



**CCA**

স্বাক্ষরিত পত্র বাস্তবিকভাবে প্রমাণিত করুন এবং নিয়মিতভাবে পরীক্ষা করুন

Certificate Policy

**Bangladesh Root CA Certificate Policy (CP)**

OID No:2.16.50.1.2


Version:3.1

26 Sep 2023



**Office of the Controller of Certifying Authorities**  
Information and Communication Technology Division  
Ministry of Posts, Telecommunications and Information Technology  
Government of the Peoples Republic of Bangladesh

<b>Title</b>	Bangladesh Root CA Certificate Policy
<b>Document Type</b>	Public
<b>Current Version</b>	3.1
<b>Approval Date:</b>	26 September 2023
<b>Previous Version</b>	3.0
<b>Previous Version Revised Date</b>	15 February 2020
<b>Pages</b>	71
<b>Status</b>	Approved
<b>Document owner</b>	Office of the Controller of the Certifying Authorities, Bangladesh

  
**Signature:**

এ. টি. এম. জিয়াউল ইসলাম  
নিয়ন্ত্রক (মুদ্রাসচিব)  
ইলেক্ট্রনিক স্বাক্ষর সার্টিফিকেট প্রদানকারী  
কর্তৃপক্ষের নিয়ন্ত্রক-এস কার্যালয়  
ভরখা ও যোগাযোগ প্রযুক্তি বিভাগ

---

(The Controller of Certifying Authorities)



## List of Abbreviations/Acronyms

CA	Certificate authority
CAA	Certificate Authority Authorization
CA/B Forum	CA/Browser Forum
CCA	Controller of Certifying Authority
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DBA	Doing Business As
e-KYC	Electronic Known Your Customer
FIPS	Federal Information Processing Standard
ICT	Information & Communication Technology
ISO	International Organization for Standardization
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PAG	PKI Assessment Guidelines
PKI	Public Key Infrastructure
RA	Registration Authority
RCAB	Root Certifying Authority of Bangladesh
RFC	Request For Comment
RM	Registration Manager
VA	Verification Authorities



### Changes History

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

Term	Release Date	Changes Log
Version 3.1	26 September 2023	<ul style="list-style-type: none"> <li>• OID number, Version and publication date has been added (page-1)</li> <li>• The name of the ministry has been changed. (page-1)</li> <li>• Document reference has been rearranged. (page-2)</li> <li>• List of Abbreviation/ Acronyms has been revised. (page-3)</li> <li>• The word 'Amended' has been omitted from Information and communication Technology (Amended) Act, 2006. ( section 1.1 and 8)</li> <li>• The number of Certifying Authorities has been increased to 8(eight) instead of 6(six). (section 1.1)</li> <li>• Information Technology (Certifying Authority) Rules, 2010 and National ICT Policy, 2018 have been added after ICT Act ,2006. Digital Security Act, 2018 has been omitted. (section 1.1)</li> <li>• Background of OID has been added in section 1.2</li> <li>• Definition of the Relying parties has been revised in sub-section 1.3.4</li> <li>• Members of the policy Authority of the CCA office have been added to comply with Ref. no.53.03.0000.18.010.18.10/2, Date: 18.03.2020 (sub-section 1.3.5.1)</li> <li>• 'Appropriate Certificate Uses' has been revised in sub-section 1.4.1</li> <li>• Sub-section 1.5.2 has been revised .</li> <li>• The definition of Electronic Signature, e-KYC, e-Sign, e-Sign Service Provider (EPS), Object Identifier (OID, Root CA, Time Stamping Service and Trusted Roles have been inserted into definition clause. (sub-section-1.6.1)</li> <li>• The elaboration of those acronyms DBA, CA\B Forum, CAA, DBA, e-KYC, FIPS, ISO, OID, OCSP, RCAB and RFC has been inserted in sub-section 1.6.2.</li> </ul>







		<ul style="list-style-type: none"> <li>• Added Root CA and CRL link in section 2.1</li> <li>• Added website link in para in section 2.2</li> <li>• Latest RFC 5322 is substituted for RFC 2822 in sub-section 3.1.4.</li> <li>• Elaboration of DBA (Doing Business As) has been added in sub-section 3.2.2.2</li> <li>• CA\Browser forum has been written instead of CA\B Forum.</li> <li>• Elaboration of CAA (Certificate Authority Authorization) has been added in sub-section 3.2.2.8.</li> <li>• Sub-section 3.2.3 is not applicable for Root CA.</li> <li>• The next line of "An organization who wishes to operate a CA in Bangladesh may complete and submit an application for certificates to CCA" has been omitted. (Sub-section- 4.1.1)</li> <li>• The following sentence "The RA Will Coordinate with the CA to approve or reject certificate application and notifies the results to Subscribers", has been omitted from sub-section 4.2.2.</li> <li>• Sub-section 4.10.1, sub-section 4.10.2 and sub-section 4.11 are not applicable for Root CA.</li> <li>• 'Trusted Roles' mentioned in section 5.2 has been revised</li> <li>• The word 'RA' has been omitted from section 5.8</li> <li>• The 'key size' mentioned in sub-section 6.1.5 has been updated.</li> <li>• The part 'to within three minutes' has been omitted from section 6.8</li> </ul>
Version 3.0	15 February 2020	The entire CP/CPS has been revised to comply with RFC 3647





Version 2.0	18 November 2013	<ul style="list-style-type: none"><li>• Office of the CCA has been allocated with Object Identifier (OID) from the Country RA for OID of Bangladesh. The OID assigned to Office of the CCA is 2.16.50.1. OID assigned to Office of the CCA is for the PKI of Bangladesh. All Licensed CAs, Certification Practice Statement (CPS), Certificate Policy (CP), and other PKI components will be using OID. The revision to this CPS is to identify the CPS document with an OID. This revision is made in 1.2.</li><li>• The contact details for this Policy Administration has also been modified which is available in 1.5.1.</li></ul>
Version 1.0	17 April 2012	<ul style="list-style-type: none"><li>• Base Version</li></ul>





## Table of Contents

<b>1</b>	<b>INTRODUCTION .....</b>	<b>15</b>
1.1	OVERVIEW .....	15
1.2	DOCUMENT NAME AND IDENTIFICATION .....	16
1.3	PKI PARTICIPANTS .....	16
1.3.1	Certification Authorities .....	17
1.3.2	Registration Authorities .....	18
1.3.3	Subscribers .....	19
1.3.4	Relying Parties .....	19
1.3.5	Other Participants .....	19
1.3.5.1	Policy Authority .....	19
1.4	CERTIFICATE USAGE .....	20
1.4.1	Appropriate Certificate Uses .....	20
1.4.2	Prohibited Certificate Uses .....	21
1.5	POLICY ADMINISTRATION .....	21
1.5.1	Organization Administering the Document .....	21
1.5.2	Contact Person .....	21
1.5.3	Person Determining CPS Suitability for the Policy .....	21
1.5.4	CPS Approval Procedures .....	21
1.5.5	CP Review and Update Procedures .....	22
1.6	DEFINITIONS AND ACRONYMS .....	22
1.6.1	Definitions .....	22
1.6.2	Acronyms .....	25
<b>2</b>	<b>PUBLICATION AND REPOSITORY RESPONSIBILITIES .....</b>	<b>26</b>
2.1	REPOSITORIES .....	26
2.2	PUBLICATION OF CERTIFICATION INFORMATION .....	26
2.3	TIME OR FREQUENCY OF PUBLICATION .....	26
2.4	ACCESS CONTROLS ON REPOSITORIES .....	26
<b>3</b>	<b>IDENTIFICATION AND AUTHENTICATION .....</b>	<b>27</b>
3.1	NAMING .....	27
3.1.1	Types of Names .....	27
3.1.2	Need for Names to be Meaningful .....	27
3.1.3	Anonymity or Pseudonymity of Subscribers .....	27
3.1.4	Rules for Interpreting Various Name Forms .....	27
3.1.5	Uniqueness of Names .....	27
3.1.6	Recognition, Authentication, and Role of Trademarks .....	27
3.2	INITIAL IDENTITY VALIDATION .....	27
3.2.1	Method to Prove Possession of Private Key .....	27
3.2.2	Authentication of Organization and Domain Identity .....	28
3.2.2.1	Identity .....	28
3.2.2.2	DBA/Tradename .....	28
3.2.2.3	Verification of Country .....	28
3.2.2.4	Validation of Domain Authorization or Control .....	29
3.2.2.4.1	Validating the Applicant as a Domain Contact .....	29
3.2.2.4.2	Email, Fax, SMS, or Postal Mail to Domain Contact .....	29
3.2.2.4.3	Phone Contact with Domain Contact .....	29
3.2.2.4.4	Constructed Email to Domain Contact .....	29
3.2.2.4.5	Domain Authorization Document .....	29





3.2.2.4.6	Agreed-Upon Change to Website.....	29
3.2.2.4.7	DNS Change.....	29
3.2.2.4.8	IP Address .....	29
3.2.2.4.9	Test Certificate .....	29
3.2.2.4.10	TLS Using a Random Number .....	29
3.2.2.5	Authentication for an IP Address .....	29
3.2.2.6	Wildcard Domain Validation .....	30
3.2.2.7	Data Source Accuracy .....	30
3.2.2.8	CAA Records .....	30
3.2.3	Authentication of Individual Identity.....	30
3.2.4	Non-verified Subscriber Information.....	31
3.2.5	Validation of Authority .....	31
3.2.6	Criteria for Interoperation .....	31
3.3	IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS.....	31
3.3.1	Identification and Authentication for Routine Re-key .....	31
3.3.2	Identification and Authentication for Re-key after Revocation .....	31
3.4	IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST .....	31
4	<b>CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS .....</b>	<b>32</b>
4.1	CERTIFICATE APPLICATION .....	32
4.1.1	Who Can Submit a Certificate Application .....	32
4.1.2	Enrollment Process and Responsibilities .....	32
4.2	CERTIFICATE APPLICATION PROCESSING.....	32
4.2.1	Performing Identification and Authentication Functions.....	32
4.2.2	Approval or Rejection of Certificate Applications .....	33
4.2.3	Time to Process Certificate Applications .....	33
4.3	CERTIFICATE ISSUANCE.....	33
4.3.1	CA Actions during Certificate Issuance .....	33
4.3.2	Notification to Subscriber by the CA of Issuance of Certificate.....	33
4.4	CERTIFICATE ACCEPTANCE .....	33
4.4.1	Conduct Constituting Certificate Acceptance .....	33
4.4.2	Publication of the Certificate by the CA.....	34
4.4.3	Notification of Certificate Issuance by the CA to Other Entities.....	34
4.5	KEY PAIR AND CERTIFICATE USAGE .....	34
4.5.1	Subscriber Private Key and Certificate Usage.....	34
4.5.2	Relying Party Public Key and Certificate Usage .....	34
4.6	CERTIFICATE RENEWAL.....	34
4.6.1	Circumstance for Certificate Renewal.....	34
4.6.2	Who May Request Renewal .....	34
4.6.3	Processing Certificate Renewal Requests .....	34
4.6.4	Notification of New Certificate Issuance to Subscriber .....	35
4.6.5	Conduct Constituting Acceptance of a Renewal Certificate.....	35
4.6.6	Publication of the Renewal Certificate by the CA.....	35
4.6.7	Notification of Certificate Issuance by the CA to Other Entities.....	35
4.7	CERTIFICATE RE-KEY.....	35
4.7.1	Circumstance for Certificate Re-key .....	35
4.7.2	Who May Request Certification of a New Public Key.....	35
4.7.3	Processing Certificate Re-keying Requests .....	35
4.7.4	Notification of New Certificate Issuance to Subscriber .....	35







4.7.5	Conduct Constituting Acceptance of a Re-keyed Certificate.....	36
4.7.6	Publication of the Re-keyed Certificate by the CA.....	36
4.7.7	Notification of Certificate Issuance by the CA to Other Entities.....	36
4.8	<b>CERTIFICATE MODIFICATION.....</b>	36
4.8.1	Circumstance for Certificate Modification.....	36
4.8.2	Who May Request Certificate Modification .....	36
4.8.3	Processing Certificate Modification Requests.....	36
4.8.4	Notification of New Certificate Issuance to Subscriber .....	36
4.8.5	Conduct Constituting Acceptance of Modified Certificate .....	36
4.8.6	Publication of the Modified Certificate by the CA .....	36
4.8.7	Notification of Certificate Issuance by the CA to Other Entities.....	36
4.9	<b>CERTIFICATE REVOCATION AND SUSPENSION.....</b>	37
4.9.1	Circumstances for Revocation.....	37
4.9.1.1	Reasons for Revoking a Subscriber Certificate.....	37
4.9.1.2	Reasons for Revoking a Subordinate CA Certificate .....	38
4.9.2	Who Can Request Revocation.....	38
4.9.3	Procedure for Revocation Request.....	39
4.9.4	Revocation Request Grace Period.....	39
4.9.5	Time within Which CA Must Process the Revocation Request.....	39
4.9.6	Revocation Checking Requirement for Relying Parties .....	39
4.9.7	CRL Issuance Frequency.....	39
4.9.8	Maximum Latency for CRLs.....	39
4.9.9	Online Revocation/Status Checking Availability.....	40
4.9.10	Online Revocation Checking Requirements .....	40
4.9.11	Other Forms of Revocation Advertisements Available.....	40
4.9.12	Special Requirements Regarding Key Compromise .....	40
4.9.13	Circumstances for Suspension.....	40
4.9.14	Who Can Request Suspension.....	40
4.9.15	Procedure for Suspension Request.....	40
4.9.16	Limits on Suspension Period .....	40
4.10	<b>CERTIFICATE STATUS SERVICES .....</b>	40
4.10.1	Operational Characteristics.....	40
4.10.2	Service Availability.....	40
4.10.3	Optional Features.....	41
4.11	<b>END OF SUBSCRIPTION.....</b>	41
4.12	<b>KEY ESCROW AND RECOVERY .....</b>	41
4.12.1	Key Escrow and Recovery Policy and Practices.....	41
4.12.2	Session Key Encapsulation and Recovery Policy and Practices.....	41
5	<b>FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS .....</b>	41
5.1	<b>PHYSICAL SECURITY CONTROLS .....</b>	41
5.1.1	Site Location and Construction .....	41
5.1.2	Physical Access .....	41
5.1.3	Power and Air Conditioning.....	42
5.1.4	Water Exposures.....	42
5.1.5	Fire Prevention and Protection.....	42
5.1.6	Media Storage .....	42
5.1.7	Waste Disposal.....	42





5.1.8	Off-site Backup .....	42
5.2	PROCEDURAL CONTROLS .....	43
5.2.1	Trusted Roles .....	43
5.2.2	Number of Persons Required per Task .....	44
5.2.3	Identification and Authentication for Each Role .....	45
5.2.4	Roles Requiring Separation of Duties .....	46
5.3	PERSONNEL CONTROLS .....	46
5.3.1	Qualifications, Experience and Clearance Requirements .....	46
5.3.2	Background Check Procedures .....	46
5.3.3	Training Requirements .....	47
5.3.4	Retraining Frequency and Requirements .....	47
5.3.5	Job Rotation Frequency and Sequence .....	47
5.3.6	Sanction for Unauthorized Actions .....	47
5.3.7	Independent Contractor Requirements .....	47
5.3.8	Documentation Supplied to Personnel .....	47
5.4	AUDIT LOGGING PROCEDURES .....	48
5.4.1	Types of Events Recorded .....	48
5.4.2	Frequency of Processing Log .....	48
5.4.3	Retention Period for Audit Log .....	48
5.4.4	Protection of Audit Log .....	48
5.4.5	Audit Log Backup Procedures .....	49
5.4.6	Audit Log Accumulation System (Internal vs. External) .....	49
5.4.7	Notification to Event-Causing Subject .....	49
5.4.8	Vulnerability Assessments .....	49
5.4.9	Penetration Test Assessments .....	49
5.5	RECORDS ARCHIVAL .....	50
5.5.1	Types of Records Archived .....	50
5.5.2	Retention Period for Archive .....	50
5.5.3	Protection of Archive .....	50
5.5.4	Archive Backup Procedure .....	50
5.5.5	Requirements for Time Stamping of Records .....	50
5.5.6	Archive Collection System (Internal or External) .....	50
5.5.7	Procedures to Obtain and Verify Archive Information .....	51
5.6	KEY CHANGEOVER .....	51
5.7	COMPROMISE AND DISASTER RECOVERY .....	51
5.7.1	Incident and Compromise Handling Procedures .....	51
5.7.2	Computing Resources, Software, and/or Data are corrupted .....	51
5.7.3	Entity Private Key Compromise Procedures .....	52
5.7.4	Business Continuity Capabilities after a Disaster .....	52
5.8	CA OR RA TERMINATION .....	53
6	TECHNICAL SECURITY CONTROLS .....	54
6.1	KEY PAIR GENERATION AND INSTALLATION .....	54
6.1.1	Key Pair Generation .....	54
6.1.2	Private Key Delivery to Subscriber .....	54
6.1.3	Public Key Delivery to Certificate Issuer .....	54
6.1.4	CA Public Key Delivery to Relying Parties .....	54
6.1.5	Key Sizes .....	54
6.1.6	Public Key Parameters Generation and Quality Checking .....	55







6.1.7	Key Usage Purposes (as per X.509 v3 Key Usage Field)	55
6.2	PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS	55
6.2.1	Cryptographic Module Standards and Controls	55
6.2.2	Private Key (n out of m) Multi-person Control	55
6.2.3	Private Key Escrow	55
6.2.4	Private Key Backup	56
6.2.5	Private Key Archival	56
6.2.6	Private Key Transfer into or from a Cryptographic Module	56
6.2.7	Private Key Storage on Cryptographic Module	56
6.2.8	Method of Activating Private Key	56
6.2.9	Method of Deactivating Private Key	56
6.2.10	Method of Destroying Private Key	56
6.2.11	Cryptographic Module Rating	56
6.3	OTHER ASPECTS OF KEY PAIR MANAGEMENT	57
6.3.1	Public Key Archival	57
6.3.2	Certificate Operational Periods and Key Pair Usage Periods	57
6.4	ACTIVATION DATA	57
6.4.1	Activation Data Generation and Installation	57
6.4.2	Activation Data Protection	57
6.4.3	Other Aspects of Activation Data	57
6.5	COMPUTER SECURITY CONTROLS	58
6.5.1	Specific Computer Security Technical Requirements	58
6.5.2	Computer Security Rating	58
6.6	LIFE CYCLE TECHNICAL CONTROLS	58
6.6.1	System Development Controls	58
6.6.2	Security Management Controls	58
6.6.3	Life Cycle Security Controls	58
6.7	NETWORK SECURITY CONTROLS	59
6.8	TIME-STAMPING	59
7	CERTIFICATE, CRL AND OCSP PROFILES	60
7.1	CERTIFICATE PROFILE	60
7.1.1	Version Number	60
7.1.2	Certificate Content and Extensions; Application of RFC 5280	60
7.1.2.1	Root CA Certificate	60
7.1.2.2	Subordinate CA Certificate	61
7.1.2.3	Subscriber Certificate	61
7.1.2.4	All Certificate	61
7.1.2.5	Application of RFC 5280	61
7.1.3	Algorithm Object Identifiers	61
7.1.4	Name Forms	61
7.1.5	Name Constraints	61
7.1.6	Certificate Policy Object Identifier	61
7.1.7	Usage of Policy Constraints Extension	61
7.1.8	Policy Qualifiers Syntax and Semantics	61
7.1.9	Processing Semantics for the Critical Certificate Policies Extension	61
7.2	CRL PROFILE	62
7.2.1	Version Number(s)	62





7.2.2	CRL and CRL Entry Extensions .....	62
7.2.2.1	Authority Key Identifier.....	62
7.2.2.2	Base CRL Number .....	62
7.2.2.3	Reason Code.....	63
7.2.2.4	Invalidity Date.....	63
7.2.2.5	Issuing Distribution Point.....	63
7.3	OCSP PROFILE.....	63
7.3.1	Version Number(s).....	63
7.3.2	Fields in OCSP Responses .....	63
7.3.3	OCSP Extensions.....	63
8	<b>COMPLIANCE AUDIT AND OTHER ASSESSMENTS .....</b>	<b>64</b>
8.1	FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT .....	64
8.2	IDENTITY/QUALIFICATIONS OF ASSESSOR .....	64
8.3	ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY .....	64
8.4	TOPICS COVERED BY ASSESSMENT .....	64
8.5	ACTIONS TAKEN AS A RESULT OF DEFICIENCY .....	64
8.6	COMMUNICATION OF RESULTS.....	64
8.7	SELF-AUDITS .....	65
9	<b>OTHER BUSINESS AND LEGAL MATTERS .....</b>	<b>66</b>
9.1	FEES .....	66
9.1.1	Certificate Issuance or Renewal Fees .....	66
9.1.2	Certificate Access Fees.....	66
9.1.3	Revocation or Status Information Access Fees .....	66
9.1.4	Fees for Other Services .....	66
9.1.5	Refund Policy.....	66
9.2	FINANCIAL RESPONSIBILITY .....	66
9.2.1	Insurance Coverage.....	66
9.2.2	Other Assets.....	66
9.2.3	Insurance or Warranty Coverage for End-entities.....	66
9.3	CONFIDENTIALITY OF BUSINESS INFORMATION .....	67
9.3.1	Scope of Confidential Information .....	67
9.3.2	Information Not within the Scope of Confidential Information.....	67
9.3.3	Responsibility to Protect Confidential Information.....	67
9.4	PRIVACY OF PERSONAL INFORMATION.....	67
9.4.1	Privacy Plan.....	67
9.4.2	Information Treated As Private.....	67
9.4.3	Information Not Deemed Private .....	67
9.4.4	Responsibility to Protect Private Information.....	67
9.4.5	Notice and Consent to Use Private Information.....	67
9.4.6	Disclosure Pursuant to Judicial or Administrative Process.....	68
9.4.7	Other Information Disclosure Circumstances.....	68
9.5	INTELLECTUAL PROPERTY RIGHTS .....	68
9.6	REPRESENTATIONS AND WARRANTIES .....	68
9.6.1	CA Representations and Warranties .....	68
9.6.2	RA Representations and Warranties.....	68
9.6.3	Subscriber Representations and Warranties .....	69
9.6.4	Relying Party Representations and Warranties .....	69
9.6.5	Representations and Warranties of Other Participants .....	69





9.7	DISCLAIMERS OF WARRANTIES .....	69
9.8	LIMITATIONS OF LIABILITY .....	69
9.9	INDEMNITIES .....	69
9.10	TERM AND TERMINATION .....	69
9.10.1	<i>Term</i> .....	69
9.10.2	<i>Termination</i> .....	70
9.10.3	<i>Effect of Termination and Survival</i> .....	70
9.11	INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS.....	70
9.12	AMENDMENTS .....	70
9.12.1	<i>Procedure for Amendment</i> .....	70
9.12.2	<i>Notification Mechanism and Period</i> .....	70
9.12.3	<i>Circumstances under Which OID Must Be Changed</i> .....	70
9.13	DISPUTE RESOLUTION PROCEDURE .....	70
9.13.1	<i>Disputes between Issuer and Subscriber</i> .....	70
9.13.2	<i>Disputes between Issuer and Relying Parties</i> .....	70
9.14	GOVERNING LAW .....	70
9.15	COMPLIANCE WITH APPLICABLE LAW .....	70
9.16	MISCELLANEOUS PROVISIONS .....	71
9.16.1	<i>Entire Agreement</i> .....	71
9.16.2	<i>Assignment</i> .....	71
9.16.3	<i>Severability</i> .....	71
9.16.4	<i>Enforcement</i> .....	71
9.16.5	<i>Force Majeure</i> .....	71
9.17	OTHER PROVISIONS .....	71



<i>Table 1: Terms and Definitions</i>	22
<i>Table 2: Acronyms</i>	25
<i>Table 3: Key requirement</i>	55
<i>Table 4: Fields in the Certificate</i>	60
<i>Table 5: Method of Digital Signature and Encryption with Object Identifier</i>	61
<i>Table 6: Item List in Certificate Revocation</i>	62



## 1 Introduction

### 1.1 Overview

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

In 2011, the Controller of Certifying Authorities (CCA) provides licenses to be Certifying Authorities to 08(eight) organizations. One important step for introduction of Digital Signature has been completed through the Root Key Generation Ceremony on April 18, 2012.

Objective of the CCA office is:

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

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

This Certificate Policy is consistent with the ICT Act, 2006, Information Technology (Certifying Authority) Rules, 2010, National ICT Policy, 2018, Public Key Infrastructure X.509 (IETF PKIX) Certificate Policy and Certification Practices Framework [RFC3647].

The general architecture is a single certificate authority. The certificate authority is a standalone self-signed CA. It is the intent of the Bangladesh Root CA to sign only licensed CAs certificate and CRL. Bangladesh Root CA conforms to SSL, EV SSL, Code Signing, EV Code Signing guidelines; application trust stores requirements; the current version of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates published at <http://www.cabforum.org>. In the event of any inconsistency between this document and those requirements, those requirements take precedence over this document.





## 1.2 Document Name and Identification

This Certificate Policy is published by the Office of the Controller of Certifying Authority (CCA) and specifies the baseline set of security controls and practices that CAs located in Bangladesh employ in issuing, revoking or suspending and publishing certificates.

Bangladesh Computer Council (BCC) in assistance with Bangladesh Telecom Regulatory Commission (BTRC), the ITU member state and Bangladesh Standard Testing Institute (BSTI), the ISO member body applied to become country Registration Author RA) for Object Identifier (OID) on 08 July 2012. Accordingly, on 30 July 2012 BCC got the approval of ITU to work as country RA (<http://www.oid-info.com/get/2.16.50>). Internet Assigned Numbers Authority (IANA) has assigned the country OID 2.16.50 to Bangladesh. BCC as country RA will issue OID in favor of office of the Controller of the Certifying Authorities which is "2.16.50.1". For identification purpose, this Certificate Policy bears an Object Identifier (OID) "2.16.50.1.2".

## 1.3 PKI Participants

### 1.3.1 PKI Authorities

#### 1.3.1.1 Controller of Certifying Authorities

(CCA) The CCA is responsible for:

1. Drafting and approval of the Bangladesh PKI CP.
2. Commissioning compliance analysis and approval of the licensed CAs CPS;
3. Accepting and processing applications from Entities desiring to become Licensed CA; and
4. Ensuring continued conformance of Licensed CAs with this CP by examining compliance audit results.

#### 1.3.1.2 Root Certifying Authority Bangladesh (RCAB)

A Root CA is a trust anchor for subscribers of a PKI domain when the subscribers act as relying party. The Root Certifying Authority of Bangladesh shall be controlled by and operated under the direction of CCA.







**CCA**

স্বাক্ষরিত পক্ষের প্রতিনিধিত্ব প্রদানকারী স্বাক্ষরিত নথি

## Certificate Policy

SSL and code signing certificates shall be issued from the special purpose trust chain created specifically for that purpose. The special purpose trust chain shall be operated in offline mode at Root CA and CA level.

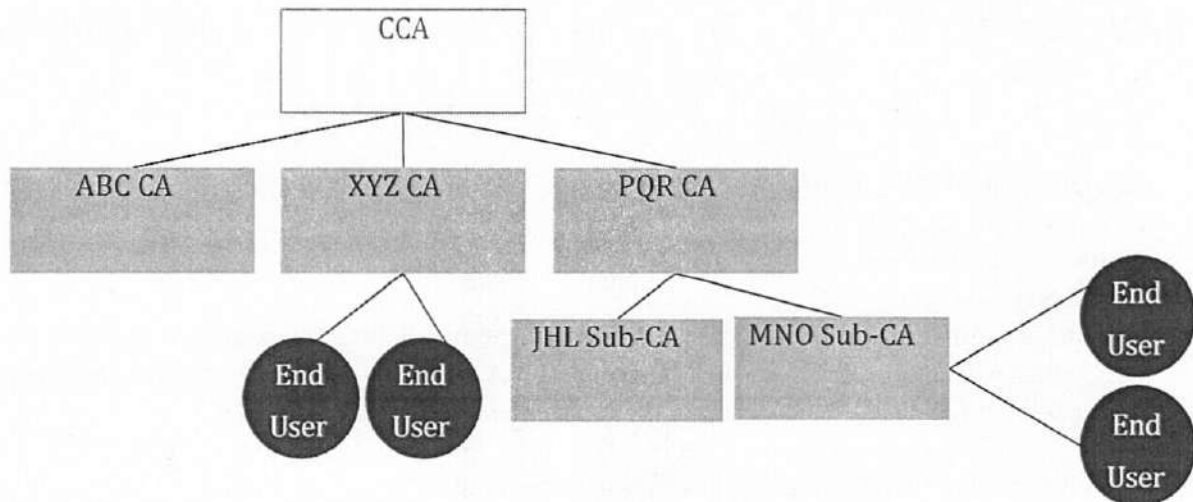
### 1.3.1.3 Sub-CA

A Certifying Authority can create sub-CAs to meet the business branding requirement. These sub-CAs, which will be part of the same legal entity as the CA, will issue certificates to the end entities or subscribers. A sub-CA shall not issue certificates to other CAs or sub-CAs.

The sub-CA model will be based on the following principles:

- ❖ The CAs MUST NOT have more than ONE level of sub-CA
- ❖ The sub-CA MUST use a sub-CA certificate issued by the CA for issuing end entity certificates
- ❖ The sub-CA must necessarily use the CAs infrastructure for issuing certificate
- ❖ The sub-CAs operations shall be subject to same audit procedures as the CA
- ❖ The certificate policies of the sub-CA must be same as or sub-set of the CA's certificate policies





#### 1.3.1.4 Certificate Status Provider (CSP)

A CSP is an authority that provides status of certificates or certification paths. CSP can be operated in conjunction with the CAs or independent of the CAs. Examples of CSP are:

1. Online Certificate Status Protocol (OCSP) Responders that provide revocation status of certificates.

2. Standard Based Certificate Validation Protocol (SCVP) Servers that validate certifications paths or provide revocation status checking services.

OCSP Responders that are keyless and simply repeat responses signed by other Responders and SCVP Servers that do not provide certificate validation services shall adhere to the same security requirements as repositories.

#### 1.3.2 Registration Authorities

The entities that establish enrollment procedures for end-user certificate applicants, perform identification and authentication of certificate applicants, initiate or pass along revocation requests for certificates, and approve applications for renewal or re-keying certificates on behalf of a CA. Subordinate organizations within a larger organization can act as RAs for the CA serving the entire organization, but RAs may also be external to the CA.





### 1.3.3 Subscribers

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

### 1.3.4 Relying Parties

A relying party is the entity that relies on the validity of the binding of the Subscriber’s identity to a public key. The relying party is responsible for deciding whether or how to check the validity of the certificate by checking the appropriate certificate status information. The relying party can use the certificate to verify the integrity of a digitally signed message, to identify the creator of a message, or to establish confidential communications with the holder of the certificate’s private key. A relying party may use information in the certificate (such as certificate policy identifiers, key usage, or extended key usage) to determine its appropriate usage. For this certificate policy, the relying party may be any entity that wishes to validate the binding of a public key to the name of a Subscriber.

### 1.3.5 Other Participants

#### 1.3.5.1 Policy Authority

A Policy Authority (PA) decides that a set of requirements for certificate issuance and use is sufficient for a given application. The PA has roles and responsibilities as follows:

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

Office of the Controller of Certifying Authorities (CCA) has setup the following Policy Authority as per the Clause 1.3.5.1 of Bangladesh Root CA Certification Practice Statement:(Ref no:53.03.0000.18.010.18.10/2, Date:18.03.2020)

SL	Name and Designation	Status
1.	Controller, Office of the CCA, ICT Division	Chairman
2.	Deputy Controller (Admin, Finance & law), Office of the CCA, ICT Division.	Member
3.	Deputy Controller (ICT), Office of the CCA, ICT Division.	Member





4.	Deputy Controller (Cyber Crime & Security), Office of the CCA, ICT Division.	Member
5.	Assistant Engineer (IT Security), Office of the CCA, ICT Division.	Member
6.	Investigation officer (Law) Office of the CCA, ICT Division.	Member
7.	Law Officer, Office of the CCA, ICT Division.	Member Secretary

**1.4 Certificate Usage****1.4.1 Appropriate Certificate Uses**

Certificate usage shall be governed by the ICT Act of 2006 and Digital Signature Certificate Interoperability Guidelines from CCA. The usage of a certificate issued under the Trust model of Bangladesh Root CA is limited to support the following core security needs:

- Authentication and non-repudiation;
- Certificate signing;
- Encipherment;
- Digital signature; and
- Certificate Revocation List (CRL) / Online Certificate Status Protocol (OCSP) signing.



#### 1.4.2 Prohibited Certificate Uses

A certificate issued in accordance with this CP shall be used only for the purpose as specified in Section 1.4.1, and in particular shall be used only to the extent the use consistent with applicable laws.

#### 1.5 Policy Administration

##### 1.5.1 Organization Administering the Document

The organization who is responsible for all aspects of this CP is which is Bangladesh Root CA operated by Office of the Controller of Certifying Authority (CCA) under ICT Ministry. In this document, "Bangladesh Root CA" will refer to Office of Controller of the Certifying Authority (CCA).

##### 1.5.2 Contact Person

<b>Office Name</b>	:	Office of the Controller of Certifying Authority
<b>Contact Person</b>	:	Deputy Controller, ICT
<b>Address</b>	:	E-14/X, BCC Bhaban, Sher-E-Bangla Nagar, Agargaon, Dhaka- 1207, Bangladesh.
<b>Email</b>	:	dc.ict@cca.gov.bd
<b>Phone</b>	:	+880 2 41025670
<b>Fax</b>	:	+880 2 41025675

##### 1.5.3 Person Determining CPS Suitability for the Policy

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

##### 1.5.4 CPS Approval Procedures

CAs issuing certificates under this CP are required to meet all facets of the CP. The CAs shall review the CPS at least annually. The PA has defined approval procedures as follows:

1. The CA issuing certificates under this CP submits the CPS to the CCA.
2. CCA reviews and makes recommendations.
3. CCA submits the CPS and proposes to the PA for an approval.
4. The PA reviews the submitted CPS and approves.
  - a. In case the PA has no further comments, the PA approves the CPS.
  - b. In case the PA has comments, the PA returns the CPS to the applicant CA for proper modification or correction before resubmission.
5. The applicant CA announces and publishes the CPS to the specified channel.



### 1.5.5 CP Review and Update Procedures

This CP shall be reviewed and update once on a year or any change in system, solution or need for business demand.

CAs operating under this CP shall recheck the latest of Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates from <https://cabforum.org/baseline-requirements-documents> at least quarterly for the purpose of development, implementation, enforcement and annually update of a Certificate Policy and Certificate Practice Statement.

### 1.6 Definitions and Acronyms

#### 1.6.1 Definitions

A list of definitions are as below.

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







Digital Signature	Digital signature is a cryptographic technique used to verify the authenticity, integrity, and non-repudiation of a digital document, message, or transaction in electronic communication or digital environments in accordance with the provisions of ICT Act 2006.
Directory Service	A storage for publication of certificates and certificate revocation lists following the X.500 Standard or LDAP.
Electronic Signature	According to the section 2(1) of ICT Act 2006 “Electronic signature” means data in an electronic form, which (a) is related with any other electronic data directly or logically; and (b) is able to satisfy the following conditions for validating the digital signature-- (i) affixing with the signatory uniquely; (ii) capable of identifying the signatory; (iii) created in safe manner or using a means under the sole control of the signatory; and (iv) related with the attached data in such a manner that is capable of identifying any alteration made in the data thereafter. “Digital signature” shall also be treated as “Electronic Signature” as per the rule 2(d) of the IT (CA) Rules, 2010.
e-KYC	Electronic Known Your Customer (e-KYC) is an electronic automated method used to verify and authenticate the identity of a e-sign subscriber as definite in rule 2(j) of the IT (CA) Rules, 2010.
e-sign	A form of electronic signature or digital signature provided and certified by CPS as per ICT Act, 2006 clause 2(1) and IT (CA) Rules 2010 where the user's private key is kept on e-sign service provider CA's end, where the user has sole control of it through appropriate ecosystem.
e-Sign Service Provider (EPS)	The CAs and their sub- CAs licensed by CCA can provide e-sign service under section under section 2(32) and 2(34) of ICT Act, 2006 and as per rules 21 of IT (CA) Rules, 2010.
Entity	An individual or server, operating unit / site, or any device that is under the control of the individual.
Key Pair	A key pair refers to two separate keys of the asymmetric cryptographic system, one of which is secret (Private Key) and another is public (Public Key). The two parts of the key pair are mathematically linked in the ways that one key lock or encrypts the plaintext, and the other unlocks or decrypts the cipher text. Neither key can perform both functions by itself. The key pair can be used to authenticate the digital signature as well as maintain the confidentiality of information.
OCSF (Online Certificate Status Protocol)	A protocol used for verifying status of a certificate.





Object Identifier (OID)	A specialized formatted number that is registered with an internationally recognized standards organization, the unique alphanumeric/numeric identifier registered under the ISO registration standard to reference a specific object or object class. In the Bangladesh PKI, OIDS are used to uniquely identify certificate policies and cryptographic algorithms.
Private Key	The key used to create a digital signature and can be used to decrypt the message that is encrypted with its pair of public key to obtain the original message.
Public Key	The key used to verify a digital signature to ensure the integrity of electronic message and also to encrypt a message to maintain its confidentiality.
Root CA	The Bangladesh PKI is a hierarchical PKI with the trust chain starting from the Root Certifying Authority of Bangladesh (RCAB). RCAB is operated by the Office of Controller of Certifying Authorities, Government of Bangladesh. Below RCAB there are Certifying Authorities (CAs) licensed by CCA to issue Digital Signature Certificates under the ICT Act, 2006. CAs can be private sector companies, Government departments or public sector companies. These are also called Licensed CAs. The Root CA's self-signed certificate is used for signing subordinate CA certificates and cross certificate.
Time Stamping service	The Time Stamping services uses in the time-stamp token shall be traceable to a Standard Time Source in Bangladesh. The Time Stamping services shall be protected against threats which could result in an undetected change to the clock that takes it outside its calibration. Examples of threats include tampering by unauthorized personnel, radio or electrical shocks. The CA shall provide a capability to detect the Time Stamping services clock being out accuracy specified in Time Stamping Services guideline for Certifying Authorities (CA), version- 2.0.
Trusted Roles	A trusted role is one whose incumbent performs functions that can introduce security problems to the PKI system if not carried out properly, whether accidentally or maliciously. It is essential that the people selected to fill these roles are held accountable to perform the designated actions correctly. Otherwise, the integrity of the CA is weakened or compromised.

**Table 1: Terms and Definitions**

### 1.6.2 Acronyms

A list of definitions are as below.

Acronym	Term
CA	Certification Authority
CA/B Forum	CA/ Browser Forum
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CAA	Certificate Authority Authorization
CCA	Controller of the Certification Authority
DN	Distinguished Name
DBA	Doing Business As
e-KYC	electronic Known Your Customer
FIPS	Federal Information Processing Standard
ISO	International Organization For Standardization
OID	Object Identifier
OCSP	Online Certificate Status Protocol
PA	Policy Authority
PIN	Personal Identification Number
PKI	Public Key Infrastructure
RA	Registration Authority
RCAB	Root Certifying Authority of Bangladesh
RFC	Request for Comment

Table 2: Acronyms



## 2 Publication and Repository Responsibilities

### 2.1 Repositories

All CAs that issue certificates under this policy are obligated to post all certificates issued by or to the CA and CRLs issued by the CA in a repository that is publicly accessible through all Uniform Resource Identifier (URI) references asserted in valid certificates issued by that CA. To promote consistent access to certificates and CRLs, the repository shall implement access controls and communication mechanism to prevent unauthorized modification or deletion of information.

Root CA Certificate repository path: rootcertificate.cca.gov.bd

CRL path: [crl.cca.gov.bd](http://crl.cca.gov.bd)

### 2.1 Publication of Certification Information

CAs shall make information publicly available on website such as CPs, CPSs, Certificates and CRLs and OCSPs responses in repositories. For public services, they are available 24 hours per day and 7 days per week. It shall ensure that its repository or repositories are implemented through trustworthy systems.

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

### 2.2 Time or Frequency of Publication

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

### 2.3 Access Controls on Repositories

The CA that issues certificates under this CP shall protect information unintended for public dissemination or modification. Certificates and CRLs in the repository shall be publicly available through the Internet. The CA shall detail what information in the repository shall be exempted from automatic availability and to whom, and under which conditions the restricted information may be made available. The CA shall maintain effective procedures and controls over the management of its repositories.







### 3.1 Naming

The CA that issues certificates under this CP shall specify the naming convention that it has adopted, such as X.501 Distinguished Names (DN). Subject Alternative Name Forms including, for example, an electronic mail address or a personal identification number may be included to ensure that the certificate of a person can be unambiguously identified.

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

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

Rules for interpreting distinguished name forms are specified in X.501. Rules for interpreting e-mail addresses are specified in RFC 5322.

The CA that issues certificates under this CP must ensure that the subject name assigned to a subscriber must identify that subscriber uniquely and unambiguously.

The CA that issues certificates under this CP reserves no liability to any certificate applicant on the usage of Distinguished Names appearing in a certificate. The right to use the name is the responsibility of the applicant and must be in accordance to the relevant laws, regulations, legal obligations or announcements.

### 3.2.1 Method to Prove Possession of Private Key

In all cases where the party named in a certificate generates its own keys, that party shall be required to prove possession on the private key, which corresponds to the public key in the certificate request. In the case where key generation is performed under the CA or RA's direct control, proof of possession is not required. The CA shall state in its CPS the method to prove possession of private key.

### 3.2.2 Authentication of Organization and Domain Identity

Requests for certificates shall include the CA name, address, and documentation of the existence of the CA. CCA shall verify the information in addition to the authenticity of the requesting representative and the representative's authorization to act in the name of the CA.

For subscriber organization certificates, the CA shall verify the existence of the organization by verifying the Certificate of Corporate Registration issued by the Department of Business Development, Ministry of Commerce. Copies of official documents require Certified True Copy from authorized representative. Public key certificates bind public keys to identities. However, the entity to be identified depends on the application for which the public keys are used. Identifying different types of entity requires different evidence and procedures. The CA that issues certificates under this CP shall state in its CPS the types of entity that the CA will support and details the required evidence and procedures.

#### 3.2.2.1 Identity

If the Subject Identity Information is to include the name or address of an organization, the CA SHALL verify the identity and address of the organization and that the address is the Applicant's address of existence or operation. The CA SHALL verify the identity and address of the Applicant using documentation provided by, or through communication with, at least one of the following:

1. A government agency in the jurisdiction of the Applicant's legal creation, existence, or recognition;
2. A third party database that is periodically updated and considered a Reliable Data Source;
3. A site visit by the CA or a third party who is acting as an agent for the CA; or
4. An Attestation Letter.
5. The CA MAY use the same documentation or communication described in 1 through 4 above to verify both the Applicant's identity and address.

#### 3.2.2.2 Doing Business As (DBA)/Tradename

CAs follows Section 3.2.2.2 of CA/Browser Forum Baseline Requirements.

#### 3.2.2.3 Verification of Country

CAs follows Section 3.2.2.3 of CA/Browser Forum Baseline Requirements.





#### 3.2.2.4 Validation of Domain Authorization or Control

This section defines the permitted processes and procedures for validating the Applicant's ownership or control of the domain. The CA SHALL confirm that prior to issuance, the CA has validated each Fully Qualified Domain Name (FQDN) listed in the Certificate using at least one of the methods listed below. Completed validations of Applicant authority may be valid for the issuance of multiple Certificates over time. In all cases, the validation must have been initiated within the time period specified in the relevant requirement (such as Section 4.2.1 of this document) prior to Certificate issuance. For purposes of domain validation, the term Applicant includes the Applicant's Parent Company, Subsidiary Company, or Affiliate. CAs SHALL maintain a record of which domain validation method, including relevant BR version number, they used to validate every domain.

Note: FQDNs may be listed in Subscriber Certificates using dNSNames in the subjectAltName extension or in Subordinate CA Certificates via dNSNames in permittedSubtrees within the Name Constraints extension.

##### 3.2.2.4.1 Validating the Applicant as a Domain Contact

CAs follows Section 3.2.2.4.1 of CA/Browser Forum Baseline Requirements.

##### 3.2.2.4.2 Email, Fax, SMS, or Postal Mail to Domain Contact

CAs follows Section 3.2.2.4.2 of CA/Browser Forum Baseline Requirements.

##### 3.2.2.4.3 Phone Contact with Domain Contact

CAs follows Section 3.2.2.4.3 of CA/Browser Forum Baseline Requirements.

##### 3.2.2.4.4 Constructed Email to Domain Contact

CAs follows Section 3.2.2.4.4 of CA/Browser Forum Baseline Requirements.

##### 3.2.2.4.5 Domain Authorization Document

CAs follows Section 3.2.2.4.5 of CA/Browser Forum Baseline Requirements.

##### 3.2.2.4.6 Agreed-Upon Change to Website

CAs follows Section 3.2.2.4.6 of CA/Browser Forum Baseline Requirements.

##### 3.2.2.4.7 DNS Change

CAs follows Section 3.2.2.4.7 of CA/Browser Forum Baseline Requirements.

##### 3.2.2.4.8 IP Address

CAs follows Section 3.2.2.4.8 of CA/Browser Forum Baseline Requirements.

##### 3.2.2.4.9 Test Certificate

CAs follows Section 3.2.2.4.9 of CA/Browser Forum Baseline Requirements.

##### 3.2.2.4.10 TLS Using a Random Number

CAs follows Section 3.2.2.4.10 of CA/Browser Forum Baseline Requirements.

#### 3.2.2.5 Authentication for an IP Address

CAs follows Section 3.2.2.5 of CA/Browser Forum Baseline Requirements.



### 3.2.2.6 Wildcard Domain Validation

CAs follows Section 3.2.2.6 of CA/ Browser Forum Baseline Requirements.

### 3.2.2.7 Data Source Accuracy

CAs follows Section 3.2.2.7 of CA/ Browser Forum Baseline Requirements.

### 3.2.2.8 Certificate Authority Authorization (CAA) Records

As part of the issuance process, the CA MUST check for CAA records and follow the processing instructions found, for each dNSName in the subjectAltName extension of the certificate to be issued, as specified in RFC 6844. If the CA issues, they MUST do so within the TTL of the CAA record, or 8 hours, whichever is greater.

When processing CAA records, CAs MUST process the issue, issue wild, and iodef property tags as specified in RFC 6844. Additional property tags MAY be supported. CAs MUST respect the critical flag and not issue a certificate if they encounter an unrecognized property with this flag set.

RFC 6844 requires that CAs "MUST NOT issue a certificate unless either (1) the certificate request is consistent with the applicable CAA Resource Record set or (2) an exception specified in the relevant Certificate Policy or Certification Practices Statement applies." For issuances conforming to these Baseline Requirements, CAs MUST NOT rely on any exceptions specified in their CP or CPS unless they are one of the following:

- CAA checking is optional for certificates for which a Certificate Transparency precertification was created and logged in at least two public logs, and for which CAA was checked.
- CAA checking is optional for certificates issued by a Technically Constrained Subordinate CA Certificate as set out in Baseline Requirements section 7.1.5, where the lack of CAA checking is an explicit contractual provision in the contract with the Applicant.
- CAA checking is optional if the CA or an Affiliate of the CA is the DNS Operator (as defined in RFC 7719) of the domain's DNS.

CAs are permitted to treat a record lookup failure as permission to issue if:

- the failure is outside the CA's infrastructure;
- the lookup has been retried at least once; and
- the domain's zone does not have a DNSSEC validation chain to the ICANN root.

CAs MUST document potential issuances that were prevented by a CAA record in sufficient detail to provide feedback to the CAB Forum on the circumstances and SHOULD dispatch reports of such issuance requests to the contact (s) stipulated in the CAA iodef record(s), if present. CAs are not expected to support URL schemes in the iodef record other than mailto: or https:

### 3.2.3 Authentication of Individual Identity

Not applicable for Root CA.





### 3.2.4 Non-verified Subscriber Information

Information that is not verified shall not be included in certificates.

### 3.2.5 Validation of Authority

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

### 3.2.6 Criteria for Interoperation

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

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

### 3.2.7 Identification and Authentication for Routine Re-key

Identification and authentication requirements are specified in Section 3.2.

### 3.2.8 Identification and Authentication for Re-key after Revocation

Identification and authentication requirements are specified in Section 3.2.

### 3.4 Identification and Authentication for Revocation Request

Identification and authentication requirements are specified in Section 3.2.



#### 4 Certificate Life-Cycle Operational Requirements

##### 4.1 Certificate Application

###### 4.1.1 Who Can Submit a Certificate Application

An organization who wishes to operate a CA in Bangladesh may complete and submit an application for certificates to CCA.

###### Enrollment Process and Responsibilities

All communications among CAs and RAs supporting the certificate application and issuance process shall be authenticated and protected from modification; any electronic transmission of shared secrets and personally identifiable information shall be protected. Communications may be electronic or out-of-band. Where electronic communications are used, cryptographic mechanisms commensurate with the strength of the public/private key pair shall be used. Out-of-band communications shall protect the confidentiality and integrity of the data. CAs are responsible for providing accurate information on their certificate applications.

##### 4.2 Certificate Application Processing

###### 4.2.1 Performing Identification and Authentication Functions

Information in certificate applications must be verified as accurate before certificates are issued. Procedures to verify information in certificate applications shall be specified in the CPS. In cases where the certificate request does not contain all the necessary information about the Applicant, the CA SHALL obtain the remaining information from the Applicant or, having obtained it from a reliable, independent, third-party data source, confirm it with the Applicant. The identification and authentication of the subscriber must meet the requirements specified for subscriber authentication as specified in Sections 3.2 and 3.3. The components of the PKI (e.g., CA or RA) that are responsible for authenticating the subscriber's identity in each case must be identified in the CPS.

CAA checking is optional for Subordinate CAs that issue SSL/TLS certificates under this CP using Name Constrained if Subordinate CA has a CAA Record Validation process for Fully Qualified Domain Names, Subordinate CA SHALL state in its CA/CPS practices on processing CAA Records for Fully Qualified Domain Names.

The CA SHALL develop, maintain, and implement documented procedures that identify and require additional verification activity for High Risk Certificate Requests prior to the Certificate's approval, as reasonably necessary to ensure that such requests are properly verified under these Requirements.

If a Delegated Third Party fulfills any of the CA's obligations under this section, the CA SHALL verify that the process used by the Delegated Third Party to identify and further verify High Risk Certificate Requests provides at least the same level of assurance as the CA's own processes.





**4.2.2 Approval or Rejection of Certificate Applications**

Any certificate application that is received by a CA that issues certificates under this CP, for which the identity and authorization of the applicant has been validated, will be duly processed. However, the CA must reject any application for which such validation cannot be completed.

The RA will coordinate with the CA to approve or reject certificate applications and notifies the results to subscribers.

**4.2.3 Time to Process Certificate Applications**

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

**4.3 Certificate Issuance****4.3.1 CA Actions during Certificate Issuance**

Upon receiving the request, the CA that issues certificate under this CP and its RA will:

- Verify the identity of the requester as specified in Section 3.2;
- Verify the authority of the requester and the integrity of the information in the certificate request as specified in Section 4.1;
- The CA must ensure the accuracy information in a CSR that conforms with Section 6. If not conform in Section 6, CA must be reject that Sub CA CSR;
- Generate and sign a certificate if all certificate requirements have been met (in the case of an RA, have the CA sign the certificate); and
- Make the certificate available to the subscriber after confirming that the CA has formally acknowledged their obligations as described in Section 9.6.3.

All authorization and other attribute information received from a prospective subscriber shall be verified before inclusion in a certificate. The responsibility for verifying prospective subscriber data shall be described in a CA's CPS.

**4.3.2 Notification to Subscriber by the CA of Issuance of Certificate**

CAs operating under this CP, or via RA if applicable, will notify the CA of the creation of a certificate and make the certificate available to the subscriber.

**4.4 Certificate Acceptance****4.4.1 Conduct Constituting Certificate Acceptance**

Upon the receipt of a certificate, the subscriber, or the applicant CA of a certificate, must proceed with the following:

- The applicant CA or the subscriber of the certificate, must verify the information contained in the certificate and either accept or reject the certificate.
- If the applicant CA or the subscriber of the certificate, fails to receive, or fails to accept the certificate within ten business days from the CA or Bangladesh Root CA, the CA or Bangladesh Root CA will revoke such certificate



All certificates shall be published in repositories

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

#### 4.5 Key Pair and Certificate Usage

#### 4.5.1 Subscriber Private Key and Certificate Usage

A subscriber can use the Private Key corresponding to the Public Key in the certificate, which is issued by CA operating under this CP, in order to generate its digital signature to other subscribers or relying parties. The applicant CA of a certificate can use the Private Key corresponding to the Public Key in the certificate to issue certificates to its subscribers. The certificate shall be used lawfully in accordance with this CP, the CPS and Terms of Service of the issuing CA.

#### 4.5.2 Relying Party Public Key and Certificate Usage

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

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

#### 4.6 Certificate Renewal

#### 4.6.1.1 Circumstance for Certificate Renewal

An Issuing CA may renew a Certificate if:

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

#### 4.6.2 Who May Request Renewal

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

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

### 4.6.3 Processing Certificate Renewal Requests

An Issuing CA may request additional information before processing a renewal request.



#### 4.6.4 Notification of New Certificate Issuance to Subscriber

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

#### 4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

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

#### 4.6.6 Publication of the Renewal Certificate by the Root CA

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

#### 4.6.7 Notification of Certificate Issuance by the Root CA to Other Entities

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

#### 4.7 Certificate Re-key

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

Certificate Re-Key consists of creating a new Certificate with a different public key and validity period while retaining all the identifying information from the old Digital Certificate. Due diligence, Key Pair generation, delivery and management are performed in accordance with this CP.

##### 4.7.1 Circumstance for Certificate Re-key

The CA that issues certificates under this CP allows Subscribers to re-key the certificate if one of the following conditions are met:

- Subscriber's certificate has less 25% life time before expiration or has already expired.
- Subscriber's certificate has been revoked.
- Subscriber needs to modify information in the certificate.

##### 4.7.2 Who May Request Certification of a New Public Key

Only the subscriber may request a new certificate.

##### 4.7.3 Processing Certificate Re-keying Requests

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

##### 4.7.4 Notification of New Certificate Issuance to Subscriber

The CA that issues certificates under this CP shall notify the result of new certificate issuance to subscriber according to the procedures specified in Section 4.3.2.



**4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate**

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

**4.7.6 Publication of the Re-keyed Certificate by the CA**

The CA that issues certificates under this CP shall publish the re-keyed according to the procedure in Section 4.4.2.

**4.7.7 Notification of Certificate Issuance by the CA to Other Entities**

The CA that issues certificates under this CP shall notify the result of certificate issuance to other entities according to the procedure in Section 4.4.3.

**4.8 Certificate Modification**

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

**4.8.1 Circumstance for Certificate Modification**

Since the interpretation of modifying certificate contents are sometimes complex, the CA that issues certificates under this CP shall not offer certificate modification. Re-certification is recommended, that means the initial registration process as described in section 3.2 must be gone through again. The new certificate shall have a different subject public key.

**4.8.2 Who May Request Certificate Modification**

Not Applicable.

**4.8.3 Processing Certificate Modification Requests**

Not Applicable.

**4.8.4 Notification of New Certificate Issuance to Subscriber**

Not Applicable.

**4.8.5 Conduct Constituting Acceptance of Modified Certificate**

Not Applicable.

**4.8.6 Publication of the Modified Certificate by the CA**

Not Applicable.

**4.8.7 Notification of Certificate Issuance by the CA to Other Entities**

Not Applicable.







#### 4.9.1.2 Reasons for Revoking a Subordinate CA Certificate

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

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

#### 4.9.2 Who Can Request Revocation

1. The Subscriber may make a request to revoke the certificate for which the subscriber is responsible.
2. The CA that issues certificates under this CP may make a request to revoke its own certificate.
3. The CA that issues certificates under this CP may also revoke any issued certificate whenever it knows or reasonably suspects that the circumstances as specified in section 4.9.1 occurred.
4. The RA may also make a request to revoke a certificate for which a subscriber is responsible whenever it knows or reasonably suspects that the circumstances as specified in section 4.9.1 occurred.
5. Court order.



#### 4.9.3 Procedure for Revocation Request

The CA that issues certificates under this CP shall provide the procedure that requester can request for revocation 24x7. Subscriber requesting revocation is required to follow the procedures such as:

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

#### 4.9.4 Revocation Request Grace Period

There is no grace period for revocation under this CP.

#### 4.9.5 Time within Which CA Must Process the Revocation Request

The CA that issues certificates under this CP must revoke certificates as quickly as practical upon endorsement of revocation request. Revocation requests should be processed within one business day or, whenever possible, before the next CRL is published.

#### 4.9.6 Revocation Checking Requirement for Relying Parties

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

#### 4.9.7 CRL Issuance Frequency

For other certificates (Root CA and/or CAs that has Sub CAs), the CRL shall be:

1. Generated once within six (6) months, or within twenty-four (24) hours of any revocation made.
2. Valid for NOT more than six (6) months from the date of generation.

The CRL which provides the status of Subscriber Certificates (Issuing CAs), the CRL shall be:

1. Generated once within seven (7) days, or within thirty (30) minutes of any revocation made.
2. Valid for NOT more than ten (10) days from the date of generation.

#### 4.9.8 Maximum Latency for CRLs

CRLs are published to repository within 30 minutes of generation.



**4.9.9 Online Revocation/Status Checking Availability**

Online status checking is optional for Bangladesh Root CA and CAs operating under this CP. Where online status checking is supported, status information shall be regularly updated and available to relying parties.

**4.9.10 Online Revocation Checking Requirements**

Relying Parties may optionally check the status of certificates through the CCA's Online Certificate Status Protocol (OCSP) service, if provided by Bangladesh Root CA, and/or check the status of subscriber certificates through the issuing CA's OCSP service, if provided by the issuing CA. Client software using online status checking need not obtain or process CRLs.

**4.9.11 Other Forms of Revocation Advertisements Available****4.9.12 Not Applicable.****4.9.13 Special Requirements Regarding Key Compromise**

The CA that issues certificate under this CP must notify Bangladesh Root CA immediately and Relying Parties as soon as practical.

**4.9.14 Circumstances for Suspension**

Suspension of Subscriber certificates (SSL/TLS) is not allowed.

For certificate, suspension is not permitted. For subscriber's certificate, CA that issues certificates under this CP shall state in its CPS the circumstances for suspension.

**4.9.15 Who Can Request Suspension**

The CA that issues certificates under this CP shall state in its CPS who can request suspension.

**4.9.16 Procedure for Suspension Request**

The CA that issues certificates under this CP shall state in its CPS the procedure for suspension request.

**4.9.17 Limits on Suspension Period**

The CA that issues certificates under this CP shall state in its CPS the limits on suspension period.

**4.10 Certificate Status Services****4.10.1 Operational Characteristics**

Not applicable.

**4.10.2 Service Availability**

Not applicable.





**4.10.3 Optional Features**

Not Applicable.

**4.11 End of Subscription**

Not applicable.

**4.12 Key Escrow and Recovery****4.12.1 Key Escrow and Recovery Policy and Practices**

No Private Key escrow process is planned for CCA Private Keys. Private Keys of the CA that issues certificates under this CP are never escrowed. Subscriber encipherment keys may be escrowed to provide key recovery. Escrowed keys shall be protected at no less than the level of security in which they are generated, delivered, and protected by the subscriber. Under no circumstances shall a subscriber signature key be held in trust by a third party. The CA that issues certificates under this CP that support private key escrow for key management keys shall specify in its CPS the policy and practice of key escrow.

**4.12.2 Session Key Encapsulation and Recovery Policy and Practices**

Not Applicable.

**5 Facility, Management, and Operational Controls****5.1 Physical Security Controls****5.1.1 Site Location and Construction**

All CA and RA operations shall be conducted within a physically protected environment that deters, prevents, and detects unauthorized use of, access to, or disclosure of sensitive information and systems. The site location and construction, when combined with other physical security protection mechanisms such as guards, high security locks, and intrusion sensors, shall provide robust protection against unauthorized access to the CA equipment and records.

**5.1.2 Physical Access**

Access to certificate issuance systems is only allowed for the responsible officers of the corresponding CA. In case other individuals need to access the service area where the CA systems are located, proper authorization must be obtained in advance. All visiting individuals must be recorded in the access log and must be accompanied by the responsible officer during the whole visit.

The certificate issuing servers and Cryptographic Module must be stored in a secure area where physical access to such systems requires dual-control and two-factor authentication.



### 5.1.3 Power and Air Conditioning

The CA shall have backup power capability sufficient to lock out input, finish any pending actions, and record the state of the equipment automatically before lack of power or air conditioning causes a shutdown. The repositories (containing certificates and CRLs) shall be provided with uninterrupted power sufficient for a minimum of 6-hour operation in the absence of commercial power, to maintain availability and avoid denial of service.

### 5.1.4 Water Exposures

The secure facilities of CAs and RAs shall be constructed and equipped, and procedures shall be implemented, to prevent floods or other damaging exposure to water, e.g.: on raised floor equipped with water sensor.

### 5.1.5 Fire Prevention and Protection

The secure facilities of CAs and RAs shall be constructed and equipped, and procedures shall be implemented, to prevent and extinguish fires or other damaging exposure to flame or smoke. These measures shall meet all local applicable safety regulations.

### 5.1.6 Media Storage

CAs and RAs shall protect the magnetic media holding backups of critical system data or any other sensitive information from water, fire, or other environmental hazards, and shall use protective measures to deter, detect, and prevent the unauthorized use of, access to, or disclosure of such media.

### 5.1.7 Waste Disposal

CAs and RAs shall implement procedures for the disposal of waste (paper, media, or any other waste) to prevent the unauthorized use of, access to, or disclosure of waste containing Confidential/Private Information.

Paper waste containing sensitive data shall be shredded before disposal. Sensitive data on magnetic or other digital media must be permanently erased before disposal.

### 5.1.8 Off-site Backup

A backup media must be stored at a secure off-site facility.



## 5.2 Procedural Controls

### 5.2.1 Trusted Roles

#### Definition of Trusted Role:

A trusted role is one whose incumbent performs functions that can introduce security problems to the PKI system if not carried out properly, whether accidentally or maliciously. It is essential that the people selected to fill these roles are held accountable to perform the designated actions correctly. Otherwise, the integrity of the CA is weakened or compromised. The functions performed in these roles form the basis of trust in the CA. The CCA defines the following roles to be trusted roles:

1. Policy Authority (PA)
2. Hardware Key Manager
3. CA Administrator
4. CA Operations Manager (CAOM)
5. Registration Authority Officer (RAO)
6. Database Administrator (DBA)
7. System Administrator (SA)
8. Network Administrator (NA)
9. Internal Auditor (IA)

All the above roles incumbents from 2-9 should not report to each other. There are three primary controls to be performed on a trusted role incumbent – (1) background checking, (2) multi-person control (segregation of duties) and (3) redundancy (at least, two persons per role). These roles are defined below for reference.

#### Description of the trusted roles:

1. **Policy Authority (PA):** The policy authority does not fall under the trusted roles. The policy authority is an entity or a committee responsible for defining, implementing, and overseeing the policies and practices that govern the operation and usage of digital certificates within an organization's PKI. The Policy Authority sets the rules and guidelines for certificate issuance, management, and usage to ensure the security, trustworthiness, and compliance of the PKI. As the PA team consists of multiple persons, two sets of PA team are not required.
2. **Hardware Key Manager:** The hardware key manager is an individual responsible for managing the distribution, storage, and protection of cryptographic keys used in digital certificates and encryption processes within the PKI ecosystem. However, the hardware key manager must not be given any role in the certificate generation / suspension / revocation processes as well as CA software configuration / CA network configuration / CA operations.
3. **CA Administrator:** The CA administrator is an individual responsible for the installation, configuration, and maintenance of the CA software. This is a critical trusted role and includes the ability to assign all other CA roles and renew the CA certificate. This is purely a technical role. Therefore, the CA administrator must not be given any role in the certificate generation / suspension / revocation processes as well as CA network configuration / physical key management.
4. **CA Operations Manager (CAOM):** The CA operations manager plays a critical role in ensuring the reliability and trust on the digital certificates. The CAOM approves certificate enrollment, suspension and revocation requests followed by systemic execution. However,





the CAOM must not be given any role in the CA software configuration / CA network configuration / subscriber handling / physical key management.

5. **Registration Authority Officer (RAO):** The RAO acts as an intermediary between certificate requestors and the CA operations manager. His/her primary function is to collect and verify the identity of certificate requestor and validate their eligibility to obtain digital certificates and perform the requestor's enrollment accordingly. However, the RAO must not be given any role in the certificate generation / suspension / revocation processes as well as CA software configuration / CA network configuration / CA operations / physical key management.
6. **Database Administrator (DBA):** The DBA is responsible for the configuration, administration, and optimization of the databases / repository used to store digital certificates, certificate revocation information, audit logs, and other critical data associated with the organization's PKI network. However, the DBA must not be given any role in the certificate generation / suspension / revocation processes as well as CA software configuration / CA network configuration / physical key management.
7. **System Administrator (SA):** The System administrator is responsible for the routine operation of the CA equipment / server and operations such as system backups and recovery or changing recording media. The SA also performs the installation, configuration, management, and maintenance of the server and system components that comprise the organization's Public Key Infrastructure. However, the SA must not be given any role in the certificate generation / suspension / revocation processes as well as CA network configuration / physical key management.
8. **Network Administrator (NA):** The Network administrator is responsible for the design, configuration, security, and maintenance of the network infrastructure that facilitates the operation of the organization's PKI network. This role involves ensuring that network components, such as routers, switches, firewalls, load balancers, and other devices, are properly configured to support the secure communication, certificate issuance, and certificate validation processes. However, the NA must not be given any role in the certificate generation / suspension / revocation processes as well as CA software configuration / physical key management.
9. **Internal Auditor (IA):** The internal auditor is a professional responsible for assessing, reviewing, and ensuring the compliance, effectiveness, and security of the organization's PKI operation. His/her primary role is to conduct independent and objective evaluations of the PKI infrastructure, policies, procedures, and controls to identify risks, vulnerabilities, and areas for improvement. However, the IA must not be given any access to the system through which he/she can manipulate any repository data. It must be read-only access.

#### 5.2.2 Number of Persons Required per Task

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

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





- Processing of third party key recovery requests.

### 5.2.3 Identification and Authentication for Each Role

CAs and RAs shall confirm the identity and authorization of all personnel seeking to become Trusted before such personnel are:

- issued with their access devices and granted access to the required facilities;
- given electronic credentials to access and perform specific functions on Information Systems and CA or RA systems.

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

The CA and RA equipment shall require, at a minimum, strong authenticated access control for remote access using multi-factor authentication. Examples of multi factor authentication include use of a password or PIN along with a time-based token, digital certificate on a hardware token or other devices that enforce a policy of what a user has and what a user knows. The CA and RA equipment shall require, at a minimum, authenticated access control (e.g., strong passwords) for local multi-party access.

Individuals holding trusted roles shall be appointed to the trusted role by an appropriate approving authority. The approval shall be recorded in a secure and auditable fashion. Individuals holding trusted roles shall accept the responsibilities of the trusted role, and this acceptance shall be recorded in a secure and auditable fashion. Identity proofing of the RA shall be performed by a member of the CA Operations Staff. Users shall authenticate themselves to all aspects of the network (servers, operating systems, applications, databases, processes, and so on) before they can access that resource.



#### 5.2.4 Roles Requiring Separation of Duties

Individuals serving as Security Auditors shall not perform or hold any other trusted role. An individual that holds any CA Operations Staff role shall not be an RA except that CA Operations Staff may perform RA functions when issuing certificates to RA.

Under no circumstances shall a CA operating under this CP be audited for compliance by any subsidiary, parent, or sibling company of its corporate holdings.

Only an individual serving in a Security Auditor role may perform internal auditing functions, with the exception of those security audit functions (e.g., configuring, archiving, deleting) that require multi-person control.

An individual that performs any trusted role shall only have one identity when accessing CA equipment.

The following roles must be performed by trusted officers:

- Verification and validation of forms such as the certificate application forms and the certificate revocation form.
- Certificate issuance and certificate revocation
- Access to CA's private key.

#### 5.3 Personnel Controls

##### 5.2.5 Qualifications, Experience and Clearance Requirements

All personnel of the CA that issues certificates under this CP must be examined with their qualifications in terms of the requisite background, experience in order to ensure their prospective job responsibilities, competency and satisfaction.

##### 5.2.6 Background Check Procedures

Prior to commencement of employment, the CA Human Resource department must conduct the following background checks:

- Identification card
- Certificate of the highest education
- Criminal records
- Professional certificate (if any)
- Confirmation letter of previous employment
- Background Check (Recheck at least every three years)

The CA that issues certificates under this CP may also exercise other measurements for background check. If the provided information is found to be false, or if the education/professional background is found unmatched, or if the person has certain criminal convictions, that person shall not be considered to work with the CA.





### 5.2.7 Training Requirements

The CA that issues certificates under this CP must provide its officers with appropriate training as well as the requisite on-the-job training needed to perform their job responsibilities related to CA operations with competency and satisfaction. The training programs include the following as relevant:

- Basic cryptography and Public Key Infrastructure (PKI) concepts
- Information Security Awareness
- Use and operation of deployed hardware and software related to CA operations
- Security Risk Management
- Disaster recovery and business continuity procedures
- Security Principles and Mechanisms,
- Common threats to the validation process, including phishing and other social engineering tactics
- Applicable Industry and Government guidelines.

### 5.2.8 Retraining Frequency and Requirements

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

### 5.2.9 Job Rotation Frequency and Sequence

The CA that issues certificates under this CP is recommended to specify in its CPS the job rotation frequency and sequence of officers.

### 5.2.10 Sanction for Unauthorized Actions

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

### 5.2.11 Independent Contractor Requirements

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

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

### 5.2.12 Documentation Supplied to Personnel

The CA that issues certificates under this CP must provide its personnel the requisite documentation needed to perform their job responsibilities competently and satisfactorily.



### 5.3 Audit Logging Procedures

#### 5.3.1 Types of Events Recorded

The CA that issues certificates under this CP must log the following significant events:

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

Log entries include the following elements:

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

#### 5.3.2 Frequency of Processing Log

The CA operated under this CP shall examine audit logs at a reasonable frequency and at least on a monthly basis.

#### 5.3.3 Retention Period for Audit Log

The Issuer CA and RA shall retain audit logs on-site until after they are reviewed. Audit logs certificates shall be retained for at least seven (7) years.

#### 5.3.4 Protection of Audit Log

The Issuer CA and RA shall implement procedures that protect archived data from destruction prior to the end of the audit log retention period. The Issuer CA and RA shall configure its systems and establish operational procedures to ensure that (i) only authorized people have read access to logs, (ii) only authorized people may archive audit logs, and (iii) audit logs are not modified. The Issuer CA's off-site storage location must be a safe and secure location that is separate from the location where the data was generated.

The Issuer CA and RA shall make records available if required for the purpose of providing evidence of the correct operation of time-stamping services for the purpose of legal proceedings. The Issuer CA shall make its audit logs available to auditors upon request.





**5.3.5 Audit Log Backup Procedures**

- Audit Logs stored in an electronic audit log system are backup in two facilities protected through restricted security perimeters.
- Events Records follow the procedures below:
- Paper-based event records are converted into electronic format before being stored in the audit log system.
- CA backup audit events specified in 5.4.1.

**5.3.6 Audit Log Accumulation System (Internal vs. External)**

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

**5.3.7 Notification to Event-Causing Subject**

Not Applicable.

**5.3.8 Vulnerability Assessments**

All Issuing CAs shall perform vulnerability assessments quarterly. Such vulnerability assessments should focus on internal and external threats that could result in unauthorized access, tampering, modification, alteration or destruction of the Certificate issuance process.

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

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

**5.3.9 Penetration Test Assessments**

The CA that issues certificates under this CP must assess security Penetration Test at least on an annual basis.



#### 5.4 Records Archival

##### 5.4.1 Types of Records Archived

CA archives:

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

##### 5.4.2 Retention Period for Archive

Records shall be retained for at least 7 years, unless there are specific requirements.

##### 5.4.3 Protection of Archive

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

##### 5.4.4 Archive Backup Procedure

Records archival are backed up on a monthly basis following the below procedures:

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

##### 5.4.5 Requirements for Time Stamping of Records

Any activity performed on or to the certification systems shall be recorded with the time and date information.

##### 5.4.6 Archive Collection System (Internal or External)

Archive Collection System is internal to the CA only.



#### 5.4.7 Procedures to Obtain and Verify Archive Information

Procedures to obtain and verify archive information are as follows:

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

#### 5.5 Key Changeover

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

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

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

#### 5.6 Compromise and Disaster Recovery

##### 5.6.1 Incident and Compromise Handling Procedures

The CA that issues certificates under this CP shall have an incident response plan and a disaster recovery plan. If compromise of a CA is suspected, an independent third-party investigation shall be performed in order to determine the nature and the degree of damage. Issuance of certificates from that CA shall be stopped immediately upon detection of a compromise. If a CA private signing key is suspected of compromise, the procedure outlined in section 5.7.3 shall be followed. Otherwise, the scope of potential damage shall be assessed in order to determine if the CA needs to be rebuilt, only some certificates need to be revoked, and/or the CA private key needs to be declared compromised. In case that there is an event affects to security of the CA system; the corresponding CA officers shall notify the PA and CCA if any of the following occur:

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

##### 5.6.2 Computing Resources, Software, and/or Data are corrupted

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



### 5.6.3 Entity Private Key Compromise Procedures

In the case of Bangladesh Root CA compromise, CCA shall notify the PA and relying parties via public announcement, and any cross-certified PKIs, of the Bangladesh Root CA compromise so that they can revoke any cross certificates issued to the Bangladesh Root CA or any Subordinate CAs and notify all Subscribers and Relying Parties to remove the trusted self-signed certificate from their trust stores. Notification shall be made in an authenticated and trusted manner. Initiation of notification to the PA and any cross-certified PKIs shall be made at the earliest feasible time and shall not exceed 24 hours beyond determination of compromise or loss unless otherwise required by law enforcement. Initiation of notification to relying parties and subscribers will be made after mediations are in place to ensure continued operation of applications and services. If the cause of the compromise can be adequately addressed, and it is determined that the PKI can be securely re-established, CCA shall then generate a new root certificate, solicit requests and issue new certificates, securely distribute the new root certificate, and re-establish any cross certificates. In case of a CA key compromise, the CA shall notify PA and Bangladesh Root CA. CCA shall revoke that CA's certificate, and the revocation information shall be published immediately in the most expedient, authenticated, and trusted manner but within 24 hours after the notification. The compromised CA shall also investigate and report to the PA and Bangladesh Root CA what caused the compromise or loss, and what measures have been taken to preclude recurrence. If the cause of the compromise can be adequately addressed and it is determined that the CA can be securely re-established, then the CA shall be reestablished. Upon re-establishment of the CA, new subscriber certificates shall be requested and issued again. When a certificate is revoked because of compromise, suspected compromise, or loss of the private key, a CRL shall be published at the earliest feasible time by the CA, but in no case more than 6 hours after notification. In case of an RA compromise, the CA shall disable the RA. In the case that the RA's key is compromised, the CA that issued RA certificate shall revoke it, and the revocation information shall be published within 24 hours in the most expedient, authenticated, and trusted manner. The compromise shall be investigated by the CA in order to determine the actual or potential date and scope of RA compromise. All certificates approved by that RA since the date of actual or potential RA compromise shall be revoked. In the event that the scope is indeterminate, then the CA compromise procedures as specified in above shall be followed.

### 5.6.4 Business Continuity Capabilities after a Disaster

The CA that issues certificates under this CP shall prepare a disaster recovery plan which have been tested, verified and continually updated. A full restoration of services will be done within 24 hours in case of disaster.







### 5.7 CA Termination

If there is any circumstance to terminate the services of the CA operating under this CP with the approval of the PA, the CA operating under this CP will notify the subscribers and all relying parties. The action plan is as follow:

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



## 6 Technical Security Controls

### 6.1 Key Pair Generation and Installation

#### 6.1.1 Key Pair Generation

The CA that issues certificates under this CP generates a key pair and stores the private key in a cryptographic key management device that meets Federal Information Processing Standard (FIPS) 140-2 Level 3 under multi-person control.

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

The CA key pair generation must create a verifiable audit trail demonstrating that the security requirements for procedures were followed. The documentation of the procedure must be detailed enough to show that the appropriate role separation was used. An independent third party shall validate the execution of the key generation procedures either by witnessing the key generation or by examining the signed and documented record of the key generation.

Subscriber key pair generation shall be performed by the subscriber. If the CA that issues certificates under this CP generates key pairs for subscriber, the CA shall generate key within a secure FIPS 140 validated cryptographic hardware.

#### 6.1.2 Private Key Delivery to Subscriber

The CA that issues certificates under this CP must generate the key pair by themselves. If the CA that issues certificates under this CP generates key pairs for subscriber, the CA shall develop a procedure to securely distribute private key to subscriber.

#### 6.1.3 Public Key Delivery to Certificate Issuer

Where key pairs are generated by the subscriber themselves, the CA that issues certificates under this CP shall provide a channel for the subscriber to securely deliver the public key and the subscriber's identity to the issuing CA. The subscribers are required to submit Certificate Signing Request in the form of PKCS #10 standard with the application by themselves.

#### 6.1.4 CA Public Key Delivery to Relying Parties

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

#### 6.1.5 Key Sizes

This CP requires use of RSA signature algorithm and additional restriction on key sizes and hash algorithms are detailed below. Certificates issued under this policy shall contain RSA public keys with the minimum key size of 4096 bits. For Code Signing minimum key sizes of 4096 bits. Find table 3 for the key requirements.

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





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

Table 3: Key requirement

## 6.1.6 Public Key Parameters Generation and Quality Checking

Not Applicable.

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

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

Public keys that are bound into subscriber certificates shall be used only for signing or encrypting.

Public keys that are bound into certificates shall be used only for signing certificates and status information such as CRLs. Only CCA shall issue certificates to CAs located in Bangladesh.

## 6.2 Private Key Protection and Cryptographic Module Engineering Controls

## 6.2.1 Cryptographic Module Standards and Controls

Bangladesh Root CA uses a FIPS 140-2 Level 3 validated hardware cryptographic module for signing operations.

The CA that issues certificates under this CP shall use a FIPS 140-2 Level 3 or higher validated hardware cryptographic module for signing operations.

Subscribers shall use a FIPS 140-2 Level 1 or higher validated hardware cryptographic module for all cryptographic operations.

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

Accessing the private key of Bangladesh Root CA and CAs operated under this CP must be performed by at least two persons.

## 6.2.3 Private Key Escrow

Private keys of the CA operated under this CP are never escrowed. The CA that issues certificates under this CP must not have any policy to keep the private key with other parties or keep subscribers' private key.



**6.2.4 Private Key Backup**

The CA's private signature key shall be backed up under the same multiparty control as the original signature key. At least one copy of the private signature key shall be stored off-site. All copies of the CA private signature key shall be accounted for and protected in the same manner as the original. CA that issues certificate under this CP shall backup its private signature key in FIPS 140-2 Level 3 validated hardware cryptographic module. The CA shall state in its CPS the backup procedure.

**6.2.5 Private Key Archival**

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

**6.2.6 Private Key Transfer into or from a Cryptographic Module**

The CA private keys may be exported from the cryptographic module only to perform CA key backup procedure. At no time, the CA private key shall exist in plaintext outside the cryptographic module.

**6.2.7 Private Key Storage on Cryptographic Module**

Bangladesh Root CA and CA operating under this CP shall store its Private Keys on a cryptographic module which complies with FIPS 140-2 Level 3 or above standard.

**6.2.8 Method of Activating Private Key**

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

**6.2.9 Method of Deactivating Private Key**

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

**6.2.10 Method of Destroying Private Key**

The CA will delete the private keys from a cryptographic module and its backup by overwriting the private key or initializing the module with the destroy function of the cryptographic module. The event of destroying the CA must be recorded into the evidence under section 5.4.

**6.2.11 Cryptographic Module Rating**

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







### 6.3 Other Aspects of Key Pair Management

#### 6.3.1 Public Key Archival

A public key is stored for a long period in the certificate.

#### 6.3.2 Certificate Operational Periods and Key Pair Usage Periods

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

The validity period of Bangladesh Root CA root certificate is 10 years and the validity period of CA Subscriber certificates is not more than 10 years. Certificate operational periods and key pair usage periods shall be assessed by the PA at least once a year or as necessary especially in an incident that is believed to significantly impact trustworthiness of the CA. Subscriber certificates issued after 1 March 2018 must have a Validity Period no greater than 825 days. Subscriber certificates issued after 1 July 2016 but prior to 1 March 2018 must have a Validity Period no greater than 39 months.

### 6.4 Activation Data

#### 6.4.1 Activation Data Generation and Installation

Activation data such as Personal Identification Number (PIN) and passwords for accessing the CA systems are user-selected and protected under multi-person control by each of whom holding that activation data. The CA operated under this CP shall use the same data generation mechanism.

#### 6.4.2 Activation Data Protection

The CA operated under this CP shall protect activation data used to unlock private keys by storing the data in secure location.

#### 6.4.3 Other Aspects of Activation Data

Not Applicable.



## 6.5 Computer Security Controls

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

### 6.5.1 Specific Computer Security Technical Requirements

The CA operated under this CP shall limit the number of applications installed on each computer to minimize security risks. Those applications are hardened based on the instructions provided by software manufacturers. In addition, installed applications shall be regularly reviewed for security updates to ensure that no vulnerability is exposed.

### 6.5.2 Computer Security Rating

No stipulation.

## 6.6 Life Cycle Technical Controls

### 6.6.1 System Development Controls

The CA operated under this CP must implement system development controls over the procurement, development and change of the CA system through aspects of its life-cycle. CA systems are implemented and tested in a non-production environment prior to implementation in a production environment. Change control procedures are in place to control and monitor all revisions and enhancements to be made to the components of such systems.

### 6.6.2 Security Management Controls

The CA operated under this CP maintains a list of acceptable products and their versions for each individual CA system component and keeps up-to-date. Changes of variables are processed through security management controls.

### 6.6.3 Life Cycle Security Controls

The CA operated under this CP can also address life-cycle security ratings based for example, on the Trusted Software Development Methodology (TSDM) level IV and V, independent life-cycle security controls audit, and the Software Engineering Institute's Capability Maturity Model (SEI-CMM).



**CCA**

স্বাক্ষরিত স্বাক্ষর নথিগত প্রমাণের স্বাক্ষর-এস স্বাক্ষর

## Certificate Policy

### 6.7 Network Security Controls

The CA network must be equipped with firewall with features to investigate data transmission at application level and detect intruders or network activities that violate the policy. It is to ensure that the system is secure. Normal users allow accessing the certificate services through the network via the website and directories only. For system management, + officers will use dedicated network to access and management purpose. Information contains in this particular network is encrypted.

### 6.8 Time-stamping

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



## 7 Certificate, CRL and OCSP Profiles

### 7.1 Certificate Profile

The certificate issued by the CA under this CP must comply with ITU-T Recommendation X.509: Information technology - Open systems interconnection - The Directory. Public- key and attribute certificate frameworks in which the certificate contains the information shown in Table 4.

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

Table 4: Fields in the Certificate

#### 7.1.1 Version Number

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

#### 7.1.2 Certificate Content and Extensions; Application of RFC 5280

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

##### 7.1.2.1 Root CA Certificate

CAs follows Section 7.1.2.1 of CA/Browser Forum Baseline Requirements.





**7.1.2.2 Subordinate CA Certificate**

CAs follows Section 7.1.2.2 of CA/ Browser Forum Baseline Requirements.

**Subscriber Certificate**

CAs follows Section 7.1.2.3 of CA/ Browser Forum Baseline Requirements. In addition, certificate Policies:policyQualifiers:qualifier:cPSuri must be mandatory.

**7.1.2.3 All Certificate**

CAs follows Section 7.1.2.4 of CA/ Browser Forum Baseline Requirements.

**7.1.2.4 Application of RFC 5280**

CAs follows Section 7.1.2.5 of CA/ Browser Forum Baseline Requirements.

**7.1.3 Algorithm Object Identifiers**

The OID of digital signature and encryption of certificate is in Table 5.

Algorithm	Object Identifier
RSAEncryption	1.2.840.113549.1.1.1
SHA512withRSAEncryption	1.2.840.113549.1.1.13
SHA512	2.16.840.1.101.3.4.2.3

*Table 5: Method of Digital Signature and Encryption with Object Identifier*

**7.1.4 Name Forms**

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

**7.1.5 Name Constraints**

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

**7.1.6 Certificate Policy Object Identifier**

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

**7.1.7 Usage of Policy Constraints Extension**

Not Applicable.

**7.1.8 Policy Qualifiers Syntax and Semantics**

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

**7.1.9 Processing Semantics for the Critical Certificate Policies Extension**

Not Applicable.



## 7.2 CRL Profile

The CA's certificate revocation list must comply with RFC5280 as the following details as in Table 6.

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

*Table 6: Item List in Certificate Revocation*

### 7.2.1 Version Number(s)

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

### 7.2.2 CRL and CRL Entry Extensions

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

#### 7.2.2.1 Authority Key Identifier

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

#### 7.2.2.2 BaseCRLNumber

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





### 7.2.2.3 ReasonCode

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

### 7.2.2.4 InvalidityDate

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

### 7.2.2.5 Issuing DistributionPoint

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

## 7.3 OCSP Profile

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

### 7.3.1 Version Number(s)

CAs shall issue Version 1 OCSP responses.

### 7.3.2 Fields in OCSP Responses

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

### 7.3.3 OCSP Extensions

No Stipulation.



## 8 Compliance Audit and Other Assessments

An Issuing CA shall have compliance audit mechanism in place to ensure that the requirements of its CP/CPS are being implemented and audited for complying with the following standards:

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

### 8.1 Frequency or Circumstances of Assessment

CAs follows Section 8.1 of CA/ Browser Forum Baseline Requirements.

### 8.2 Identity/Qualifications of Assessor

WebTrust auditors must meet the requirements of CA/ Browser forum baseline requirements.

Assessor's Relationship to Assessed Entity

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

### 8.3 Assessor's Relationship to assessed Entity

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

### 8.4 Topics Covered by Assessment

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

### 8.5 Actions Taken As a Result of Deficiency

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

### 8.6 Communication of Results

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





**8.7 Self-Audits**

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



## 9.1 Fees

### 9.1.1 Certificate Issuance or Renewal Fees

The CA operated under this CP shall provide the fee including renewal fee of each type of certificate that the CA issued.

### 9.1.2 Certificate Access Fees

The CA operated under this CP shall not include fees for certificate access.

### 9.1.3 Revocation or Status Information Access Fees

The CA operated under this CP shall not include fees for revocation or Status Information access.

#### 9.1.4 Fees for Other Services

The CA operated under this CP shall declare the other fees.

### 9.1.5 Refund Policy

The CA operated under this CP shall provide reasonable refund policy.

## 9.2 Financial Responsibility

This CP contains no limits on the use of certificates issued by CAs under the policy. Rather, entities, acting as relying parties, shall determine what financial limits, if any, they wish to impose for certificates used to consummate a transaction.

### 9.2.1 Insurance Coverage

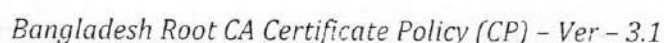
The CA operated under this CP shall disclose insurance related to the CA operation.

### 9.2.2 Other Assets

The CA operated under this CP shall disclose other assets.

### 9.2.3 Insurance or Warranty Coverage for End-entities

The CA operated under this CP shall provide reasonable insurance or warranty coverage for end entities.



**9.3 Confidentiality of Business Information****9.3.1 Scope of Confidential Information**

The CA keeps following information in the scope of confidential information:

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

**9.3.2 Information Not within the Scope of Confidential Information**

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

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

**9.3.3 Responsibility to Protect Confidential Information**

The CA under this CP must have security measure in place to protect confidential information.

**9.4 Privacy of Personal Information****9.4.1 Privacy Plan**

CAs under this CP shall develop, implement and maintain a privacy plan. The privacy plan shall document what personally identifiable information is collected, how it is stored and processed, and under what conditions the information may be disclosed.

**9.4.2 Information Treated As Private**

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

**9.4.3 Information Not Deemed Private**

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

**9.4.4 Responsibility to Protect Private Information**

The CA has implemented security measure to protect private information.

**9.4.5 Notice and Consent to Use Private Information**

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



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

Not Applicable.

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

### 9.6.1 CA Representations and Warranties

- Procedures are implemented in accordance with this CP.
- Any certificates issued that assert the policy OIDs identified in this CP were issued in accordance with the stipulations of this CP.
- The Certification Practice Statement (CPS) will be provided, as well as any subsequent changes, for conformance assessment.
- The CA operation is maintained in conformance to the stipulations of the CPS.
- The registration information is accepted only from approved RAs operating under an approved CPS.
- All information contained in the certificate issued by the CA is valid and appropriate. Evidence that due diligence was exercised in validating the information contained in the certificates is maintained.
- Certificates of CA found to have acted in a manner counter to their obligations in accordance with section 9.6.3 will be revoked.
- All information regarding certificate issuance and certificate revocation are processed through the procedures specified in the CPS of the corresponding CA.

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





**9.6.3 Subscriber Representations and Warranties**

By using the subscriber certificate, the subscriber assures that

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

**9.6.4 Relying Party Representations and Warranties**

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

**9.6.5 Representations and Warranties of Other Participants**

Warranties of other participants are optional for CAs under this CP.

**9.7 Disclaimers of Warranties**

The statement under clause 9.6 cannot be terminated or forfeited unless it is amended to conform to the law.

**9.8 Limitations of Liability**

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

**9.9 Indemnities**

In case the damage occurs to the CA from the actions of subscribers or relying parties, the corresponding CA reserves the right to claim damages.

**9.10 Term and Termination****9.10.1 Term**

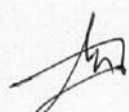
This CP takes effect from the date of publication upon the approval of the Policy Authority.

In case of changes in technical requirements, subscribers must comply with the changes in a timely manner.

The changes must be made within one year from the date that the subscriber has been formally informed.

**9.10.2 Termination**

This CP takes effect until it is terminated.



**9.10.2 Effect of Termination and Survival**

The requirements of this CP remain in effect through the end of the archive period for the last certificate issued.

**9.11 Individual Notices and Communications with Participants**

The CA will communicate to those participants using the reliable channel as soon as possible in accordance with the importance of information.

**9.12 Amendments****9.12.1 Procedure for Amendment**

An amendment of this CP requires approval by the PA before announcement. The amendment shall be performed under laws, regulation or other related service announcements of Bangladesh Root CA.

**9.12.2 Notification Mechanism and Period**

Bangladesh Root CA reserves the right to revise this document. In case there are any significant changes, CCA will announce on the website before the date of enforcement.

**9.12.3 Circumstances under Which OID Must Be Changed**

If PA determines an amendment necessitates a change in an OID, then the revised version of this CP will also contain a revised OID. Otherwise, amendments do not require an OID change.

**9.13 Dispute Resolution Procedure****9.13.1 Disputes between Issuer and Subscriber**

CAs operating under this CP shall state in its CPS a dispute resolution clause and procedures to resolve disputes and claims among CAs operating under this CP and the subscribers. In any case, CAs operating under this CP or subscribers may submit any dispute to PA. PA shall have jurisdiction to settle the dispute.

**9.13.2 Disputes between Issuer and Relying Parties**

CAs operating under this CP shall state in its CPS a dispute resolution clause and procedures to resolve disputes and claims among CAs operating under this CP and the relying parties. In any case, CAs operating under this CP or relying parties may submit any dispute to the PA. The PA has jurisdiction over the dispute.

**9.14 Governing Law**

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

**9.15 Compliance with Applicable Law**

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



**9.16 Miscellaneous Provisions****9.16.1 Entire Agreement**

The CPS of a CA operating under this CP shall be considered as part of the agreement between the CA and the subscribers.

**9.16.2 Assignment**

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

**9.16.3 Severability**

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

**9.16.4 Enforcement**

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

**9.16.5 Force Majeure**

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

**9.17 Other Provisions**

Not Applicable.

