Interoperability Guidelines for Digital Signature Certificates issued under Information Technology Act

Version 2.1

December 2009

Controller of Certifying Authorities

Department of Information Technology

Ministry of Communications and Information Technology

Document Control

Document Name	Digital Certificates Interoperability Guidelines
Status	Release
Version	2.1
Last update	15 November 2010
Document Owner	Controller of Certifying Authorities, India

Table of contents

Foreword 4
Scope and applicability 5
Revisions 5
The interoperability model 5
Organizational Guidelines 7
Certificate Profile Guidelines 8
Field Definitions 9
Standard Extensions Definition 19
Private Extensions 40
Annexure I – Issuer and Subject field specification 43
Annexure II - Special Purpose Certificates 72
Annexure III - Reference Certificate Profiles 76
CA Certificate Profile 76
Sub-CA Certificate Profile 78
End User Certificate Profile (issued for personal use) 79
End User Certificate Profile (issued for organization use) 80
SSL Certificate Profile 82
System Certificate Profile 83
Time Stamping Authority Certificate Profile 84
Code Signing Certificate Profile 85
OCSP Responder Certificate Profile 87
Encryption Certificate 88
CRL Profile 90
Annexure IV – Application Developer Guidelines 91
Change History 93

Foreword

The office of Controller of Certifying Authorities (CCA) was set up under the Information Technology (IT) in the year 2000. One of the primary objectives was to promote the use of Digital Signatures for authentication in e-commerce & e-governance. Towards facilitating this, the CCA licensed eight Certifying Authorities (CAs) to issue Digital Signature Certificates (DSC) under the IT Act 2000. The standards and practices to be followed were defined in the Rules and Regulations under the Act and the Guidelines that are issued by CCA from time to time.

The Root Certifying Authority of India (RCAI) was set up by the CCA to serve as the root of trust in the hierarchical Public Key Infrastructure (PKI) model that has been set up in the country. The RCAI with its self-signed Root Certificate issues Public Key Certificates to the licensed CAs, while these licensed CAs in turn issue DSCs to end-users.

To gauge the extent of usage of Digital Signatures and the challenges that are being faced in further proliferating growth, a survey was carried out in the year 2007. One of the key findings of the survey was the lack of interoperability between DSCs issued by different CAs resulting in users having to obtain multiple number of DSCs for use across different applications.

This Guideline is the result of the effort made by the office of CCA to achieve interoperability across DSCs issued by different CAs. The first draft DSC profile was circulated widely to the Department of Information Technology, Central Government Departments, IT Secretaries of all States, CAs & major application developers and also published on CCAs website for comments from the public at large. Based on the feedback received, the draft was revised and sent for comments to an international expert in this area. The observations and specific recommendations received in this regard have now been incorporated and the profile that has been prepared is in line with international standards and best practices. These Guidelines also include profiles of other special purpose certificates including Time stamping, OCSP responder, SSL Server, SSL Client, Encryption and Code signing.

We thank all those who have contributed in the framing of these Guidelines and look forward to their continued interest and implementation.

Introduction

As part of the interoperability initiative of the CCA, a comparative analysis of the certificates in use in India was carried out. Also the certificates were compared with the CCA rules and regulations for certificate formats. The comparative analysis of the certificates has highlighted that the majority of the interoperability problems in certificates are due to inconsistency in the 'Issuer' and 'Subject' fields of the certificates. Additionally, many fields were interpreted differently by the CAs. Some key observations from the comparative analysis revealed:

1. The 'Issuer' field in the digital certificates has been interpreted and /or used in 20 different ways especially its sub-fields. The variations ranged from name of the application for which the certificate is meant to company / organization names operating applications.
2. The 'Subject' field shows variety of usage for its sub fields. We observed non-standard implementation of the organization parameters. The Organization Unit sub field interpretation varies across the Certifying Authorities and contains information such as certificate class, subject designations, application specific information etc.
3. There is variation in usage and interpretation of almost all fields in the certificate including fields such as Authority Key Identifier, Key Usage, CRL distribution points etc.

Another major problem of interoperability arose from issuance of various different classes of certificates by each of the Certifying Authorities. There is currently no standard mechanism either for applications or by human inspection of certificate fields to determine the class of the certificate. Although various certifying authorities have attempted to include classes of certificates in various certificate fields or extensions, these are largely non-standard and create uncertainty for end users and applications on interpretation of the fields or extensions.

Many certifying authorities were found to be using sub-CAs for issuing digital certificates. The issue of sub-CA and its place in the overall PKI hierarchy created interoperability issues especially in path development and path validation for applications.

The analysis of the certificate and the applications highlighted the need to create a detailed guideline which addressed the above interoperability issues. This report and guidelines has been issued as part of the CCA interoperability project for digital certificates in India. The guidelines herein are mandated to the licensed certifying authorities in India. Additionally these guidelines are to help applications interpret and process the certificate fields in a uniform manner thus increasing the interoperability of the certificates across applications and ensuring secure usage of the certificates.

Scope and applicability

These guidelines are applicable to all licensed certifying authorities and are to be implemented for all certificates issued by them and their sub-CAs. The guidelines are in continuation and complimentary to the existing rules and regulations issued by the Controller of Certifying Authorities under the powers conferred upon it by the IT Act 2000. These guidelines shall be interpreted along with the existing rules and regulations. In case of any contradictions with any rules and regulations issued prior to these guidelines being issued, these guidelines will be considered as final, unless a clarification stating otherwise has been issued by the CCA.

Revisions

CCA may review and issue updated versions of this document. The revised document will be available on the CCA website.

The interoperability model

The interoperability challenges facing the Indian PKI are two fold - first being standardization of certificate fields and second being the scalability of accommodating business requirements of various classes of certificates and sub-CAs. The interoperability model that has been defined by the CA recommends two major initiatives – organizational guidelines and certificate profile guidelines.

Organizational Guidelines: Under this initiative, the CCA has recommended changes in the way Certifying Authorities are structured and issue certificates. This includes flexibility in operating sub-CAs for business purposes.

Certificate Profile Guidelines: Under Certificate Profile guidelines, CCA has issued detailed guidelines pertaining to certificate fields and extensions. This includes guidance on mandated or recommended values, interpretation and usage for certificate fields / extensions.

Organizational Guidelines

The current India PKI organization structure consists of the Controller of Certifying Authority as the apex body and the Root Certifying Authority of India (RCAI). The RCAI is responsible for issuing digital certificates to Licensed Certifying Authorities (henceforth referred to Certifying Authorities or CA) as per the IT Act 2000. The CAs are responsible for issuing further digital certificates to the end users.

Recommended Organization Hierarchy

In order to facilitate greater flexibility to Certifying Authorities, the CCA allowed the creation of sub-CAs. As per this model, a Certifying Authority can create a sub-CA to meet his business branding requirement. However the sub-CA will be part of the same legal entity as the CA.

- 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
  - A CA with sub-CA must necessarily issue end entity certificates only through its sub-CA. The only exception will be for code signing and time stamping certificates, which may directly be issued by the CA.

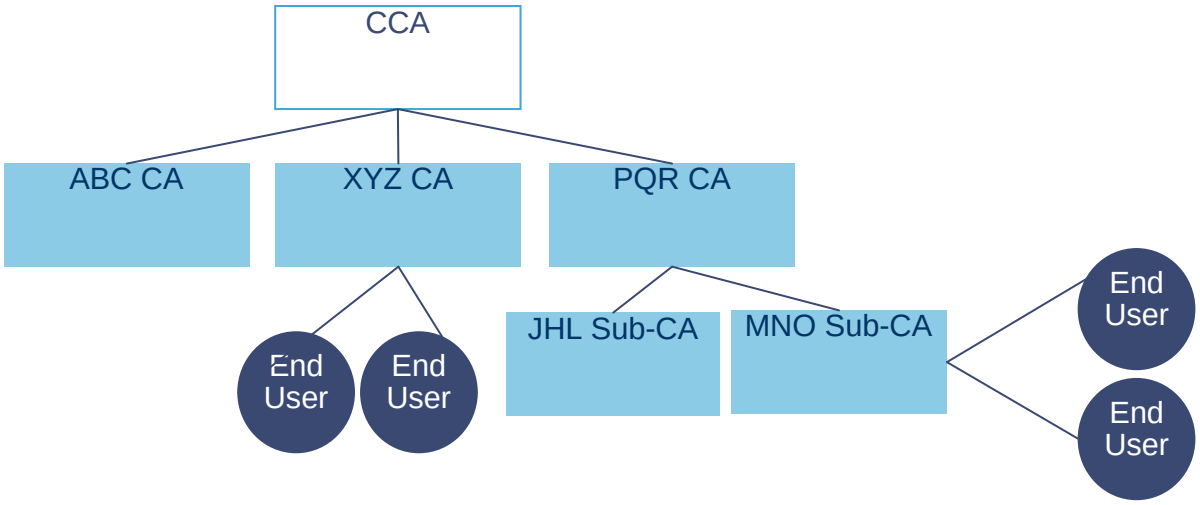

Figure 1: Recommended PKI Hierarchy with sub-CAs

Certificate Profile Guidelines

One of the most important aspects of interoperability is the uniform interpretation of Digital Certificate fields and extensions. The Certificate Profile Guidelines specifies the format of the digital certificate and classifies each of the fields / extensions as following:

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.

Prohibited – 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.

Applications Using Digital Certificates

Applications are to process digital certificates as mentioned in the application developer guidance mentioned in annexure III.

Field Definitions

1. Field Name: **Version**

Mandatory	☑
Optional	☐
Special Purpose	☐
Customisable	☐
Prohibited	☐

Field description	Describes the version of certificate format adopted
Interpretation & usage	This field describes the version of the encoded certificate. Version field is used by the ASN.1 decoding software to parse the certificate.
Compliance Standards	RFC 5280
Type	Positive Integer
Length	1 Integer
Mandated Value	The mandated value is 2. (i.e. The certificate must be in the version 3 format)

2. Field Name: Serial Number

Mandatory	☑
Optional	☐
Special Purpose	☐
Customisable	☐
Prohibited	☐

Field description	Number allocated to a certificate by the issuer CA, unique for a given issuer CA
Interpretation & usage	The serial number field along with the Issuer DN is unique identifier for certificate
Compliance Standards	RFC 5280
Type	Positive Integer
Length	Max 20 Octets (bytes)
Mandated Value	Positive number unique to each certificate issued by a CA.

3. Field Name: Signature

Mandatory	☑
Optional	☐
Special Purpose	☐
Customisable	☐
Prohibited	☐

Field description	Issuer signature algorithm identifier
Interpretation & usage	The signature field identifies the algorithm used by the CA to sign the certificate. This field is used to invoke the appropriate hashing and signature verification algorithm.
Compliance Standards	RFC 5280, RFC 3279, RFC 4055, and RFC 4491
Type	Algorithm OID and Algorithm dependent parameters
Mandated Value	OID for SHA1 with RSA Encryption (null parameters) {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5} OR OID for SHA256 with RSA Encryption (null parameters) {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}

4. Field Name: Issuer

Mandatory	☑
Optional	☐
Special Purpose	☐
Customisable	☐
Prohibited	☐

Field description	Uniquely Identifies the Certifying Authority issuing the certificate
Interpretation & usage	The issuer field identifies the entity that has issued and signed the certificate
Compliance Standards	RFC 5280, X.520
Type	SEQUENCE OF Relative Distinguished Names (RDNs) in printable string format
Mandated Value	Refer Annexure I

6. Field Name: Validity

Mandatory	☑
Optional	☐
Special Purpose	☐
Customisable	☐
Prohibited	☐

Field description	Time interval during which the CA warrants that it will maintain information about the status of the certificate (hence certificate is valid)
Interpretation & usage	The Validity fields are used to assess if the certificate issued is valid. The validity is represented as Sequence of two dates during which the certificate is valid inclusive.
Compliance Standards	RFC 5280
Type	UTC Time / Generalized time
Mandated Value	▪ Validity expressed in UTC Time for certificates valid through 2049 ▪ Validity expressed in Generalized Time for certificates valid through 2050 and beyond ▪ Certificate MUST contain a well defined expiration date. ▪ Sub-CA certificate validity must not exceed CA certificate validity.

6. Field Name: Subject

Mandatory	☑
Optional	☐
Special Purpose	☐
Customisable	☐
Prohibited	☐

Field description	The subject field associates an entity (named in the field) with the public key in the certificate.
Interpretation & usage	The Distinguished Name mentioned in the Subject identifies the owner of the certificate – or the entity to whom the certificate has been issued.
Compliance Standards	RFC 5280, X.520
Type	SEQUENCE OF Relative Distinguished Names (RDNs) in printable string format (except for variations mentioned in Annexure I)
Mandated Value	Refer Annexure I

7. Field Name: Subject Public Key Info

Mandatory	☑
Optional	☐
Special Purpose	☐
Customisable	☐
Prohibited	☐

Field description	Contains the public key algorithm for the subject public key being certified. Also contains the subject public key and the parameters.
Interpretation & usage	Algorithm identifier identifies the algorithm with which the key is used.
Compliance Standards	RFC 5280, RFC 3279, RFC 4055, RFC 4491
Type	OID, OID dependent parameters and Key in bitstring format
Mandated Value	***For CA & sub-CA:*** rsaEncryption, 2048 RSA Key modulus, Public Exponent = $2^{16}+1$ ***For end user***: rsaEncryption, 1024 RSA Key modulus, Public Exponent = $2^{16}+1$ From January 1,2011, CAs must issue 2048-bit RSA SubCA and end-entity certificates

8. Field Name: Unique Identifiers

Mandatory	☐
Optional	☐
Special Purpose	☐
Customisable	☐
Prohibited	☑

Field description	Unique identifier for a subject and issuer names (Subject Unique Identifier, Issuer Unique Identifier)
Interpretation & usage	The certificates MUST NOT generate / use unique identifier for Subject or Issuer.
Compliance Standards	RFC 5280
Type	Printable String
Mandated Value	Field not to be used

9. Field Name: signatureAlgorithm

Mandatory	☑
Optional	☐
Special Purpose	☐
Customisable	☐
Prohibited	☐

Field description	Issuer signature algorithm identifier
Interpretation & usage	The signature field identifies the algorithm used by the CA to sign the certificate. This field is used to invoke the appropriate hashing and signature verification algorithm
Compliance Standards	RFC 5280, RFC 3279, RFC 4055, and RFC 4491
Type	Algorithm OID and Algorithm dependent parameters
Mandated Value	OID for SHA1 with RSA Encryption (null parameters) {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5} OR OID for SHA256 with RSA Encryption (null parameters) {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11} If parameters are present, in this field, they shall be ignored. CAs should make SHA2 end-entity certificates available to customers from January 1 2012.

10. Field Name: signatureValue

Mandatory	☑
Optional	☐
Special Purpose	☐
Customisable	☐
Prohibited	☐

Field description	This field contains the signature on the certificate
Interpretation & usage	The value in this field is used for signature verification. For example, for RSA, this field is decrypted using the public key, then unpadded, and then matched against the hash of the certificate.
Compliance Standards	RFC 5280
Type	Bit string
Mandated Value	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.

Standard Extensions Definition

1. Std. Extension : Authority Key Identifier

Mandatory	☑
Optional	☐
Special Purpose	☐
Customisable	☐
Prohibited	☐
Reserved for future use	☐

Field description	The authority key identifier extension provides means of identifying the public key corresponding to signing key used (by CA) to sign the certificate.
Interpretation & usage	The authority key identifier is used to facilitate certificate path construction.
Compliance Standards	RFC 5280
Type	Octet string
Critical / Non Critical	Non Critical

Mandated Value	This field may be absent in the RCAI certificate. All CAs MUST have Authoritykeyidentifier value same as SubjectkeyIdentifier Value of RCAI* CA Authoritykeyidentifier = Root Certifying Authority of India (RCAI)* SubjectkeyIdentifier (currently 4f 1e c0 58 27 d8 b8 e4) Authoritykeyidentifier value for a certificate shall be the same as the SubjectkeyIdentifier for the Issuer. In other words, certificates issued by a CA shall contain the Authoritykeyidentifier value as the same as the SubjectkeyIdentifier in the CA's own certificate.
Calculation Method	Calculation method has been specified in the SubjectkeyIdentifier section.

* With respect to creation of separate distinct chain for special operations, RCAI will refer to Root Certifying Authority of India Certificate for the respective special operation

2. Std. Extension : Subject Key Identifier

Mandatory	☑
Optional	☐
Special Purpose	☑
Customisable	☐
Prohibited	☐
Reserved for future use	☐

Note: This field is mandatory for all CA / sub-CA / end entity certificates

Field description	The subject key identifier extension provides means of identifying certificates that contain a particular key when the subject has multiple certificates with multiple keys.
Interpretation & usage	The subject key identifier is used to facilitate certificate path construction.
Compliance Standards	RFC 5280
Type	Octet string
Critical / Non Critical	Non Critical
Mandated Value	A CA shall always honour the subject key identifier value requested in a certificate request (e.g., PKCS-10 request). Honouring requested value is critical to interoperability when RCAI issues a CA certificate or a CA issues a sub-CA certificate.

Recommended Value	Subject key identifier can be calculated as per any of the method mentioned below. Any other method which provides a statistically unique value associated with the Public key is also acceptable.
Calculation Method	SubjectKeyIdentifier should be composed of the 160-bit SHA-1 hash of value of the BIT STRING subjectPublicKey in the certificate (excluding the tag, length, and number of unused bits). OR The SubjectKeyIdentifier should be composed of a four-bit type field with value 0100 followed by the least significant 60 bits of SHA-1 hash of the value of the BIT STRING subjectPublicKey (excluding the tag, length, and number of unused bits).

3. Std. Extension : Key Usage

Mandatory	☑
Optional	☐
Special Purpose	☐
Customisable	☐
Prohibited	☐
Reserved for future use	☐

Field description	Key Usage field defines the cryptographic purpose of the key contained in the certificate.
Interpretation & usage	The applications implementing cryptography must interpret this field and restrict the usage of the key accordingly.
Compliance Standards	RFC 5280
Type	Bit string
Critical / Non Critical	Critical
Mandated Value	For CA Certificates, the following key usage MUST be asserted ▪ cRLSign ▪ keyCertsign For end entity signature Certificates, following key usage MUST be asserted ▪ digitalSignature ▪ nonRepudiation

	The following key usage MUST NOT be set / asserted for end entity certificates ▪ cRLSign ▪ keyCertsign

4. Std. Extension : Certificate Policies

Mandatory	☑
Optional	☐
Special Purpose	☐
Customisable	☐
Prohibited	☐
Reserved for future use	☐

Field description	Contains policy information terms in the form of OIDs and qualifiers.
Interpretation & usage	CCA certificate policy the certificate is valid for; and all the lower level CCA certificate policies.
Compliance Standards	RFC 5280
Type	OID, IA5 string
Critical / Non Critical	Non Critical
Mandated Value	The value must contain the OID representing the RCAI certificate policy the certificate is valid for; and all the lower level certificate polices. The end entity certificate should contain User Notice qualifier ‘explicit text’ encoded as Visible string. The string should state the highest Certificate Policy for which the certificate is valid for - as defined by the CCA. The maximum length of the ‘explicit Text’ field is 200 characters.

5. Std. Extension : Policy Mappings

Mandatory	☐
Optional	☐
Special Purpose	☐
Customisable	☐
Prohibited	☑
Reserved for future use	☐

Field description	Lists pairs of OIDs for issuerDomainPolicy and subject DomainPolicy
Interpretation & usage	The use of this Extension is prohibited by the CCA.
Compliance Standards	RFC 5280
Type	SEQUENCE of pairs of OID, each pair itself is a SEQUENCE
Critical / Non Critical	Non Critical
Mandated Value	Field is to not be used

6. Std. Extension : Subject Alternative Name

Mandatory	☐
Optional	☑
Special Purpose	☐
Customisable	☐
Prohibited	☐
Reserved for future use	☐

Field description	Provides additional field to bind the certificate / public key to an identity
Interpretation & usage	Depending upon the type of certificate, the Subject Alternative name must be set to be email ID, IP address or domain name.
Compliance Standards	RFC 5280
Type	Email ID / IP Address / URL / DNS Name
Critical / Non Critical	Non Critical
Mandated Value	Not Applicable
Recommended Value	The following are the recommended formats ▪ For end-entity certificates, email address for RFC822 Name may be included ONLY after verification. It shall be encoded as IA5String ▪ For machine certificates IP Address as mentioned in RFC791 may be

	included in the form of Octet string in network byte order. ▪ For machine certificates, domain name may be included using the structure defined in Section 3.5 of [RFC1034] and encoded as IA5String

7. Std. Extension : Issuer Alternative Name

Mandatory	☐
Optional	☐
Special Purpose	☐
Customisable	☐
Prohibited	☑
Reserved for future use	☐

Field description	This extension is used for binding internet style identities to the issuer.
Interpretation & usage	The use of this field is Prohibited by the CCA.
Compliance Standards	RFC 5280
Type	Email ID / IP Address / URL / DNS Name
Critical / Non Critical	Non Critical
Mandated Value	Extension not to be used

8. Std. Extension : Subject Directory Attributes

Mandatory	☐
Optional	☑
Special Purpose	☐
Customisable	☐
Prohibited	☐
Reserved for future use	☐

Field description	This extension is used to convey subject authorisations.
Interpretation & usage	Field used to convey identification attributes of the subject.
Compliance Standards	RFC 5280
Type	Sequence of attributes
Critical / Non Critical	Non Critical
Mandated Value	Not applicable.
Recommended Value	CCA will provide guidance on this as needs arise.

9. Std. Extension : Basic Constraints

Mandatory	☑
Optional	☐
Special Purpose*	☑
Customisable	☐
Prohibited	☐
Reserved for future use	☐

Note: Mandatory in RCAI, CA & Sub-CA certificates and to be absent in end entity certificates.

Field description	The basic constraints extension identifies whether the subject of the certificate is a CA and the maximum number of CAs may follow in the certification path
Interpretation & usage	The use of this field is used to validate if the public key contained can be used to verify Certificate and CRL signatures and the length of certificate path.
Compliance Standards	RFC 5280
Type	Boolean, Numeric
Critical / Non Critical	Critical
Mandated Value	For a certifying Authority & sub-CA, Basic Constraints field for CA Boolean must be asserted. RCAI self-signed CA certificate shall not contain pathLengthConstraint. CA certificate shall contain pathLengthConstraint = 0 if there are no sub-CA for that licensed CA.

	CA certificate shall contain pathLengthConstraint = 1 if there are sub-CAs for that licensed CA. Sub-CA certificate shall contain pathLengthConstraint = 0. For end user certificate, the field MUST NOT be present.

10. Std. Extension : Name Constraints

Mandatory	☐
Optional	☐
Special Purpose	☐
Customisable	☐
Prohibited	☑
Reserved for future use	☐

Field description	Defines the namespace which can and/or can not be used in subject and subject alternative fields of the certificates issued by the subject CA
Interpretation & usage	Use of this field is prohibited by the CCA
Compliance Standards	RFC 5280
Type	Domain name / IP address /directoryName
Critical / Non Critical	Critical
Mandated Value	Field is not to be used

11. Std. Extension : Policy Constraints

Mandatory	☐
Optional	☐
Special Purpose	☐
Customisable	☐
Prohibited	☑
Reserved for future use	☐

Field description	Limits the policy mapping or mandates an acceptable policy in certificate path.
Interpretation & usage	Use of this field is prohibited by the CCA
Compliance Standards	RFC 5280
Type	OIDs
Critical / Non Critical	Critical
Mandated Value	Field is not to be used

12. Std. Extension : Extended Key Usage

Mandatory	☐
Optional	☑
Special Purpose	☑
Customisable	☐
Prohibited	☐
Reserved for future use	☐

Field description	Further limits the use of a certificate based on cryptographic application.
Interpretation & usage	This field is to be used only for special purpose certificates. For special purpose certificates, refer Annexure II
Compliance Standards	RFC 5280
Type	OID
Critical / Non Critical	Critical / Non Critical as listed below
Mandated Value	None
Recommended Value	CAs MAY configure the following extended key usage as per guidance provided in Annexure II only ▪ id-kp-serverAuth {1 3 6 1 5 5 7 3 1} (for server certificates) – Non Critical ▪ id-kp-clientAuth {1 3 6 1 5 5 7 3 2} (for end user and system certificates) –

	Non Critical ▪ id-kp-codeSigning {1 3 6 1 5 5 7 3 3} (for signing software) -- Critical ▪ id-kp-emailProtection {1 3 6 1 5 5 7 3 4} (email clients) – Non Critical ▪ id-kp-OCSPSigning {1 3 6 1 5 5 7 3 9} (for OCSP Responder Certificate) -- Critical ▪ id-kp-timestamping {1 3 6 1 5 5 7 3 8} (for time stamp authority) -- Critical ▪ anyExtendedKeyUsage {2 5 29 37 0} (for any and all applications) – Non Critical

13. Std. Extension : CRL Distribution Point

Mandatory	☑
Optional	☐
Special Purpose	☐
Customisable	☐
Prohibited	☐
Reserved for future use	☐

Field description	The CRL distribution points extension identifies the location and method by which CRL information can be obtained.
Interpretation & usage	The field is interpreted as a Distribution Point URI.
Compliance Standards	RFC 5280
Type	URI, IA5String
Critical / Non Critical	Non Critical
Mandated Value	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.

14. Std. Extension : Inhibit Any Policy

Mandatory	☐
Optional	☐
Special Purpose	☐
Customisable	☐
Prohibited	☑
Reserved for future use	☐

Field description	When set, this field inhibits an explicit match with special anyPolicy OID { 2 5 29 32 0 }
Interpretation & usage	This field is prohibited to be used by CCA
Compliance Standards	RFC 5280
Type	OID
Critical / Non Critical	Critical
Mandated Value	This field must not be used.

15. Std. Extension : Freshest CRL

Mandatory	☐
Optional	☐
Special Purpose	☐
Customisable	☐
Prohibited	☑
Reserved for future use	☐

Field description	The freshest CRL extension identifies how delta CRL information is obtained.
Interpretation & usage	The use of this field is prohibited by the CCA
Compliance Standards	RFC 5280
Type	URI
Critical / Non Critical	Non Critical
Mandated Value	This field must not be used.

Private Extensions

1. Pvt. Internet Extension : Authority Information Access

Mandatory	☑
Optional	☐
Special Purpose	☐
Customisable	☐
Prohibited	☐
Reserved for future use	☐

Field description	The extension provides information for accessing information and services of the issuer.
Interpretation & usage	The field is used to access information regarding the issuer (such as issuer certificate) and the OCSP service
Compliance Standards	RFC 5280
Type	URI
Critical / Non Critical	Non Critical
Mandated Value	The id-ad-caIssuers MUST point to certificates issued to the CA issuing the certificate containing this field. This 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]. The id-ad-ocsp accesslocation must specify the location of the OCSP responder as an HTTP URL encoded as IA5String using the syntax defined in [RFC5280] for CAs using OCSP. If OCSP is not used, id-ad-ocsp accesslocation accessMethod must not be present.

2. Pvt. Internet Extension : Subject Information Access

Mandatory	☐
Optional	☐
Special Purpose	☐
Customisable	☐
Prohibited	☑
Reserved for future use	☐

Field description	The extension provides information for accessing information and services regarding the subject
Interpretation & usage	The use of this field is prohibited by the CCA
Compliance Standards	RFC 5280
Type	URI
Critical / Non Critical	Non Critical
Mandated Value	This field must not be used.

Annexure I – Issuer and Subject field specification

Background

The issuer field identifies the entity that has signed and issued the certificate. It is required that the Issuer field MUST contain a non-empty distinguished name (DN). The issuer field is defined as the X.501 type Name [X.501].

Subject field associates the public key in the certificate with an entity. The subject field MUST be populated for all certificates issued by a CA. The Subject field MUST contain a X.500 distinguished name (DN). Again, the Subject field too must follow X.501 distinguished name format.

A distinguished name consist of a hierarchical structure composed of attributes such as Common name, organization, organization unit, common name etc. and the corresponding vales for these attributes. The standard set of attributes is defined in the X.520 specification.

As explained in the first section of this report, the India PKI hierarchy is depicted in the figure below.

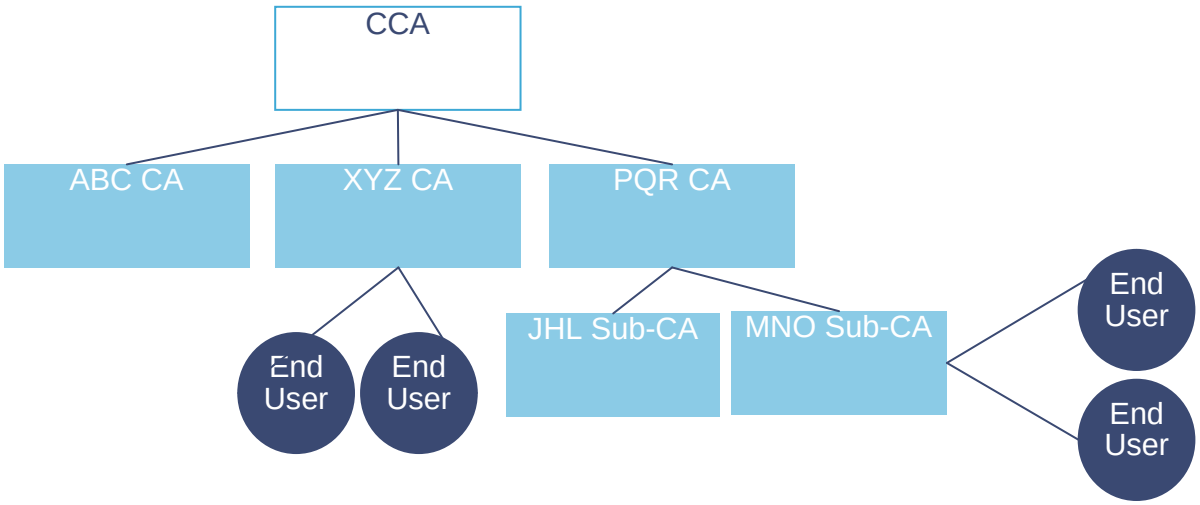

Figure 2: PKI Hierarchy

Naming Conventions

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 {Generation Qualifier} (re-issuance number}	XYZ CA 2009 XYZ CA 2009-1
Sub-CA	"Certifying Authority Name" sub-CA for "Branding Name" {Generation qualifier} (re-issuance number}	XYZ Sub CA for Income Tax 2009 XYZ Sub CA for Income Tax 2009-1

Note: The generation qualifier will be used only on re-issuance of certificate keys for the CA. The generation qualifier necessarily is to be in the form of 4 digit year (yyyy). In case multiple certificates have been issued in the same year, the year indicator is to be followed by hyphen and digit indicating the re-issuance of certificate. E.g. When a certificate is issued in 2009, the CA name will be XYZ CA 2009. When the certificate is reissued in the same year, the CA name will be indicate as 2009 – 1.

Each Relative Distinguished Name (RDN) shall contain a single attribute type and associated value.

Attribute values shall be encoded as specified below:

Sr. 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	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

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.

Sr. No.	Certificate Type	Issuer	Subject
1	RCAI*	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

CCA Certificate – SUBJECT and ISSUER specifications

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

Sr. No.	Attribute	Value
1	Common Name (CN)	CCA India {Generation Qualifier} (re-issuance number}
2	Organisation (O)	India PKI*
3	Country (C)	India (IN)

CA Certificate –Issuer specifications

Sr. No.	Attribute	Value
1	Common Name (CN)	CCA India {Generation Qualifier} (re-issuance number}
2	Organisation (O)	India PKI*
3	Country (C)	India (IN)

* With respect to creation of separate distinct chain for special operation "O=India PKI" will be substituted with "O=India PKI (XXXXXXXXXXX operations)"

CA Certificate – SUBJECT specifications

Sr. No.	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 organisational recommendations section)
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 • Locality / colony name • (nearest) Street Name • Town / Suburb / Village • City name (if applicable) • District
4	State / Province	Max Length: 60 Characters • State / province where the Certifying Authority has its head office or registered office
5.	Postal Code	Pin Code of the CA's head office or registered office address
6	Organisational Unit (OU)	"Certifying Authority"
7	Organisation (O)	Max Length: 64 Characters Legal Name of the Organisation operating the CA*

* With respect to creation of separate distinct chain for special operation "O= Legal Name of the Organization operating CA " will be substituted with "O= Legal Name of the Organization operating CA (XXXXXXXXXXX operations)"

8	Country (C)	Max Length: 2 Characters Country code as per the verified residential / office address

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

Sr. 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	State / Province	Same as SUBJECT field in Issuer CA certificate
5.	Postal Code	Same as SUBJECT field in Issuer CA certificate
6	Organisational Unit (OU)	Same as SUBJECT field in Issuer CA certificate
7	Organisation (O)	Same as SUBJECT field in Issuer CA certificate
8	Country (C)	Same as SUBJECT field in Issuer CA certificate

Sub-CA Certificate – Subject specifications

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

End User Certificate (Issued by a Sub-CA) – Issuer specifications
Issuer Field for Sub-CA MUST be same as the Subject Field for the Sub-CA have been again provided here for easy reference

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

End User Certificate –Subject Specifications

Sn.	Attribute	Definition
1.	• Common Name	Max Length: 64 Characters • The Common name MUST be constructed in the following manner • **CN = "Surname" "Given Name" "Father / Husband's name" "Initials"** • ***Surname*** • The surname is name 'inherited' by and individual from individual's parent or assumed by marriage. • In the Indian 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, 'gotra', trade, Indian tile, Indian 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.

Sn.	Attribute	Definition
		• ***Father / Husband's name*** • This is the given name for the individual's father or husband. Father / Husband's name MAY be substituted with an initial. • ***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	This attribute should be populated with the SHA 256 hash of the PAN number of the end user. The hash must be calculated for the PAN number after deleting all leading and trailing blanks. In case PAN has not been provided, this field must be omitted.
3.	Unique Identifier	This is a reserved attribute and shall be used in the future for SHA 256 hash of Citizen ID or any other Unique ID for individuals. Currently this attribute is omitted.
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.
5	Postal Code	PIN Code for the for Subject's residential or office address.
6	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"
7	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"
8	Country	Max Length: 2 Characters Country code as per the verified residential / office address

Certificate Subject & Issuer Examples

The subject and issuer profiles starting CA certificate onwards are illustrated below.

1. (n)Code Solutions

CA Certificate

Issuer DN

Attribute	Value
Common Name (CN)	CCA India 2007
Organization (O)	India PKI*
Country (C)	India (IN)

Subject DN

Attribute	Value
Common Name (CN)	(n)Code Solutions CA {Generation Qualifier} (re-issuance number}
House Identifier	301, GNFC Infotower
Street Address	Bodakdev, S G Road, Ahmedabad
State / Province	Gujarat
Postal Code	380054
Organizational Unit (OU)	Certifying Authority
Organization (O)	Gujarat Narmada Valley Fertilizers Company Ltd.**
Country (C)	IN

* With respect to creation of separate distinct chain for special operation "O=India PKI" will be substituted with "O=India PKI (XXXXXXXXXXX operations)"

** With respect to creation of separate distinct chain for special operation "O= Legal Name of the Organization operating CA " will be substituted with "O= Legal Name of the Organization operating CA (XXXXXXXXXXX operations)"

Sub-CA Certificate

Issuer DN

Attribute	Value
Common Name (CN)	(n)Code Solutions CA {Generation Qualifier} {Re-issuance Number}
House Identifier	301, GNFC Infotower
Street Address	Bodakdev, S G Road, Ahmedabad
State / Province	Gujarat
Postal Code	380054
Organizational Unit (OU)	Certifying Authority
Organization (O)	Gujarat Narmada Valley Fertilizers Company Ltd.**
Country (C)	IN

Subject DN

Attribute	Value
Common Name (CN)	(n)Code Solutions sub-CA for Income Tax {Generation Qualifier} {Re-issuance Number}
Organizational Unit (OU)	Sub-CA
Organization (O)	Gujarat Narmada Valley Fertilizers Company Ltd.**
Country (C)	IN

End User Certificate Profile (issued by CA)

Issuer DN

Attribute	Value
Common Name (CN)	(n)Code Solutions CA {Generation Qualifier} {Re-issuance Number}
House Identifier	301, GNFC Infotower
Street Address	Bodakdev, S G Road, Ahmedabad
State / Province	Gujarat
Postal Code	380054
Organizational Unit (OU)	Certifying Authority
Organization (O)	Gujarat Narmada Valley Fertilizers Company Ltd.**
Country (C)	IN

Subject DN

** With respect to creation of separate distinct chain for special operation "O= Legal Name of the Organization operating CA " will be substituted with "O= Legal Name of the Organization operating CA (XXXXXXXXXXX operations)"

Attribute	Value
Common Name (CN)	Joshi Amrut Manohar
Serial Number	794dbed34bedd3659726f53e44b482b5fc30c76f44baa328522047551c1a4fa4
State or Province Name	Uttar Pradesh
Postal Code	226020
Organizational Unit (OU)	Marketing
Organization (O)	OM Constructions Pvt. Ltd.
Country (C)	IN

End User Certificate Profile (issued by sub-CA)

Issuer DN

Attribute	Value
Common Name (CN)	(n)Code Solutions sub-CA for Income Tax {Generation Qualifier} {Re-issuance Number}
Organizational Unit (OU)	Sub-CA
Organization (O)	Gujarat Narmada Valley Fertilizers Company Ltd.**
Country (C)	IN

Subject DN

Attribute	Value
Common Name (CN)	Joshi Amrut Manohar
Serial Number	794DBED34BEDD3659726F53E44B482B5FC30C76F44BAA328522047551C1A4FA4
State or Province Name	Uttar Pradesh
Postal Code	226020
Organizational Unit (OU)	Marketing
Organization (O)	OM Constructions Pvt. Ltd.
Country (C)	IN

** With respect to creation of separate distinct chain for special operation "O= Legal Name of the Organization operating CA " will be substituted with "O= Legal Name of the Organization operating CA (XXXXXXXXXXX operations)"

2. MTNL TrustLine

CA Certificate

Issuer DN

Attribute	Value
Common Name (CN)	CCA India 2007
Organization (O)	India PKI*
Country (C)	India (IN)

Subject DN

Attribute	Value
Common Name (CN)	MTNL TrustLine CA {Generation Qualifier} {Re-issuance Number}
House Identifier	5515, 5th Floor, Core - V Mahanagar Doorsanchar Sadan
Street Address	CGO Complex, Lodhi Road,
State / Province	New Delhi
Postal Code	110003
Organizational Unit (OU)	Certifying Authority
Organization (O)	Mahanagar Telephone Nigam Limited**
Country (C)	IN

* With respect to creation of separate distinct chain for special operation "O=India PKI" will be substituted with "O=India PKI (XXXXXXXXXXX operations)"

** With respect to creation of separate distinct chain for special operation "O= Legal Name of the Organization operating CA " will be substituted with "O= Legal Name of the Organization operating CA (XXXXXXXXXXX operations)"

Sub-CA Certificate

Issuer DN

Attribute	Value
Common Name (CN)	MTNL TrustLine CA {Generation Qualifier} {Re-issuance Number}
House Identifier	5515, 5th Floor, Core - V Mahanagar Doorsanchar Sadan
Street Address	CGO Complex, Lodhi Road,
State / Province	New Delhi
Postal Code	110003
Organizational Unit (OU)	Certifying Authority
Organization (O)	Mahanagar Telephone Nigam Limited**
Country (C)	IN

Subject DN

Attribute	Value
Common Name (CN)	MTNL TrustLine sub-CA for Income Tax {Generation Qualifier} {Re-issuance Number}
Organizational Unit (OU)	Sub-CA
Organization (O)	Mahanagar Telephone Nigam Limited**
Country (C)	IN

End User Certificate Profile (issued by CA)

Issuer DN

Attribute	Value
Common Name (CN)	MTNL TrustLine CA {Generation Qualifier} {Re-issuance Number}
State / Province	New Delhi
Postal Code	110003
Organizational Unit (OU)	Certifying Authority
Organization (O)	Mahanagar Telephone Nigam Limited**
Country (C)	IN

Subject DN

** With respect to creation of separate distinct chain for special operation "O= Legal Name of the Organization operating CA " will be substituted with "O= Legal Name of the Organization operating CA (XXXXXXXXXXX operations)"

Attribute	Value
Common Name (CN)	Joshi Amrut Manohar
Serial Number	794DBED34BEDD3659726F53E44B482B5FC30C76F44BAA328522047551C1A4FA4
State or Province Name	Uttar Pradesh
Postal Code	226020
Organizational Unit (OU)	Marketing
Organization (O)	OM Constructions Pvt. Ltd.
Country (C)	IN

End User Certificate Profile (issued by sub-CA)

Issuer DN

Attribute	Value
Common Name (CN)	MTNL TrustLine sub-CA for Income Tax {Generation Qualifier} {Re-issuance Number}
Organizational Unit (OU)	Sub-CA
Organization (O)	Mahanagar Telephone Nigam Limited**
Country (C)	IN

Subject DN

Attribute	Value
Common Name (CN)	Joshi Amrut Manohar
Serial Number	794DBED34BEDD3659726F53E44B482B5FC30C76F44BAA328522047551C1A4FA4
State or Province Name	Uttar Pradesh
Postal Code	226020
Organizational Unit (OU)	Marketing
Organization (O)	OM Constructions Pvt. Ltd.
Country (C)	IN

** With respect to creation of separate distinct chain for special operation "O= Legal Name of the Organization operating CA " will be substituted with "O= Legal Name of the Organization operating CA (XXXXXXXXXXX operations)"

3. TCS CA

CA Certificate

Issuer DN

Attribute	Value
Common Name (CN)	CCA India 2007
Organization (O)	India PKI*
Country (C)	India (IN)

Subject DN

Attribute	Value
Common Name (CN)	TCS CA {Generation Qualifier} {Re-issuance Number}
House Identifier	11th Floor, Air India Building
Street Address	Nariman Point, Mumbai
State / Province	Maharashtra
Postal Code	400 021
Organizational Unit (OU)	Certifying Authority
Organization (O)	Tata Consultancy Services Ltd.**
Country (C)	IN

* With respect to Mauritius Operations, “O=India PKI” will be substituted with “O=India PKI for Mauritius Operations”

** With respect to creation of separate distinct chain for special operation "O= Legal Name of the Organization operating CA " will be substituted with "O= Legal Name of the Organization operating CA (XXXXXXXXXXX operations)"

Sub-CA Certificate

Issuer DN

Attribute	Value
Common Name (CN)	TCS CA {Generation Qualifier} {Re-issuance Number}
House Identifier	11th Floor, Air India Building
Street Address	Nariman Point, Mumbai
State / Province	Maharashtra
Postal Code	400 021
Organizational Unit (OU)	Certifying Authority
Organization (O)	Tata Consultancy Services Ltd.**
Country (C)	IN

Subject DN

Attribute	Value
Common Name (CN)	TCS sub-CA for Income Tax {Generation Qualifier} {Re-issuance Number}
Organizational Unit (OU)	Sub-CA
Organization (O)	Tata Consultancy Services Ltd.**
Country (C)	IN

End User Certificate Profile (issued by CA)

Issuer DN

Attribute	Value
Common Name (CN)	TCS CA {Generation Qualifier} {Re-issuance Number}
House Identifier	11th Floor, Air India Building
Street Address	Nariman Point, Mumbai
State / Province	Maharashtra
Postal Code	400 021
Organizational Unit (OU)	Certifying Authority
Organization (O)	Tata Consultancy Services Ltd.**
Country (C)	IN

Subject DN

** With respect to creation of separate distinct chain for special operation "O= Legal Name of the Organization operating CA " will be substituted with "O= Legal Name of the Organization operating CA (XXXXXXXXXXX operations)"

Attribute	Value
Common Name (CN)	Joshi Amrut Manohar
Serial Number	794DBED34BEDD3659726F53E44B482B5FC30C76F44BAA328522047551C1A4FA4
State or Province Name	Uttar Pradesh
Postal Code	226020
Organizational Unit (OU)	Marketing
Organization (O)	OM Constructions Pvt. Ltd.
Country (C)	IN

End User Certificate Profile (issued by sub-CA)

Issuer DN

Attribute	Value
Common Name (CN)	TCS sub-CA for Income Tax {Generation Qualifier} {Re-issuance Number}
Organizational Unit (OU)	Sub-CA
Organization (O)	Tata Consultancy Services Ltd.**
Country (C)	IN

Subject DN

Attribute	Value
Common Name (CN)	Joshi Amrut Manohar
Serial Number	794DBED34BEDD3659726F53E44B482B5FC30C76F44BAA328522047551C1A4FA4
State or Province Name	Uttar Pradesh
Postal Code	226020
Organizational Unit (OU)	Marketing
Organization (O)	OM Constructions Pvt. Ltd.
Country (C)	IN

** With respect to creation of separate distinct chain for special operation "O= Legal Name of the Organization operating CA " will be substituted with "O= Legal Name of the Organization operating CA (XXXXXXXXXXX operations)"

4. iTrust CA (IDRBT)

CA Certificate

Issuer DN

DN Attribute	Value
Common Name (CN)	CCA India 2007
Organization (O)	India PKI*
Country (C)	India (IN)

Subject DN

Attribute	Value
Common Name (CN)	IDRBT CA {Generation Qualifier} {Re-issuance Number}
House Identifier	Castle Hills
Street Address	Road No. 1, Masab Tank, Hyderabad
State / Province	Andhra Pradesh
Postal Code	500 057
Organizational Unit (OU)	Certifying Authority
Organization (O)	Institute for Development & Research in Banking Technology**
Country (C)	IN

* With respect to creation of separate distinct chain for special operation "O=India PKI" will be substituted with "O=India PKI (XXXXXXXXXXX operations)"

** With respect to creation of separate distinct chain for special operation "O= Legal Name of the Organization operating CA " will be substituted with "O= Legal Name of the Organization operating CA (XXXXXXXXXXX operations)"

Sub-CA Certificate

Issuer DN

Attribute	Value
Common Name (CN)	IDRBT CA {Generation Qualifier} {Re-issuance Number}
House Identifier	Castle Hills
Street Address	Road No. 1, Masab Tank, Hyderabad
State / Province	Andhra Pradesh
Postal Code	500 057
Organizational Unit (OU)	Certifying Authority
Organization (O)	Institute for Development & Research in Banking Technology**
Country (C)	IN

Subject DN

Attribute	Value
Common Name (CN)	IDRBT sub-CA for Income Tax {Generation Qualifier} {Re-issuance Number}
Organizational Unit (OU)	Sub-CA
Organization (O)	Institute for Development & Research in Banking Technology**
Country (C)	IN

End User Certificate Profile (issued by CA)

Issuer DN

Attribute	Value
Common Name (CN)	IDRBT CA {Generation Qualifier} {Re-issuance Number}
House Identifier	Castle Hills
Street Address	Road No. 1, Masab Tank, Hyderabad
State / Province	Andhra Pradesh
Postal Code	500 057
Organizational Unit (OU)	Certifying Authority
Organization (O)	Institute for Development & Research in Banking Technology**
Country (C)	IN

Subject DN

** With respect to creation of separate distinct chain for special operation "O= Legal Name of the Organization operating CA " will be substituted with "O= Legal Name of the Organization operating CA (XXXXXXXXXXX operations)"

Attribute	Value
Common Name (CN)	Joshi Amrut Manohar
Serial Number	794DBED34BEDD3659726F53E44B482B5FC30C76F44BAA328522047551C1A4FA4
State or Province Name	Uttar Pradesh
Postal Code	226020
Organizational Unit (OU)	Marketing
Organization (O)	OM Constructions Pvt. Ltd.
Country (C)	IN

End User Certificate Profile (issued by sub-CA)

Issuer DN

Attribute	Value
Common Name (CN)	IDRBT sub-CA for Income Tax {Generation Qualifier} {Re-issuance Number}
Organizational Unit (OU)	Sub-CA
Organization (O)	Institute for Development & Research in Banking Technology**
Country (C)	IN

Subject DN

Attribute	Value
Common Name (CN)	Joshi Amrut Manohar
Serial Number	794DBED34BEDD3659726F53E44B482B5FC30C76F44BAA328522047551C1A4FA4
State or Province Name	Uttar Pradesh
Postal Code	226020
Organizational Unit (OU)	Marketing
Organization (O)	OM Constructions Pvt. Ltd.
Country (C)	IN

** With respect to creation of separate distinct chain for special operation "O= Legal Name of the Organization operating CA " will be substituted with "O= Legal Name of the Organization operating CA (XXXXXXXXXXX operations)"

5. NIC CA

CA Certificate

Issuer DN

Attribute	Value
Common Name (CN)	CCA India 2007
Organization (O)	India PKI*
Country (C)	India (IN)

Subject DN

Attribute	Value
Common Name (CN)	NIC CA {Generation Qualifier} {Re-issuance Number}
House Identifier	Ministry of Communications and Information Technology, A-Block,
Street Address	CGO Complex, Lodhi Road,
State / Province	New Delhi
Postal Code	110 003
Organizational Unit (OU)	Certifying Authority
Organization (O)	National Informatics Centre**
Country (C)	IN

* With respect to creation of separate distinct chain for special operation "O=India PKI" will be substituted with "O=India PKI (XXXXXXXXXXX operations)"

** With respect to creation of separate distinct chain for special operation "O= Legal Name of the Organization operating CA " will be substituted with "O= Legal Name of the Organization operating CA (XXXXXXXXXXX operations)"

Sub-CA Certificate

Issuer DN

Attribute	Value
Common Name (CN)	NIC CA {Generation Qualifier} {Re-issuance Number}
House Identifier	Ministry of Communications and Information Technology, A-Block,
Street Address	CGO Complex, Lodhi Road,
State / Province	New Delhi
Postal Code	110 003
Organizational Unit (OU)	Certifying Authority
Organization (O)	National Informatics Centre**
Country (C)	IN

Subject DN

Attribute	Value
Common Name (CN)	NIC sub-CA for Income Tax {Generation Qualifier} {Re-issuance Number}
Organizational Unit (OU)	Sub-CA
Organization (O)	National Informatics Centre**
Country (C)	IN

End User Certificate Profile (issued by CA)

Issuer DN

Attribute	Value
Common Name (CN)	NIC CA {Generation Qualifier} {Re-issuance Number}
House Identifier	Ministry of Communications and Information Technology, A-Block,
Street Address	CGO Complex, Lodhi Road,
State / Province	New Delhi
Postal Code	110 003
Organizational Unit (OU)	Certifying Authority
Organization (O)	National Informatics Centre**
Country (C)	IN

Subject DN

** With respect to creation of separate distinct chain for special operation "O= Legal Name of the Organization operating CA " will be substituted with "O= Legal Name of the Organization operating CA (XXXXXXXXXXX operations)"

Attribute	Value
Common Name (CN)	Joshi Amrut Manohar
Serial Number	794DBED34BEDD3659726F53E44B482B5FC30C76F44BAA328522047551C1A4FA4
State or Province Name	Uttar Pradesh
Postal Code	226020
Organizational Unit (OU)	Marketing
Organization (O)	OM Constructions Pvt. Ltd.
Country (C)	IN

End User Certificate Profile (issued by sub-CA)

Issuer DN

Attribute	Value
Common Name (CN)	NIC sub-CA for Income Tax {Generation Qualifier} {Re-issuance Number}
Organizational Unit (OU)	Sub-CA
Organization (O)	National Informatics Centre**
Country (C)	IN

Subject DN

Attribute	Value
Common Name (CN)	Joshi Amrut Manohar
Serial Number	794DBED34BEDD3659726F53E44B482B5FC30C76F44BAA328522047551C1A4FA4
State or Province Name	Uttar Pradesh
Postal Code	226020
Organizational Unit (OU)	Marketing
Organization (O)	OM Constructions Pvt. Ltd.
Country (C)	IN

** With respect to creation of separate distinct chain for special operation "O= Legal Name of the Organization operating CA " will be substituted with "O= Legal Name of the Organization operating CA (XXXXXXXXXXX operations)"

7. Safescrypt CA

CA Certificate

Issuer DN

Attribute	Value
Common Name (CN)	CCA India 2007
Organization (O)	India PKI*
Country (C)	India (IN)

Subject DN

Attribute	Value
Common Name (CN)	Safescrypt CA {Generation Qualifier} {Re-issuance Number}
House Identifier	II Floor, Tidel Park,
Street Address	4 Canal Bank Road, Taramani, Chennai,
State / Province	Tamil Nadu
Postal Code	600 113
Organizational Unit (OU)	Certifying Authority
Organization (O)	Safescrypt Ltd.**
Country (C)	IN

* With respect to creation of separate distinct chain for special operation "O=India PKI" will be substituted with "O=India PKI (XXXXXXXXXXX operations)"

** With respect to creation of separate distinct chain for special operation "O= Legal Name of the Organization operating CA " will be substituted with "O= Legal Name of the Organization operating CA (XXXXXXXXXXX operations)"

Sub-CA Certificate

Issuer DN

Attribute	Value
Common Name (CN)	Safescrypt CA {Generation Qualifier} {Re-issuance Number}
House Identifier	II Floor, Tidel Park,
Street Address	4 Canal Bank Road, Taramani, Chennai,
State / Province	Tamil Nadu
Postal Code	600 113
Organizational Unit (OU)	Certifying Authority
Organization (O)	Safescrypt Ltd.**
Country (C)	IN

Subject DN

Attribute	Value
Common Name (CN)	Safescrypt sub-CA for Income Tax {Generation Qualifier} {Re-issuance Number}
Organizational Unit (OU)	Sub-CA
Organization (O)	Safescrypt Ltd.**
Country (C)	IN

End User Certificate Profile (issued by CA)

Issuer DN

Attribute	Value
Common Name (CN)	Safescrypt CA {Generation Qualifier} {Re-issuance Number}
House Identifier	II Floor, Tidel Park,
Street Address	4 Canal Bank Road, Taramani, Chennai,
State / Province	Tamil Nadu
Postal Code	600 113
Organizational Unit (OU)	Certifying Authority
Organization (O)	Safescrypt Ltd.**
Country (C)	IN

Subject DN

** With respect to creation of separate distinct chain for special operation "O= Legal Name of the Organization operating CA " will be substituted with "O= Legal Name of the Organization operating CA (XXXXXXXXXXX operations)"

Attribute	Value
Common Name (CN)	Joshi Amrut Manohar
Serial Number	794DBED34BEDD3659726F53E44B482B5FC30C76F44BAA328522047551C1A4FA4
State or Province Name	Uttar Pradesh
Postal Code	226020
Organizational Unit (OU)	Marketing
Organization (O)	OM Constructions Pvt. Ltd.
Country (C)	IN

End User Certificate Profile (issued by sub-CA)

Issuer DN

Attribute	Value
Common Name (CN)	Safescrypt sub-CA for Income Tax {Generation Qualifier} {Re-issuance Number}
Organizational Unit (OU)	Sub-CA
Organization (O)	Safescrypt Ltd.**
Country (C)	IN

Subject DN

Attribute	Value
Common Name (CN)	Joshi Amrut Manohar
Serial Number	794DBED34BEDD3659726F53E44B482B5FC30C76F44BAA328522047551C1A4FA4
State or Province Name	Uttar Pradesh
Postal Code	226020
Organizational Unit (OU)	Marketing
Organization (O)	OM Constructions Pvt. Ltd.
Country (C)	IN

** With respect to creation of separate distinct chain for special operation "O= Legal Name of the Organization operating CA " will be substituted with "O= Legal Name of the Organization operating CA (XXXXXXXXXXX operations)"

8. e-Mudhra CA

CA Certificate

Issuer DN

Attribute	Value
Common Name (CN)	CCA India 2007
Organization (O)	India PKI*
Country (C)	India (IN)

Subject DN

Attribute	Value
Common Name (CN)	e-Mudhra CA {Generation Qualifier} {Re-issuance Number}
House Identifier	TOWER No 5,3-6 Floor, International Info Park,
Street Address	Vashi, Navi Mumbai
State / Province	Maharashtra
Postal Code	400 703
Organizational Unit (OU)	Certifying Authority
Organization (O)	3i Infotech Consumer Services Ltd**
Country (C)	IN

* With respect to creation of separate distinct chain for special operation "O=India PKI" will be substituted with "O=India PKI (XXXXXXXXXXX operations)"

** With respect to creation of separate distinct chain for special operation "O= Legal Name of the Organization operating CA " will be substituted with "O= Legal Name of the Organization operating CA (XXXXXXXXXXX operations)"

Sub-CA Certificate

Issuer DN

Attribute	Value
Common Name (CN)	e-Mudhra CA {Generation Qualifier} {Re-issuance Number}
House Identifier	TOWER No 5,3-6 Floor, International Info Park,
Street Address	Vashi, Navi Mumbai
State / Province	Maharashtra
Postal Code	400 703
Organizational Unit (OU)	Certifying Authority
Organization (O)	3i Infotech Consumer Services Ltd**
Country (C)	IN

Subject DN

Attribute	Value
Common Name (CN)	e-Mudhra sub-CA for Income Tax {Generation Qualifier} {Re-issuance Number}
Organizational Unit (OU)	Sub-CA
Organization (O)	3i Infotech Consumer Services Ltd**
Country (C)	IN

End User Certificate Profile (issued by CA)

Issuer DN

Attribute	Value
Common Name (CN)	e-Mudhra CA {Generation Qualifier} {Re-issuance Number}
House Identifier	TOWER No 5,3-6 Floor, International Info Park,
Street Address	Vashi, Navi Mumbai
State / Province	Maharashtra
Postal Code	400 703
Organizational Unit (OU)	Certifying Authority
Organization (O)	3i Infotech Consumer Services Ltd**
Country (C)	IN

Subject DN

** With respect to creation of separate distinct chain for special operation "O= Legal Name of the Organization operating CA " will be substituted with "O= Legal Name of the Organization operating CA (XXXXXXXXXXX operations)"

Attribute	Value
Common Name (CN)	Joshi Amrut Manohar
Serial Number	794DBED34BEDD3659726F53E44B482B5FC30C76F44BAA328522047551C1A4FA4
State or Province Name	Uttar Pradesh
Postal Code	226020
Organizational Unit (OU)	Marketing
Organization (O)	OM Constructions Pvt. Ltd.
Country (C)	IN

End User Certificate Profile (issued by sub-CA)

Issuer DN

Attribute	Value
Common Name (CN)	e-Mudhra sub-CA for Income Tax {Generation Qualifier} {Re-issuance Number}
Organizational Unit (OU)	Sub-CA
Organization (O)	3i Infotech Consumer Services Ltd**
Country (C)	IN

Subject DN

Attribute	Value
Common Name (CN)	Joshi Amrut Manohar
Serial Number	794DBED34BEDD3659726F53E44B482B5FC30C76F44BAA328522047551C1A4FA4
State or Province Name	Uttar Pradesh
Postal Code	226020
Organizational Unit (OU)	Marketing
Organization (O)	OM Constructions Pvt. Ltd.
Country (C)	IN

** With respect to creation of separate distinct chain for special operation "O= Legal Name of the Organization operating CA " will be substituted with "O= Legal Name of the Organization operating CA (XXXXXXXXXXX operations)"

Annexure II - Special Purpose Certificates

Generally digital certificates are issued to persons for the purpose of digital signature. However some special uses of digital certificate exists for which the certificate fields and extensions vary. These certificates are termed by CCA as special purpose certificates. The special purpose certificates issues by a licensed CA will be compliant with the specifications mentioned in this document. Additionally, licensed CA may not issue any type of special certificates other than those mentioned herein unless explicit approval from CCA has been obtained for the same. The special purpose certificates approved by CCA are as follows.

1. SSL Certificate

The SSL or secure sockets layer certificate is a certificate assigned to web server. The variation in the certificate fields and extensions as compared to general specification is as follows

Sn.	Field / Extension	Variation
1.	• Subject Name	• The CN in the Subject Name MAY contain either ▪ Qualified domain name ▪ IP addresses of the server as a printable string in "network byte order", as specified in [RFC791]
2.	• Key Usage	• The key usage field MUST have ONLY the following parameters set ▪ Digital Signature, Key Encipherment
3.	• Extended Key usage	• If present, extended key usage MUST include ▪ Server authentication id-kp-serverAuth {1 3 6 1 5 5 7 3 1} ▪ Client Authentication id-kp-clientAuth {1 3 6 1 5 5 7 3 2}
4.	• Subject Alternative Name	The Subject alternative name shall contain the DNS name for the server / web page as an IA5 string

2. System Certificates

Where certificates need to be issued to computer systems for the purpose of machine to machine authentication, it is of paramount importance that the certificate contains a unique identification relating to the systems. At the same time, it is essential that the applications making use of such certificates are designed to verify the system with the digital certificate being used. The certificate field requirements for system certificates include

Sn.	Field / Extension	Variation
1.	• Subject Name	• The CN in the Subject Name MUST contain either ▪ IP Address of the system as a printable string in "network byte order", as specified in [RFC791] ▪ 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 (such as CPU identifier) as a printable string
2.	• Key Usage	▪ Server authentication ▪ Client Authentication
3.	• Subject Alternative Name	• Subject Alternative Name MUST contain either ▪ IP Address of the system as a octet string in "network byte order", as specified in [RFC791] ▪ dnsName in IA5String format

Applications wishing to utilise these certificates must be developed to independently verify the CN vis-à-vis the actual at the time of each transaction. Additionally, the private key of the certificate should be held in a secure token or smart cards. For applications processing sensitive or high value transactions, it is recommended that the private key be stored in a Hardware Security Module (HSM).

3. Time stamping authority certificate

Licensed CAs in India my issue certificates for the purpose of time stamping. It is recommended by the CCA that a time stamping certificate should be exclusively used for the purpose. The only variation for time stamping certificate will be the Extended Key Usage extension. The extension should be set as

Sn.	Field / Extension	Variation
1.	• Subject	Should follow same naming conventions as a CA with “CA” and “Certifying Authority” replaced with “TSA” and “Time Stamping Authority” respectively
2.	• Key Usage	Digital Signature
3.	• Extended Key Usage	Time stamping id-kp-timestamping {1 3 6 1 5 5 7 3 8} -- Critical

These certificates are to be issued to persons or agencies acting as time stamping authorities.

4. Code Signing

Signing of software code is gaining importance. End users and corporations may wish to sign the software code to indicate genuineness of the software. Certificates may be issued by licensed CAs for code signing purposes. The certificate key usage field MUST be set as follows

Sn.	Field / Extension	Variation
1.	• Key Usage	▪ Digital Signature
2.	• Extended Key Usage	▪ Code Signing id-kp-codeSigning {1 3 6 1 5 5 7 3 3} -- Critical

5. Encryption Certificate

Certificates for encryption of information must be separate from normal end-user / subscriber digital signature certificate. The certificate may be used for data encryption / decryption or email protection. The variations would exist in the key usage and extended key usage fields as below

Sn.	Field / Extension	Variation
1.	• Key Usage	• Key encipherment

6. OCSP Responder Certificate

The OCSP responder certificates will have the following variation in the fields.

Sn.	Field / Extension	Variation
1.	Validity Period	Validity expressed in UTC Time for certificates valid through 2049
2.	Subject Distinguished Name	Common Name (CN): <OCSP Responder Name> Organisational Unit (OU): OCSP Responder Organisation (O): Legal Name of the OCSP Organization Country (C): Country code as per the verified office address
3.	Key Usage	DigitalSignature
4.	Certificate Policies	The value must contain the OID representing the CCA certificate policy the certificate is valid for; and all the lower level certificate polices.
5.	Extended Key Usage	id-kp-OCSPSigning {1 3 6 1 5 5 7 3 9}

Annexure III - Reference Certificate Profiles

This section provides reference certificate profiles for use of Certifying Authority for creation and issuance of Digital Certificate.

Legend
M: Mandatory
O: Optional

C: Critical
NC: Non Critical

CA Certificate Profile

Sn.	Field	M/O	C/NC	Value
1.	Version	M	NA	The mandated value is 2. (i.e., The certificate must be in a version 3 format)
2.	Serial Number	M	NA	Positive number of maximum Length 20 bytes and unique to each certificate issued by a CA.
3.	Issuer Signature Algorithm	M	NA	SHA1 with RSA Encryption (null parameters) OR SHA256 with RSA Encryption (null parameters)
4.	Issuer Distinguished Name	M	NA	Common Name (CN): CCA India {Generation Qualifier} {Re-issuance Number}* Organisation (O): India PKI* Country (C): India (IN)
5.	Validity Period	M	NA	Validity expressed in UTC Time for certificates valid through 2049
6.	Subject Distinguished Name	M	NA	Common Name (CN): "Certifying Authority Name" CA {Generation Qualifier} (re-issuance number} House Identifier: 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 / registered office address Street Address: This attribute value MUST contain following parameters of the CA's head office / registered office address Locality / colony name

* With respect to Mauritius Operations, "O=India PKI" will be substituted with "O=India PKI for Mauritius Operations"

					(nearest) Street Name Town / Suburb / Village City name (if applicable) District
				State / Province	State / province where the Certifying Authority has its head office or registered office
				Postal Code	Pin Code
				Organisational Unit (OU)	"Certifying Authority"
				Organisation (O)	Legal Name of the CA
				Country (C)	Country code as per the verified CAs head office or registered office address
7.	Subject Public Key Information	M	NA	rsaEncryption {1 2 840 113549 1 1 1}, 2048 RSA Key modulus, public exponent	
8.	Issuer's Signature Algorithm	M	NA	sha-1WithRSAEncryption {1 2 840 113549 1 1 5} (null parameters) orsha256 WithRSAEncryption {1 2 840 113549 1 1 11} (null parameters)	
9.	Signature Value	M	NA	Issuer CA's signature	
Extensions					
1.	Authority Key Identifier	M	NC	Root Certifying Authority of India (RCAI) SubjectkeyIndetifier (currently 4f 1e c0 58 27 d8 b8 e4)	
2.	Subject Key Identifier	M	NC	Octet String of unique value associated with the Public key	
3.	Key Usage	M	C	keyCertSign, cRLSign	
4.	Certificate Policies	M	NC	The value must contain the OID representing the CCA certificate policy the certificate is valid for; and all the lower level certificate polices.	
5.	Basic Constraints	M	C	CA Boolean = True, pathLenConstraints 0 or 1 depending on sub-CA	
6.	CRL Distribution Points	M	NC	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.	
7.	Authority Information Access	M	NC	The id-ad-caIssuers OID shall be absent. The id-ad-ocsp accesslocation must specify the location of the OCSP responder, using the conventions defined in [RFC2560] if RCAI uses OCSP. If RCAI does not use OCSP AIA extension shall be absent.	

Sub-CA Certificate Profile

Sn.	Field	M/O	C/NC	Value
1.	Version	M	NA	The mandated value is 2. (i.e., The certificate must be in a version 3 format)
2.	Serial Number	M	NA	Positive number of maximum Length 20 bytes and unique to each certificate issued by a CA.
3.	Issuer Signature Algorithm	M	NA	SHA1 with RSA Encryption (null parameters) OR SHA256 with RSA Encryption (null parameters)
4.	Issuer Distinguished Name	M	NA	Must be same as Subject DN of the Issuing CA
5.	Validity Period	M	NA	Validity expressed in UTC Time for certificates valid through 2049
6.	Subject Distinguished Name	M	NA	Common Name (CN): "Certifying Authority Name" sub-CA for "Branding Name" {Generation qualifier} (re-issuance number} Organisational Unit (OU): Sub-CA Organisation (O): Legal Name of the Sub-CA (same as CA legal name) Country (C): Country code as per the verified office address
7.	Subject Public Key Information	M	NA	rsaEncryption {1 2 840 113549 1 1 1}, 2048 RSA Key modulus, public exponent
8.	Issuer's Signature	M	NA	sha-1WithRSAEncryption {1 2 840 113549 1 1 5} (null parameters) orsha256 WithRSAEncryption {1 2 840 113549 1 1 11} (null parameters)
9.	Signature Value	M	NA	Issuer CA's signature
Extensions				
1.	Authority Key Identifier	M	NC	Issuing CA SubjectkeyIndetifier
2.	Subject Key Identifier	M	NC	Octet String of unique value associated with the Public key
3.	Key Usage	M	C	keyCertSign, cRLSign
4.	Certificate Policies	M	NC	The value must contain the OID representing the CCA certificate policy the certificate is valid for; and all the lower level certificate polices.
5.	Basic Constraints	M	C	CA Boolean = True, pathLenConstraints = 0
6.	CRL Distribution Points	M	NC	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.

7.	Authority Information Access	M	NC	The id-ad-calssuers OID MUST point to the certificate issued to the Licensed CA by RCAI. 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]. The id-ad-ocsp accesslocation must specify the location of the OCSP responder, using the conventions defined in [RFC2560] for CAs using OCSP. If OCSP is not used, the OID must not be present.

End User Certificate Profile (issued for personal use)

Sn.	Field	M/O	C/NC	Value
1.	Version	M	NA	The mandated value is 2. (i.e., The certificate must be in a version 3 format)
2.	Serial Number	M	NA	Positive number of maximum Length 20 bytes and unique to each certificate issued by a CA.
3.	Issuer Signature Algorithm	M	NA	SHA1 with RSA Encryption (null parameters) OR SHA256 with RSA Encryption (null parameters)
4.	Issuer Distinguished Name	M	NA	Must be same as Subject DN of the issuing CA
5.	Validity Period	M	NA	Validity expressed in UTC Time for certificates valid through 2049
6.	Subject Distinguished Name	M	NA	Common Name (CN): Name string of maximum 64 characters constructed in the following manner "Surname" "Given Name" "Father / Husband's name" "Initials" Serial Number: This attribute should be populated with the SHA 256 hash of the PAN number of the end user. The hash must be calculated for the PAN number after deleting all leading and trailing blanks. In case PAN has not been provided, this field must be omitted. State / Province: State / province for verified residential address Postal Code: PIN Code for the for Subject's residential address.

				Organisation (O) Personal Country (C) Country code as per the verified residential address
7.	Subject Public Key Information	M	NA	rsaEncryption, 1024 RSA Key modulus, public exponent
8.	Issuer's Signature	M	NA	sha-1WithRSAEncryption {1 2 840 113549 1 1 5} (null parameters) or sha256 WithRSAEncryption {1 2 840 113549 1 1 11} (null parameters)
9.	Signature Value	M	NA	Issuer CA's signature
Extensions				
1.	Authority Key Identifier	M	NC	Issuing CA SubjectkeyIndetifier
2.	Subject Key Identifier	M	NC	Octet String of unique value associated with the Public key
3.	Key Usage	M	C	DigitalSignature, nonRepudiation
4.	Certificate Policies	M	NC	The value must contain the OID representing the CCA certificate policy the certificate is valid for; and all the lower level certificate polices.
5.	Subject Alternative Name	O	NC	Email Address
6.	CRL Distribution Points	M	NC	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.
7.	Authority Information Access	M	NC	The id-ad-caIssuers 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]. The id-ad-ocsp accesslocation must specify the location of the OCSP responder, using the conventions defined in [RFC2560] for CAs using OCSP. If OCSP is not used, the OID must not be present.

End User Certificate Profile (issued for organization use)

Sn.	Field	M/O	C/NC	Value
1.	Version	M	NA	The mandated value is 2. (i.e., The certificate must be in a version 3

				format)
2.	Serial Number	M	NA	Positive number of maximum Length 20 bytes and unique to each certificate issued by a CA.
3.	Issuer Signature Algorithm	M	NA	SHA1 with RSA Encryption (null parameters) OR SHA256 with RSA Encryption (null parameters)
4.	Issuer Distinguished Name	M	NA	Must be same as Subject DN of the issuing CA
5.	Validity Period	M	NA	Validity expressed in UTC Time for certificates valid through 2049
6.	Subject Distinguished Name	M	NA	Common Name (CN): Name string of maximum 64 characters constructed in the following manner "Surname" "Given Name" "Father / Husband's name" "Initials" Serial Number: This attribute should be populated with the SHA 256 hash of the PAN number of the end user. The hash must be calculated for the PAN number after deleting all leading and trailing blanks. In case PAN has not been provided, this field must be omitted. State / Province: • State / province for verified Office address Postal Code: • PIN Code for the for Subject's Office address. Organisation Unit: • 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	M	NA	rsaEncryption, 1024 RSA Key modulus, public exponent
8.	Issuer's Signature	M	NA	sha-1WithRSAEncryption {1 2 840 113549 1 1 5} (null parameters) or sha256 WithRSAEncryption {1 2 840 113549 1 1 11} (null parameters)
9.	Signature Value	M	NA	Issuer CA's signature
Extensions				
1.	Authority Key Identifier	M	NC	Issuing CA SubjectkeyIndetifier
2.	Subject Key Identifier	M	NC	Octet String of unique value associated with the Public key
3.	Key Usage	M	C	DigitalSignature, nonRepudiation

4.	Certificate Policies	M	NC	The value must contain the OID representing the CCA certificate policy the certificate is valid for; and all the lower level certificate polices.
5.	Subject Alternative Name	O	NC	Email Address
6.	CRL Distribution Points	M	NC	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.
7.	Authority Information Access	M	NC	The id-ad-caIssuers 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]. The id-ad-ocsp accesslocation must specify the location of the OCSP responder, using the conventions defined in [RFC2560] for CAs using OCSP. If OCSP is not used, the OID must not be present.

SSL Certificate Profile

Sn.	Field	M/O	C/NC	Value
1.	Version	M	NA	The mandated value is 2. (i.e., The certificate must be in a version 3 format)
2.	Serial Number	M	NA	Positive number of maximum Length 20 bytes and unique to each certificate issued by a CA.
3.	Issuer Signature Algorithm	M	NA	SHA1 with RSA Encryption (null parameters) OR SHA256 with RSA Encryption (null parameters)
4.	Issuer Distinguished Name	M	NA	Must be same as Subject DN of the issuing CA
5.	Validity Period	M	NA	Validity expressed in UTC Time for certificates valid through 2049
6.	Subject Distinguished Name	M	NA	The CN in the Subject Name MAY contain either ▪ Qualified domain name ▪ IP addresses of the server as a printable string in "network byte order", as specified in [RFC791]
7.	Subject Public Key Information	M	NA	rsaEncryption, 1024 RSA Key modulus, public exponent
8.	Issuer's Signature	M	NA	sha-1WithRSAEncryption {1 2 840 113549 1 1 5} (null parameters) or sha256 WithRSAEncryption {1 2 840 113549 1 1 11} (null parameters)

9.	Signature Value	M	NA	Issuer CA's signature
Extensions				
1.	Authority Key Identifier	M	NC	Issuing CA SubjectkeyIndetifier
2.	Subject Key Identifier	M	NC	Octet String of unique value associated with the Public key
3.	Key Usage	M	C	Key Encipherment and Digital Signature
4.	Certificate Policies	M	NC	The value must contain the OID representing the CCA certificate policy the certificate is valid for; and all the lower level certificate polices.
5.	Subject Alternative Name	M	NC	dnsName for the server / web page as an IA5 string
6.	Extended Key Usage	O	NC	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}
7.	CRL Distribution Points	M	NC	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.

System Certificate Profile

Sn.	Field	M/O	C/NC	Value
1.	Version	M	NA	The mandated value is 2. (i.e., The certificate must be in a version 3 format)
2.	Serial Number	M	NA	Positive number of maximum Length 20 bytes and unique to each certificate issued by a CA.
3.	Issuer Signature Algorithm	M	NA	SHA1 with RSA Encryption (null parameters) OR SHA256 with RSA Encryption (null parameters)
4.	Issuer Distinguished Name	M	NA	Must be same as Subject DN of the issuing CA
5.	Validity Period	M	NA	Validity expressed in UTC Time for certificates valid through 2049
6.	Subject Distinguished Name	M	NA	The CN in the Subject Name MUST contain either ▪ IP Address of the system as a printable string in "network byte order", as specified in [RFC791] ▪ 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
7.	Subject Public Key Information	M	NA	rsaEncryption, 1024 RSA Key modulus, public exponent

8.	Issuer's Signature	M	NA	sha-1WithRSAEncryption {1 2 840 113549 1 1 5} (null parameters) or sha256 WithRSAEncryption {1 2 840 113549 1 1 11} (null parameters)
9.	Signature Value	M	NA	Issuer CA's signature
Extensions				
1.	Authority Key Identifier	M	NC	Issuing CA SubjectkeyIndetifier
2.	Subject Key Identifier	M	NC	Octet String of unique value associated with the Public key
3.	Key Usage	M	C	Key Encipherment and Digital Signature
4.	Certificate Policies	M	NC	The value must contain the OID representing the CCA certificate policy the certificate is valid for; and all the lower level certificate polices.
5.	Subject Alternative Name	M	NC	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] ▪ dnsName in IA5String format
6.	Extended Key Usage	O	NC	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}
7.	CRL Distribution Points	M	NC	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.

Time Stamping Authority Certificate Profile

Sn.	Field	M/O	C/NC	Value
1.	Version	M	NA	The mandated value is 2. (i.e., The certificate must be in a version 3 format)
2.	Serial Number	M	NA	Positive number of maximum Length 20 bytes and unique to each certificate issued by a CA.
3.	Issuer Signature Algorithm	M	NA	SHA1 with RSA Encryption (null parameters) OR SHA256 with RSA Encryption (null parameters)
4.	Issuer Distinguished Name	M	NA	Must be same as Subject DN of the Issuing CA
5.	Validity Period	M	NA	Validity expressed in UTC Time for certificates valid through 2049
6.	Subject Distinguished Name	M	NA	Common Name (CN) <Time Stamping Authority Name> {Generation qualifier} (re-issuance number}

				Organisational Unit (OU) Organisation (O) Country (C)	Time Stamping Authority Legal Name of the TSA Organization Country code as per the verified office address
7.	Subject Public Key Information	M	NA	rsaEncryption, 2048 RSA Key modulus, public exponent	
8.	Issuer's Signature	M	NA	sha-1WithRSAEncryption {1 2 840 113549 1 1 5} (null parameters) or sha256 WithRSAEncryption {1 2 840 113549 1 1 11} (null parameters)	
9.	Signature Value	M	NA	Issuer CA's signature	
Extensions					
1.	Authority Key Identifier	M	NC	Issuing CA SubjectkeyIndetifier	
2.	Subject Key Identifier	M	NC	Octet String of unique value associated with the Public key	
3.	Key Usage	M	C	DigitalSignature	
4.	Certificate Policies	M	NC	The value must contain the OID representing the CCA certificate policy the certificate is valid for; and all the lower level certificate polices.	
5.	Extended Key Usage	M	C	id-kp-timestamping {1 3 6 1 5 5 7 3 8}	
6.	CRL Distribution Points	M	NC	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.	
7.	Authority Information Access	M	NC	The id-ad-caIssuers 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]. The id-ad-ocsp accesslocation must specify the location of the OCSP responder, using the conventions defined in [RFC2560] for CAs using OCSP. If OCSP is not used, the OID must not be present.	

Code Signing Certificate Profile

Sn.	Field	M/O	C/NC	Value
1.	Version	M	NA	The mandated value is 2. (i.e., The certificate must be in a version 3

				format)
2.	Serial Number	M	NA	Positive number of maximum Length 20 bytes and unique to each certificate issued by a CA.
3.	Issuer Signature Algorithm	M	NA	SHA1 with RSA Encryption (null parameters) OR SHA256 with RSA Encryption (null parameters)
4.	Issuer Distinguished Name	M	NA	Must be same as Subject DN of the issuing CA
5.	Validity Period	M	NA	Validity expressed in UTC Time for certificates valid through 2049
6.	Subject Distinguished Name	M	NA	Common Name (CN): Name string of maximum 64 characters constructed in the following manner "Surname" "Given Name" "Father / Husband's name" "Initials" Or Legal Name of the Organisation House Identifier: This attribute MUST contain the • Flat number, Apartment name and Plot no. OR • House Name / Number and Plot Number Of the individuals verified OFFICE address Street Address: This attribute value MUST contain following parameters of the Subject's OFFICE address • Locality / colony name • (nearest) Street Name • Town / Suburb / Village • City name (if applicable) • District State / Province: • State / province for verified Office address Postal Code: • PIN Code for the for Subject's Office address. Organisation (O): Legal Name of the organisation Country (C): Country code as per the verified Office address

7.	Subject Public Key Information	M	NA	rsaEncryption, 1024 RSA Key modulus, public exponent
8.	Issuer's Signature	M	NA	sha-1WithRSAEncryption {1 2 840 113549 1 1 5} (null parameters) or sha256 WithRSAEncryption {1 2 840 113549 1 1 11} (null parameters)
9.	Signature Value	M	NA	Issuer CA's signature
Extensions				
1.	Authority Key Identifier	M	NC	Issuing CA SubjectkeyIndetifier
2.	Subject Key Identifier	M	NC	Octet String of unique value associated with the Public key
3.	Key Usage	M	C	DigitalSignature
4.	Extended Key Usage	M	C	id-kp-codeSigning {1 3 6 1 5 5 7 3 3}
5.	Certificate Policies	M	NC	The value must contain the OID representing the CCA certificate policy the certificate is valid for; and all the lower level certificate polices.
6.	CRL Distribution Points	M	NC	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.
7.	Authority Information Access	M	NC	The id-ad-caIssuers 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]. The id-ad-ocsp accesslocation must specify the location of the OCSP responder, using the conventions defined in [RFC2560] for CAs using OCSP. If OCSP is not used, the OID must not be present.

OCSP Responder Certificate Profile

Sn.	Field	M/O	C/NC	Value
1.	Version	M	NA	The mandated value is 2. (i.e., The certificate must be in a version 3 format)
2.	Serial Number	M	NA	Positive number of maximum Length 20 bytes and unique to each certificate issued by a CA.
3.	Issuer Signature Algorithm	M	NA	SHA1 with RSA Encryption (null parameters) OR SHA256 with RSA Encryption (null parameters)
4.	Issuer Distinguished Name	M	NA	Must be same as Subject DN of the Issuing CA
5.	Validity Period	M	NA	Validity expressed in UTC Time for certificates valid through 2049
6.	Subject Distinguished Name	M	NA	

				Common Name (CN) <OCSP Responder Name> Organisational Unit (OU) OCSP Responder Organisation (O) Legal Name of the OCSP Organization Country (C) Country code as per the verified office address
7.	Subject Public Key Information	M	NA	rsaEncryption, 2048 RSA Key modulus, public exponent
8.	Issuer's Signature	M	NA	sha-1WithRSAEncryption {1 2 840 113549 1 1 5} (null parameters) or sha256 WithRSAEncryption {1 2 840 113549 1 1 11} (null parameters)
9.	Signature Value	M	NA	Issuer CA's signature
1.	Authority Key Identifier	M	NC	Issuing CA SubjectkeyIndetifier
2.	Subject Key Identifier	M	NC	Octet String of unique value associated with the Public key
3.	Key Usage	M	C	DigitalSignature
4.	Certificate Policies	M	NC	The value must contain the OID representing the CCA certificate policy the certificate is valid for; and all the lower level certificate polices.
5.	Extended Key Usage	M	C	id-kp-OCSPSigning {1 3 6 1 5 5 7 3 9}
6.	CRL Distribution Points	O	NC	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 complete HTTP URI pointing to a DER encoded partitioned CRL for all reasons. DistributionPointName shall contain the fullName and thus shall not contain nameRelativeToCRLIssuer reasons and cRLIssuer fields shall be absent.
7.	Authority Information Access	M	NC	The id-ad-caIssuers 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].

Encryption Certificate

Sn.	Field	M/O	C/NC	Value
1.	Version	M	NA	The mandated value is 2. (i.e., The certificate must be in a version 3 format)

2.	Serial Number	M	NA	Positive number of maximum Length 20 bytes and unique to each certificate issued by a CA.
3.	Issuer Signature Algorithm	M	NA	SHA1 with RSA Encryption (null parameters) OR SHA256 with RSA Encryption (null parameters)
4.	Issuer Distinguished Name	M	NA	Must be same as Subject DN of the issuing CA
5.	Validity Period	M	NA	Validity expressed in UTC Time for certificates valid through 2049
6.	Subject Distinguished Name	M	NA	Common Name (CN): Name string of maximum 64 characters constructed in the following manner "Surname" "Given Name" "Father / Husband's name" "Initials" Serial Number: This attribute should be populated with the SHA 256 hash of the PAN number of the end user. The hash must be calculated for the PAN number after deleting all leading and trailing blanks. In case PAN has not been provided, this field must be omitted. State / Province: • State / province for verified residential address Postal Code: • PIN Code for the for Subject's residential address. Organisation (O): Personal Country (C): Country code as per the verified residential address
7.	Subject Public Key Information	M	NA	rsaEncryption, 1024 RSA Key modulus, public exponent
8.	Issuer's Signature	M	NA	sha-1WithRSAEncryption {1 2 840 113549 1 1 5} (null parameters) or sha256 WithRSAEncryption {1 2 840 113549 1 1 11} (null parameters)
9.	Signature Value	M	NA	Issuer CA's signature
Extensions				
1.	Authority Key Identifier	M	NC	Issuing CA SubjectkeyIndetifier
2.	Subject Key Identifier	M	NC	Octet String of unique value associated with the Public key
3.	Key Usage	M	C	Key encipherment
4.	Certificate Policies	M	NC	The value must contain the OID representing the CCA certificate policy the certificate is valid for; and all the lower level certificate polices.
5.	Subject Alternative	O	NC	Email Address

	Name			
6.	CRL Distribution Points	M	NC	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.
7.	Authority Information Access	M	NC	The id-ad-caIssuers 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]. The id-ad-ocsp accesslocation must specify the location of the OCSP responder, using the conventions defined in [RFC2560] for CAs using OCSP. If OCSP is not used, the OID must not be present.

CRL Profile

Sn.	Field	M/O	C/NC	Value
1.	Version	M		Should be Version 2 (Field value 1)
2.	Issuer Signature Algorithm	M	NA	sha-1WithRSAEncryption {1 2 840 113549 1 1 5} or sha256 WithRSAEncryption {1 2 840 113549 1 1 11}
3.	Issuer Distinguished Name	M	NA	Unique X.500 Issuing CA DN Single value shall be encoded in each RDN. Furthermore, each value shall be encoded as a printable string.
4.	thisUpdate	M	NA	Expressed in UTCTime until 2049
5.	nextUpdate	M	NA	Expressed in UTCTime until 2049 (>= thisUpdate + CRL issuance frequency)
6.	Revoked certificates list	M	NA	0 or more 2-tuple of certificate serial number and revocation date (in Generalized Time)
7.	Issuer's Signature	M	NA	sha-1WithRSAEncryption {1 2 840 113549 1 1 5} or sha256 WithRSAEncryption {1 2 840 113549 1 1 11}
Extensions				
1.	CRL Number	O	NC	Monotonically increasing integer (never repeated)
2.	Authority Key Identifier	M	NC	Octet String (must be the same as in Authority Key Identifier field in certificates issued by the CA)
CRL Entry Extensions				
1.	Reason Code	O	NC	Must be included when reason code = key compromise or CA compromise

Annexure IV – Application Developer Guidelines

Application developers are to develop applications in compliance with RFC5280 certificate profile. A number of commercial and open source PKI toolkits are available which can be used to develop a standard validation process. Some of the tool kits available include

- Microsoft CAPI for Windows environments
- Microsoft CNG for Vista and Server 2008 environments
- NSS for Linux and Unix environments
- Sun Java toolkit
- Open Source PKIF for Windows, Unix, Linux, .NET, and Java environments.
- Toolkits from PKI vendors

The following guidelines provide the minimum validations and certificate processing which needs to be carried out by applications to establish trust in the certificate presented to them by the user.

Pre-requisites

1. As a prerequisite, the applications need to establish a trust anchor. The trust anchor for the Indian PKI would be the CCA Root Certifying Authority of India (RCAI) Certificate. The certificate needs to be downloaded and installed in the application in a secure manner after verification of the certificate thumbprint.
2. The system should know the Certificate Policy OID(s) acceptable to it. For example an application may accept only Class III certificate or both Class II and Class III – depending upon the level of assurance required.
3. Applications should be able to determine the prospective certification path. Since the Indian PKI has limited number of CAs and Sub-CA with no cross certification, the CA certificates and sub-CA certificates are easily obtainable manually. Applications also may download the issuers certificate from the URI specified in Authority Information Access (AIA) field
4. The applications should have the capability to check the validity of the certificate with CRLs (and OCSP in the future)

Simplified Certificate Validation Steps

Application developers should carry out certification path validation in accordance to specifications in RFC 5280. The following steps are minimum validations to be performed by an application as an interim measure until it implements the compete path validation algorithm as mentioned in RFC5280.

1. Determine the prospective certificate path starting with end-entity certificate to trust anchor by following the AIA pointers in iterative manner.
2. for ***each certificate*** in the certification path starting with the certificate issued by the RCAI
    a. verify the signature on the certificate using the public key from the previous certificate
    b. verify that the current time is within the certificate validity
    c. verify that certificate is not revoked (using CRL or OCSP). This will require verifying signature on the CRL using the same key that was used to verify the signature on the certificate in step 2.a above. For OCSP, the signature is verified on OCSP Response and signature on OCSP Responder certificate is verified using the same key that was used to verify the signature on the certificate in step 2.a above.
    d. certificate issuer name corresponds to subject name in the previous certificate
3. Determine the intersection set of all the policies in the certification path and determine if it confirms to acceptable application policy

4. for all certificates other than end user certificate verify that basicConstraints extension is present and cA is set to TRUE and path length constraint is not violated per RFC 5280.

If any of the above fails, then reject the certificate. Once, the certificate passes the above mentioned validations, verify the use of the public key within the application is consistent with the Key Usage and Extended Key Usage extensions set on the certificate. If not, reject the certificate.

Certificate Use

The use of the certificate is to be consistent with the Key Usage and Extended Key Usage Extensions specified. The application can use the following information from the validated certificate: Subject DN, Subject Alternative Name, Subject Public Key algorithm, public key and associated parameters,

Change History

1. Migration to 2048-bit RSA key lengths

Date	15-11-2010
Contents	Field Definition
section	7. Field Name: Subject Public Key Info, Mandated Value
Page no	15

Version 2.0	Version 2.1
For CA & sub-CA: rsaEncryption, 2048 RSA Key modulus, Public Exponent = $2^{16}+1$ ***For end user***: rsaEncryption, 1024 RSA Key modulus, Public Exponent = $2^{16}+1$	***For CA & sub-CA:*** rsaEncryption, 2048 RSA Key modulus, Public Exponent = $2^{16}+1$ ***For end user***: rsaEncryption, 2048 RSA Key modulus, Public Exponent = $2^{16}+1$ From January 1,2011, CAs must issue 2048-bit RSA SubCA and end-entity certificates.

2. Migration to Secure Hash Algorithms SHA2

Date	15-11-2010
Contents	Field Definition
Section	7. Field Name: SignatureAlgorithms, Mandated Value
Page no	17

Version 2.0	Version 2.1
OID for SHA1 with RSA Encryption (null parameters) {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5} OR OID for SHA256 with RSA Encryption (null parameters) {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11} If parameters are present, in this field, they shall be ignored.	OID for SHA1 with RSA Encryption (null parameters) {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5} OR OID for SHA256 with RSA Encryption (null parameters) {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11} If parameters are present, in this field, they shall be ignored CAs should make SHA2 end-entity certificates available to customers from January 1 2012.

3. User Notice - IA5 string to Visible String

Date	15-11-2010
Contents	Standard Extension Definition
section	4. Certificate Policies, Mandated Value
Page no	25

Version 2.0	Version 2.1
The end entity certificate should contain User Notice qualifier ‘ explicit text’ encoded as IA5 string	The end entity certificate should contain User Notice qualifier ‘ explicit text’ encoded as Visible string

4. Key usage - CA and SubCA Certificate Profile

Date	15-11-2010
Contents	CA and SubCA Certificate Profile
section	key usage
Page no	76-79

Version 2.0	Version 2.1
keyCertSign ,cRLSign, DigitalSignature, nonRepudiation	keyCertSign, cRLSign

5. CRL Profile – Hold Instruction removed

Date	15-11-2010
Contents	CRL Profile
section	CRL Entry Extension, Hold Instruction
Page no	90

Version 2.0	Version 2.1
Hold Instruction-O-NC- id-holdinstruction-reject. This extension must be present only if reason code = certificateHold	Removed