules as an initial identity validation.

## **3.4 Identification and Authentication for Revocation Request**

In this case Requestor's public key will be used for authentication. See section 4.4.2 for details on who can request a certificate revocation.

# **4 Certificate Life-Cycle Operational Requirements**

## **4.1 Certificate Application**

Licensed CAs in Bangladesh PKI are required to submit their certificate signing request along with a formal application to CCA.

### **4.1.1 Who can submit Certificate Application**

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

### **4.1.2 Enrollment Process and Responsibilities**

There is a formal enrollment process for licensed CAs. Their responsibility is as defined in the ICT Act 2006 (amended in 2009), IT (CA) Rules 2010, License Document and other guidelines issued by CCA.

## **4.2 Certificate Application Processing**

Office of the CCA will perform initial identity validation and authentication of the application by scrutinizing the License document and other documents mentioned in Section 3.2.2. After the application processing, based on the identity validation and authentication, CCA can approve or reject an application by noticing reasons whatsoever to the applicant.

## **4.3 Certificate Issuance**

After approval of the application, CCA will process the certificate signing request (CSR) and check the compliance with the Interoperability Guideline and other guidelines issued by CCA. If the application and CSR are found compliant, CCA will sign the request and issue certificate to the Applicant in an offline secure media.

## **4.4 Certificate Acceptance**

The licensed CAs are required to submit an acceptance letter to CCA while receiving the certificate issued to them. CCA will publish the issued certificate within 24 hours to the certificate repository after acceptance. CCA will notify in its website about the certificate been issued.

## **4.5 Key Pair and Certificate Usage**

Root CA private key is only used to sign licensed CAs certificate and CRLs. Public key and the Root Certificate is used by the relying parties for trusted path validation as the root of trust in Bangladesh PKI.

## **4.6 Certificate Renewal**

No Stipulation.

## **4.7 Certificate Re-key**

No Stipulation.

## **4.8 Certificate Modification**

No Stipulation.

## **4.9 Certificate Revocation and Suspension**

### **4.9.1 Circumstances for Revocation**

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

- CCA suspend or revoke the license as per Section 26 (1) of the ICT Act 2006 (amended in 2009);
- The licensee breach any direction made upon him as per the ICT Act 2006 (amended in 2009), IT (CA) Rules 2010, License Document and other guidelines issued by CCA;
- The licensed CA private key is lost or suspected to be compromised;
- The information in the licensed CA certificate is suspected to be inaccurate;

- Incorrect information submitted while issuance or renewal of license or issuance of certificate;
- Licensee breaches terms and conditions mentioned in the license;
- The licensee is bankrupt or wound-up or become unable to continue CA operations;
- The trust of Bangladesh PKI affects by the licensee;
- The licensed CA no longer needs the certificate to generate EE certificates;
- The licensee violates his/her own CP/CPS; or
- Any other reason deems required revocation of the certificate of the licensee by CCA.

#### **4.9.2 Who Can Request Revocation**

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

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

#### **4.9.3 Procedure for Revocation Request**

The entity requesting the revocation must authenticate itself to the CCA. After validating the Revocation request CCA will revoke the certificate, publish the CRL and record the reasons and other necessary relevant documents.

#### **4.9.4 Time within which Root CA must process the revocation request**

CCA will process revocation within 3 working days of receiving the revocation request message. The Root CA does not support Certificate Suspension, if any mistrust arise as described in 4.9.1, Root CA will revoke certificate involve in that mistrust activities.

#### **4.9.5 CRL Issuance Frequency**

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

#### **4.9.6 Maximum latency for CRLs**

Maximum latency for CRLs is one day.

#### **4.9.7 Online Revocation/status checking availability**

An OCSP service will be made available.

#### **4.9.8 Online Revocation checking requirements**

No stipulation.

#### **4.9.9 Other forms of revocation advertisement available**

No stipulation.

#### **4.9.10 Circumstances for Suspension**

No stipulation.

#### **4.10 Certificate Status Services**

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

#### **4.11 End of Subscription**

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

#### **4.12 Key Escrow and Recovery**

No Stipulation.

#### **4.13 Security Audit Procedures**

Security audit will be performed every six month.

### **5 Facility, Management and Operational Controls**

#### **5.1 Physical Security Controls**

##### **5.1.1 Site Location and construction**

Root CA Bangladesh is located at Office of the CCA, BCC Bhaban, Agargaon, Dhaka. The Root CA construction is made complying best practices and proper security controls. The Root CA system is designed to have isolated collocation trust center in order to maintain utmost security.

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

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

##### **5.1.2 Physical Access**

The CCA Data center maintains a restricted access procedure for authorized personnel only. 6 tiers of access control is present –

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

- 6<sup>th</sup> tier: 4<sup>th</sup> Iron door of strong room.

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

### **5.1.3 Power and Air Conditioning**

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

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

### **5.1.4 Water Exposures**

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

### **5.1.5 Fire prevention and protection**

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

### **5.1.6 Media Storage**

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

### **5.1.7 Waste Disposal**

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

### **5.1.8 Off-site Backup**

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

## **5.2 Procedural Controls**

### **5.2.1 Trusted Roles**

A trusted role is one whose incumbent performs functions that can introduce security problems if not carried out properly, whether accidentally or maliciously. The people selected to fill these roles must be extraordinarily responsible or the integrity of the PKI is weakened. The functions performed in these roles form the basis of trust for all uses of the CCA. The following are the trusted roles for root CA:

- Controller



- Deputy Controller
- Assistant Controller
- Assistant Engineer
- Assistant Programmer

### 5.2.2 Number of Persons required per Task

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

### 5.2.3 Identification and authentication for each role

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

### 5.2.4 Roles requiring separation of duties

No individual will be assigned more than one trusted Role.

## 5.3 Personnel Security Controls

### 5.3.1 Qualification, Experience and Clearance requirements

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

### 5.3.2 Background Check Procedures

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

### 5.3.3 Training Requirements

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

### 5.3.4 Retraining Frequency and Requirements

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

### 5.3.5 Job Rotation frequency and sequence

Job rotation frequency for every role is 6 months.

### **5.3.6 Sanctions for unauthorized actions**

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

### **5.3.7 Independent contractor requirements**

No Stipulation.

### **5.3.8 Documentation Supplied to personnel**

Root CA will make available to its personnel all the guidelines issued by CCA, Root CA CPS and any relevant documents required to perform their jobs.

## **5.4 Audit Logging Procedure**

### **5.4.1 Types of Events Recorded**

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

- System start-up and shutdown;
- Root CA application start-up and shutdown;
- Attempts to create, remove, set passwords or change the system privileges of the PKI users and Administrators;
- Changes to Root CA details and/or keys;
- Changes to certificate creation policies (e.g. validity period);
- Login and logout attempts;
- Unauthorized attempts at network access to the Root CA system;
- Unauthorized attempts to access system files;
- Generation of Root CA keys;
- Creation and revocation of certificates;
- Attempts to initialize, remove, enable, and disable Subscribers or Designated Certificate Holders, as well as attempts to update and recover their keys;

### **5.4.2 Frequency of Processing Data**

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

### **5.4.3 Retention period for Security Audit Data**

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

### **5.4.4 Protection of Security Audit Data**

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

#### **5.4.5 Security Audit Data Backup Procedure**

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

#### **5.4.6 Audit Collection System (Internal or External)**

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

#### **5.4.7 Notification to Event-Causing Subject**

Event-causing subjects are not notified.

#### **5.4.8 Vulnerability Assessment**

No Stipulation.

### **5.5 Records Archival**

#### **5.5.1 Types of Event Recorded**

The following events are recorded and archived

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

#### **5.5.2 Retention Period for Archives**

Minimum retention period is 7 years.

#### **5.5.3 Protection of Archive**

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

#### **5.5.4 Archive Backup Procedure**

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

#### **5.5.5 Requirements for time-stamping of Records**

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

#### **5.5.6 Archive Collection System (Internal or External)**

Only authorized and authenticated personnel are allowed to handle archive.

#### **5.5.7 Procedures to obtain and verify archive information**

Backup media is verified just after taking backup operation. Off-site back up is also verified

once in 6 months for integrity.

## **5.6 Key Changeover**

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

## **5.7 Compromise and Disaster Recovery**

### **5.7.1 Incident and Compromise Handling Procedures**

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

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

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

### **5.7.3 Root CA private key Compromise Recovery Procedure**

If the Root CA private key is compromised or is suspected to be compromised, it will:

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

### **5.7.4 Business Continuity Capabilities after a Disaster**

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

## **5.8 Root CA Termination**

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

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

## **6 Technical Security Controls**

### **6.1 Key Pair Generation and Installation**

#### **6.1.1 Key Pair Generation**

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

#### **6.1.2 Private Key Delivery to Subscriber**

CCA will never generate any private key other than its own private key and this private key will be stored in a FIPS 140-2 Level 3 validated Hardware Security Module inside the strong room and will not be delivered to anyone whatsoever the reason is.

#### **6.1.3 Public Key Delivery to Certificate Issuer**

Root CA public key is delivered attaching with corresponding Licensed CA's public key after receiving and approving their CSR. This is delivered offline as a chain certificate in a secure and trustworthy manner. The procedures for CSR and certificate delivery are subject to negotiation with each requestor.

#### **6.1.4 CA Public Key Delivery to relying parties**

Root CA Certificate and public key is available at the website of CCA ([www.cca.gov.bd](http://www.cca.gov.bd))

#### **6.1.5 Key Sizes**

The Root CA key size is 2048 bits.

#### **6.1.6 Public Key Parameters Generation**

No stipulation.

#### **6.1.7 Parameter Quality Checking**

No stipulation.

#### **6.1.8 Key usage Purposes**

The Root CA private key is used to sign licensed CAs certificate and CRLs. In accordance with Digital Certificate Interoperability Guideline, the Certificate key Usage field of Root Certificate has the following values:

keyUsage= cRLSign, keyCertSign

### **6.2 Private Key Protection and Cryptographic Module Engineering Controls**

#### **6.2.1 Cryptographic Module Standards & Controls**

The Root CA uses a FIPS 140-2 Level 3 validated Hardware Security Module. The HSM is

control by multiple persons. The cryptographic module is kept in a data safe and when necessary (e.g to sign any CSR), it is taken out with access of multiple persons.

#### **6.2.2 Private Key multi person control**

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

#### **6.2.3 Private Key escrow**

No Stipulation.

#### **6.2.4 Private Key backup**

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

#### **6.2.5 Private Key archival**

The Root CA private key is not archived after it is expired.

#### **6.2.6 Private Key archival**

The Root CA private key is not transferrable to anywhere but taking into backup token while taking backup.

#### **6.2.7 Private Key Storage on cryptographic Module**

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

#### **6.2.8 Method of Activating Private Key**

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

#### **6.2.9 Method of Deactivating Private Key**

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

#### **6.2.10 Method of Destroying Private Key**

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

### **6.3 Other Aspects of Key Pair Management**

#### **6.3.1 Public Key Archival**

The root CA public key will be archived and will be kept securely. The archival period is 7 years or more if deem so by the Controller.

### **6.3.2 Certificate operational periods and key pair usage period**

Once the Root CA certificate is generated, it is valid for 10 years.

### **6.4 Activation Data**

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

### **6.5 Computer Security Controls**

#### **6.5.1 Specific Computer Security Technical Requirements**

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

#### **6.5.2 Computer Security Rating**

No stipulations.

### **6.6 Life-Cycle Security Controls**

No stipulations.

### **6.7 Network Security Controls**

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

### **6.8 Time Stamping**

No stipulations.

## **7 Certificate, CRL and OCSP Profiles**

### **7.1 Certificate Profile**

#### **7.1.1 Version number**

X.509 v3.

#### **7.1.2 Certificate Extensions**

authorityKeyIdentifier: Hash value of Root CA public key  
subjectKeyIdentifier: Hash value of Root CA public key  
Key Usage: Certificate Signing, Off-line CRL Signing, CRL Signing  
Certificate Policy: OID Specific  
subjectAltName: Not Used by Root CA  
Basic Constraints: CA  
cRLDistributionPoints: [crl.cca.gov.bd](http://crl.cca.gov.bd)

### 7.1.3 Algorithm Object identifiers

Signature Algorithm is 1.2.840.113549.1.1.11 SHA256 with RSA Encryption

### 7.1.4 Name Forms

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

CN=Root CA Bangladesh, O= Office of the CCA, C=BD

### 7.1.5 Name Constraints

Not used by Root CA.

### 7.1.6 Certificate Policy Object Identifier

No Stipulation

### 7.1.7 Usage of Policy Constraints Extensions

Not used by Root CA.

### 7.1.8 Policy qualifier syntax and semantics

Not supported.

## 7.2 CRL Profile

### 7.2.1 Version

X.509 v2.

### 7.2.2 CRL and CRL Entry Extensions

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

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

invalidityDate : GeneralizedTime

## 7.3 OCSP Profile

No Stipulation.

## 8 Compliance Audit & Other Assessments

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

### 8.1 Frequency or circumstances of assessment

Root CA infrastructure and its operations are audited once a year as per the audit checklist of Root CA assessment.



## **8.2 Identity/qualification of assessor**

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

## **8.3 Assessor's relationship to assessed entity**

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

## **8.4 Topics covered by assessment**

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

## **8.5 Actions taken as a result of deficiency**

If irregularities are found by the auditor, Root CA is informed in writing of the findings. Root CA submits a report to the auditor as to any remedial action to be taken take in response to the identified deficiencies. This report includes a time for completion to be consulted with the auditor.

## **8.6 Communication of results**

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

# **9 Other Business and Legal Matter**

## **9.1 Fees**

### **9.1.1 Certificate issuance and renewal fees**

No fees are charged for Certificates issued by Root CA.

### **9.1.2 Certificate Access fees**

No fees are charged for accessing Certificates from this service.

### **9.1.3 Revocation or status information access fees**

No fees are charged for revocation or status information access.

### **9.1.4 Fees for other service**

No Stipulation.

## **8.2 Identity/qualification of assessor**

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

## **8.3 Assessor's relationship to assessed entity**

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

## **8.4 Topics covered by assessment**

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

## **8.5 Actions taken as a result of deficiency**

If irregularities are found by the auditor, Root CA is informed in writing of the findings. Root CA submits a report to the auditor as to any remedial action to be taken take in response to the identified deficiencies. This report includes a time for completion to be consulted with the auditor.

## **8.6 Communication of results**

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

# **9 Other Business and Legal Matter**

## **9.1 Fees**

### **9.1.1 Certificate issuance and renewal fees**

No fees are charged for Certificates issued by Root CA.

### **9.1.2 Certificate Access fees**

No fees are charged for accessing Certificates from this service.

### **9.1.3 Revocation or status information access fees**

No fees are charged for revocation or status information access.

### **9.1.4 Fees for other service**

No Stipulation.

### **9.1.5 Refund Policy**

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

## **9.2 Financial Responsibility**

No Financial responsibility is involved with Office of the CCA.

### **9.2.1 Insurance Coverage**

No insurance coverage is accepted by Root CA.

### **9.2.2 Other assets**

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

### **9.2.3 Insurance or Warranty coverage for end entities**

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

## **9.3 Confidentiality of Business Information**

### **9.3.1 Scope of Confidential Information**

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

### **9.3.2 Information not within the scope of confidential information**

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

### **9.3.3 Responsibility to protect confidential information**

All Bangladesh PKI participants shall be responsible for protecting the confidential information they possess in accordance with the Privacy policy and applicable laws and Agreements.

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

## **9.4 Privacy of Personal Information**

### **9.4.1 Privacy Plan**

Root CA will prevent licensed CA identifying information from disclosure.

### **9.4.2 Information treated as private**

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

### 9.4.3 Information not deemed as private

Information made available public by Root CA is not private.

### 9.4.4 Responsibility to protect private information

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

### 9.4.5 Notice and consent to use private information

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

### 9.4.6 Disclosure pursuant to judicial or administrative process

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

### 9.4.7 Other information disclosure circumstances

No Stipulation.

## 9.5 Intellectual Property Rights

No Stipulation.

## 9.6 Representation and Warranties

### 9.6.1 Root CA representation & warranties

Root CA will:

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

### 9.6.2 CA representation & warranties

The Licensed CA must:

- Have a valid CP/CPS
- Promise to follow its CPS, and promptly update its CPS document when policies change
- Publish a name and contact information of the party responsible for this licensed CA
- Maintain a web site and corresponding URL where information about this licensed CA may be found by the general public
- Provide reasonable proof of right to use trademarked or well-known

organizational names or domain identifiers in its subject name.

### 9.6.3 Relying Party representation & warranties

Relying parties must:

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

Relying parties must not:

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

Relying parties may:

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

### 9.6.4 Repository representation & warranties

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

[www.cca.gov.bd](http://www.cca.gov.bd)

The following pages deal with individual items from 2.6.1:

CCA root CA information: <http://www.cca.gov.bd>

CRL information PEM:

<http://crl.cca.gov.bd>

### 9.7 Disclaimers of Warranties

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

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

### 9.8 Limitations of Liability

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

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

## **9.9 Indemnities**

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

## **9.10 Term and Termination**

### **9.10.1 Term**

The CPS becomes effective upon its publication in the repository.

### **9.10.2 Termination**

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

### **9.10.3 Effect of termination and survival**

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

## **9.11 Individual Notices and communications with participants**

The document is available at: <http://www.cca.gov.bd>

## **9.12 Amendments**

### **9.12.1 Procedure for amendment**

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

### **9.12.2 Notification mechanism and period**

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

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

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

## **9.13 Dispute Resolution Procedure**

Root CA will only issue certificate to licensed CAs. Any dispute between CAs and CCA will be resolved as per Act, Rules and Guidelines.

#### 9.14 **Governing Law**

This policy is subordinate to all applicable Bangladesh government laws and statutes.

#### 9.15 **Compliance with Applicable Law**

This policy is subordinate to all applicable Bangladesh government laws and statutes.

#### 9.16 **Miscellaneous Provisions**

No Stipulation.

#### 9.17 **Other Provisions**

No Stipulation.



## Bibliography

[INFN CP] <http://security.fi.infn.it/CA/CPS/> INFN CA Policy and CPS.

[GridCP] <http://gridcp.es.net/> Global Grid Forum CP

[EuroPKI] - EuroPKI Certificate Policy, Version 1.1 (Draft 4), October 2000

[FBCA] - X.509 Certificate Policy For The Federal Bridge Certification Authority (FBCA), Version 1.0, 18 December 1999

[NCSA] - National Computational Science Alliance, Certificate Policy, Version 0.9.1, June 30, 1999

[OpenSSL] - <http://www.openssl.org/>

[PAG] American Bar Associations PKI Assessment Guidelines ("PAG")  
<http://www.abanet.org/scitech/ec/isc/pag/pag.html>

[RFC3647] - S. Chokani and W. Ford, Internet X.509 Infrastructure Certificate Policy and Certification Practices Framework, RFC 3647, November 2003

[RFC5280] - R. Housley &al, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, RFC 5280, May 2008

[TrustID]- TrustID Certificate Policy  
<http://www.digistrust.com/certificates/policy/tsindex.html>