Digital Certificate Interoperability Guideline
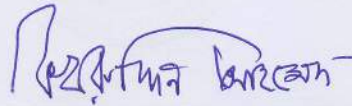
Document Title	Digital Certificate Interoperability Guideline
Document Type	Public
Author	
Reviewer Version	1.1
Revision Date	16 November 2020
Note	49
Status	Published

Signature

Office of the Controller of Certifying Authorities
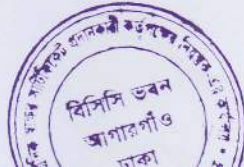### Ministry of Information & Communication Technology
Government of Bangladesh

Document Control

Document Title	Digital Certificate Interoperability Guideline
Document Type	Public
Version	1.4
Previous Version	1.3
Revision Date	18 November 2013
Pages	49
Status	Published

Signature:

(Golam Fakhruddin Ahmed Chowdhury)
Controller of Certifying Authorities

Purpose of Revision

For smooth operation among CAs Office of the CCA made some modification in the Interoperability Guideline. The modification is made after getting Object Identifier (OID) for Bangladesh PKI. The revision is made on the following clauses:

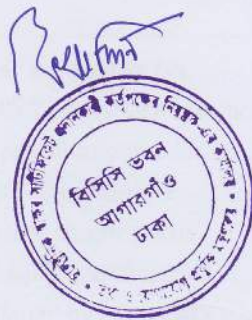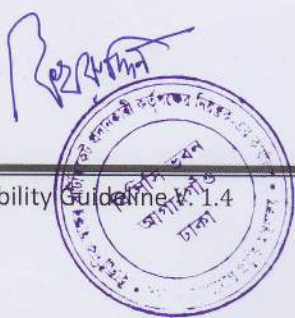| Sl.	Clause	Modification
1.	3.1.2 Certificate Extension Field Row 6 (certificatePolicies)	For Root Certificate this field is made "Optional" instead of "Mandatory"
2.	3.1.2 Certificate Extension Field Row 14 (cRLDistributionPoints)	For Root Certificate this field is made "Optional" instead of "Mandatory" since Currently Root CA will not use any CRL for its own certificate
3.	3.2.2 Certificate Extension Field Row 14 (cRLDistributionPoints)	CA certificate shall use CRL of CCA as the CRL distribution point in their certificate.
4.	3.3.2 Certificate Extension Field Row 6 (certificatePolicies)	OID value notified in CCA website shall be used for identifying certificate
5.	3.4.1 Common EE Profile -> Certificate Extension Field Row 6 (certificatePolicies)	Depending on the Class of certificate CA shall assign corresponding OID value notified in CCA website
6.	G Appendix I- Convention & Specification -> 1. Naming Convention	Common Name (CN) shall be in the format given there.
7.	G Appendix I- Convention & Specification -> 3, 4 and 5	Common Name (CN) shall be in the format as given.

Table of Contents

A. Reference

[1] RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

[2] Asia PKI Interoperability Guideline (Version 2.0, Draft) Book 1; Asia PKI Forum Interoperability Working Group (IOWG), March, 2005

[3] Asia PKI Interoperability Guideline (Version 2.0, Draft) Book 2; Asia PKI Forum Interoperability Working Group (IOWG), March, 2005

[4] John Linn, RSA Laboratories: Trust Models and Management in Public-Key Infrastructures, 6 November 2000
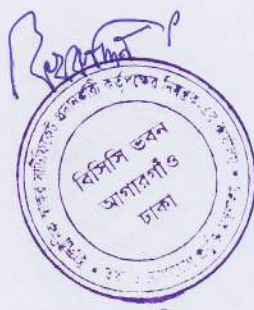
B. Introduction

It becomes important to establish a PKI framework for Bangladesh in order to perform a secure e-business and e-transactions not only inside country but also around the globe. However, as it is found in other countries that if interoperability issues of digital certificates among different CAs are not focused in early phase of CA operations in a country, it becomes costly to adopt revised standard at later phase of operation.

The trust model of the PKI is based on the trust on CA. The CA issues certificate to end entities (EE). Henceforth, EE of other CA needs that these CAs needs smooth interoperable operation, and the certificates issued by those CAs have to be trusted by each other. In order to achieve this interoperable situation, CAs have to agree to accept common specification, harmonize their certificate profiles to each other. This document provides a recommended profile for this interoperability.

Based on **RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile** and Asia PKI Forum Interoperability Guideline, this document is prepared to reduce interoperability issues among Bangladeshi CAs. It is recomended to all Licensed CAs to follow the instruc ons of this guideline.

C. Document Structure

The document is structured in a way so that CAs or relying parties can easily understand and create profile for different type of certificates. This document describes the different PKI model available in the globe, the Bangladesh PKI Model, definition of different certificate fields as per RFC 5280, specification of different certificates and its fields.

D. Scope

This guideline is applicable to all licensed CAs including Root CA, Bangladesh. While initiating and implementing CA operations, CAs are recommended to follow the instructions illustrated in this guideline for issuing digital certificates and CRLs. This guideline is issued by the Controller of Certifying Authorities as per the supremacy specified in Section 89 of the ICT Act 2006 (amended in 2009) to ensure interoperability among licensed CAs. Instructions of this guideline shall be interpreted along with the existing Act, Rules and Guidelines. Incase of any inconsistency with any existing Rules, Guideline or Notification this guideline shall be interpreted as final unless otherwise clarified.

E. PKI Trust Model

There are various PKI Models available in the globe. Those are:

1. Hierarchy Model
2. Cross-Certification Model
3. Cross-Recognition Model
4. Bridge Model
5. Certificate Trust List Model

1. Hierarchy Model

In hierarchical PKI model, there's a trusted root CA which issue certificates only to accredited CAs. The accredited CAs may issue certificates to subordinate CAs and/or end users and/or other relying parties.
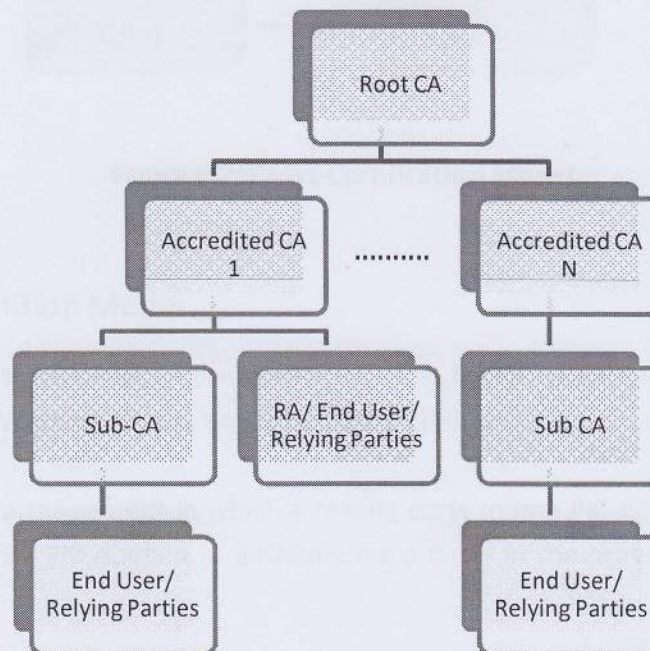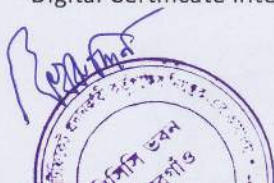

Figure E.1: Hierarchical Model

2. Cross-Certification Model

In Cross-certification, instead of a hierarchy, CAs deal with each other as peers and choose whether or not to trust each other. In this model CAs issue cross certificates to each other to trust each others' end user certificate.

This model is also known as Mesh model. This model is apt in situation where organizations are not in hierarchy structure. Path construction in this model is significantly complicated than hierarchical model. In cross-certification model one CA issues cross certificate to another CA, the certificate contains a CA signature key used for issuing certificates.
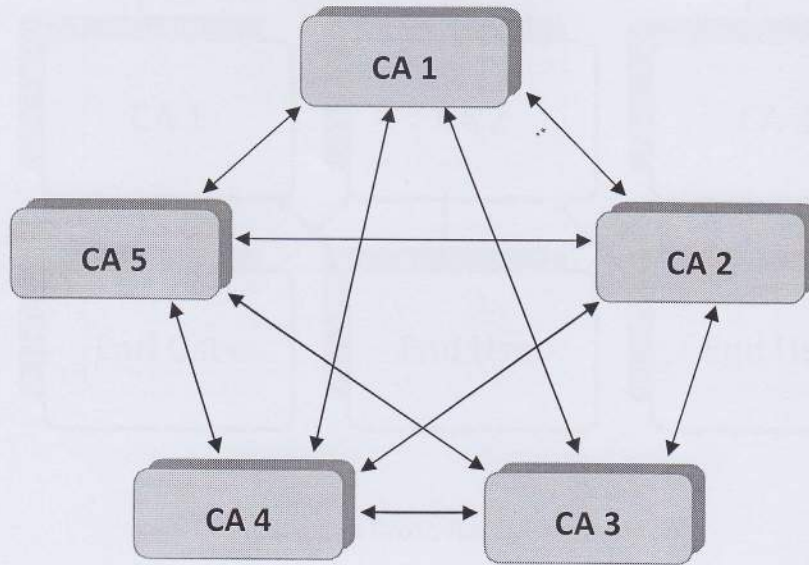
Figure E.2: Cross-Certification Model

3. Cross-Recognition Model

Cross Recognition is a concept considered by Asia Pacific Economic Cooperation (APEC) Telecommunication Working Group, and is defined as follows:

"An interoperability arrangement in which a relying party in one PKI domain can use authority information in another PKI domain to authenticate a party in the other PKI domain, and vice-versa."

In practice, cross-recognition means that certificates issued in a domain that has been recognised may be relied upon with some confidence by relying parties in the recognising domain. Cross-recognition differs from cross-certification in several respects. For example, there is no mutual (or even unilateral) recognition between CAs. Cross-recognition is based on the belief that independent CAs would be licensed or audited by a mutually recognised trusted authority known as trusted coordinating authority.
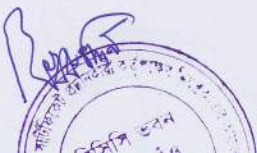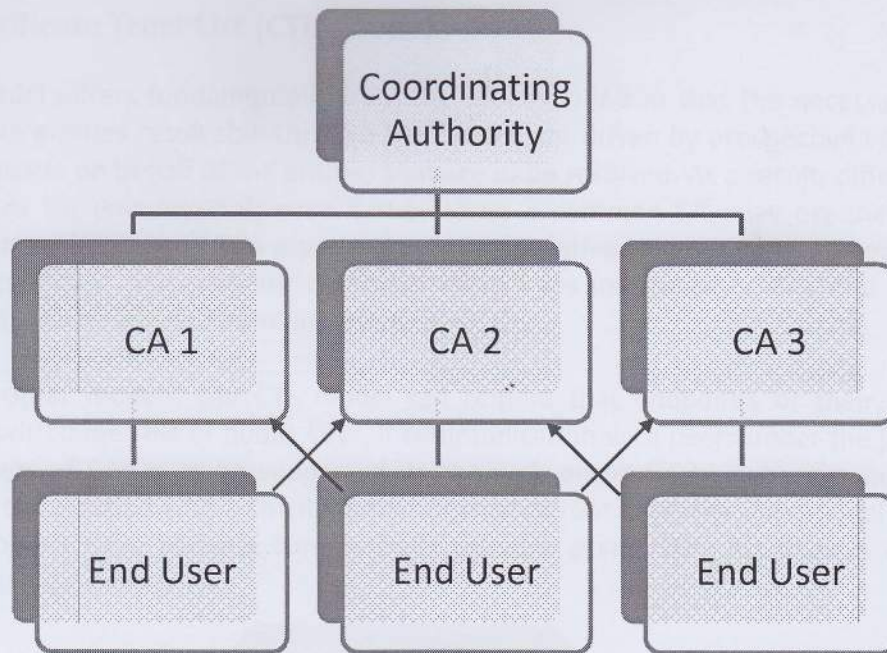
Figure E.3: Cross-Recognition Model

4. Bridge Model

The Bridge CA model embodies a central cross-certification authority, whose purpose is to provide cross-certificates rather than acting as the root of certification paths. Within the Bridge CA model, a participant is preconfigured with the public key of its local CA to act as a trust anchor; configured knowledge of the Bridge CA's own public key is not required.
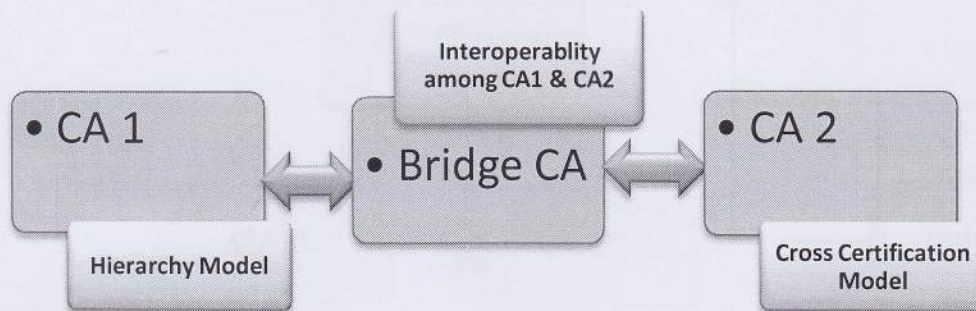
Figure E.4: Bridge Model

This model combines aspects of both the root model and the cross-certification model. In this model the bridge CA is responsible for providing interoperability among CAs. PKI of different models can be joined together into a single interoperable network using the bridge model.
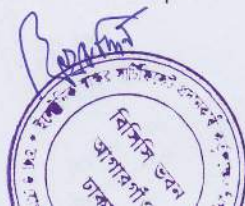
5.   Certificate Trust List (CTL) Model

The CTL model differs fundamentally from the other models in that the necessary actions to make remote entities resolvable through trust paths are driven by prospective verifiers rather than being made on behalf of the entities that are to be resolved. As a result, different verifiers within a trust list environment, even if they share a common CA, may experience different results when seeking to validate a particular entity. Relative to cross-certified approaches, use of trust lists moves management overhead away from intermediary CAs and towards end systems and their associated administrators.

Unlike the other models, the CTL model can require that endpoints or their delegates be configured with large sets of public keys, if communication with peers under the jurisdiction of large numbers of CAs is to be supported. In the web environment, where huge numbers of browsers are preloaded with a small number of trusted root keys, the operational franchises of root key holders have become commercially valuable assets. The list itself is electronically signed to ensure its integrity.
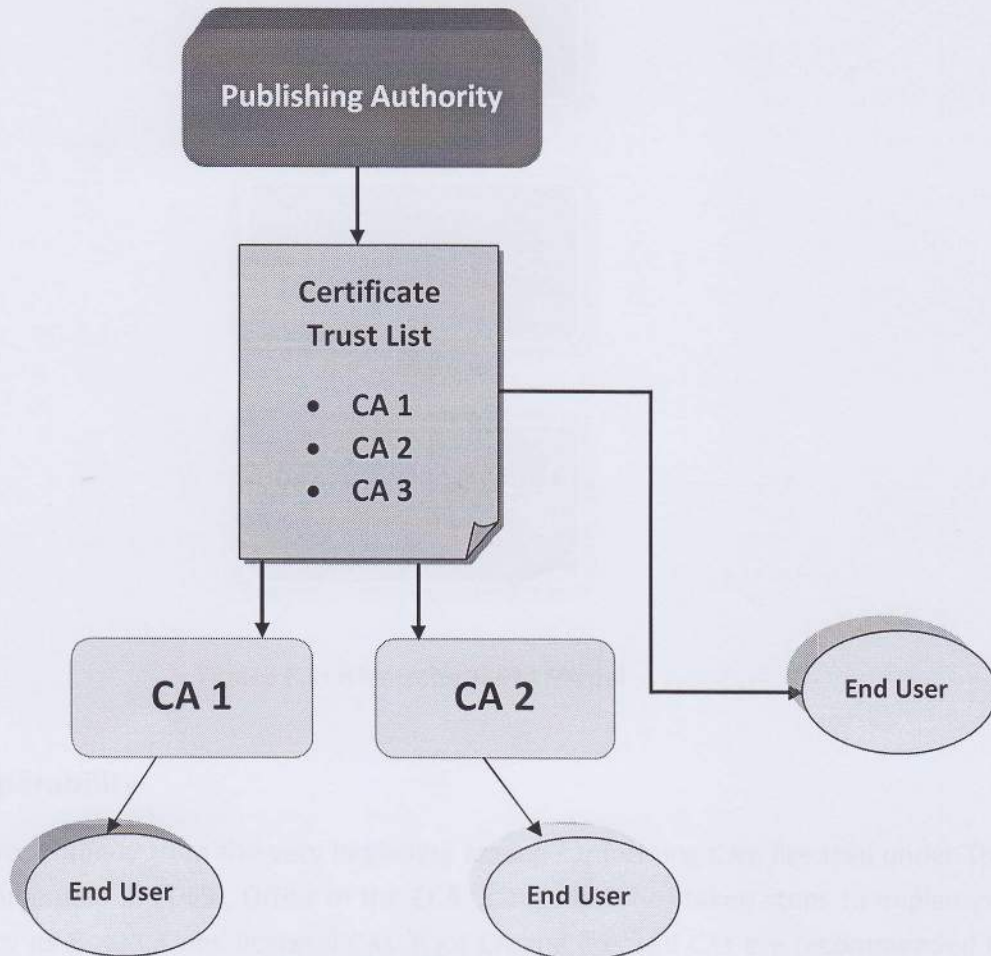
Figure E.5: CTL Model
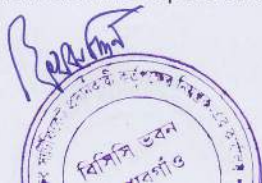
F.   Bangladesh PKI

1. Trust Model

ICT Act 2006 (amended in 2009) and IT (CA) Rules 2010 refers the hierarchical PKI model for Bangladesh. Hierarchical PKI model is simple to implement and strongly interoperable. Office of the CCA will act as the Root CA in the hierarchy. Bangladesh Root CA will certify the licensed CAs which in turns will certify the descendants of licensed CAs. Within this model, each participant must have knowledge of the root CA's public key, which forms the fundamental trust anchor for all participants. Root CA will be remain off-line, contributing to reduced compromise potential for its private key.

```
┌─────────────────────┐
│     Root CA         │
│   Bangladesh        │
└─────────────────────┘
          │
          ▼
┌─────────────────────┐
│    Licensed CAs     │
└─────────────────────┘
          │
          ▼
┌─────────────────────┐
│   Relying Parties/  │
│     End User        │
└─────────────────────┘
```

Figure F.1: Hierarchical PKI Model

2. Interoperability

To ensure interoperability from the very beginning among conforming CAs, licensed under The ICT Act 2006 (amended in 2009), Office of the CCA, Bangladesh has taken steps to implement this guideline by its Root CA and licensed CAs. Root CA and licensed CAs are recommended to follow the profile mentioned in this guideline. Before defining the profile value to ensure interoperability, it is better to have understanding on each field of Certificate and CRL.
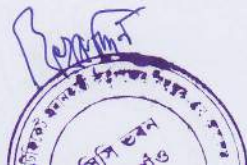
2.1. Certificate Basic Fields

tbsCertificate

The field contains the names of the subject and issuer, a public key associated with the subject, a validity period, and other associated information. The tbsCertificate usually includes extensions. Every TBSCertificate contains the names of the subject and issuer, a public key associated with the subject, a validity period, a version number, and a serial number; some MAY contain optional unique identifier fields.

signatureAlgorithm

The signatureAlgorithm field contains the identifier for the cryptographic algorithm used by the CA to sign this certificate. The algorithm identifier is used to identify a cryptographic algorithm. The OBJECT IDENTIFIER component identifies the algorithm. This field MUST contain the same algorithm identifier as the signature field in the sequence tbsCertificate.

signatureValue

The signatureValue field contains a digital signature computed upon the ASN.1 DER encoded tbsCertificate. This signature value is encoded as a BIT STRING and included in the signature field. By generating this signature, a CA certifies the validity of the information in the tbsCertificate field.

Version

This field describes the version of the encoded certificate. When extensions are used, as expected in this profile, version MUST be 3 (value is 2). If no extensions are present, but a UniqueIdentifier is present, the version SHOULD be 2 (value is 1); however, the version MAY be 3.

Serial Number

The serial number MUST be a positive integer assigned by the CA to each certificate. It MUST be unique for each certificate issued by a given CA (i.e., the issuer name and serial number identify a unique certificate). CAs MUST force the serialNumber to be a non-negative integer. Certificate users MUST be able to handle serialNumber values up to 20 octets. Conforming CAs MUST NOT use serialNumber values longer than 20 octets.

Signature

This field contains the algorithm identifier for the algorithm used by the CA to sign the certificate. This field MUST contain the same algorithm identifier as the signatureAlgorithm field.
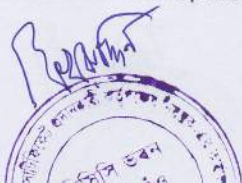
Issuer

The issuer field identifies the entity that has signed and issued the certificate. The issuer field MUST contain a non-empty distinguished name (DN). The Name describes a hierarchical name composed of attributes, such as country name, and corresponding values, such as US. CAs conforming to this profile MUST use either the PrintableString or UTF8String encoding of DirectoryString, with two exceptions.

Standard sets of attributes have been defined in the X.500 series of specifications [X.520]. Implementations of this specification MUST be prepared to receive the following standard attribute types in issuer and subject names:

- country,
- organization,
- organizational unit,
- distinguished name qualifier,
- state or province name,
- common name (e.g., "Susan Housley"), and
- serial number.

In addition, implementations of this specification SHOULD be prepared to receive the following standard attribute types in issuer and subject names:

- locality,
- title,
- surname,
- given name,
- initials,
- pseudonym, and
- generation qualifier (e.g., "Jr.", "3rd", or "IV").

Certificate users MUST be prepared to process the issuer distinguished name and subject distinguished name fields to perform name chaining for certification path validation. Name chaining is performed by matching the issuer distinguished name in one certificate with the subject name in a CA certificate.

Validity

The certificate validity period is the time interval during which the CA warrants that it will maintain information about the status of the certificate.

The field is represented as a SEQUENCE of two dates:

the date on which the certificate validity period begins (notBefore) and the date on which the certificate validity period ends (notAfter). The validity period for a certificate is the period of time from notBefore through notAfter.

In some situations, devices are given certificates for which no good expiration date can be assigned. For example, a device could be issued a certificate that binds its model and serial number to its public key; such a certificate is intended to be used for the entire lifetime of the device.

UTCTime

The universal time type, UTCTime, is a standard ASN.1 type intended for representation of dates and time. UTCTime specifies the year through the two low-order digits and time is specified to the precision of one minute or one second. UTCTime includes either Z (for Zulu, or Greenwich Mean Time) or a time differential. UTCTime values MUST be expressed in Greenwich Mean Time (Zulu) and MUST include seconds (i.e., times are YYMMDDHHMMSSZ), even where the number of seconds is zero.

GeneralizedTime

The generalized time type, GeneralizedTime, is a standard ASN.1 type for variable precision representation of time. GeneralizedTime values MUST be expressed in Greenwich Mean Time (Zulu) and MUST include seconds (i.e., times are YYYYMMDDHHMMSSZ), even where the number of seconds is zero. GeneralizedTime values MUST NOT include fractional seconds.

Subject

The subject field identifies the entity associated with the public key stored in the subject public key field. If the subject is a CA, then the subject field MUST be populated with a non-empty distinguished name matching the contents of the issuer field in all certificates issued by the subject CA. If the subject is a CRL issuer, then the subject field MUST be populated with a non-empty distinguished name matching the contents of the issuer field in all CRLs issued by the subject CRL issuer. A CA MAY issue more than one certificate with the same DN to the same subject entity. The subject field is defined as the X.501 type Name. The syntax and associated object identifiers (OIDs) for these attribute types are provided in the ASN.1 modules in Appendix A.

When encoding attribute values of type DirectoryString, conforming CAs MUST use PrintableString or UTF8String encoding, with the following exceptions:

- When the subject of the certificate is a CA, the subject field MUST be encoded in the same way as it is encoded in the issuer field in all certificates issued by the subject CA.
- When the subject of the certificate is a CRL issuer, the subject field MUST be encoded in the same way as it is encoded in the issuer field in all CRLs issued by the subject CRL issuer.
- TeletexString, BMPString, and UniversalString are included for backward compatibility, and SHOULD NOT be used for certificates for new subjects.

Subject Public Key Info

This field is used to carry the public key and identify the algorithm with which the key is used (e.g., RSA, DSA, or Diffie-Hellman). The algorithm is identified using the AlgorithmIdentifier structure.

Unique Identifiers

These fields MUST only appear if the version is 2 or 3. The subject and issuer unique identifiers are present in the certificate to handle the possibility of reuse of subject and/or issuer names over time.

Extensions

This field MUST only appear if the version is 3.

2.2. Certificate Extensions

The extensions defined for X.509 v3 certificates provide methods for associating additional attributes with users or public keys and for managing relationships between CAs. The X.509 v3 certificate format also allows communities to define private extensions to carry information unique to those communities. Each extension in a certificate is designated as either critical or non-critical. A certificate-using system MUST reject the certificate if it encounters a critical extension it does not recognize or a critical extension that contains information that it cannot process. A non-critical extension MAY be ignored if it is not recognized, but MUST be processed if it is recognized. Each extension includes an OID and an ASN.1 structure. When an extension appears in a certificate, the OID appears as the field extnID and the corresponding ASN.1 DER encoded structure is the value of the octet string extnValue. A certificate MUST NOT include more than one instance of a particular extension.

Conforming CAs MUST support key identifiers, basic constraints, key usage, and certificate policies extensions.

At a minimum, applications conforming to this profile MUST recognize the following extensions: key usage, certificate policies, subject alternative name, basic constraints, name constraints, policy constraints, extended key usage, and inhibit anyPolicy.

2.2.1 Standard Extension

Authority Key Identifier

The authority key identifier extension provides a means of identifying the public key corresponding to the private key used to sign a certificate. The identification MAY be based on either the key identifier (the subject key identifier in the issuer's certificate) or the issuer name and serial number.

Subject Key Identifier
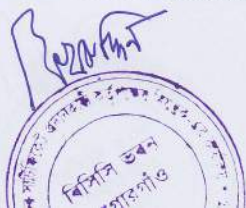
The subject key identifier extension provides a means of identifying certificates that contain a particular public key. To facilitate certification path construction, this extension MUST appear in all conforming CA certificates, that is, all certificates including the basic constraints extension (Section 4.2.1.9) where the value of cA is TRUE. In conforming CA certificates, the value of the subject key identifier MUST be the value placed in the key identifier field of the authority key identifier extension (Section 4.2.1.1) of certificates issued by the subject of this certificate. Applications are not required to verify that key identifiers match when performing certification path validation. For CA certificates, subject key identifiers SHOULD be derived from the public key or a method that generates unique values.

Key Usage

The key usage extension defines the purpose (e.g., encipherment, signature, certificate signing) of the key contained in the certificate. The usage restriction might be employed when a key that could be used for more than one operation is to be restricted.

```
KeyUsage ::= BIT STRING {
        digitalSignature (0),
        nonRepudiation (1), -- recent editions of X.509 have
        -- renamed this bit to contentCommitment
        keyEncipherment (2),
        dataEncipherment (3),
        keyAgreement (4),
        keyCertSign (5),
        cRLSign (6),
        encipherOnly (7),
        decipherOnly (8) }
```

Certificate Policies

The certificate policies extension contains a sequence of one or more policy information terms, each of which consists of an object identifier (OID) and optional qualifiers. Optional qualifiers, which MAY be present, are not expected to change the definition of the policy. A certificate policy OID MUST NOT appear more than once in a certificate policies extension.

Policy Mappings

This extension is used in CA certificates. It lists one or more pairs of OIDs; each pair includes an issuerDomainPolicy and a subjectDomainPolicy. The pairing indicates the issuing CA considers its issuerDomainPolicy equivalent to the subject CA's subjectDomainPolicy.

The policy mapping defines the list of policies associated with the subject CA that may be accepted as comparable to the issuerDomainPolicy.

Subject Alternative Name
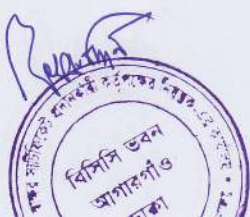
The subject alternative name extension allows identities to be bound to the subject of the certificate. These identities may be included in addition to or in place of the identity in the subject field of the certificate. Defined options include an Internet electronic mail address, a DNS name, an IP address, and a Uniform Resource Identifier (URI). Other options exist, including completely local definitions. Multiple name forms, and multiple instances of each name form, MAY be included.

Because the subject alternative name is considered to be definitively bound to the public key, all parts of the subject alternative name MUST be verified by the CA.

If the subject field contains an empty sequence, then the issuing CA MUST include a subjectAltName extension that is marked as critical. When including the subjectAltName extension in a certificate that has a non-empty subject distinguished name, conforming CAs SHOULD mark the subjectAltName extension as non-critical.

Issuer Alternative Name

This extension is used to associate Internet style identities with the certificate issuer. Issuer alternative names are not processed as part of the certification path validation algorithm. (That is, issuer alternative names are not used in name chaining and name constraints are not enforced.). Where present, conforming CAs SHOULD mark this extension as noncritical.

Subject Directory Attributes

The subject directory attributes extension is used to convey identification attributes (e.g., nationality) of the subject. The extension is defined as a sequence of one or more attributes. Conforming CAs MUST mark this extension as non-critical.

Basic Constraints

The basic constraints extension identifies whether the subject of the certificate is a CA and the maximum depth of valid certification paths that include this certificate.

Conforming CAs MUST include this extension in all CA certificates that contain public keys used to validate digital signatures on certificates and MUST mark the extension as critical in such certificates. This extension MAY appear as a critical or noncritical extension in CA certificates that contain public keys used exclusively for purposes other than validating digital signatures on certificates.

```
BasicConstraints ::= SEQUENCE {
cA                   BOOLEAN DEFAULT FALSE,
pathLenConstraint    INTEGER (0..MAX) OPTIONAL }
```

Name Constraints

The name constraints extension, which MUST be used only in a CA certificate, indicates a name space within which all subject names in subsequent certificates in a certification path MUST be located. Restrictions apply to the subject distinguished name and apply to subject alternative names. Restrictions apply only when the specified name form is present. If no name of the type is in the certificate, the certificate is acceptable.

Name constraints are not applied to self-issued certificates (unless the certificate is the final certificate in the path).

Conforming CAs MUST mark this extension as critical and SHOULD NOT impose name constraints on the x400Address, ediPartyName, or registeredID name forms. Conforming CAs MUST NOT issue certificates where name constraints is an empty sequence.

Policy Constraints

The policy constraints extension can be used in certificates issued to CAs. The policy constraints extension constrains path validation in two ways. It can be used to prohibit policy mapping or require that each certificate in a path contain an acceptable policy identifier.

If the inhibitPolicyMapping field is present, the value indicates the number of additional certificates that may appear in the path before policy mapping is no longer permitted.

Conforming CAs MUST NOT issue certificates where policy constraints is an empty sequence. Conforming CAs MUST mark this extension as critical.

Extended Key Usage

This extension indicates one or more purposes for which the certified public key may be used, in addition to or in place of the basic purposes indicated in the key usage extension. In general, this extension will appear only in end entity certificates.

Key purposes may be defined by any organization with a need. Object identifiers used to identify key purposes MUST be assigned in accordance with IANA or ITU-T Recommendation.

This extension MAY, at the option of the certificate issuer, be either critical or non-critical.

CRL Distribution Points

The CRL distribution points extension identifies how CRL information is obtained. The extension SHOULD be non-critical, but this profile RECOMMENDS support for this extension by CAs and applications.

The cRLDistributionPoints extension is a SEQUENCE of DistributionPoint. A DistributionPoint consists of three fields, each of which is optional: distributionPoint, reasons, and cRLIssuer.

Inhibit anyPolicy

The inhibit anyPolicy extension can be used in certificates issued to CAs. The inhibit anyPolicy extension indicates that the special anyPolicy OID, with the value { 2 5 29 32 0 }, is not considered an explicit match for other certificate policies except when it appears in an intermediate self-issued CA certificate. The value indicates the number of additional non-self-issued certificates that may appear in the path before anyPolicy is no longer permitted. For example, a value of one indicates that anyPolicy may be processed in certificates issued by the subject of this certificate, but not in additional certificates in the path. Conforming CAs MUST mark this extension as critical.

Freshest CRL (Delta CRL Distribution Point)

The freshest CRL extension identifies how delta CRL information is obtained. The extension MUST be marked as non-critical by conforming CAs.

2.2.2 Private Internet Extensions

This section defines two extensions for use in the Internet Public Key Infrastructure. These extensions may be used to direct applications to on-line information about the issuer or the subject. Each extension contains a sequence of access methods and access locations. The access method is an object identifier that indicates the type of information that is available. The access location is a GeneralName that implicitly specifies the location and format of the information and the method for obtaining the information.

Authority Information Access

The authority information access extension indicates how to access information and services for the issuer of the certificate in which the extension appears. Information and services may include on-line validation services and CA policy data. (The location of CRLs is not specified in this extension; that information is provided by the cRLDistributionPoints extension.) This extension may be included in end entity or CA certificates. Conforming CAs MUST mark this extension as non-critical.

Subject Information Access

The subject information access extension indicates how to access information and services for the subject of the certificate in which the extension appears. When the subject is a CA, information and services may include certificate validation services and CA policy data. When the subject is an end entity, the information describes the type of services offered and how to access them.

2.3.   CRL Fields

2.3.1 CertificateList Fields

The CertificateList is a SEQUENCE of three required fields. The fields are described in detail in the following subsections.
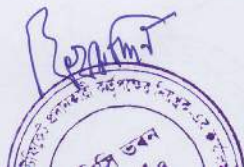
tbsCertList

The first field in the sequence is the tbsCertList. This field is itself a sequence containing the name of the issuer, issue date, issue date of the next list, the optional list of revoked certificates, and optional CRL extensions. When there are no revoked certificates, the revoked certificates list is absent. When one or more certificates are revoked, each entry on the revoked certificate list is defined by a sequence of user certificate serial number, revocation date, and optional CRL entry extensions.

signatureAlgorithm

The signatureAlgorithm field contains the algorithm identifier for the algorithm used by the CRL issuer to sign the CertificateList. The field is of type AlgorithmIdentifier. [RFC3279], [RFC4055], and [RFC4491] list supported algorithms for this specification, but other signature algorithms MAY also be supported. This field MUST contain the same algorithm identifier as the signature field in the sequence tbsCertList.

signatureValue

The signatureValue field contains a digital signature computed upon the ASN.1 DER encoded tbsCertList. The ASN.1 DER encoded tbsCertList is used as the input to the signature function. This signature value is encoded as a BIT STRING and included in the CRL signatureValue field. The details of this process are specified for each of the supported algorithms in [RFC3279], [RFC4055], and [RFC4491].

CAs that are also CRL issuers MAY use one private key to digitally sign certificates and CRLs. Applications that perform CRL checking MUST support certification path validation when certificates and CRLs are digitally signed with the same CA private key.

2.3.2 Certificate List "To Be Signed"

The certificate list to be signed, or TBSCertList, is a sequence of required and optional fields. The required fields identify the CRL issuer, the algorithm used to sign the CRL, and the date and time the CRL was issued. This profile requires conforming CRL issuers to include the nextUpdate field and the CRL number and authority key identifier CRL extensions in all CRLs issued.

Version

This optional field describes the version of the encoded CRL. When extensions are used, as required by this profile, this field MUST be present and MUST specify version 2 (the integer value is 1).

Signature

This field contains the algorithm identifier for the algorithm used to sign the CRL. [RFC3279], [RFC4055], and [RFC4491] list OIDs for the most popular signature algorithms used in the Internet PKI. This field MUST contain the same algorithm identifier as the signatureAlgorithm field in the sequence CertificateList.

This Update
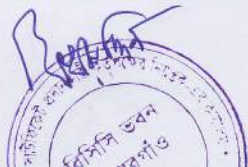
This field indicates the issue date of this CRL. thisUpdate may be encoded as UTCTime or GeneralizedTime. CRL issuers conforming to this profile MUST encode thisUpdate as UTCTime for dates through the year 2049. CRL issuers conforming to this profile MUST encode thisUpdate as GeneralizedTime for dates in the year 2050 or later. Conforming applications MUST be able to process dates that are encoded in either UTCTime or GeneralizedTime.

Next Update

This field indicates the date by which the next CRL will be issued. The next CRL could be issued before the indicated date, but it will not be issued any later than the indicated date. CRL issuers SHOULD issue CRLs with a nextUpdate time equal to or later than all previous CRLs. nextUpdate may be encoded as UTCTime or GeneralizedTime. Conforming CRL issuers MUST include the nextUpdate field in all CRLs.

Revoked Certificates

When there are no revoked certificates, the revoked certificates list MUST be absent. Otherwise, revoked certificates are listed by their serial numbers. Certificates revoked by the CA are uniquely identified by the certificate serial number.

Extensions

This field may only appear if the version is 2. If present, this field is a sequence of one or more CRL extensions.

2.4. CRL Extensions

Authority Key Identifier

The authority key identifier extension provides a means of identifying the public key corresponding to the private key used to sign a CRL. The identification can be based on either the key identifier (the subject key identifier in the CRL signer's certificate) or the issuer name and serial number. This extension is especially useful where an issuer has more than one signing key, either due to multiple concurrent key pairs or due to changeover. Conforming CRL issuers MUST use the key identifier method, and MUST include this extension in all CRLs issued.

Issuer Alternative Name

The issuer alternative name extension allows additional identities to be associated with the issuer of the CRL. Defined options include an electronic mail address (rfc822Name), a DNS name, an IP address, and a URI. Multiple instances of a name form and multiple name forms may be included. Whenever such identities are used, the issuer alternative name extension MUST be used. Conforming CRL issuers SHOULD mark the issuerAltName extension as non-critical.

CRL Number

The CRL number is a non-critical CRL extension that conveys a monotonically increasing sequence number for a given CRL scope and CRL issuer. This extension allows users to easily determine when a particular CRL supersedes another CRL. CRL numbers also support the
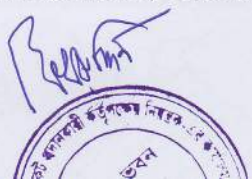
identification of complementary complete CRLs and delta CRLs. CRL issuers conforming to this profile MUST include this extension in all CRLs and MUST mark this extension as non-critical.

If a CRL issuer generates delta CRLs in addition to complete CRLs for a given scope, the complete CRLs and delta CRLs MUST share one numbering sequence.

Delta CRL Indicator

The delta CRL indicator is a critical CRL extension that identifies a CRL as being a delta CRL. Delta CRLs contain updates to revocation information previously distributed, rather than all the information that would appear in a complete CRL. The use of delta CRLs can significantly reduce network load and processing time in some environments. Delta CRLs are generally smaller than the CRLs they update, so applications that obtain delta CRLs consume less network bandwidth than applications that obtain the corresponding complete CRLs. Applications that store revocation information in a format other than the CRL structure can add new revocation information to the local database without reprocessing information.

When a conforming CRL issuer generates a delta CRL, the delta CRL MUST include a critical delta CRL indicator extension. When a delta CRL is issued, it MUST cover the same set of reasons and the same set of certificates that were covered by the base CRL it references. A complete CRL and a delta CRL MAY be combined if the following four conditions are satisfied:

a) The complete CRL and delta CRL have the same issuer.
b) The complete CRL and delta CRL have the same scope. The two CRLs have the same scope if either of the following conditions are met:
   1) The issuingDistributionPoint extension is omitted from both the complete CRL and the delta CRL.
   2) The issuingDistributionPoint extension is present in both the complete CRL and the delta CRL, and the values for each of the fields in the extensions are the same in both CRLs.
c) The CRL number of the complete CRL is equal to or greater than the BaseCRLNumber specified in the delta CRL. That is, the complete CRL contains (at a minimum) all the revocation information held by the referenced base CRL.
d) The CRL number of the complete CRL is less than the CRL number of the delta CRL. That is, the delta CRL follows the complete CRL in the numbering sequence.

Issuing Distribution Point

The issuing distribution point is a critical CRL extension that identifies the CRL distribution point and scope for a particular CRL, and it indicates whether the CRL covers revocation for end entity certificates only, CA certificates only, attribute certificates only, or a limited set of reason codes. Although the extension is critical, conforming implementations are not required to support this extension. However, implementations that do not support this extension MUST either treat the status of any certificate not listed on this CRL as unknown or locate another CRL that does not contain any unrecognized critical extensions. If the distributionPoint field is absent, the CRL
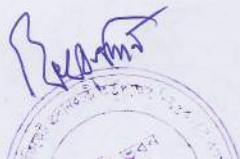
MUST contain entries for all revoked unexpired certificates issued by the CRL issuer, if any, within the scope of the CRL. Conforming CRLs issuers MUST NOT issue CRLs where the DER encoding of the issuing distribution point extension is an empty sequence.

Authority Information Access

This section defines the use of the Authority Information Access extension in a CRL. The syntax and semantics defined in Section 4.2.2.1 for the certificate extension are also used for the CRL extension. This CRL extension MUST be marked as non-critical.

Reason Code

The reasonCode is a non-critical CRL entry extension that identifies the reason for the certificate revocation. CRL issuers are strongly encouraged to include meaningful reason codes in CRL entries; however, the reason code CRL entry extension SHOULD be absent instead of using the unspecified (0) reasonCode value.

Invalidity Date

The invalidity date is a non-critical CRL entry extension that provides the date on which it is known or suspected that the private key was compromised or that the certificate otherwise became invalid. This date may be earlier than the revocation date in the CRL entry, which is the date at which the CA processed the revocation. When a revocation is first posted by a CRL issuer in a CRL, the invalidity date may precede the date of issue of earlier CRLs, but the revocation date SHOULD NOT precede the date of issue of earlier CRLs. Whenever this information is available, CRL issuers are strongly encouraged to share it with CRL users.

Certificate Issuer

This CRL entry extension identifies the certificate issuer associated with an entry in an indirect CRL, that is, a CRL that has the indirectCRL indicator set in its issuing distribution point extension. When present, the certificate issuer CRL entry extension includes one or more names from the issuer field and/or issuer alternative name extension of the certificate that corresponds to the CRL entry. If this extension is not present on the first entry in an indirect CRL, the certificate issuer defaults to the CRL issuer.

Conforming CRL issuers MUST include in this extension the distinguished name (DN) from the issuer field of the certificate that corresponds to this CRL entry. The encoding of the DN MUST be identical to the encoding used in the certificate. CRL issuers MUST mark this extension as critical since an implementation that ignored this extension could not correctly attribute CRL entries to certificates. This specification RECOMMENDS that implementations recognize this extension.

3. Certificate Profile

There are various types of certificate. For Bangladesh PKI, those are mainly: Root CA Certificate, CA Certificates, and End Entity Certificates. Before defining each certificate profile, the Guideline specifies the format of the digital certificate and classifies each of the fields/extensions as follows:
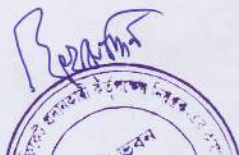
Mandatory – These fields or extensions are mandated by the CCA and MUST be present in the certificates issued by the Certifying Authorities. Additionally the content of the fields MUST be as per the guidance provided in this document.

Optional – The CA may use this field at its discretion. However, in case the field is being used, the applicable guidance or the compliance standards specified MUST be adhered to.

Special Purpose – These fields may be used only in certain circumstances. In all such cases, additional guidance will be provided by the CCA Customizable – Customizable fields are non standard extensions notified by CCA which may have interpretations depending upon usage / application / industry.

Not used – These fields or extensions are NOT to be included or used in Digital Certificates unless notified by CCA regarding the usage and format.

Reserved for Future Use – These extensions are reserved by CCA for use in the future and additional guidance is expected from CCA before these can be utilized in the Digital Certificates. Until such time CA MUST NOT use these fields / extensions.

The following specification also provides guidance on other important aspects of the field including the length, data type and mandated values. The certifying authorities must issue certificates in accordance with the guidance provided in this documents.

3.1. Root CA Certificate Profile

The ROOT CA's self-signed certificate is used for signing subordinate CA certificates and cross certificate. The ROOT CA certificate will be used to provide the public key of the trust anchor and the initial information of the certificate path processing.

3.1.1 Basic Fields

SL	FIELD	NOTE
1.	version (Mandatory)	Since extension field appears in this profile, the value MUST be set to 2 (v3).
2.	serialNumber (Mandatory)	Unique integer. Up to 20 octets.
3.	Signature (Mandatory)	1.2.840.113549.1.1.11 SHA256 with RSA Encryption
4.	issuer (Mandatory)	X.500 DN. For details about attribute values, see Appendix-G on page 39
5.	Validity (Mandatory)	UTCTIME
6.	subject (Mandatory)	X.500 DN. And see issuer. for Root CA subject and issuer is same
7.	subjectPublicKeyInfo (Mandatory)	1.2.840.113549.1.1.1 (rsaEncryption) For Root CA: 2,048 bit
8.	issuerUniqueID	

SL	FIELD	NOTE
	(not used)	
9.	subjectUniqueID (not used)	
10.	SignatureAlgorithm (mandatory)	1.2.840.113549.1.1.11 SHA256 with RSA Encryption
11.	signatureValue (Mandatory)	Encoded as Bit string Must contain the signature in accordance with the algorithm. For RSA, this is the value generated by hashing the certificate, then padding, and then performing the RSA private key operation.

3.1.2 Certificate Extension Field

SL	FIELD	NOTE
1.	authorityKeyIdentifier (Mandatory, non-critical)	**keyIdentifier (Mandatory):** The hash value of Issuer's public key. **authorityCertIssuer (optional):** DN **authCertSerialNumber (optional):** INTEGER When AuthCertIssuer is used, AuthCertSerialNum must be set as well and vice versa.
2.	subjectKeyIdentifier (Mandatory, non-critical)	For Root Certificate it'll be the hash value of subject/issuer public key, since subject & issuer is same for Root certificate. The keyIdentifier is composed of the 160-bit SHA-1 hash of the value of the BIT STRING subjectPublicKey (excluding the tag, length, and number of unused bits).
3.	keyUsage (Mandatory, critical)	For CA Certificates, the following key usage MUST be asserted ⅄ cRLSign ⅄ keyCertsign
4.	extKeyUsage (not used)	
5.	privateKeyUsagePeriod (not used)	
6.	certificatePolicies (Optional, critical)	certPolicyID should be denoted with OID, IA5String. Root CA Bangladesh will not use this field in its certificate. This field is a mandatory field for CA certificate and subscriber certificate.
7.	policyMappings (not used)	
8.	subjectAltName (optional, non-critical)	If the PKI domain wants to include Electronic mail, DNS Name or URI in the certificate, this field will be used. The values shall be encoded as IA5String

SL	FIELD	NOTE
9.	issuerAltName (not used)	
10.	subjectDirectryAttributes (not used)	
11.	basicConstraints (Mandatory, critical)	cA=TRUE (Boolean) pathLenConstraint=optional (INTEGER)
12.	nameConstraints (not used)	
13.	policyConstraints (not used)	
14.	cRLDistributionPoints (Optional, non-critical)	LDAP or HTTP or both can be used. ldap://hostname[:portnumber]/dn?attr[;binary] (e.g.,<ldap://ldap.example.com/cn=example%20CA,dc=example,dc=com?certificateRevocationList;binary>) http://<URI>/CRLname.crl (as per RFC 2585)
15.	inhibitAnyPolicy (not used)	
16.	freshestCRL (not used)	

3.1.3 Private Internet Extension

SL	FIELD	NOTE
1	Authority Information Access (Optional, non-critical)	If the PKI domain uses OCSP, this field will be used.
2	Subject Information Access (not used)	

3.2. CA Certificate Profile

The CA certificate is a certificate, issued by the Root CA. It has also two fields:

3.2.1 Certificate Basic field

SL	FIELD	NOTE
1	version (Mandatory)	Since extension field appears in this profile, the value MUST be set to 2 (v3).
2	serialNumber (Mandatory)	Unique integer. Up to 20 octets.
3	Signature (Mandatory)	1.2.840.113549.1.1.11 SHA256 with RSA Encryption
4	issuer (Mandatory)	X.500 DN. For details about attribute values, see Appendix-G
5	Validity (Mandatory)	UTCTIME
6	subject (Mandatory)	X.500 DN. And see Appendix-G.
7	subjectPublicKeyInfo	1.2.840.113549.1.1.1 (rsaEncryption)

SL	FIELD	NOTE
	(Mandatory)	For CA: 2,048 bits
8	issuerUniqueID (not used)	
9	subjectUniqueID (not used)	
10	SignatureAlgorithm (mandatory)	1.2.840.113549.1.1.11 SHA256 with RSA Encryption
11	signatureValue (Mandatory)	Encoded as Bit string Must contain the signature in accordance with the algorithm. For RSA, this is the value generated by hashing the certificate, then padding, and then performing the RSA private key operation.

3.2.2 Certificate Extension field

SL	FIELD	NOTE
1.	authorityKeyIdentifier (Mandatory, non-critical)	**keyIdentifier (Mandatory):** The hash value of Issuer's pubic key. **authorityCertIssuer (optional):** DN **authCertSerialNum (optional):** INTEGER When AuthCertIssuer is used, AuthCertSerialNum must be set as well. Vice versa.
2.	subjectKeyIdentifier (Mandatory, non-critical)	The value of the subjectKeyIdentifier MUST be the value placed in the keyIdentifier field of the authorityKeyIdentifier extension of certificate issued by the subject of this certificate. The keyIdentifier is composed of the 160-bit SHA-1 hash of the value of the BIT STRING subjectPublicKey (excluding the tag, length, and number of unused bits).
3.	keyUsage (Mandatory, critical)	keyCertSign, cRLSign
4.	extKeyUsage (not used)	
5.	privateKeyUsagePeriod (not used)	
6.	certificatePolicies (Mandatory, ether critical or non-critical [1])	certPolicyID MUST be present. And should be denoted with OID, IA5String
7.	policyMappings (Not used)	

---

[1]   It must be verified of a policy by the case of non-critical as well as the case of critical.

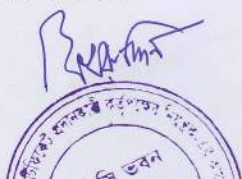| SL	FIELD	NOTE
8.	subjectAltName (optional, non-critical)	If the PKI domain wants to include Electronic mail, DNS Name or URI in the certificate, this field will be used. The values shall be encoded as IA5String.
9.	issuerAltName (optional, non-critical)	If the PKI domain wants to include Electronic mail, DNS Name or URI in the certificate, this field will be used. The values shall be encoded as IA5String. Where present, the value will be same as subject alternative name of the issuer of the certificate.
10.	subjectDirectryAttributes (not used)	
11.	basicConstraints (Mandatory, critical)	cA=TRUE pathLenConstraint=optional (INTEGER)
12.	nameConstraints (not used)	
13.	policyConstraints (not used)	
14.	cRLDistributionPoints (Mandatory, non-critical)	LDAP or HTTP or both can be used. ldap://hostname[:portnumber]/dn?attr[;binary] (e.g.,<ldap://ldap.example.com/cn=example%20CA,dc=example,dc=com?certificateRevocationList;binary>) http://<URI>/CRLname.crl (as per RFC 2585) CA certificate will carry the CRL of Root CA as its CRL Distribution Point.
15.	authorityInfoAccess (optional)	If the PKI domain uses OCSP, this field will be used.
16.	inhibitAnyPolicy (not used)	
17.	freshestCRL (optional)	
18.	subjectInfoAccessSyntax (not used)	

3.3. Sub-CA Certificate Profile

The Sub-CA certificate is a certificate, issued by the CA. It has also two fields like CA certificate profile:

3.3.1 Certificate Basic field

SL	FIELD	NOTE
1	version (Mandatory)	Since extension field appears in this profile, the value MUST be set to 2 (v3).
2	serialNumber (Mandatory)	Unique integer. Up to 20 octets.
3	Signature (Mandatory)	1.2.840.113549.1.1.11 SHA256 with RSA Encryption
4	issuer (Mandatory)	X.500 DN of Issuing CA. For details about attribute values, see Appendix-G

SL	FIELD	NOTE
5	Validity (Mandatory)	UTCTIME
6	subject (Mandatory)	X.500 DN. And see Appendix-G.
7	subjectPublicKeyInfo (Mandatory)	1.2.840.113549.1.1.1 (rsaEncryption) For sub-CA: 2,048 bits
8	issuerUniqueID (not used)	
9	subjectUniqueID (not used)	
10	SignatureAlgorithm (mandatory)	1.2.840.113549.1.1.11 SHA256 with RSA Encryption
11	signatureValue (Mandatory)	Encoded as Bit string Must contain the signature in accordance with the algorithm. For RSA, this is the value generated by hashing the certificate, then padding, and then performing the RSA private key operation.

3.3.2 Certificate Extension field

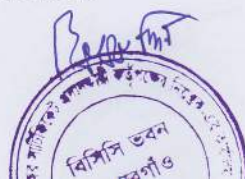| SL	FIELD	NOTE
1.	authorityKeyIdentifier (Mandatory, non-critical)	**keyIdentifier (Mandatory):** The hash value of Issuer's pubic key. **authorityCertIssuer (optional):** DN **authCertSerialNum (optional):** INTEGER When AuthCertIssuer is used, AuthCertSerialNum must be set as well. Vice versa.
2.	subjectKeyIdentifier (Mandatory, non-critical)	The value of the subjectKeyIdentifier MUST be the value placed in the keyIdentifier field of the authorityKeyIdentifier extension of certificate issued by the subject of this certificate. The keyIdentifier is composed of the 160-bit SHA-1 hash of the value of the BIT STRING subjectPublicKey (excluding the tag, length, and number of unused bits).
3.	keyUsage (Mandatory, critical)	keyCertSign, cRLSign
4.	extKeyUsage (not used)	
5.	privateKeyUsagePeriod (not used)	
6.	certificatePolicies (Mandatory, ether critical or	certificatePolicies of Sub-CA shall be within the issuing CAs certificate policy. In case of Sub-CA is a Class, CA shall

SL	FIELD	NOTE
	non-critical [2])	use the OID value notified in the website of CCA. certPolicyID MUST be present. And shall be denoted with OID, IA5String
7.	policyMappings (Not used)	
8.	subjectAltName (optional, non-critical)	If the PKI domain wants to include Electronic mail, DNS Name or URI in the certificate, this field will be used. The values shall be encoded as IA5String.
9.	issuerAltName (optional, non-critical)	If the PKI domain wants to include Electronic mail, DNS Name or URI in the certificate, this field will be used. The values shall be encoded as IA5String. Where present, the value will be same as subject alternative name of the issuer of the certificate.
10.	subjectDirectryAttributes (not used)	
11.	basicConstraints (Mandatory, critical)	cA=TRUE pathLenConstraint=optional (INTEGER) [1 for sub-CA]
12.	nameConstraints (not used)	
13.	policyConstraints (not used)	
14.	cRLDistributionPoints (Mandatory, non-critical)	LDAP or HTTP or both can be used. ldap://hostname[:portnumber]/dn?attr[;binary] (e.g.,<ldap://ldap.example.com/cn=example%20CA,dc=example,dc=com?certificateRevocationList;binary>) http://<URI>/CRLname.crl (as per RFC 2585)
15.	authorityInfoAccess (optional)	If the PKI domain uses OCSP, this field will be used.
16.	inhibitAnyPolicy (not used)	
17.	freshestCRL (optional)	
18.	subjectInfoAccessSyntax (not used)	

3.4.   End Entity Certificate

End entity certificate profiles are stated in the following sub-sections. In every EE certificate, the basic fields are same. The extensions are different depending on the usage of the certificate. The keyUsage field is to define the usage of a certificate.

---

[2]   It must be verified of a policy by the case of non-critical as well as the case of critical.
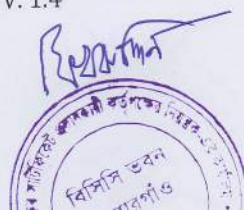
3.4.1 Common EE Profile

Certificate Basic field

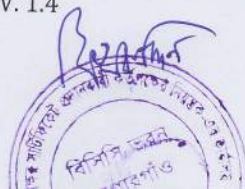| SL	FIELD	NOTE
1	version (Mandatory)	Since extension field appears in this profile, the value MUST be set to 2 (v3).
2	serialNumber (Mandatory)	Unique integer. Up to 20 octets.
3	Signature (Mandatory)	1.2.840.113549.1.1.11 SHA256 with RSA Encryption
4	issuer (Mandatory)	X.500 DN. For details about attribute values, see Appendix-G on page 39
5	Validity (Mandatory)	UTCTIME
6	subject (Mandatory)	X.500 DN. And see issuer.
7	subjectPublicKeyInfo (Mandatory)	1.2.840.113549.1.1.1 (rsaEncryption) For end user: 2048 bit
8	issuerUniqueID (not used)	
9	subjectUniqueID (not used)	
10	SignatureAlgorithm (mandatory)	1.2.840.113549.1.1.11 SHA256 with RSA Encryption
11	signatureValue (Mandatory)	Encoded as Bit string Must contain the signature in accordance with the algorithm. For RSA, this is the value generated by hashing the certificate, then padding, and then performing the RSA private key operation.

Certificate Extension field

SL	FIELD	NOTE
1	authorityKeyIdentifier (Mandatory, non-critical)	keyId(Mandatory): The hash value of Issuer's public key. authorityCertIssuer(optional): DN authCertSerialNum(optional): INTEGER When AuthCertIssuer is used, AuthCertSerialNum must be set as well. Vice versa.
2	subjectKeyIdentifier (Mandatory, non-critical)	For end entity certificates, subject key identifiers SHOULD be derived from the public key. The keyIdentifier is composed of the 160-bit SHA-1 hash of the value of the BIT STRING subjectPublicKey (excluding the tag, length, and number of unused bits).
3	keyUsage (Mandatory,	digitalSignature, nonRepudiation

SL	FIELD	NOTE
	critical)	
4	extKeyUsage (optional, Special Purpose)	It will be required for OCSP, SSL, etc certificates by using any or multiple of the following parameters: id-kp-serverAuth OBJECT IDENTIFIER ::= { id-kp 1 } id-kp-clientAuth OBJECT IDENTIFIER ::= { id-kp 2 } id-kp-codeSigning OBJECT IDENTIFIER ::= { id-kp 3 } id-kp-emailProtection OBJECT IDENTIFIER ::= { id-kp 4 } id-kp-timeStamping OBJECT IDENTIFIER ::= { id-kp 8 } id-kp-OCSPSigning OBJECT IDENTIFIER ::= { id-kp 9 }
5	privateKeyUsagePeriod (not used)	
6	certificatePolicies (Mandatory, ether critical or non-critical [3])	certPolicyID MUST be present. And should be denoted with OID, IA5String. Depending on the Class of the Certificate corresponding OID (notified in CCA website) shall be used.
7	policyMappings (not used)	
8	subjectAltName (optional, non-critical)	If the PKI domain wants to include Electronic mail, DNS Name or URI or etc in the certificate, this field will be used. The field SubjectAltName can be any of the following values: otherName [0] OtherName rfc822Name [1] IA5String dNSName [2] IA5String x400Address [3] ORAddress directoryName [4] Name ediPartyName [5] EDIPartyName uniformResourceIdentifier [6] IA5String iPAddress [7] OCTET STRING registeredID [8] OBJECT IDENTIFIER
9	issuerAltName (optional, non-critical)	If the PKI domain wants to include Electronic mail, DNS Name or URI in the certificate, this field will be used. The values shall be encoded as IA5String. Where present, the value will be same as subject alternative name of the issuer of the certificate.
10	subjectDirectryAttributes (not used)	
11	basicConstraints (optional, critical)	

---

[3] It must be verified of a policy by the case of non-critical as well as the case of critical.

SL	FIELD	NOTE
12	nameConstraints (not used)	
13	policyConstraints (not used)	
14	cRLDistributionPoints (Mandatory, non-critical)	LDAP or HTTP or both can be used. ldap://hostname[:portnumber]/dn?attr[;binary] (e.g.,<ldap://ldap.example.com/cn=example%20CA,dc=example,dc=com?certificateRevocationList;binary>) http://<URI>/CRLname.crl (as per RFC 2585)
15	authorityInfoAccess (not used)	If the PKI domain uses OCSP, this field will be used.
16	inhibitAnyPolicy (not used)	
17	freshestCRL (not used)	
18	subjectInfoAccessSyntax (not used)	

3.4.2 Identification Certificate

Certificate Extension field

keyUsage (Mandatory, critical)	digitalSignature, nonRepudiation

3.4.3 Secure E-Mail Certificate

Certificate Extension field

keyUsage (Mandatory, critical)	digitalSignature, nonRepudiation and keyEncipherment
subjectAltName (Mandatory, non-critical)	If the PKI shall include Electronic mail address in the certificate and the values shall be encoded as IA5String

3.4.4 Encryption Certificate

Certificate Extension field

keyUsage (Mandatory, critical)	keyEncipherment
subjectAltName (Mandatory, non-critical)	Electronic mail address in the certificate

3.4.5 SSL Certificate Profile

Sl.	Field	Note
1.	Version (Mandatory)	The mandated value is 2. (i.e., The certificate must be in a version 3 format)
2.	Serial Number (Mandatory)	Positive number of maximum Length 20 bytes and unique to each certificate issued by a CA.
3.	Issuer Signature Algorithm (Mandatory)	SHA256 with RSA Encryption (null parameters)

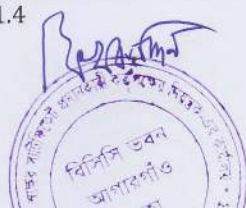| SI.	Field	Note
4.	Issuer Distinguished Name (Mandatory)	Must be same as Subject DN of the issuing CA
5.	Validity Period (Mandatory)	Validity expressed in UTC Time for certificates valid through 2049
6.	Subject Distinguished Name (Mandatory)	Common Name (CN) Fully Qualified Domain Name(FQDN) **Optional Attributes** State / Province State / province for verified Office address Organisation Unit(OU) Department / Division to which the individual belongs within his organisation Organisation (O) Legal Name of the organisation the person belongs to Country (C) Country code as per the verified Office address
7.	Subject Public Key Information (Mandatory)	rsaEncryption, minimum 2048 RSA Key modulus, public exponent
8.	Issuer's Signature (Mandatory)	sha256WithRSAEncryption {1 2 840 113549 1 1 11} (null parameters)
9.	Signature Value (Mandatory)	Issuer CA's signature
10.	Authority Key Identifier (Mandatory, Not Critical)	Issuing CA SubjectkeyIndetifier
11.	Subject Key Identifier (Mandatory, Not Critical)	Octet String of unique value associated with the Public key
12.	Key Usage (Mandatory, Critical)	Key Encipherment and Digital Signature
13.	Certificate Policies (Mandatory, Not Critical)	The value must contain the OID representing the CCA certificate policy the certificate is valid for; and all the lower level certificate polices.
14.	Subject Alternative Name (Mandatory, Not Critical)	Subject Alternative Name: ⬚ dnsName(s) for the server(s) / web page as an IA5 string ⬚IP addresses of the server as a printable string in "network byte order", as specified in RFC791 for IPv4 and RFC 2460 for IPv6

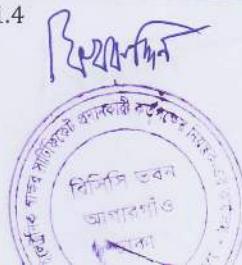| SI.	Field	Note
15.	Extended Key Usage (Optional, Not Critical)	If present, extended key usage shall include ⬚ id-kp-serverAuth {1 3 6 1 5 5 7 3 1} ⬚ id-kp-clientAuth {1 3 6 1 5 5 7 3 2}
16.	CRL Distribution Points (Mandatory, Not Critical)	DistributionPointName MUST be set and MUST contain a complete HTTP URI pointing to a DER encoded full and complete CRL for all reasons. DistributionPointName shall contain the fullName and thus shall not contain nameRelativeToCRLIssuer Reasons and cRLIssuer fields shall be absent.

3.4.6 OCSP Responder Certificate Profile

SI.	Field	Note
1.	Version (Mandatory)	The mandated value is 2. (i.e., The certificate must be in a version 3 format)
2.	Serial Number (Mandatory)	Positive number of maximum Length 20 bytes and unique to each certificate issued by a CA.
3.	Issuer Signature Algorithm (Mandatory)	SHA256withRSAEncryption (null parameters)
4.	Issuer Distinguished Name (Mandatory)	Must be same as Subject DN of the Issuing CA
5.	Validity Period (Mandatory)	Validity expressed in UTC Time for certificates valid through 2049
6.	Subject Distinguished Name (Mandatory)	Common Name (CN) <OCSP Responder Name> Organisational Unit OCSP Responder (OU) Organisation (O) Legal Name of the OCSP Organization Country (C) Country code as per the verified office address
7.	Subject Public Key Information (Mandatory)	rsaEncryption, 2048 RSA Key modulus, public exponent
8.	Issuer's Signature (Mandatory)	sha256 WithRSAEncryption {1 2 840 113549 1 1 11} (null parameters)
9.	Signature Value (Mandatory)	Issuer CA"s signature
10.	Authority Key Identifier (Mandatory, Not Critical)	Issuing CA SubjectkeyIndetifier
11.	Subject Key Identifier (Mandatory, Not Critical)	Octet String of unique value associated with the Public key
12.	Key Usage (Mandatory, Critical)	DigitalSignature

Sl.	Field	Note
13.	Certificate Policies (Mandatory, Not Critical)	The value must contain the OID representing the CCA certificate policy the certificate is valid for; and all the lower level certificate polices.
14.	Extended Key Usage (Mandatory, Critical)	id-kp-OCSPSigning {1 3 6 1 5 5 7 3 9}
15.	CRL Distribution Points (Optional, Not Critical)	Must be present if no-check extension is absent. Must be absent if no-check extension is present. DistributionPointName MUST be set and MUST contain a completeHTTP URI pointing to a DER encoded partitioned CRL for allreasons. DistributionPointName shall contain the fullName and thusshall not contain nameRelativeToCRLIssuer
16.	Authority Information Access (Mandatory, Not Critical)	The id-ad-ca Issuers OID MUST point to certificates issued to the CA issuing the certificate containing this field. The OID should specify a HTTP URI which points to a single DER encoded certificate or a collection of DER encoded certificates in a BER or DER encoded "certs-only" CMS message as specified in [RFC3852].

3.4.7 System Certificate Profile

Sl.	Field	Value
1.	Version (Mandatory)	The mandated value is 2. (i.e., The certificate must be in a version 3 format)
2.	Serial Number (Mandatory)	Positive number of maximum Length 20 bytes and unique to each certificate issued by a CA.
3.	Issuer Signature Algorithm (Mandatory)	SHA256 with RSA Encryption (null parameters)
4.	Issuer Distinguished Name (Mandatory)	Must be same as Subject DN of the issuing CA
5.	Validity Period (Mandatory)	Validity expressed in UTC Time for certificates valid through 2049
6.	Subject Distinguished Name (Mandatory)	The CN in the Subject NameMUST contain either • IP Address of the system as a printable string in "network byte order", as specified in RFC791 for IPv4 and RFC 2460 for IPv6 • MAC Address of primary network interface as a printable string • Serial number (CPU or any electronically verifiable serial number) as a printable string • Unique ID as a printable string

Sl.	Field	Value
7.	Subject Public Key Information (Mandatory)	rsaEncryption, with minimum 2048 RSA Key modulus, public exponent
8.	Issuer"s Signature (Mandatory)	sha256 WithRSAEncryption {1 2 840 113549 1 1 11} (null parameters)
9.	Signature Value (Mandatory)	Issuer CA"s signature
10.	Authority Key Identifier (Mandatory, Not Critical)	Issuing CA SubjectkeyIndetifier
11.	Subject Key Identifier (Mandatory, Not Critical)	Octet String of unique value associated with the Public key
12.	Key Usage (Mandatory, Critical)	Key Encipherment and Digital Signature
13.	Certificate Policies (Mandatory, Not Critical)	The value must contain the OID representing the CCA certificate policy the certificate is valid for; and all the lower level certificate polices.
14.	Subject Alternative Name (Mandatory, Not Critical)	The CN in the Subject Name MUST contain either ▢IP Address of the system as a octet string in "network byte order", as specified in RFC791 for IPv4 and RFC 2460 for IPv6 ▢ dnsName in IA5String format
15.	Extended Key Usage (Optional, Not Critical)	If present, extended key usage shall include ▢ id-kp-serverAuth {1 3 6 1 5 5 7 3 1} ▢ id-kp-clientAuth {1 3 6 1 5 5 7 3 2}
16.	CRL Distribution Points (Mandatory, Not Critical)	DistributionPointName MUST be set and MUST contain a complete HTTP URI pointing to a DER encoded full and complete CRL for all reasons. DistributionPointName shall contain the fullName and thus shall not contain nameRelativeToCRLIssuer reasons and cRLIssuer fields shall be absent.

3.5. ARL/CRL Profile

Authority Revocation List (ARL) and Certificate Revocation List (CRL) are used to check whether a certificate in the certification path has not been revoked or not. This profile distinguishes the ARL and CRL in order for the CA to customize their revocation policy. This design policy suggests that the IWG profile accepts the CA revocation information in the CRL, which primarily includes the EE revocation information. In addition, the profile of this guideline accepts the separate/multiple CRL distribution policy based on the revocation reasons and serial number, for instance. This is up to the decision of the CA issuing policy. The application should handle the revocation policy of the CA.
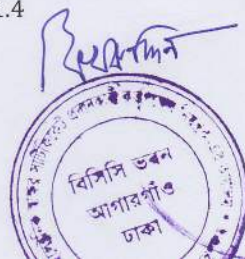
ARL/CRL Basic field

SL	FIELD	NOTE
1	Version (Mandatory)	Since extension field appears in this profile, the value MUST be set to 1 (v2).
2	signature (Mandatory)	1.2.840.113549.1.1.11 SHA256 with RSA Encryption
3	issuer (Mandatory)	X.500 DN. For details about attribute values, see Appendix-G on page 39
4	thisUpdate (Mandatory)	UTCTIME
5	nextUpdate (Mandatory)	UTCTIME
6	revokedCertificates (Mandatory)	Certificate Serial Number and revocation date in GeneralizedTime

ARL/CRL EntryExtensions

SL	FIELD	NOTE
1	ReasonCode (Mandatory, non-critical)	Value of this field may be any/all given below: unspecified (0), keyCompromise (1), cACompromise (2), affiliationChanged (3), superseded (4), cessationOfOperation (5), certificateHold (6), removeFromCRL (8), privilegeWithdrawn (9), aACompromise (10)
2	holdInstructionCode (not used)	
3	invalidityDate (optional, non-critical)	GeneralizedTime
4	CertificateIssuer (not used)	

ARL/CRL Extensions

SL	FIELD	NOTE
1	authorityKeyIdentifier (Mandatory, non-critical)	**keyId(Mandatory):** The hash value of Issuer's pubic key (SHA1 160bit). **authorityCertIssuer(optional):** DN **authCertSerialNum(optional):** INTEGER When AuthCertIssuer is used, AuthCertSerialNum must be set as well. Vice versa.
2	issuerAltName (not-used)	
3	cRLNumber (Mandatory, non-critical)	unique integer. up to 20 octets.
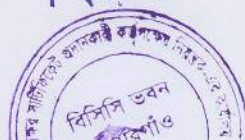
SL	FIELD	NOTE
4	deltaCRLIndicator (optional, critical)	If the PKI domain wants to use dCRL, this field will be used.
5	issuingDistributionPoint	
6	freshestCRL (optional, non-critical)	If the PKI domain wants to use dCRL, this field will be used.
7	crlScope (not-used)	
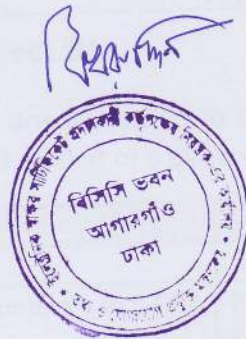
G. Appendix-I: Convention & Specification

1. Naming convention

In order to standardize the naming for the CAs and sub-CAs, the following guideline is to be adopted for determining the "Common Name" (CN) for CAs and Sub-CAs.

| Entity	Naming (Common name)	Example
Certifying Authority	"Certifying Authority Name" CA "YYYY"	XYZ CA 2013
Sub-CA	"Certifying Authority Name" sub-CA for "Branding Name"	XYZ Sub CA for Income Tax XYZ Sub CA for Class 2 Certificate

Each Relative Distinguished Name (RDN) shall contain a single attribute type and associated value. Attribute values shall be encoded as specified below:

Sl. No	Attribute Type	Attribute Value Encoding
1	Country	Printable String
2	Organisation	Printable String
3	Organisation Unit	Printable String
4	Post Code	Printable String
5	State/Province (Not applicable for Root CA and CA certificate profile)	Printable String
6	Street Address	Printable String
7	House Identifier	Printable String
8	Common Name	Printable String
9	Serial Number	Printable String
10	Unique Identifier	Bit String

2. Specifications for Issuer and Subject DN

The summary of issuer and subject fields are presented in the table below. Note that the attributes are presented in a reverse order than that of a directory structure.

Sl.	Certificate Type	Issuer	Subject
1	CCA	Self	Same as issuer
2	Licensed CA	Same as Subject in CCA Certificate	Refer licensed CA Subject Specifications
3	Sub CA	Same as subject in licensed CA Certificate	Refer sub CA Subject Specifications
4	End User (certificate issued by sub-CA)	Same as subject for issuing CA (or sub-CA) Certificate	Refer End user subject specifications
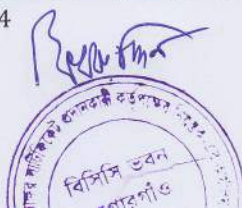
3. CCA Certificate – Subject Specifications

The CCA certificate must comply with following distinguished name specifications for both subject and issuers (for a self signed certificate)

Sl.	Attribute	Value
1	Common Name (CN)	Root CA Bangladesh "YYYY"
2	Organisation (O)	Office of the CCA
3	Country (C)	BD

4. CA Certificate –Issuer Specifications

Sl.	Attribute	Value
1	Common Name (CN)	Root CA Bangladesh "YYYY"
2	Organisation (O)	Office of the CCA
3	Country (C)	BD

5. CA Certificate – SUBJECT specifications

Sl.	Attribute	Value
1	Common Name (CN)	Max Length: 64 characters Licensed (subject) CA Name (name by which it will be commonly known) (Refer Naming Conventions section in organizational recommendations section) e.g. XYZ CA "YYYY"
2	House Identifier	Max Length: 60 Characters This attribute MUST contain the • Flat number, Apartment name and Plot no. OR • House Name/Number and Plot Number of the CA's head office or registered office address
3	Street Address	Max Length: 60 Characters This attribute value MUST contain following parameters of the CA's head office or registered office address
4	Locality	Name of City/District where CA's head office or registered office address is. This field is optional if City/District is added in Street Address.
5	State / Province	Not applicable for CA certificate
6	Postal Code	Postal Code of the CA's head office or registered office address

Sl.	Attribute	Value
7	Organisational Unit (OU)	"Certifying Authority"
8	Organisation (O)	Legal Name of the Organisation operating the CA Max Length: 64 Characters
9	Country (C)	Country code as per the verified residential/office address Max Length: 2 Characters

6. Sub-CA Certificate – Issuer specifications

Issuer Field for Sub-CA MUST be same as the Subject Field for the CA have been again provided here for easy reference

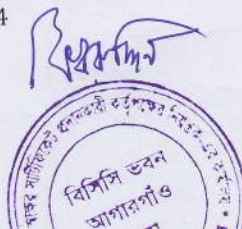| Sl. No	Attribute	Value
1	Common Name (CN)	Same as SUBJECT field in Issuer CA certificate
2	House Identifier	Same as SUBJECT field in Issuer CA certificate
3	Street Address	Same as SUBJECT field in Issuer CA certificate
4	Locality	Same as SUBJECT field in Issuer CA certificate
5	State / Province	Not Applicable
6	Postal Code	Same as SUBJECT field in Issuer CA certificate
7	Organisational Unit (OU)	Same as SUBJECT field in Issuer CA certificate
8	Organisation (O)	Same as SUBJECT field in Issuer CA certificate
9	Country (C)	Same as SUBJECT field in Issuer CA certificate

7. Sub-CA Certificate – Subject specifications

A. Internal Sub-CA

Sl. No	Attribute	Value
1	Common Name (CN)	Sub-CA Common Name (refer CA naming conventions)
2	Organisation Unit (OU)	Sub-CA
3	Organisation (O)	Legal Name of the Organisation operating the Sub-CA (same as the O in Issuer field of Issuer CA certificate)
4	Country (C)	Max Length: 2 Characters Country code as per the verified residential/office address

B. External Sub-CA

Sl. No	Attribute	Value
1	Common Name (CN)	Sub-CA Common Name (refer CA naming conventions)

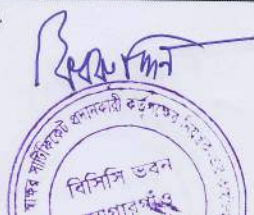| Sl. No	Attribute	Value
2	House Identifier	Max Length: 60 Characters This attribute MUST contain the • Flat number, Apartment name and Plot no. OR • House Name/Number and Plot Number of the CA's head office or registered office address
3	Street Address	Max Length: 60 Characters This attribute value MUST contain following parameters of the CA's head office or registered office address
4	Locality	Name of City/District where CA's head office or registered office address is.
5	State / Province	Not applicable for CA certificate
6	Postal Code	Postal Code of the CA's head office or registered office address
7	Organisation (O)	Legal Name of the Organisation operating the Sub-CA
8	Country (C)	Max Length: 2 Characters Country code as per the verified residential/office address

8. End User Certificate (Issued by a Sub-CA) – Issuer specifications

A. End User Certificate Issued by Internal Sub-CA

Sl. No	Attribute	Value
1	Common Name (CN)	Same as SUBJECT field in issuing sub
2	Organisational Unit (OU)	Same as SUBJECT field in issuing sub
3	Organisation (O)	Same as SUBJECT field in issuing sub
4	Country (C)	Same as SUBJECT field in issuing sub

B. End User Certificate Issued by External Sub-CA

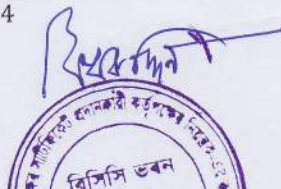| Sl. No	Attribute	Value
1	Common Name (CN)	Same as SUBJECT field in issuing sub
2	House Identifier	Same as SUBJECT field in issuing sub
3	Street Address	Same as SUBJECT field in issuing sub
4	Locality	Same as SUBJECT field in issuing sub
5	State/Province	Same as SUBJECT field in issuing sub
6	Organisational Unit (OU)	Same as SUBJECT field in issuing sub
7	Organisation (O)	Same as SUBJECT field in issuing sub
8	Country (C)	Same as SUBJECT field in issuing sub

9. End User Certificate – Subject Specifications

SL	Attribute	Definition
1	Common Name	**Max Length: 64 Characters** • The Common name MUST be constructed in the following manner • CN = "Surname" "Given Name" "Initials" **Surname** • The surname is name inherited by and individual from individual's parent or assumed by marriage. • In the Bangladeshi context, Surname is same as last name or family name. In certain populations, where the use of Surname is not prevalent, the Surname will mean the part of the name which is common with the individual's parents or spouse (assumed from marriage). • Where none of the above criteria are satisfied and where applicable, the house name, tribe, trade, tile, salutation which is an integral part of the person's name is to be used as the surname. • The Surname MUST not be Blank or substituted by initials. **Given Names** • Given name is the name which is given to an individual by parent, or chosen by the individual, or by the name by which the individual is known. • The given Name MUST not be Blank or substituted by initials. • Generation qualifier if any (Jr. II) MUST be appended to the given name with a space distinguishing both. **Initials** • This being a completely optional field and MAY contain initials of parts of person's name not already addressed in and of the above attributes.
2	Serial Number	Serial Number must contain 3 letter prefix of type of Identity and 160 bit SHA1 digest of Subjects Identity value. Valid Identity Numbers are National Identity (NID), Passport Number (PPN), Birth Registration Number (BRN) and Tax Identification Number (TIN). (e.g. if Subjects' Identification type is passport and the passport number is OC8739XXXX, then the serial number field will contain PPN and digest of OC8739XXXX (i.e. something like **PPN5b6a26d4d6acd2af8238b49ffa38a40fdb61162d** Here the red part is in plain text and blue part is the hash value)

SL	Attribute	Definition
3	Unique Identifier	This is a reserved attribute for future use and shall be used in the future for SHA256 hash of National ID or any other Unique ID for individuals.
4	State or Province Name	Max Length: 60 Characters This attribute value MUST be populated with the name of the State / Province of Subject's residential or office address (if any).
5	locality	City/District of Subjects residential or office address.
6	Postal Code	Post Code for the for Subject's residential or office address.
7	Organisation Unit	Max Length: 64 Characters This attribute MUST either contain the name of the department or sub-division of the organisation the person belongs to if the certificate is being issued for official purposes OR must not be used. The Organisational unit must not be present when the organisation has been marked as "personal"
8	Organisation	Max Length: 64 Characters This attribute MUST contain either Name of the organisation the person belongs to – if such information has been verified by the CA OR Contain string "Personal"
9	Country	Max Length: 2 Characters For Bangladesh, Country code is BD

10. Certificate Validity in Bangladesh PKI

A notification has been issued by the Controller regarding certificate validity of different type of certificate. The notification is available at www.cca.gov.bd

The certificate validity is given as below with some addition to the notification:

Sl.	Certificate Type	Subject	Issuer	Validity
1.	Root CA Certificate	Root CA Bangladesh	Root CA Bangladesh	10 years
2.	Licensed CA Certificate	Name of Licensed CA as per CA Subject Specification	Root CA Bangladesh	5 years
3.	Sub-CA Certificate	As per Sub-CA Subject Specification	Name of Licensed CA	3 Years
4.	End User Certificate (Class 1 & 2)	As per End User Subject Specification	Name of Licensed CA/ Name of Sub-CA	1/2 Years
5.	End User Certificate (Class 3)	As per End User Subject Specification	Name of Licensed CA/ Name of Sub-CA	2 Years

11. Certificate Signing Request (CSR) by CAs

Activities Required by a Licensed CA:

Each CA should formulate the Certificate Authorities in his CA signing application server as per the guideline and following PKCS#10. The signing software should generate a CSR file with extension .csr or .pem or .txt or .req or in any compatible format. The licensed CA should deliver this PKCS#10 CSR to the Office of the CCA for processing and signing. CA may deliver this file to Office of the CCA by CD/DVD or in any secure media.

Sample CSR:

```
-----BEGIN CERTIFICATE REQUEST-----
MIICwjCCAaoCAQAwfTELMAkGA1UEBhMCQkQxDTALBgNVBAgTBE5vbmUxDjAMBgNV
BAcTBURoYWthMQ8wDQYDVQQKEwZDQU5hbWUxCzAJBgNVBAsTAkNBMREwDwYDVQQD
EwhDQU5hbWVDQTEeMBwGCSqGSIb3DQEJARYPaW5mb0BjYW5hbWUuY29tMIIBIjAN
BgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA6/oLwbW6jzptLUl1YodlFpXltu/A
DRAkQribwVyuFEqea37SMEx6pUDtJ7amz1VnNNHOQVSgBL/RHZlCSC1DBCSqSfPl
9NnXNUpGpZbzG3IrswNgRMHwG/6AxEt/g5K6P4tUS7H9QNoILnNZpMWcCnPiPdFV
itsK82elr7SEUvxqYSRA9+t56BFwHDv+m4ToTpjiy9hwjWZKKT7b4AY7C/Ui+4w8
htLspV2D+HiKOJPrJnaRIW/Tpe8ceBFHRlR7tB2KlhQoCqjLDgMthXcFVkKmM6OX
CwLSYigq+2j1H1QvbXoTOX0c0LFtDIWLPHnt9GopVbdB6rX0n9hEYngxNwIDAQAB
oAAwDQYJKoZIhvcNAQEEBQADggEBAC9A96WeMCODYeg28iyaUJco3FHkrLpr4StF
FUzIo5otWsFylkkEhLGGm8YaglfnhmJ7pueVJ478i+rkLqXmeg+jTi8uuoq9FmcZ
+Ejvc3WGkySSNehwo5MryB4MpkQFrWFeQUzMr4dz9GWQl+xZhLUqoOiTdP33XqfW
Jd6cWut3oHltvU+7gHMKlFqRR0MA7FYprgORQppAdyRsYFsIehSRgcQnrOWnx5Fu
8bDCOhlixRMpkK6UZDOCP7Gl6vvDakj9/ouGgIjf1HhKRSobZfVeTqdoop1LFJf7
R9s3dz6bvu2E2xPEzDUlJ27CL7ADLelHiAl/cbrjH1NvQShQPMk=
-----END CERTIFICATE REQUEST-----
```

H. Appendix-II: Acronym

ARL	Authority Revocation List
ASN.1	Abstract Syntax Notation One
B2B	Business to Business
BER	Basic Encoding Rules
CA	Certification Authority
CCA	Controller of Certifying Authorities
CRL	Certificate Revocation List
CC	Cross Certification
CN	Common Name
DAP	Directory Access Protocol
DER	Distinguished Encoding Rules
DIT	Directory Information Tree
DN	Distinguished Name
EE	End entity
LDAP	Lightweight Directory Access Protocol
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PKCS	Public Key Cryptography Standard
POP	Proof of Possession
RDN	Relative Distinguished Name
RA	Registration Authority
SCA	Subordinate CA
TBS	To-Be-Signed
VA	Validation Authority