Interoperability Guidelines for Digital Signature Certificates issued under Electronic Transaction Act

Version 1.0

Controller:

Nepal Government

OFFICE OF CONTROLLER OF CERTIFICATION

Ministry of Communications and Information Technology

Singhadurbar, Kathmandu, Nepal

2079

Document Control

Document Name	**Digital Signature Certificates Interoperability Guidelines (OCC-IOG)**
Status	**Release**
Version	**1.0**
Release	**June 2022**
Document Owner	**Office of Controller of Certification, Kathmandu, Nepal**

Table of contents

Introduction:

There are basically three reasons why we need PKI interoperability. First is the need of the users to rely upon different trusted services, second is by the providers of trusted services to interoperate between themselves and their customers as well as with other trusted service providers, and third is by solution vendors' need to meet the user and service provider requirements.

As in present scenario some of the major PKI standards activities, it is becoming increasingly clear that interoperability in PKI may have a difficult road ahead due to lack of clear standards. Although standards are instrumental in promoting interoperability, many standards do not guarantee it in a Multi-CA environment. Each group's standardization efforts differ in terms of their approach, focus, and scope.

As a National Leader and governing body of Nepal PKI The OCC carried out the interoperability initiative in Nepal. A comparative analysis of the certificates in use in Nepal was carried out. Beside this comparison IOG documents of other countries were also studied thoroughly. Also, the certificates were compared with the OCC 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 may interpret differently by the CAs which may cause in-consistency. Some key observations from the comparative analysis we found that:

The 'Issuer' field in the digital certificates may be interpreted and /or used in inconsistence 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.

The 'Subject' field may be used for variety of usage for its sub fields. There may be non-standard implementation of the organization parameters. The Organization Unit sub field interpretation may vary across the Certifying Authorities and contains information such as certificate class, subject designations, application specific information etc.

There may be 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 may arise 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. There is possibility that various certifying authorities may 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.

Certifying Authorities can use sub-CAs for issuing digital certificates. There may be 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 have been issued as part of the OCC interoperability for digital certificates in Nepal. The guidelines herein are mandated to the licensed certifying authorities in Nepal. 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 OCC under the powers conferred upon it by the Electronic Transaction Act 2063. 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 OCC.

Revisions

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

The interoperability models

The interoperability challenges facing the Nepal 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 OCC 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, OCC 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 Nepal PKI organization structure consists of the Office of controller of certification (OCC) as the apex body and the Root Certifying Authority of Nepal (RCAN). The RCAN is responsible for issuing digital certificates to Licensed Certifying Authorities (henceforth referred to Certifying Authorities or CA) as per the Electronic Transaction Act 2063. The CAs are responsible for issuing further digital certificates to the end users.

Recommended Organization Hierarchy

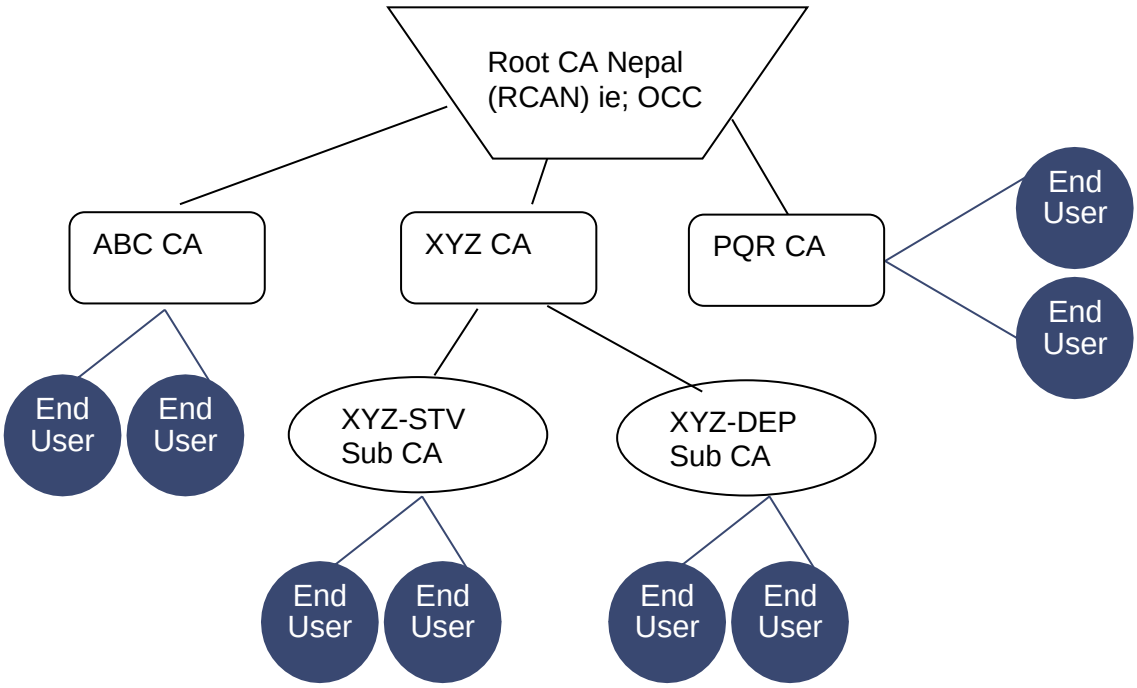
In order to facilitate greater flexibility to Certifying Authorities, the OCC allowed the creation of sub-CAs. As per this model, a Certifying Authority can create a sub-CA to meet his business branding requirement. However, the sub-CA willbe part of the same legal entity as the CA.

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 OCSP Responder Certificates, which may directly be issued by the CA.
- A CA should have separate offline certificate issuance system for issuance of SSL and Code signing certificates under special purpose trust chain. A separate CA must be used for issuance of SSL and Code Signing certificates. A single issuing CA must not be used to issue both server authentication and code signing certificates.

PKI Hierarchy



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 OCC 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 guidanceor 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 OCC

Customizable – Customizable fields are non-standard extensions notified by OCC 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 OCC regarding the usage and format.

Reserved for Future Use – These extensions are reserved by OCC for use in the future and additional guidance is expected from OCC 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 document

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)

Field description	**Describes the version of certificate format adopted**
Interpretation & usage	This field describes the version of the encoded certificate. Version field isused by the ASN.1 decoding software to parse the certificate.
Compliance Standards	RFC 2459,
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)

Field description	Number allocated to a certificate by the issuer CA, unique for a given issuerCA
Interpretation & usage	The serial number field along with the Issuer DN is unique identifier forcertificate
Compliance Standards	RFC 2459,
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)

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 signatureverification algorithm.
Compliance Standards	RFC 2459, RFC 3279, RFC 4055, and RFC 4491
Type	Algorithm OID and Algorithm dependent parameters
Mandated Value	OID for SHA256 with RSA Encryption (null parameters) {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11} or OID for ECDSA with SHA256 {1 2 840 10045 4 3 2} (encoding MUST omitthe parameters Field)

4. Field Name: Issuer (MANDATORY)

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 2459, X.520
Type	SEQUENCE OF Relative Distinguished Names (RDNs) in printable stringformat
Mandated Value	Refer Annexure I

5. Field Name: Validity (MANDATORY)

Field description	Time interval during which the CA warrants that it will maintain informationabout 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 thecertificate is valid inclusive.
Compliance Standards	RFC 2459
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 2050and beyond ▪ Certificate MUST contain a well-defined expiration date. ▪ Sub-CA certificate validity must not exceed CA certificate validity.

6. Field Name: Subject (MANDATORY)

Field description	The subject field associates an entity (named in the field) with the public keyin the certificate.
Interpretation & usage	The Distinguished Name mentioned in the Subject identifies the owner of thecertificate – or the entity to whom the certificate has been issued.
Compliance Standards	RFC 2459, X.520
Type	SEQUENCE OF Relative Distinguished Names (RDNs) in printable stringformat (except for variations mentioned in Annexure I)
Mandated Value	Refer Annexure I

7. Field Name: Subject Public Key Info (MANDATORY)

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 2459, 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, 2048 RSA Key modulus, Public Exponent =$2^{16}+1$ ***For Sub-CA and end user:*** ecPublicKey { 1.2.840.10045.2.1}, namedCurve, { 1.2.840.10045.3.1.7} (NIST curve P-256)

8. Field Name: Unique Identifiers (PROHIBITED)

Field description	Unique identifier for a subject and issuer names (Subject Unique Identifier,Issuer Unique Identifier)
Interpretation & usage	©
Compliance Standards	RFC 2459,
Type	Bit string
Mandated Value	Field not to be used

9. Field Name: signature Algorithm (MANDATORY)

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 signatureverification algorithm
Compliance Standards	RFC 2459, , RFC 3279, RFC 4055, and RFC 4491
Type	Algorithm OID and Algorithm dependent parameters
Mandated Value	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. Or OID for ECDSA with SHA256 {1 2 840 10045 4 3 2 }

10. Field Name: Signature Value (MANDATORY)

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 2459
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)

Field description	The authority key identifier extension provides means of identifying the publickey 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 2459
Type	Octet string
Critical / Non-Critical	Non-Critical
	This field may be absent in the RCAN certificate. All CAs MUST have Authority key identifier value same as subject

Mandated Value	key IdentifierValue of RCAN* CA Authority key identifier = Root Certifying Authority of Nepal (RCAN)*Subject key Identifier Authority key identifier value for a certificate shall be the same as the Subject key Identifier for the Issuer. In other words, certificates issued by a CA shall contain the Authority key identifier value as the same as the Subject key Identifier in the CA's own certificate.
Calculation Method	Calculation method has been specified in the Subject key identifier section
* With respect to creation of separate distinct chain for special operations, RCAN will refer to Root Certifying Authority of Nepal Certificate for the respectivespecial operation	

2. Std. Extension: Subject Key Identifier (MANDATORY, SPECIAL PURPOSE)

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

Field description	The subject key identifier extension provides means of identifying certificatesthat 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 2459
Type	Octet string
Critical / Non-Critical	Non-Critical
Mandated Value	A CA shall always honor the subject key identifier value requested in a certificate request (e.g., PKCS-10 request). Honoring requested value is critical to interoperability when RCAN 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 mentionedbelow. Any other method which provides a statistically unique value associated with the Public key is also acceptable.
Calculation Method	Subject Key Identifier should be composed of the 160-bit SHA-1 hash of value of the BIT STRING subject Public Key in the certificate (excluding the tag, length, and number of unused bits). OR The Subject Key Identifier 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 valueof the BIT STRING subject Public Key (excluding the tag, length, and number of unused bits).

3. Std. Extension: Key Usage (MANDATORY)

Field description	Key Usage field defines the cryptographic purpose of the key contained in thecertificate.
Interpretation & usage	The applications implementing cryptography must interpret this field andrestrict the usage of the key accordingly.
Compliance Standards	RFC 2459
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(Optional) The following key usage MUST NOT be set / asserted for end entitycertificates ▪ cRLSign keyCertsign

4. Std. Extension: Certificate Policies (MANDATORY)

Field description	Contains policy information terms in the form of OIDs and qualifiers.
Interpretation & usage	OCC certificate policy the certificate is valid for; and all the lower level OCC certificate policies.
Compliance Standards	RFC 2459
Type	OID, IA5 string
Critical / Non-Critical	Non-Critical
Mandated Value	The value must contain the OID representing the RCAN 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 OCC. The maximum length of the 'explicit Text' field is 200 characters explicit Text- Values for short validity (30 Min) DSC may be any one of the following: - 'NID online eKYC Biometric- Single factor', 'NID online eKYC OTP-Single Factor', 'NID Offline eKYC OTP and PIN - Multi Factor', 'Organizational KYC OTP and PIN - Multi Factor', 'Banking eKYC OTP and PIN -Multi Factor' , 'PAN KYC OTP and PIN - Multi Factor' , CA KYC OTP and PIN -Multi Factor' Values for long validity DSC may be any one of the following:- 'Class III Certificate', :- 'Class II certificate – Remote'

5. Std. Extension: Policy Mappings (PROHIBITED)

Field description	Lists pairs of OIDs for issuer Domain Policy and subject Domain Policy
Interpretation & usage	The use of this Extension is prohibited by the OCC.
Compliance Standards	RFC 2459
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 (OPTIONAL)

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 beset to be email ID, IP address or domain name.
Compliance Standards	RFC 2459
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 beincluded 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.

7. Std. Extension: Issuer Alternative Name (PROHIBITED)

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 OCC.
Compliance Standards	RFC 2459
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 (OPTIONAL)

Field description	This extension is used to convey subject authorizations.
Interpretation & usage	Field used to convey identification attributes of the subject.
Compliance Standards	RFC 2459
Type	Sequence of attributes
Critical / Non-Critical	Non-Critical
Mandated Value	Not applicable.
Recommended Value	OCC will provide guidance on this as needs arise.

9. Std. Extension: Basic Constraints (Mandatory, Special Purpose*)

Note: Mandatory in RCAN, CA, Sub-CA certificates and end entity certificates.

Field description	The basic constraints extension identifies whether the subject of the certificateis 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 usedto verify Certificate and CRL signatures and the length of certificate path.
Compliance Standards	RFC 2459
Type	Boolean, Numeric
Critical / Non-Critical	Critical
Mandated Value	For a certifying Authority & sub-CA, Basic Constraints field for CA Booleanmust be asserted. RCAN 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 forthat licensed CA. Sub-CA certificate shall contain pathLengthConstraint = 0 For end user certificate, the field MUST have value CA= False

10. Std. Extension: Name Constraints (PROHIBITED)

Field description	Defines the namespace which can and/or cannot 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 OCC
Compliance Standards	RFC 2459
Type	Domain name / IP address /directoryName
Critical / Non-Critical	Critical
Mandated Value	Field is not to be used

11. Std. Extension: Policy Constraints (PROHIBITED)

Field description	Limits the policy mapping or mandates an acceptable policy in certificate path.
Interpretation & usage	Use of this field is prohibited by the OCC
Compliance Standards	RFC 2459
Type	OIDs
Critical / Non-Critical	Critical
Mandated Value	Field is not to be used

12. Std. Extension: Extended Key Usage (Mandatory, Special Purpose)

Field description	Further limits the use of a certificate based on cryptographic application.
Interpretation & usage	This field is mandatory to be in all certificates. For special purpose certificates, refer Annexure II
Compliance Standards	RFC 2459
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 guidanceprovided in Annexure II only ▪ id-kp-serverAuth {1 3 6 1 5 5 7 3 1} (for SSL 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 ▪ Smart Card Logon {1.3.6.1.4.1.311.20.2.2} (for end user certificates) –Non Critical ▪ MSFT Document Signing: {1.3.6.1.4.1.311.10.3.12} – Non Critical ▪ Adobe Certified Document Signing {1.2.840.113583.1.1.5} – Non Critical

13. Std. Extension: CRL Distribution Point (MANDATORY)

Field description	The CRL distribution points extension identifies the location and method bywhich CRL information can be obtained.
Interpretation & usage	The field is interpreted as a Distribution Point URI.
Compliance Standards	RFC 2459
Type	URI, IA5String
Critical / Non Critical	Non Critical
Mandated Value	Distribution Point Name MUST be set and MUST contain a complete HTTPURI pointing to a DER encoded full and complete CRL for all reasons. Distribution Point Name shall contain the full Name and thus shall not contain name Relative To CRL Issuer reasons and cRL Issuer fields shall be absent.

14. Std. Extension: Inhibit Any Policy (PROHIBITED)

Field description	When set, this field inhibits an explicit match with special any Policy OID { 2 5 29 32 0 }
Interpretation & usage	This field is prohibited to be used by OCC
Compliance Standards	RFC 2459
Type	OID
Critical / Non Critical	Critical
Mandated Value	This field must not be used.

15. Std. Extension : Freshest CRL (PROHIBITED)

Field description	The freshest CRL extension identifies how delta CRL information is obtained.
Interpretation & usage	The use of this field is prohibited by the OCC
Compliance Standards	RFC 2459
Type	URI
Critical / Non-Critical	Non-Critical
Mandated Value	This field must not be used.

16. Std. Extension: Signed Certificate Timestamp List (Special Purpose)

Field description	Signed Certificate Timestamp (SCT) returned by Log operators when a validcertificate is submitted to a log
Interpretation & usage	To be included only in the SSL certificates
Compliance Standards	RFC 2459, 6962
Type	OCTET STRING
Critical / Non Critical	Non Critical
Mandated Value	If present , at least one SCT MUST be included.

Private Extensions

1. Pvt. Internet Extension: Authority Information Access (MANDATORY)

Field description	The extension provides information for accessing information and services ofthe issuer.
Interpretation & usage	The field is used to access information regarding the issuer (such as issuercertificate) and the OCSP service
Compliance Standards	RFC 2459
Type	URI
Critical / Non-Critical	Non-Critical
Mandated Value	The id-ad-CA Issuers MUST point to certificates issued to the CA issuing the certificate containing this field. This should specify a HTTP URI which pointsto 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 access location 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 access location access Method must not be present.

2. Pvt. Internet Extension: Subject Information Access (PROHIBITED)

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 OCC
Compliance Standards	RFC 2459
Type	URI
Critical / Non-Critical	Non-Critical
Mandated Value	This field must not be used.

****

Annexure I

Issuer and Subject field specification

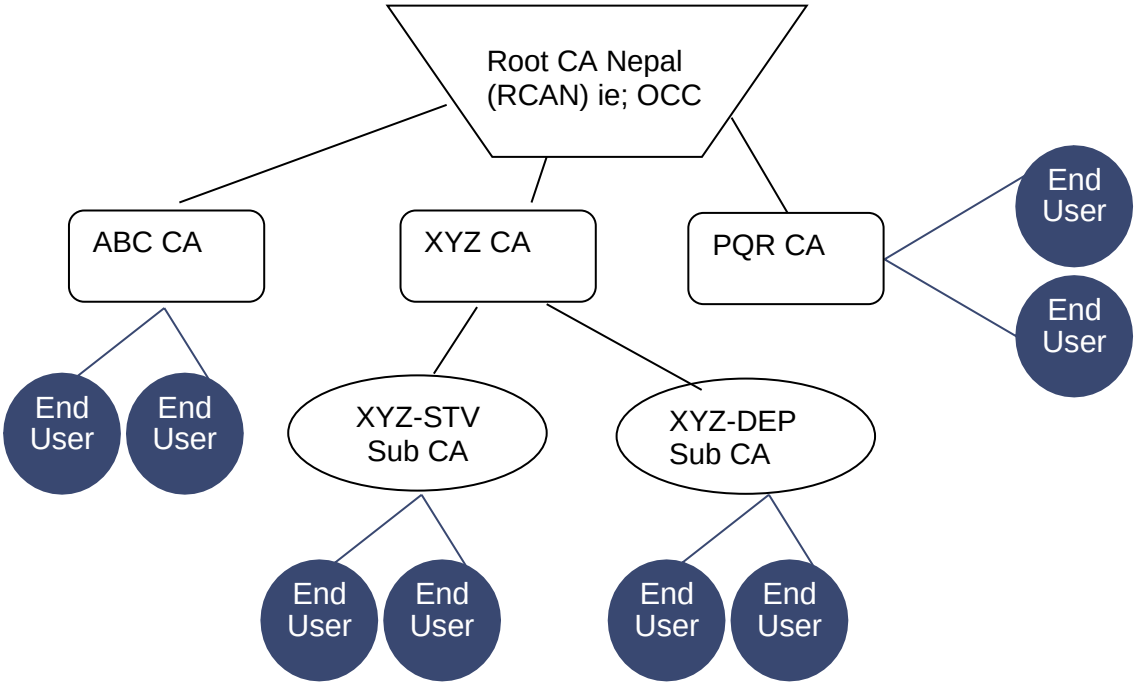
Background

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 consists of a hierarchical structure composed of attributes such as Common name, organization, organization unit, Country 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 Nepal PKI hierarchy is depicted in the figure below



Naming Conventions

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

Entity	Naming (Common Name)	Example
Certifying Authority	"Certifying Authority Name" CA {Generation Qualifier}(issuance number}	XYZ CA 2015 XYZ CA 2015-1
Sub-CA	"Certifying Authority Name" sub-CA for "BrandingName" {Generation qualifier} (Issuance number }	XYZ Sub CA for OCR 2015 XYZ Sub CA for OCR 2015-1

Note: The generation qualifier will be the generation qualifier of Root CA. The generation qualifier necessarily is to be in the form of 4 digit year (yyyy). In case multiple certificates have been issued the year, indicator is to be followed by hyphen and digit indicating the sequence number of issuances of certificate. E.g. When a root certificate is issued in 2015, the CA name will be XYZ CA 2015. When the next CA certificate is reissued, the CA name will be indicate as 2015 –1.

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 areverse order than that of a directory structure.

SN	Certificate Type	Issuer	Subject
1	RCAN*	Self →	Same as issuer
2	Licensed CA	Same as Subject in OCC 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

OCC Certificate – SUBJECT and ISSUER specifications
The OCC certificate must comply with following distinguished name specifications for both subject and issuers (for a self-signed certificate)

SN	Attribute	Value
1	Common Name (CN)	NepalRootCA {Generation Qualifier} (Issuance number }
2	Organization (O)	OCC Nepal*
3	Country (C)	Nepal (NP)

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 easyreference

SN	Attribute	Value
1	Common Name (CN)	Same as SUBJECT field in Issuer CA certificate
2	Organizational Unit (OU)	Same as SUBJECT field in Issuer CA certificate
3	Organization (O)	Same as SUBJECT field in Issuer CA certificate
4	Country (C)	Same as SUBJECT field in Issuer CA certificate

Sub-CA Certificate – Subject specifications

SN	Attribute	Value
1	Common Name (CN)	Sub-CA Common Name (refer CA naming conventions)
2	Organizational Unit (OU)	Sub-CA
3	Organization (O)	Legal Name of the Organization 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 easyreference

SN	Attribute	Value
1	Common Name (CN)	Same as SUBJECT field in issuing sub-CA
2	Organizational Unit (OU)	Same as SUBJECT field in issuing sub-CA
3	Organization (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 should be the name of the person as in records
2.	email	This attribute should be populated with the email of the person.
3	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.
4	Street	Max Length: 60 Characters "This attribute shall be used for populating street address of person.
5	City	Max Length: 60 Characters (optional) This attribute must be populated with City address of person.
	Organization Unit	Max Length: 64 Characters This attribute MUST either contain the name of the department or sub- division of the organization the person belongs to if the certificate is being issued for official purposes OR must not be used. In case meaningful OUhas not been provided, this field must be omitted. The Organizational unit must not be present when the organization has beenmarked as "personal"

7	Organization	Max Length: 64 Characters This attribute MUST contain either Name of the organization the person belongs to – if such information hasbeen 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. XYZ CA

CA Certificate

Issuer DN

Attribute	Value
Common Name (CN)	NepalRootCA-2020
Organization (O)	OCC Nepal*
Country (C)	Nepal (NP)

Subject DN

Attribute	Value
Common Name (CN)	XYZ CA {Generation Qualifier} {Issuance number }
Organizational Unit (OU)	Certifying Authority
Organization (O)	XYZ Pvt LTD.
Country (C)	NP

*With respect to creation of separate distinct chain for special operation "O=Nepal PKI" will be substituted with "O=Nepal 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)	XYZ CA {Generation Qualifier} {Issuancenumber }
Organizational Unit (OU)	Certifying Authority
Organization (O)	Digital Nepal Network Pvt Ltd.**
Country (C)	NP

Subject DN

Attribute	Value
Common Name (CN)	XYZ sub-CA for Income Tax {Generation Qualifier} {Issuance number }
Organizational Unit (OU)	Sub-CA
Organization (O)	Digital Nepal Network Pvt Ltd..**
Country (C)	NP

End User Certificate Profile (issued by CA)

Issuer DN

Attribute	Value
Common Name (CN)	XYZ CA {Generation Qualifier} {Issuancenumber}
Organizational Unit (OU)	Certifying Authority
Organization (O)	Digital Nepal Network pvt Ltd.**
Country (C)	NP

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 (XXXXXXXXXX operations)"

Subject DN

Attribute	Value
Common Name (CN)	Sunita Sharma
Serial Number	794dbed34bedd3659726f53e44b482b5fc30c76f44baa3285 22047551c1a4fa4
Organizational Unit (OU)	Administration
Organization (O)	Login Overseas Recruitment.
Country (C)	NP

End User Certificate Profile (issued by sub-CA)

Issuer DN

Attribute	Value
Common Name (CN)	XYZ sub-CA for Income Tax {GenerationQualifier} {Issuance number }
Organizational Unit (OU)	Sub-CA
Organization (O)	Digital Nepal Network Pvt Ltd.**
Country (C)	NP

Subject DN

Attribute	Value
Common Name (CN)	Sunita Sharma
email	Personal email
State or Province Name	Bagmati
Street	Street of the person
City (I)	Kathmandu
Organizational Unit (OU)	Administration
Organization (O)	Login Overseas Recruitment.
Country (C)	NP

3.	Extended Key usage	Extended key usage MUST include at least one of the following 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	Subject Alternative Name: Fully Qualified Domain Name(FQDN) Note: Subject Alternative Name extension MUST contain at least one entry. Each entry MUST be either a dNS Name containing the Fully-Qualified Domain Name. Wildcard FQDNs are permitted. A CA may issue an SSL Certificate with wildcard in the right-most label of the Domain Name provided that issuance complies with the requirements as mentioned in the SSL Guidelines dns Name(s) for the server(s) as an IA5 string

1. 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 byteorder", 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	Key Encipherment, Digital Signature
3.	Subject Alternative Name	Subject Alternative Name may contain IP Address of the system as a octet string in "network byte order",as specified in [RFC791]
4.	Extended Key Usage	id-kp-clientAuth {1 3 6 1 5 5 7 3 2}

**

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

2. Time stamping authority certificate

Licensed CAs in Nepal my issue certificates for the purpose of time stamping. It is recommended by the OCC that a timestamping 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 These certificates are to be issued to persons or agencies acting as time stamping authorities.

Sn	Field / Extension	Variation
1.	Subject	Should follow same naming conventions as a CA with "CA" and "CertifyingAuthority" 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

3. Code Signing

Signing of software code is gaining importance. End users and corporations may wish to sign the software code toindicate 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	Variation

**

4. Encryption Certificate

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

Sn.	Field / Extension	Variation
1.	Key Usage	• Key encipherment
2.	Extended Key Usage	• Encrypting File System EKU=1.3.6.1.4.1.311.10.3.4 -- Critical

5. 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 <OCSP Responder Name>(CN) Organizational Unit (OU) OCSP Responder Organization (O) Legal Name of the OCSP Organization Country (C) Country code as per the verified office address
3.	Key Usage	Digital Signature
4.	Certificate Policies	The value must contain the OID representing the OCC certificate policy thecertificate 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}

6. Organizational Document Signer Certificate

The Document Signer Certificates are issued to organizational software applications for operating automatically to authenticate documents/information attributed to the organization by using Digital Signature applied on the document documents/Information. The certificate field requirements for Document Signer Certificates include.

Sn.	Field / Extension	Variation
1.	Subject Name	Common Name (CN) DS Legal Name of the Organization (number) • DS represent Documents/Information Signer. • (number) should be appended to differentiate the certificate(s)issued to same organization **Other Attributes** • Serial Number • This attribute should be populated with the SHA 256 hash of the PANnumber of organization. The hash must be calculated for the PAN number after deleting all leading and trailing blanks. In case PAN hasnot been provided, this field must be omitted. •State / Province • State / province for verified Organization address •Organization Unit(OU) • Department / Division to which the individual belongs within his • Organization. In case meaningful OU has not been provided, this fieldmust be omitted •Organization (O) • Legal Name of the Organization the person belongs to • Country (C) • Country code as per the verified Office address
2.	Key Usage	• Digital Signature, nonrepudiation(O)
3	Extended Key Usage	Secure E-Mail {1.3.6.1.5.5.7.3.4} (Optional) • MSFT Document Signing {1.3.6.1.4.1.311.10.3.12} Mandatory Adobe Document Signing {1.2.840.113583.1.1.5} (Optional)
4	Certificate Policies	• The value must contain the OID representing the OCC certificate policythe certificate is valid for; and all the lower level certificate polices. The value must contain the policy ID to limits the usage of this certificate only in the context of automated signing and also to reflect Organizational accountability. Relying party application should validate accordingly. This certificate is not meant for individual signing purpose.

Annexure III

Reference Certificate Profiles

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

Legend
M: MandatoryO: 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 3format)
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	SHA256 with RSA Encryption (null parameters)
4.	Issuer Distinguished Name	M	NA	Common Name (CN) NepalRootCA {Generation Qualifier} {Issuance number}* Organization (O) OCC Nepal* Country (C) Nepal (NP)
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} (Issuance number} Organizational Unit (OU) "Certifying Authority" Organization (O) Legal Name of the CA Country (C) Country code as per the verified CAs head office or registered office address
7.	Subject Public KeyInformation	M	NA	rsaEncryption {1 2 840 113549 1 1 1}, 2048 RSA Key modulus,public exponent
8	Issuer's Signature Algorithm	M	NA	sha256 With RSA Encryption {1 2 840 113549 1 1 11} (null parameters)

9.	Signature Value	M	NA	Issuer CA's signature

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

Extensions				
1.	Authority Key Identifier	M	NC	Root Certifying Authority of Nepal (RCAN) Subject key Indetifier
2.	Subject Key Identifier	M	NC	Octet String of unique value associated with the Public key
3.	Key Usage	M	C	Key CertSign, cRLSign
4.	Certificate Policies	M	NC	The value must contain the OID representing the OCC certificatepolicy the certificate is valid for; and all the lower level certificatepolices.
5.	Basic Constraints	M	C	CA Boolean = True, pathLenConstraints 0 or 1 depending on sub-CA
6.	CRL Distribution Points	M	NC	Distribution Point Name MUST be set and MUST contain a complete HTTP URI pointing to a DER encoded full and complete CRL for all reasons. Distribution Point Name shall contain the full Name and thusshall not contain name Relative To CRL Issuer reasons and cRL Issuer fields shall be absent.
7.	Authority Information Access	M	NC	The id-ad-caIssuers OID shall be absent. The id-ad-ocsp access location must specify the location of the OCSP responder, using the conventions defined in [RFC2560] if OCC uses OCSP. If OCC does not use OCSP AIA extension shallbe absent.
8.	Extended Key Usage	O	NC	extended key usage shall include(only for the CA issuing SSLcertificates) ▪ id-kp-serverAuth {1 3 6 1 5 5 7 3 1} ▪ id-kp-clientAuth {1 3 6 1 5 5 7 3 2} ▪ id-kp-emailProtection {1 3 6 1 5.5 7 3 4}

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 3format)
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	SHA256 with RSA Encryption (null parameters)or ECDSA with SHA256 {1 2 840 10045 4 3 2}
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} (Issuance number} Organizational Unit (OU) Sub-CA Organization Legal Name of the Sub-CA (same as CA legal name) (O) Country (C) Country code as per the verified office address
7.	Subject Public KeyInformation	M	NA	rsaEncryption {1 2 840 113549 1 1 1}, 2048 RSA Key modulus,public exponent or ecPublicKey { 1.2.840.10045.2.1}, named Curve, {1.2.840.10045.3.1.7} (NIST curve P-256)
8.	Issuer's Signature	M	NA	sha256 With RSAEncryption {1 2 840 113549 1 1 11} (nullparameters) or ECDSA with SHA256 {1 2 840 10045 4 3.2} (encoding MUST omit the parameters Field)
9.	Signature Value	M	NA	Issuer CA's signature
Extensions				
1.	Authority Key Identifier	M	NC	Issuing CA Subject key Indetifier
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 OCC certificatepolicy 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	Distribution Point Name MUST be set and MUST contain a complete HTTP URL pointing to a DER encoded full and complete CRL for all

				reasons. Distribution Point Name shall contain the full Name andthus shall not contain name Relative To CRL Issuer reasons and cRLIssuer fields shall be absent.
7.	Authority Information Access	M	NC	The id-ad-caIssuers OID MUST point to the certificate issued to the Licensed CA by OCC. 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 access location 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.
8.	Extended Key Usage	O	NC	If present, extended key usage shall include(only for the CA issuingSSL certificates) • id-kp-serverAuth {1 3 6 1 5 5 7 3 1} • id-kp-clientAuth {1 3 6 1 5 5 7 3 2} • id-kp-emailProtection {1 3 6 1 5.5 7 3 4}

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 eachcertificate issued by a CA.
3.	Issuer Signature Algorithm	M	NA	SHA256 with RSA Encryption (null parameters)or ECDSA with SHA256 {1 2 840 10045 4 3 2}
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 string of maximum64 charactersName (CN) The Common name should be the name of the person as in records State / ProvinceState / province for verified residential address email email of the person Street Street of the person City (i) city of the person Organization (O)Personal Country (C)Country code as per the verified residential address

7.	Subject Public Key Information	M	NA	rsaEncryption, 2048 RSA Key modulus, public exponentor ecPublicKey { 1.2.840.10045.2.1}, named Curve, { 1.2.840.10045.3.1.7} (NIST curve P-256)
8.	Issuer's Signature	M	NA	sha256 With RSA Encryption {1 2 840 113549 1 1 11} (nullparameters) or ECDSA with SHA256 {1 2 840 10045 4 3 2}(encoding MUST omit the parameters Field)
9.	Signature Value	M	NA	Issuer CA's signature
Extensions				
1.	Authority Key Identifier	M	NC	Issuing CA Subject key Identifier
2.	Subject Key Identifier	M	NC	Octet String of unique value associated with the Public key
3.	Key Usage	M	C	Digital Signature, non-Repudiation (optional)
4.	Certificate Policies	M	NC	The value must contain the OID representing the OCC certificatepolicy the certificate is valid for; and all the lower level certificatepolices. explicit Text- Values for short validity (30 Min) DSC may be any one of the following:- 'NID online eKYC Biometric- Single factor', 'NID online eKYC OTP-Single Factor', 'NID Offline eKYC OTP and PIN -Multi Factor', 'Organizational KYC OTP and PIN -Multi Factor', 'Banking eKYC OTP and PIN -Multi Factor' , 'PAN KYC OTP and PIN -Multi Factor' , CA KYC OTP and PIN - Multi Factor' Values for long validity DSC may be any one of the following:- 'Class III Certificate', :- 'Class II certificate –Remote'
5.	Basic Constraints	M	C	CA Boolean = False
6.	Subject Alternative Name	O	NC	Email Address
7.	CRL Distribution Points	M	NC	Distribution Point Name MUST be set and MUST contain a complete HTTP URI pointing to a DER encoded full and completeCRL for all reasons. Distribution Point Name shall contain the full Name and thus shall not contain name Relative To CRL Issuer reasons and cRL Issuer fields shall be absent.
8.	Authority Information Access	M	NC	The id-ad-calssuers 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 certificate in a BER or DER encoded

				"certs-only" CMS message as specified in [RFC3852]. The id-ad-ocsp access location 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.
9.	Extended Key Usage	M	NC	Extended key usage shall include at least one of the following • id-kp-email Protection {1 3 6 1 5.5 7 3 4} • MSFT Document Signing: {1.3.6.1.4.1.311.10.3.12}The optional EKUs are given below • Smart Card Logon {1.3.6.1.4.1.311.20.2.2 • Adobe Certified Document Signing {1.2.840.113583.1.1.5 }

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 3format)
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	SHA256 with RSA Encryption (null parameters) or ECDSA with SHA256 {1 2 840 10045 4 3 2}
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 DistinguishedName	M	NA	Common Name Name string of maximum 64 characters(CN) The Common name should be the name of the person as in records State / Province State / province for verified Office address Email official email of person. Street address of person City (I) City of person Organization Department / Division to which the individual Unit belongs within his Organization In case meaningful OU has not been provided, this field must be omitted. Organization Legal Name of the Organization the person (O)belongs to Country (C) Country code as per the verified Office address

7.	Subject Public Key Information	M	NA	rsaEncryption, 2048 RSA Key modulus, public exponentor ecPublicKey { 1.2.840.10045.2.1}, named Curve, { 1.2.840.10045.3.1.7} (NIST curve P-256)
8.	Issuer's Signature	M	NA	sha256 With RSAEncryption {1 2 840 113549 1 1 11} (nullparameters) or ECDSA with SHA256 {1 2 840 10045 4 3 2} (encoding MUST omit the parameters Field)
9.	Signature Value	M	NA	Issuer CA's signature

Extensions				
1	Authority Key Identifier	M	NC	Issuing CA Subject key Indetifier
2	Subject Key Identifier	M	NC	Octet String of unique value associated with the Public key
3	Key Usage	M	C	Digital Signature, nonrepudiation(optional)
4	Certificate Policies	M	NC	The value must contain the OID representing the OCC certificatepolicy the certificate is valid for; and all the lower level certificatepolices. explicit Text- Values for short validity (30 Min) DSC may be any one of the following: - 'NID online eKYC Biometric- Single factor', 'NID online eKYC OTP-Single Factor', 'NID Offline eKYC OTP and PIN -Multi Factor', 'Organizational KYC OTP and PIN -Multi Factor', 'Banking eKYC OTP and PIN -Multi Factor' , 'PAN KYC OTP and PIN -Multi Factor' , CA KYC OTP and PIN -Multi Factor' Values for long validity DSC may be any one of the following:-'Class III Certificate', :- 'Class II certificate – Remote'
5	Basic Constraints	M	C	CA Boolean = False
6	Subject Alternative Name	O	NC	Email Address
7	CRL Distribution Points	M	NC	Distribution Point Name MUST be set and MUST contain a complete HTTP URI pointing to a DER encoded full and complete CRL for all reasons. Distribution Point Name shall contain the full Name and thusshall not contain name Relative To CRL Issuer reasons and cRL Issuer fields shall be absent.
8	Authority InformationAccess	M	NC	The id-ad-caIssuers OID MUST point to certificates issued to the CAissuing 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 access location must specify the location of the OCSP responder, using the conventions defined in [RFC2560] forCAs using OCSP. If OCSP is not used, the OID must not be present.
9	Extended Key Usage	M	NC	Extended key usage shall include at least one of the following • id-kp-email Protection {1 3 6 1 5.5 7 3 4} • MSFT Document Signing: {1.3.6.1.4.1.311.10.3.12}The following are optional ▪ Adobe Certified Document Signing {1.2.840.113583.1.1.5} ▪ Smart Card Logon {1.3.6.1.4.1.311.20.2.2

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 eachcertificate issued by a CA.
3	Issuer Signature Algorithm	M	NA	SHA256 with RSA Encryption (null parameters)or ECDSA with SHA256 {1 2 840 10045 4 3 2}(encoding MUST omit the parameters Field)
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) Fully Qualified Domain Name Note : Common Name is optional. If present, this field MUST contain a Fully-Qualified Domain Name that is one of the values contained in the Certificate's subject AltName extension. Wildcard FQDNs are permitted. A CA may issue an SSL Certificate with wildcard in the right-most label of the Domain Name provided that issuance complies with the requirements as mentioned in the SSL Guidelines.**Optional Attributes** State / Province State / province for verified Office addressOrganization Unit(OU). Department / Division to which the individual belongs within his Organization. In case meaningful OU has not been provided, this field must be omitted. Organization (O) Legal Name of the Organization the person belongs toCountry (C) Country code as per the verified Office address
7	Subject Public Key Information	M	NA	rsaEncryption, 2048 RSA Key modulus, public exponentor ecPublicKey { 1.2.840.10045.2.1}, named Curve, { 1.2.840.10045.3.1.7} (NIST curve P-256)
8	Issuer's Signature	M	NA	sha256 With RSAEncryption {1 2 840 113549 1 1 11} (nullparameters) or ECDSA with SHA256 {1 2 840 10045 4 3 2}(encoding MUST omit the parameters Field)
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 OCC certificate policythe certificate is valid for; and all the lower level certificate polices.
5	Basic Constraints	M	C	CA Boolean = False
6	Subject AlternativeName	M	NC	Subject Alternative Name: Fully Qualified Domain Name(FQDN) Note: Subject Alternative Name extension MUST contain at least one entry. Each entry MUST be either a dNS Name containing the Fully- Qualified Domain Name. Wildcard FQDNs are permitted. A CA may issue an SSL Certificate with wildcard in the right-most label of the Domain Name provided that issuance complies with the requirements as mentioned in the Guidelines for issuance of SSL Certificates dnsName(s) for the server(s) as an IA5 string
7	Extended Key Usage	M	NC	Extended key usage shall include at least one of the following • id-kp-serverAuth {1 3 6 1 5 5 7 3 1} • id-kp-clientAuth {1 3 6 1 5 5 7 3 2}
8	CRL Distribution Points	M	NC	Distribution Point Name MUST be set and MUST contain a complete HTTP URI pointing to a DER encoded full and complete CRL for all reasons. Distribution Point Name shall contain the full Name and thus shall not contain name Relative To CRL Issuer reasons and cRL Issuer fields shall be absent.
9	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 i[RFC2560] for CAs usingOCSP. If OCSP is not used, the OID must not be present.
10	Signed Certificate Time stamp List	O	NC	OID: 1.3.6.1.4.1.11129.2.4.2- The SCT data corresponding to the end-entity certificate from at least one log operator. If SCT obtained from more than one log, SCTs can be directly embedded in the certificate, by encoding the Signed Certificate Time stamp List structure as an ASN.1 OCTET STRING and inserting the resulting data in the TBS Certificate as an X.509v3 certificate extension (OID 1.3.6.1.4.1.11129.2.4.2).

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 3format)
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	SHA256 with RSA Encryption (null parameters)or ECDSA with SHA256 {1 2 840 10045 4 3 2}
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 aprintable string ▪ Serial number (CPU or any electronically verifiableserial number) as a printable string ▪ Unique ID as a printable string
7.	Subject Public Key Information	M	NA	rsaEncryption, 2048 RSA Key modulus, public exponent or ecPublicKey { 1.2.840.10045.2.1}, named Curve, {1.2.840.10045.3.1.7} (NIST curve P-256)
8.	Issuer's Signature	M	NA	sha256 With RSAEncryption {1 2 840 113549 1 1 11} (nullparameters) or ECDSA with SHA256 {1 2 840 10045 4 3 2}(encoding MUST omit the parameters Field)
9.	Signature Value	M	NA	Issuer CA's signature

Extensions				
1.	Authority Key Identifier	M	NC	Issuing CA Subject key Indetifier
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 OCC certificate policythe certificate is valid for; and all the lower level certificate polices.
5.	Basic Constraints	M	C	CA Boolean = False
6.	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]
7.	Extended Key Usage	M	NC	Extended key usage shall include • id-kp-clientAuth {1 3 6 1 5 5 7 3 2}
8.	CRL Distribution Points	M	NC	Distribution Point Name MUST be set and MUST contain a complete HTTP URI pointing to a DER encoded full and complete CRL for all reasons. Distribution Point Name shall contain the full Name and thusshall not contain name Relative To CRL Issuer 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 eachcertificate issued by a CA.
3.	Issuer Signature Algorithm	M	NA	SHA256 with RSA Encryption (null parameters)or ECDSA with SHA256 {1 2 840 10045 4 3 2}
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} (Issuance number } Organizational Unit (OU) Time Stamping Authority Organization (O) Legal Name of the TSA Organization Country (C) Country code as per the verified office address
7.	Subject Public Key Information	M	NA	rsaEncryption, 2048 RSA Key modulus, public exponentor ecPublicKey { 1.2.840.10045.2.1}, named Curve,{1.2.840.10045.3.1.7} (NIST curve P-256)

8.	Issuer's Signature	M	NA	sha256 With RSAEncryption {1 2 840 113549 1 1 11} (nullparameters) or ECDSA with SHA256 {1 2 840 10045 4 3 2} (encoding MUST omit the parameters Field)
9.	Signature Value	M	NA	Issuer CA's signature
Extensions				
1.	Authority Key Identifier	M	NC	Issuing CA Subject key Indetifier
2.	Subject Key Identifier	M	NC	Octet String of unique value associated with the Public key
3.	Key Usage	M	C	Digital Signature
4.	Certificate Policies	M	NC	The value must contain the OID representing the OCC certificatepolicy the certificate is valid for; and all the lower level certificatepolices.
5.	Basic Constraints	M	C	CA Boolean = False
6.	Extended Key Usage	M	C	id-kp-timestamping {1 3 6 1 5 5 7 3 8}
7.	CRL Distribution Points	M	NC	Distribution Point Name MUST be set and MUST contain a complete HTTP URI pointing to a DER encoded full and complete CRL for all reasons. Distribution Point Name shall contain the full Name and thusshall not contain name Relative To CRL Issuer reasons and cRL Issuer fields shall be absent.
8.	Authority Informati onAccess	M	NC	The id-ad-caIssuers OID MUST point to certificates issued to the CAissuing 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 access location must specify the location of the OCSP responder, using the conventions defined in[RFC2560] forCAs 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 3format)
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	SHA256 with RSA Encryption (null parameters)or ECDSA with SHA256 {1 2 840 10045 4 3 2}
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 Name string of maximum 64 characters (CN) constructed in the following manner Common name should be the name of theperson as in records Or Legal Name of the OrganizationHouse Identifier This attribute MUST contain the • Flat number, Apartment name and Plot no. OR • House Name / Number and Plot NumberOf 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. Organization (O) Legal Name of the 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 or ecPublicKey { 1.2.840.10045.2.1}, namedCurve, { 1.2.840.10045.3.1.7} (NIST curve P-256)
8.	Issuer's Signature	M	NA	sha256 WithRSAEncryption {1 2 840 113549 1 1 11} (nullparameters) or ECDSA with SHA256 {1 2 840 10045 4 3 2} (encoding MUST omit the parameters Field)
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 OCC certificatepolicy the certificate is valid for; and all the lower level certificatepolices.
6.	Basic Constraints	M	C	CA Boolean = False
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 thusshall not contain nameRelativeToCRLIssuer reasons and cRLIssuer fields shall be absent.
8.	Authority Information Access	M	NC	The id-ad-caIssuers OID MUST point to certificates issued to the CAissuing 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 ib [RFC2560] forCAs 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 eachcertificate issued by a CA.
3.	Issuer Signature Algorithm	M	NA	SHA256 with RSA Encryption (null parameters) Or ECDSA with SHA256 {1 2 840 10045 4 3 2}
4.	Issuer DistinguishedName	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 DistinguishedName	M	NA	Common Name (CN) <OCSP Responder Name> Organizational Unit (OU) OCSP Responder Organization (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 exponentor ecPublicKey { 1.2.840.10045.2.1}, namedCurve, { 1.2.840.10045.3.1.7} (NIST curve P-256)
8.	Issuer's Signature	M	NA	sha256 WithRSAEncryption {1 2 840 113549 1 1 11} (nullparameters) or ECDSA with SHA256 {1 2 840 10045 4 3 2} (encoding MUST omit the parameters Field)
9.	Signature Value	M	NA	Issuer CA's signature

1.	Authority Key Identifier	M	NC	Issuing CA Subject key Indetifier
2.	Subject Key Identifier	M	NC	Octet String of unique value associated with the Public key
3.	Key Usage	M	C	Digital Signature
4.	Certificate Policies	M	NC	The value must contain the OID representing the OCC certificatepolicy the certificate is valid for; and all the lower level certificatepolices.
5.	Basic Constraints	M	C	CA Boolean = False
6.	Extended Key Usage	M	C	id-kp-OCSPSigning {1 3 6 1 5 5 7 3 9}
7.	OCSP No revocation checking	M	NC	id-pkix-ocsp-nocheck=NULL{ 1.3.6.1.5.5.7.48.1.5}
8.	Authority Informatio nAccess	M	NC	The id-ad-ca Issuers OID MUST point to certificates issued to the CAissuing 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 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 3format)
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	SHA256 with RSA Encryption (null parameters) or ECDSA with SHA256 {1 2 840 10045 4 3 2}
4.	Issuer Distinguish edName	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 Distinguish edName	M	NA	Common Name Name string of maximum 64 characters (CN) constructed in the following manner The Common name should be the name of the person as in records State / Province State / province for verified residential address Organization Personal(O) Country (C) Country code as per the verified residential address

7.	Subject Public Key Informatio n	M	NA	rsaEncryption, 2048 RSA Key modulus, public exponentor ecPublicKey { 1.2.840.10045.2.1}, namedCurve, { 1.2.840.10045.3.1.7} (NIST curve P-256)
8.	Issuer's Signature	M	NA	sha256 WithRSAEncryption {1 2 840 113549 1 1 11} (nullparameters) or ECDSA with SHA256 {1 2 840 10045 4 3 2}(encoding MUST omit the parameters Field)
9.	Signature Value	M	NA	Issuer CA's signature
Extensions				
1.	Authority Key Identifier	M	NC	Issuing CA Subject key Identifier
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 OCC certificate policy the certificate is valid for; and all the lower level certificatepolices.
5.	Basic Constraints	M	C	CA Boolean = False
6.	Subject Alternative Name	O	NC	Email Address
7.	Extended Key Usage	M	C	Encrypting File System EKU=1.3.6.1.4.1.311.10.3.4
8.	CRL Distribution Points	M	NC	Distribution Point Name MUST be set and MUST contain a complete HTTP URI pointing to a DER encoded full and complete CRL for all reasons. Distribution Point Name shall contain the full Name and thusshall not contain name Relative To CRL Issuer reasons and cRLIssuer fields shall be absent.
9.	Authority Information Access	M	NC	The id-ad-ca Issuers OID MUST point to certificates issued to the CA issuing the certificate containing this field. The OID should specify a HTTP URI which points to a single DER encoded certificate or a collection of DER encoded certificates in a BER or DER encoded "certs-only" CMS message as specified in [RFC3852]. The id-ad-ocsp access location 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.

Encryption 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 3format)
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	SHA256 with RSA Encryption (null parameters)or ECDSA with SHA256 {1 2 840 10045 4 3 2}
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 DistinguishedName	M	NA	Common Name (CN) Name string of maximum 64 characters constructed in the following manner The Common name should be the name of the person as in records. State / Province State / province for verified Office address Organization Unit(OU) Department / Division to which the individual belongs within his Organization. In case meaningful OU has not been provided, this field must be omitted. Organization (O) Legal Name of the Organization the person belongs to Country (C) Country code as per the verified residential address
7.	Subject Public Key Information	M	NA	rsaEncryption, 2048 RSA Key modulus, public exponentor ecPublicKey { 1.2.840.10045.2.1}, namedCurve, { 1.2.840.10045.3.1.7} (NIST curve P-256)
8.	Issuer's Signature	M	NA	sha256 WithRSAEncryption {1 2 840 113549 1 1 11} (nullparameters) or ECDSA with SHA256 {1 2 840 10045 4 3 2} (encoding MUST omit the parameters Field)
9.	Signature Value	M	NA	Issuer CA's signature

Extensions				
1.	Authority Key Identifier	M	NC	Issuing CA Subject key Identifier
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 OCC certificatepolicy the certificate is valid for; and all the lower level certificate polices.
5.	Basic Constraints	M	C	CA Boolean = False
6.	Subject Alternative Name	O	NC	Email Address
7.	Extended Key Usage	M	C	Encrypting File System EKU=1.3.6.1.4.1.311.10.3.4
8.	CRL Distribution Points	M	NC	Distribution Point Name MUST be set and MUST contain a complete HTTP URI pointing to a DER encoded full and complete CRL for all reasons. Distribution Point Name shall contain the full Name and thusshall not contain name Relative To CRL Issuer reasons and cRL Issuer fields shall be absent.
9.	Authority Information Access	M	NC	The id-ad-ca Issuers OID MUST point to certificates issued to the CAissuing 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 access location must specify the location of the OCSP responder, using the conventions defined in [RFC2560] forCAs using OCSP. If OCSP is not used, the OID must not be present.

Organizational Document Signer 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 3format)
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	SHA256 with RSA Encryption (null parameters)or ECDSA with SHA256 {1 2 840 10045 4 3 2}
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 DistinguishedName	M	NA	Common Name (CN) DS Legal Name of the Organization (number) • DS represent Documents/Information Signer. • (number) should be appended to differentiate the certificate(s) issued to same Organization State / Province • State / province for verified Office address Organization Unit(OU) Department / Division to which the Subject Organization. In case meaningful OU has not been provided, this field must be omitted. Organization (O) Legal Name of the Organization Country (C) Country code as per the verified Office address
7.	Subject Public Key Information	M	NA	rsaEncryption, 2048 RSA Key modulus, public exponentor ecPublicKey { 1.2.840.10045.2.1}, namedCurve, { 1.2.840.10045.3.1.7} (NIST curve P-256)
8.	Issuer's Signature	M	NA	sha256 With RSAEncryption {1 2 840 113549 1 1 11} (nullparameters) or ECDSA with SHA256 {1 2 840 10045 4 3 2}(encoding MUST omit the parameters Field)
9.	Signature Value	M	NA	Issuer CA's signature

Extensions				
1.	Authority Key Identifier	M	NC	Issuing CA Subject key Identifier
2.	Subject Key Identifier	M	NC	Octet String of unique value associated with the Public key
3.	Key Usage	M	C	Digital Signature, non Repudiation(O)
4.	Subject Alternative Name	O	NC	Email Address
5.	Extended Key Usage	M	NC	At least one of the following is mandatorySecure E-Mail {1.3.6.1.5.5.7.3.4} MSFT Document Signing {1.3.6.1.4.1.311.10.3.12} The optional EKU is given below Adobe Document Signing {1.2.840.113583.1.1.5}
6.	Certificate Policies	M	NC	The value must contain the OID representing the OCC certificatepolicy the certificate is valid for; and all the lower level certificate polices. The value must contain the policy ID, 2.16.356.100.10.1 also
7.	Basic Constraints	M	C	CA Boolean = False
8.	CRL Distribution Points	M	NC	Distribution Point Name MUST be set and MUST contain a complete HTTP URI pointing to a DER encoded full and complete CRL for all reasons. Distribution Point Name shall contain the full Name and thus shall not contain name Relative To CRL Issuer reasons and cRL Issuer fields shall be absent.
9.	Authority Information Access	M	NC	The id-ad-caIssuers OID MUST point to certificates issued to the CAissuing 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 access location 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	sha256 With RSA Encryption {1 2 840 113549 1 1 11}or ECDSA with SHA256 {1 2 840 10045 4 3 2}
3.	Issuer Distinguished Name	M	NA	Unique X.500 Issuing CA DN Single value shall be encoded in each RDN. Furthermore, eachvalue 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 issuancefrequency)
6.	Revoked certificates list	M	NA	0 or more 2-tuple of certificate serial number and revocation date (inGeneralized Time)
7.	Issuer's Signature	M	NA	sha256 WithRSAEncryption {1 2 840 113549 1 1 11}or ECDSA with SHA256 {1 2 840 10045 4 3 2} (encoding MUST omit the parameters Field)

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 incertificates issued by the CA)
CRL Entry Extensions				
1.	Reason Code	O	NC	Must be included when reason code = key compromise or CAcompromise

Annexure IV

– Application Developer Guidelines

Application developers are to develop applications in compliance with RFC 2459 certificate profile. A number ofcommercial 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 Different 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

- As a prerequisite, the applications need to establish a trust anchor. The trust anchor for the Nepal PKI would bethe OCC , Root Certifying Authority of Nepal (RCAN) Certificate. The certificate needs to be downloaded and installed in the application in a secure manner after verification of the certificate thumb print.

- 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.

- Applications should be able to determine the prospective certification path. Since the Nepal 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.

- 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 2459, . The following steps are minimum validations to be performed by an application as an interim measure until it implementsthe compete path validation algorithm as mentioned in RFC 2459.

- Determine the prospective certificate path starting with end-entity certificate to trust anchor by following the AIA pointers in iterative manner.

- for ***each certificate*** in the certification path starting with the certificate issued by the OCC.

- verify the signature on the certificate using the public key from the previous certificate

- verify that the current time is within the certificate validity

- 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.

- certificate issuer name corresponds to subject name in the previous certificate

- Determine the intersection set of all the policies in the certification path and determine if it confirms to acceptable application policy.

- For all certificates other than end user certificate verify that basic Constraints extension is present and CA is set to TRUE and path length constraint is not violated per RFC 2459.
- 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, and Subject Public Key algorithm, public key and associated parameters. The use certificate is also consistent with policy- id listed in the Certificate Policies field to ascertain the certificate is used only for indented purpose,

Annexure V

Application Owner Guidelines

These Guidelines are intended for Application Owners for planning implementation of Digital Signature facility intheir applications.

1. Based on Risk Analysis and security requirements for the applications and relying parties, Application Owners should decide the Assurance Level (Class) of the Digital Signature Certificates which is suitable for them.

2. The DSCs issued by Licensed CAs hold same assurance level for the same class. In Digital Signature enabled applications, the application owners should accept DSCs issued by any of the Licensed CAs as long as they belong to the specified class or higher.

3. Application owners shall not impose the requirements of any additional DSC fields or private key storage requirements other than those mentioned in the Guidelines issued by OCC.

4. Application owners should accept higher class certificates if lower class certificates of the same been specified by Application Owners for their application.

5. Each type of certificate (Digital Signature, encryption, document signer, SSL, code signer etc) is intended for specific purpose. Application owners should use each type of certificates in consistent with their intended purpose.