Ethiopian National PKI Technical Standards Guideline

Draft Version 1.0

INFORMATION NETWORK SECURITY AGENCY

2012 E.C.

Document Control

Document Name	Ethiopian National PKI Technical Standards Guideline
Status	Draft
Version	1.0
Last Update	New Release
Document Owner	INSA

Table of Contents

Foreword

The Electronic Signature Proclamation No.1072/2018 states that the Information Network Security Agency (INSA) shall act as is the Root Certificate Authority pursuant to the mandate given to it in its establishment Proclamation. The Ethiopian PKI has a hierarchical structure, INSA as a trust anchor of the hierarchy.

INSA as a Root CA has a self-signed Root Certificate that issues Public Key Certificates to the Subordinate CA while Subordinate CAs in turn issue Digital Certificate to end-users.

Certificates may be used in a wide range of applications and environments covering a broad spectrum of interoperability goals and a broader spectrum of operational and assurance requirements. The goal of this document is to establish a common baseline for generic applications requiring broad interoperability and limited special purpose requirements.

This guideline is used to prevent the lack of interoperability between Digital Certificates issued by different Certificate Providers resulting in users having to obtain multiple number of Digital Certificates for use across different applications.

The profiles found in this guideline are prepared in line with international standards and best practices. This guideline includes profiles of certificates including Time stamping Certificate, OCSP responder Certificate, Document Signer Certificate, SSL Certificate, End User Digital Signature Certificate, Encryption Certificate and Code signing Certificate.

1. Introduction

The need to create a detailed guideline is to address the above interoperability issues. This guideline has been issued as part of the National Root CA of Ethiopian PKI as an interoperability guideline for digital certificates issued in the country.

The guidelines here are instructed to the licensed certificate providers in Ethiopia. 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.

2. Scope

These guidelines are applicable to all Subordinate CAs and are to be implemented for all certificates issued by them.

These guidelines shall be interpreted along with the existing rules and regulations. unless a clarification stating otherwise has been issued by The National Root Certificate Authority (INSA).

INSA has the authority to review and issue updated versions of this document. The revised document will be available on the Root CA's website.

3. Normative references

This section defines standards that shall be followed by all Subordinate CAs for carrying out their functions. Every Subordinate CA shall observe the following standards for carrying out different activities associated with its functions.

RFC5280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

RFC2560 -X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP

RFC 3161- Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)

RFC4210- Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP)

RFC2511- Internet X.509 Certificate Request Message Format

RFC2587-Internet X.509 Public Key Infrastructure LDAPv2 Schema

RFC2585- Internet X.509 Public Key Infrastructure Operational Protocols: FTP and HTTP

PKCS#1- RSA Cryptography Standard

PKCS#3- Diffie-Hellman Key Agreement Standard

PKCS#5- Password Based Encryption Standard

PKCS#6-Extended-Certificate Syntax Standard

PKCS#7- Cryptographic Message Syntax standard

PKCS#8- Private Key Information Syntax standard

PKCS#9- Selected Attribute Types

PKCS#10- RSA Certification Request

PKCS#11- Cryptographic Token Interface Standard

PKCS#12- Portable format for storing/transporting a user's private keys and certificates

PKCS#13- Elliptic Curve Cryptography Standard

PKCS#15- Cryptographic Token Information Format Standard

FIPS 180-4- Secure Hash Standard

FIPS 186-3- Digital Signature Standard (DSS)

FIPS 140-2 - Security Requirement for Cryptographic Modules

X.500- X.500 for publication of Public Key Certificates and Certificate Revocation Lists

X.501 - Information technology - Open Systems Interconnection - The Directory: Models

X.509 version 3- X.509 version 3 Certificates as specified in ITU

X.509 version 2- X.509 version 2 Certificate Revocation Lists

Electronic Signature Proclamation- Electronic Signature Proclamation No.1072/2018

Regulation- Electronic signature regulation (Draft)

CA-Browser-Forum-. Baseline Requirements for the issuance and Management of Publicly Trusted Certificates.

CA-Browser-Forum - Baseline-Requirements-for-the-Issuance-and-Management-of-CodeSigning-Certificates

WebTrust for Certification Authorities - Web trust principles and criteria for certificate authorities

4. Informative references

This reference defines standards that are more detailed technical documents and are meant to provide Subordinate CAs with a starting point for implementing practices to execute their functions. It is helpful if the Subordinate CAs observe the following standards for carrying out different activities associated with their functions.

RFC3647- Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework.

RFC2587- Internet X.509 Public Key Infrastructure LDAPv2 Schema

RFC3281- An Internet Attribute Certificate Profile for Authorization

RFC3039- Internet X.509 Public Key Infrastructure Qualified Certificates Profile

5. Definitions and Acronyms

5.1. Definitions

Mandatory (M) – These fields or extensions are mandated by INSA 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 (O) – 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.

Critical(C) – A certificate using system MUST reject the certificate if it encounters a critical extension it does not recognize;

Non-critical (NC) – a non-critical extension MAY be ignored if it is not recognized.

Pr1ohibited – These fields or extensions are NOT to be included or used in Digital Certificates unless notified by INSA regarding the usage and format.

notBefore- the date on which the certificate validity period begins. **notAfter -** the date on which the certificate validity period ends.

Subordinate CA - refers to those CAs that live between the root and end entity certificates.

X.509 – is a recommended standard to address specific certificate and CRL profile associated with internet.

Microsoft CryptoAPI (Microsoft Cryptography API) - is an application programming interface included with Microsoft Windows operating systems that provides services to enable developers to secure Windows-based applications using cryptography.

Microsoft CNG - Windows Vista features an update to the Crypto API known as Cryptography API: Next Generation (CNG).

Network Security Services (NSS) – It is a set of libraries designed to support cross-platform development of security-enabled client and server applications.

5.2. Acronyms

CA Certificate Authority

CMP Certificate Management Protocol

DN1 Distinguished Name

NA Not-applicable

OCSP Online certificate status Protocol

PKI Public Key Infrastructure

RDN Relative Distinguished Names

SSL Secure Socket Layer

AIA Authority Information Access

NIST National Institute of Standards and Technology

ISO International Organization for Standardization

OID Object Identifier

PKIF PKI Framework

DSA Digital Signature Algorithm

API1 Application Program Interface

RSA Rivest, Shamir, and Adelman

KCDSA Korea Certification based Digital Signature Algorithm

ECDSA Elliptic Curve Digital Signature Algorithm

6. 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 as Defined above.

6.1. Field Definition

This section presents a profile for public key certificates that will foster interoperability and a reusable PKI. This section is based upon the X.509 v3 certificate format and the standard certificate extensions defined in [X.509].

Field Name: **Version**	
Mandatory/Optional	Mandatory

Field description	Describes the version of the encoded certificate
Interp1retation & 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).

Table 1.Version Field

Field Name : **Serial Number**	
Mandatory/Optional	Mandatory
Field description	The serial number is a unique positive integer assigned for a certificate in a given CA
Interpretation & usage	It MUST be unique for each certificate issued by a given CA (i.e., the issuer name and serial number identify a unique certificate).
Compliance Standards	RFC 5280
Type	Positive Integer
Length	Certificate users MUST be able to handle serial Number values up to 20 octets
Mandated Value	Positive number unique to each certificate issued by a CA.

Table 2. Serial Number Field

Field Name : **Signature**	
Mandatory/Optional	Mandatory
Field description	Issuer signature algorithm identifier

Interpretation & usage	Contains the algorithm identifier for the algorithm used by the CA to sign the certificate. 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 SHA256 with RSA Encryption (null parameters) {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}

Table 3. Signature Field

Field Name : **Issuer**	
Mandatory/Optional	Mandatory
Field description	Uniquely Identifies the Certifying Authority issuing the certificate
Interpretation & usage	The issuer field identifies the entity that has signed and issued the certificate
Compliance Standards	RFC 5280, X.520
Type	MUST contain a non-empty distinguished name (DN)
Mandated Value	Refer Field specification Section

Table 4. Issuer Field

Field Name : **Validity**	
Mandatory/Optional	Mandatory
Field description	The certificate validity period is the time interval during which the CA warrants that it will maintain information about the status of the certificate.
Interpretation & usage	The Validity fields are used to assess if the certificate issued is valid. The field is represented as a SEQUENCE of two

	dates, notBefore and notAfter
Compliance Standards	RFC 5280
Type	UTC Time or 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

Table 5. Validity Field

Field Name : **Subject**	
Mandatory/Optional	Mandatory
Field description	The subject field identifies the entity associated with the public key stored in the subject public key field.
Interpretation & usage	The Distinguished Name mentioned in the Subject identifies the owner of the certificate.
Compliance Standards	RFC 5280
Type	SEQUENCE OF Relative Distinguished Names (RDNs) in printable string format.
Mandated Value	Refer Field specification Section

Table 6.Subject Field

Field Name : **Subject Public Key Info**	
Mandatory/Optional	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	This field is used to carry the public key and identify the algorithm with which the key is used
Compliance Standards	RFC 5280
Type	OID, OID dependent parameters and Key in bitstring format

Mandated Value	For Root CA: rsaEncryption, 4096 RSA Key For SUBORDINATE CA: rsaEncryption, 4096 RSA Key For End Entity : rsaEncryption, 2048 RSA Key

Table 7.Subject Public Key Info Field

Field Name : **Unique Identifiers**	
Mandatory/Optional	Prohibited
Field description	Unique identifier for a subject and issuer names (Subject Unique Identifier, Issuer Unique Identifier)
Interpretation & usage	These fields MUST only appear if the version is 2 or 3. These fields MUST NOT appear if the version is 1. unique identifiers are present in the certificate to handle the possibility of reuse of subject and/or issuer names over time
Compliance Standards	RFC 5280
Type	Bit string
Mandated Value	CAs conforming to this profile MUST NOT generate certificates with unique identifiers. Applications conforming to this profile SHOULD be capable of parsing certificates that include unique identifiers, but there are no processing requirements
Field Name : **Unique Identifiers**	
	Associated with the unique identifiers. Field not to be used

Table 8.Unique Identifiers Field

Field Name : **Signature Algorithm**	
Mandatory/Optional	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 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 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

Table 9.Signature Algorithm Field

Field Name : **Signature Value**	
Mandatory/Optional	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 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.

Table 10.Signature Value Field

6.2. Standard Extension Definition

This section identifies standard certificate extensions defined in [X.509] for use in the Internet PKI. Each extension is associated with an OID defined in [X.509]. The extensions defined for

X.509 v3 certificates provide methods for associating additional attributes with users or public keys and for managing relationships between CAs.

Standard Extension : **Authority Key Identifier**	
Mandatory/Optional	Mandatory
Field description	The authority key identifier extension provides a means of identifying the public key corresponding to the private key used to sign a 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	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.

Table 11.Authority Key Identifier Standard Extension

Standard Extension : **Subject Key Identifier**	
Mandatory/Optional	Mandatory
Field description	The subject key identifier extension provides a means of identifying certificates that contain a particular public key.
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 honor the subject key identifier value requested in a certificate request (e.g., PKCS-10 request). Honoring requested value is critical to interoperability when RCAI issues a CA certificate or a CA issues a Subordinate CA certificate.
Calculation Method	The keyIdentifier is composed of the 160-bit SHA-1 hash of the value of the BIT STRING subjectPublicKey (excluding the tag, length, and number of unused bits).

Standard Extension : **Subject Key Identifier**	
	The keyIdentifier is composed of a four-bit type field with the value 0100 followed by the least significant 60 bits of the SHA-1 hash of the value of the BIT STRING subjectPublicKey (excluding the tag, length, and number of unused bits).
Recommended Value	Subject key identifier can be calculated as per any of the method mentioned above. Any other method which provides a statistically unique value associated with the Public key is also acceptable.

Table 12.Subject Key Identifier Standard Extension

Standard Extension : **Key Usage**	
Mandatory/Optional	Mandatory
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

Table 13.Key Usage Standard Extension

Standard Extension : **Certificate Policies**	
Mandatory/Optional	Mandatory
Field description	Contains policy information terms in the form of OIDs and qualifiers.
Interpretation & usage	Ethiopian X.509 Certificate Policy the certificate is valid for; and all the lower 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 Ethiopian X.509 Certificate Policy the certificate is valid for; and all the lower level certificate polices.

Table 14.Certificate Policies Standard Extension

Standard Extension : **Policy Mappings**	
Mandatory/Optional	Prohibited
Field description	Lists pairs of OIDs for issuerDomainPolicy and subject DomainPolicy
Interpretation & usage	The use of this Extension is prohibited by INSA.
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

Table 15. Policy Mappings Standard Extension

Standard Extension : **Subject Alternative Name**	
Mandatory/Optional	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 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

Table 16. Subject Alternative Name Standard Extension

Standard Extension : **Issuer Alternative Name**	
Mandatory/Optional	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 INSA.
Compliance Standards	RFC 5280
Type	Email ID / IP Address / URL / DNS Name
Critical / Non Critical	Non Critical
Mandated Value	Extension not to be used

Table 17. Issuer Alternative Name Standard Extension

Standard Extension : **Subject Directory Attributes**	
Mandatory/Optional	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 5280
Standard Extension : **Subject Directory Attributes**	
Type	Sequence of attributes
Critical / Non Critical	Non Critical
Mandated Value	Not Applicable
Recommended Value	Root CA will provide guidance on this as needs arise.

Table 18. Subject Directory Attributes Standard Extension

Standard Extension : **Basic Constraints**	
Mandatory/Optional	Mandatory
Field description	identifies whether the subject of the certificate is a CA and the maximum number of CAs may follow in the certification path
Interpretation & usage	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. INSA self-signed CA certificate shall not contain pathLengthConstraint. CA certificate shall contain pathLengthConstraint = 0 if there are no Subordinate CA Subordinate CA certificate shall contain pathLengthConstraint= 0. For end user certificate, the field MUST have value CA= False

Table 19.Basic Constraints Standard Extension

Standard Extension : **Name Constraints**	
Mandatory/Optional	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	The use of this field is Prohibited
Compliance Standards	RFC 5280
Type	Domain name / IP address /directoryName
Critical / Non Critical	Critical
Mandated Value	Extension not to be used

Table 20.Name Constraints Standard Extension

Standard Extension : **Policy Constraints**	
Mandatory/Optional	Prohibited
Field description	Limits the policy mapping or mandates an acceptable policy in certificate path.
Interpretation & usage	The use of this field is Prohibited.
Compliance Standards	RFC 5280
Type	OIDs
Critical / Non Critical	Critical
Mandated Value	Extension not to be used

Table 21.Policy Constraints Standard Extension

Standard Extension : **Extended Key Usage**	
Mandatory/Optional	Mandatory
Field description	Further limits the use of a certificate based on cryptographic application.
Interpretation & usage	This field is mandatory to be in all certificates.
Compliance Standards	RFC 5280
Type	OID
Critical / Non Critical	Critical / Non Critical as provided in section 8

Mandated Value	None
Recommended Value	CAs MAY configure extended key usage as per guidance provided in Section 8.

Table 22. Extended Key Usage Standard Extension

Standard Extension : **CRL Distribution Point**	
Mandatory/Optional	Mandatory
Field description	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. Reasons and cRLIssuer fields shall be absent.

Table 23.CRL Distribution Point Standard Extension

Standard Extension : **Inhibit Any Policy**	
Mandatory/Optional	Prohibited
Field description	When set, this field inhibits an explicit match with special anyPolicy OID { 2 5 29 32 0 }
Interpretation & usage	The use of this field is Prohibited.
Compliance Standards	RFC 5280
Type	OID
Critical / Non Critical	Critical
Mandated Value	Extension not to be used

Table 24.Inhibit Any Policy Standard Extension

Standard Extension : **Freshest CRL**	
Mandatory/Optional	Prohibited
Field description	Identifies how delta CRL information is obtained.
Interpretation & usage	The use of this field is Prohibited by INSA.
Compliance Standards	RFC 5280
Type	URI
Critical / Non Critical	Non Critical
Mandated Value	Extension not to be used

Table 25.Freshest CRL Standard Extension

Standard Extension : **Signed Certificate Timestamp List**	
Mandatory/Optional	Optional
Field description	Signed Certificate Timestamp (SCT) returned by Log operators when a valid certificate is submitted to a log.
Interpretation & usage	To be included only in the SSL certificates
Compliance Standards	RFC 5280 , 6962
Type	OCTET STRING
Critical / Non Critical	Non Critical
Mandated Value	If present, at least one SCT MUST be included.

Table 26. Signed Certificate Timestamp List Standard Extension

6.3. Private Extensions

This section defines two extensions for use in the Internet Public Key Infrastructure. These extensions may be used to direct applications to on-line information about the issuer or the subject.

Each extension contains a sequence of access methods and access locations.

Private Internet Extension : **Authority Information Access**	
Mandatory/Optional	Mandatory
Field description	The extension provides information for accessing information and services of the issuer.

Private Internet Extension : **Authority Information Access**	
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].

Table 27.Authority Information Access private. Internet Extension

Private Internet Extension : **Subject Information Access**	
Mandatory/Optional	Prohibited
Field description	The extension provides information for accessing information and services regarding the subject
Interpretation & usage	The use of this field is Prohibited
Compliance Standards	RFC 5280
Type	URI
Critical / Non Critical	Non Critical
Mandated Value	This field must not be used.

Table 28.Subject Information Access Private. Internet Extension

7. Field Specification

7.1. Naming Convention

In order to standardize the naming for the Root CA and Subordinate CA, the following guideline is to be adopted for determining the ‘Common Name’ (CN) for Root CA and Subordinate CA.

Entity	**Naming (Common Name)**	**Example**

Root CA	"Root CA Name" CA {Generation Qualifier} (issuance number}	INSA National Root CA 2020 INSA National Root CA 2020-1
Subordinate CA	"Certifying Authority Name" Subordinate CA {Generation qualifier} (Issuance number }	Government CA 2020 Government CA 2020-1

Table 29.Naming Convection

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 issuance of certificate. E.g. When a root certificate is issued in 2009, the CA name will be XYZ CA 2009. When the next CA certificate is reissued, the CA name will be indicating 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:

No.	Attribute Type	Attribute Value Encoding
1	Country	Printable String
2	Organization	Printable String
3	Organization 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	pseudonym	Printable String

No.	Attribute Type	Attribute Value Encoding
11	Telephone Number	Printable String
12	Title	Printable String

Table 30.Attribute type and associated value

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.

No.	Certificate Type	Issuer	Subject
1	Root CA	Root CA	Root CA
2	Subordinate CA	Same as Subject in Root CA Certificate	Refer Subordinate CA Subject Specifications
3	End User (certificate issued by Subordinate CA)	Same as subject for Certificate Subordinate CA	Refer End user subject specifications

Table 31.Summary of issuer and subject fields

7.2. Issuer

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].

The summary of issuer specification fields is presented in the table below.

Root CA Certificate - Issuer specifications

No.	Attribute	Value
1	Common Name (CN)	INSA National Root CA (Issuance number }
2	Organization (O)	Information Network Security Agency
3	Country (C)	Ethiopia (ET)

Table 32.Root CA Certificate - Issuer specifications

SUBORDINATE CA Certificate –Issuer specifications

No.	Attribute	Value
1	Common Name (CN)	INSA National Root CA (Issuance number }
2	Organization (O)	Information Network Security Agency
3	Country (C)	Ethiopia (ET)

Table 33.SUBORDINATE CA Certificate –Issuer specifications

End User Certificate (Issued by Subordinate CA) – Issuer specifications

No.	Attribute	Value
1	Common Name (CN)	Same as Common Name (CN) field in Subordinate CA
2	Organizational Unit (OU)	Same as Organizational Unit (OU) field in Subordinate CA
3	Organization (O)	Same as Organization (O) field in Subordinate CA
4	State / Province	Same as State / Province field in Subordinate CA
5	Country (C)	Same as Country (C) field in Subordinate CA

Table 34.End User Certificate (Issued by SUBORDINATE CA) – Issuer specifications

7.3. Subject

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.

The summary of subject specification fields is presented in the table below.

Root CA Certificate - Subject specifications

No.	Attribute	Value
1	Common Name (CN)	INSA National Root CA (Issuance number }
2	Organization (O)	Information Network Security Agency
3	Country (C)	Ethiopia (ET)

Table 35.Root CA Certificate - Subject specifications

Subordinate CA – Subject specifications

No.	Attribute	Value
1	Common Name (CN)	Max Length: 64 characters • Subordinate CA Name (name by which it will be commonly known) (Refer Naming Conventions section in organizational recommendations section)
2	Organizational Unit (OU)	"Subordinate CA"
3	Organization (O)	Max Length: 64 Characters Legal Name of the Organization operating the CA*
4	State / Province	Max Length: 60 Characters • State / province where the Certifying Authority has its head office or registered office
5	Country (C)	Max Length: 2 Characters Country code as described in the ISO 3166 international standard.

Table 36.SUBORDINATE CA – Subject specifications

End User Certificate – Subject specifications

No.	Attribute	Definition
1.	Common Name	Max Length: 64 Characters Human: CN=name Server or service: CN=IP address or domain name Device: CN=serial number
2.	TIN number	This attribute should be populated with the TIN number
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	Telephone Number	" Mobile Number for individuals" (optional) (2.5.4.20 - id-at-telephone Number)
5	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 OU has not been provided, this field must be omitted. The Organizational unit must not be present when the organization has been marked as "personal"
No.	**Attribute**	**Definition**
6	Organization	Max Length: 64 Characters This attribute MUST contain either The Name of the organization the person belongs to – if such information has been verified by the CA OR Contain string "Personal"
7	Country	Max Length: 2 Characters Country code as described in the ISO 3166 international standard.

Table 37.End User Certificate – Subject specifications

8. Reference Certificate Profiles

8.1. Root CA Certificate

Field	Mandatory/ Optional	Critical/ Non critical	Note
Version	M	NA	The mandated value is 2. (i.e., The certificate must be in a version 3 format)

Serial Number	M	NA	Minimum 8 Bytes , Maximum 20 Bytes
Issuer Signature Algorithm	M	NA	SHA256 with RSA Encryption (null parameters)
Issuer Distinguished Name	M	NA	Common Name (CN) - INSA National Root CA (Issuance number) Organization (O) - Information Network Security Agency Country (C) - Ethiopia (ET)
Validity Period	M	NA	Generalized Time (20 years)
Subject Distinguished Name	M	NA	Common Name (CN) - INSA National Root CA (Issuance number) Organization (O) - Information Network Security Agency Country (C) - Ethiopia (ET)
Subject Public Key Information	M	NA	rsaEncryption {1 2 840 113549 1 1 1}, 4096 RSA Key modulus, public exponent
X.509 V3 extensions			
Authority Key Identifier	Mandatory	Non critical	National Root CA Subject Key Identifier
Subject Key Identifier	Mandatory	Non critical	Octet String of unique value associated with the Public key
Key usage	Mandatory	Critical	keyCertSign, cRLSign
Basic Constraints	Mandatory	Critical	Subject Type=CA ,Path Length Constraint=None

Table 38.Root CA Certificate

8.2. Subordinate CA Certificate

Field	Mandatory/ Optional	Critical/ Non critical	Note
Version	M	NA	The mandated value is 2. (i.e., The certificate must be in a version 3 format)

Serial Number	M	NA	Minimum 8 Bytes , Maximum 20 Bytes
Issuer Signature Algorithm	M	NA	SHA256 with RSA Encryption (null parameters)
Issuer Distinguished Name	M	NA	Common Name (CN) - INSA National Root CA (Issuance number) Organization (O) - Information Network Security Agency Country (C) - Ethiopia (ET)
Validity Period	M	NA	Generalized Time (10 years)
Subject Distinguished Name	M	NA	Common Name (CN) - Max Length: 64 characters • SUBORDINATE CA Name (name by which it will be commonly known) (Refer Naming Conventions section in organizational recommendations section) Organizational Unit (OU) - "Certificate Provider" Organization (O) - Max Length: 64 Characters Legal Name of the Organization operating the CA* State / Province - Max Length: 60 Characters • State / province where the Certifying Authority has its head office or registered office Country (C) - Max Length: 2 Characters Country code as per the verified residential / office address
Subject Public Key Information	M	NA	rsaEncryption {1 2 840 113549 1 1 1}, 4096 RSA Key modulus, public exponent

X.509 V3 extensions			
Authority Key Identifier	Mandatory	Non critical	National Root CA Subject Key Identifier
Subject Key Identifier	Mandatory	Non critical	SUBORDINATE CA Subject Key Identifier
Key usage	Mandatory	Critical	keyCertSign, cRLSign
Certificate Policies	Mandatory	Non critical	Policy OID , Policy Qualifier
Basic Constraints	Mandatory	Critical	Subject Type=true ,Path Length Constraint=0
CRL Distributions Points	Mandatory	Non critical	URL pointing to CRL Distribution
Authority Information Access	Mandatory	Non critical	URL pointing to CA Issuer Certificate

Table 39.Subordinate CA Certificate

8.3. Time Stamping Authority Certificate

Field	**Mandatory/ Optional**	**Critical/ Non critical**	**Note**
Version	M	NA	The mandated value is 2. (i.e., The certificate must be in a version 3 format)
Serial Number	M	NA	Minimum 8 Bytes , Maximum 20 Bytes
Issuer Signature Algorithm	M	NA	SHA256 with RSA Encryption (null parameters) or ECDSA with SHA256 {1 2 840 10045 4 3 2}
Issuer Distinguished Name	M	NA	CN= Certificate Provider Name, O=Organization, OU=Organizational Unit,

			ST=Name of State, C=ET
Validity Period	M	NA	Generalized Time (Maximum 10 Years)
Subject Distinguished Name	M	NA	CN= Time Stamping Authority Name OU=Organization Unit Name O=Organization Name ST=Name of State C=ET
Subject Public Key Information	M	NA	rsaEncryption, 2048 RSA Key modulus, public exponent
X.509 V3 extensions			
Authority Key Identifier	Mandatory	Non critical	Subordinate CA Subject Key Identifier
Subject Key Identifier	Mandatory	Non critical	Subject Key Identifier
Key usage	Mandatory	Critical	digitalSignature
Certificate policies	Mandatory	Non critical	Policy OID , Policy Qualifier
Extended Key Usage	Mandatory	Critical	timestamping
CRL Distribution Points	Mandatory	Non critical	URL pointing to CRL Distribution
Authority Information Access	Mandatory	Non critical	OCSP locator URL, URL pointing to CA Issuer Certificate

Table 40.Time Stamping Authority Certificate

8.4. OCSP Responder Certificate

Field	Mandatory/ Optional	Critical/ Non critical	Note
Version	M	NA	The mandated value is 2. (i.e., The certificate

			must be in a version 3 format)
Serial Number	M	NA	Minimum 8 Bytes , Maximum 20 Bytes
Issuer Signature Algorithm	M	NA	SHA256 with RSA Encryption (null parameters) or ECDSA with SHA256 {1 2 840 10045 4 3 2}
Issuer Distinguished Name	M	NA	CN= Certificate Provider Name, O=Organization, OU=Organizational Unit, ST=Name of State, C=ET
Validity Period	M	NA	Generalized Time (2 Years)
Subject Distinguished Name	M	NA	CN= OCSP Responder Name OU=Organization Unit Name O=Organization Name ST=Name of State C=ET
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)
X.509 V3 extensions			
Authority Key Identifier	Mandatory	Non critical	Subordinate CA Subject Key Identifier
Subject Key Identifier	Mandatory	Non critical	Subject Key Identifier
Key usage	Mandatory	Critical	digitalSignature
Certificate policies	Mandatory	Non critical	Policy OID , Policy Qualifier
Basic Constraints	Optional	Non critical	Subject Type=End Entity,Path Length Constraint=None
Extended Key Usage	Mandatory	Critical	OCSPSigning

CRL Distribution Points	Mandatory	Non critical	URL pointing to CRL Distribution
Authority Information Access	Mandatory	Non critical	OCSP locator URL, URL pointing to CA Issuer Certificate
OCSP No Check	Mandatory	Non critical	This extension tells a client that it is not necessary to check the certificate status of this certificate .

Table 41.OCSP Responder Certificate

8.5. SSL Certificate

Field	Mandatory/ Optional	Critical/ Non critical	Note
Version	M	NA	The mandated value is 2. (i.e., The certificate must be in a version 3 format)
Serial Number	M	NA	Minimum 8 Bytes , Maximum 20 Bytes
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)
Issuer Distinguished Name	M	NA	CN= Certificate Provider Name, O=Organization, OU=Organizational Unit, ST=Name of State, C=ET
Validity Period	M	NA	Generalized Time (2 Years)
Subject Distinguished Name	M	NA	CN=Fully Qualified Domain Name(FQDN) OU=Organization Unit Name O=Organization Name ST=Name of State C=ET

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)
X.509 V3 extensions			
Authority Key Identifier	Mandatory	Non critical	Subordinate CA Subject Key Identifier
Subject Key Identifier	Mandatory	Non critical	Octet String of unique value associated with the Public key
Key usage	Mandatory	Critical	digitalSignature, keyEncipherment
Certificate policies	Mandatory	Non critical	Policy OID , Policy Qualifier
Subject Alternative Name	Optional	Non critical	dnsName(s) for server ,IP address of the server
Basic Constraints	Optional	Non critical	Subject Type=End Entity Path Length Constraint=None
Extended Key Usage	Mandatory	Critical	serverAuth, clientAuth
CRL Distribution Points	Mandatory	Non critical	URL pointing to CRL Distribution
Authority Information Access	Mandatory	Non critical	OCSP locator URL, URL pointing to CA Issuer Certificate

Table 42.SSL Certificate

8.6. System Certificate

Field	Mandatory/ Optional	Critical/ Non critical	Note
Version	M	NA	The mandated value is 2. (i.e., The certificate must be in a version 3 format)
Serial Number	M	NA	Minimum 8 Bytes , Maximum 20 Bytes

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)
Issuer Distinguished Name	M	NA	CN= Certificate Provider Name, O=Organization, OU=Organizational Unit, ST=Name of State, C=ET
Validity Period	M	NA	Generalized Time (2 Years)
Subject Distinguished Name	M	NA	CN=unique identifier
Subject Public Key Information	M	NA	rsaEncryption, 2048 RSA Key modulus, public exponent or
Field	**Mandatory/ Optional**	**Critical/ Non critical**	**Note**
			ecPublicKey { 1.2.840.10045.2.1}, namedCurve, { 1.2.840.10045.3.1.7} (NIST curve P-256)
X.509 V3 extensions			
Authority Key Identifier	Mandatory	Non critical	SUBORDINATE CA Subject Key Identifier
Subject Key Identifier	Mandatory	Non critical	Octet String of unique value associated with the Public key
Key usage	Mandatory	Critical	digitalSignature, keyEncipherment,dataEncipherment
Certificate policies	Mandatory	Non critical	Policy OID , Policy Qualifier

Basic Constraints	Optional	Non critical	Subject Type=End Entity ,Path Length Constraint=None
Extended Key Usage	Optional	Non critical	serverAuth, clientAuth
CRL Distribution Points	Mandatory	Non critical	URL pointing to CRL Distribution
Authority Information Access	Mandatory	Non critical	OCSP locator URL, URL pointing to CA Issuer Certificate

Table 43.System Certificate

8.7. Code Signing Certificate

Field	Mandatory/ Optional	Critical/ Non critical	Note
Version	M	NA	The mandated value is 2. (i.e., The certificate must be in a version 3 format)
Serial Number	M	NA	Minimum 8 Bytes , Maximum 20 Bytes
Issuer Signature Algorithm	M	NA	SHA256 with RSA Encryption (null parameters) or ECDSA with SHA256 {1 2 840 10045 4 3 2}
Issuer Distinguished Name	M	NA	CN= Certificate Provider Name, O=Organization, OU=Organizational Unit, ST=Name of State, C=ET
Validity Period	M	NA	Generalized Time (2 Years)
Subject Distinguished Name	M	NA	CN= “Organization Name” or “FirstNameMiddleName LastName” ST=Name of State

			C=ET
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)
X.509 V3 extensions			
Authority Key Identifier	Mandatory	Non critical	SUBORDINATE CA Subject Key Identifier
Subject Key Identifier	Mandatory	Non critical	Subject Key Identifier
Key usage	Mandatory	Critical	digitalSignature
Certificate policies	Mandatory	Non critical	Policy OID , Policy Qualifier
Basic Constraints	Optional	Non critical	Subject Type=End Entity, Path Length Constraint=None
Extended Key Usage	Mandatory	Non critical	codeSigning
CRL Distribution Points	Mandatory	Non critical	URL pointing to CRL Distribution
Authority Information Access	Mandatory	Non critical	OCSP locator URL, URL pointing to CA Issuer Certificate

Table 44.Code signing Certificate

8.8. Organizational Document Signer Certificate

Field	Mandatory/ Optional	Critical/ Non critical	Note
Version	M	NA	The mandated value is 2. (i.e., The certificate must be in a version 3 format)
Serial Number	M	NA	Minimum 8 Bytes , Maximum 20 Bytes
Issuer Signature Algorithm	M	NA	SHA256 with RSA Encryption (null parameters) or ECDSA with SHA256 {1 2 840 10045 4 3 2}

Issuer Distinguished Name	M	NA	CN= Certificate Provider Name , O=Organization ,OU=Organizational Unit , ST=Name of State, C=ET
Validity Period	M	NA	Generalized Time (2 Years)
Subject Distinguished Name	M	NA	CN= Document Signer Name OU=Organization Unit Name O=Organization Name ST=Name of State C=ET
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)
X.509 V3 extensions			
Authority Key Identifier	Mandatory	Non critical	Issuing CA Subject Key Identifier
Subject Key Identifier	Mandatory	Non critical	Subject Key Identifier
Key usage	Mandatory	Critical	digitalSignature,nonRepudiation
Certificate policies	Mandatory	Non critical	Policy OID , Policy Qualifier
Basic Constraints	Optional	Non critical	Subject Type=End Entity,Path Length Constraint=None
Extended Key Usage	Optional	Non critical	MSFT Document Signer , Adobe Document Signer
CRL Distribution Points	Mandatory	Non critical	URL pointing to CRL Distribution
Authority Information	Mandatory	Non	OCSP locator URL, URL pointing to CA

Access		critical	Issuer Certificate

Table 45.Organizational Document Signer Certificate

8.9. End User Digital Signature Certificate (Personal Use)

Field	Mandatory/ Optional	Critical/ Non critical	Note
Version	M	NA	The mandated value is 2. (i.e., The certificate must be in a version 3 format)
Serial Number	M	NA	Minimum 8 Bytes , Maximum 20 Bytes
Issuer Signature Algorithm	M	NA	SHA256WithRSA
Issuer Distinguished Name	M	NA	CN= Certificate Provider Name, O=Organization Name, OU=Organizational Unit Name, ST=Name of State, C=ET
Validity Period	M	NA	Generalized Time (2 Years)
Subject Distinguished Name	M	NA	CN=FirstNameMiddleNameLastName, NID= [This attribute should be populated with the SHA256 hash of National ID], O=Personal, ST=Name of State, C=ET
Subject Public Key Information	M	NA	RSA 2048
X.509 V3 extensions			
Authority Key Identifier	Mandatory	Non critical	Issuing CA Subject Key Identifier
Subject Key Identifier	Mandatory	Non critical	Subject Key Identifier

Key usage	Mandatory	Critical	digitalSignature, nonrepudiation
Certificate policies	Mandatory	Non critical	Policy OID , Policy Qualifier
Subject Alternative Name	Optional	Non critical	E=username@domain.com
Basic Constraints	Optional	Non critical	Subject Type=End Entity Path Length Constraint=None
Extended Key Usage	Optional	Non critical	emailProtection
CRL Distribution Points	Mandatory	Non critical	URL pointing to CRL Distribution
Authority Information Access	Mandatory	Non critical	OCSP locator URL, URL pointing to CA Issuer Certificate

Table 46.End User Digital Signature Certificate (Personal Use)

8.10. End User Digital Signature Certificate (Organizational Use)

Field	Mandatory/ Optional	Critical/ Non critical	Note
Version	M	NA	The mandated value is 2. (i.e., The certificate must be in a version 3 format)
Serial Number	M	NA	Minimum 8 Bytes , Maximum 20 Bytes
Issuer Signature Algorithm	M	NA	SHA256WithRSA
Issuer Distinguished Name	M	NA	CN= Certificate Provider Name, O=Organization Name, OU=Organizational Unit Name, ST=Name of State, C=ET
Validity Period	M	NA	Generalized Time (2 Years)

Subject Distinguished Name	M	NA	CN=FirstNameMiddleNameLastName NID= [This attribute should be populated with the SHA256 hash of National ID] OID= [This attribute should be populated with the SHA256 hash of Organizational ID] O= Organization Name, O= Organizational Unit, ST=Name of State C=ET
Subject Public Key Information	M	NA	RSA 2048
X.509 V3 extensions			
Authority Key Identifier	Mandatory	Non critical	Issuing CA Subject Key Identifier
Subject Key Identifier	Mandatory	Non critical	Subject Key Identifier
Key usage	Mandatory	Critical	Keyencipherment ; dataencipherment
Certificate policies	Mandatory	Non critical	Policy OID , Policy Qualifier
Subject Alternative Name	Optional	Non critical	E=username@domain.com
Basic Constraints	Optional	Non critical	Subject Type=End Entity Path Length Constraint=None
Extended Key Usage	Optional	Non critical	emailProtection
CRL Distribution Points	Mandatory	Non critical	URL pointing to CRL Distribution
Authority Information Access	Mandatory	Non critical	OCSP locator URL, URL pointing to CA Issuer Certificate

Table 47.End User Digital Signature Certificate (Organizational Use)

8.11. End User Encryption Certificate (Personal Use)

Field	Mandatory/ Optional	Critical/ Non critical	Note
Version	M	NA	The mandated value is 2. (i.e., The certificate must be in a version 3 format)
Serial Number	M	NA	Minimum 8 Bytes , Maximum 20 Bytes
Issuer Signature Algorithm	M	NA	SHA256WithRSA
Issuer Distinguished Name	M	NA	CN= Certificate Provider Name, O=Organization, OU=Organizational Unit Name, ST=Name of State, C=ET
Validity Period	M	NA	Generalized Time (2 Years)
Subject Distinguished Name	M	NA	CN=FirstNameMiddleNameLastName, NID= [This attribute should be populated with the SHA256 hash of National ID], O=Personal, ST=Name of State, C=ET
Subject Public Key Information	M	NA	RSA 2048
X.509 V3 extensions			
Authority Key Identifier	Mandatory	Non critical	Issuing CA Subject Key Identifier
Subject Key Identifier	Mandatory	Non critical	Subject Key Identifier
Key usage	Mandatory	Critical	Keyencipherment ; dataencipherment
Certificate policies	Mandatory	Non critical	Policy OID , Policy Qualifier

Subject Alternative Name	Optional	Non critical	E=username@domain.com
Basic Constraints	Optional	Non critical	Subject Type=End Entity Path Length Constraint=None
Extended Key Usage	Optional	Non critical	emailProtection
CRL Distribution Points	Mandatory	Non critical	URL pointing to CRL Distribution
Authority Information Access	Mandatory	Non critical	OCSP locator URL, URL pointing to CA Issuer Certificate

Table 48.End User Encryption Certificate (Personal Use)

8.12. End User Encryption Certificate (Organizational Use)

Field	Mandatory/ Optional	Critical/ Non critical	Note
Version	M	NA	The mandated value is 2. (i.e., The certificate must be in a version 3 format)
Serial Number	M	NA	Minimum 8 Bytes , Maximum 20 Bytes
Issuer Signature Algorithm	M	NA	SHA256WithRSA
Issuer Distinguished Name	M	NA	CN= Certificate Provider Name , O=Organization Name ,OU=Organizational Unit Name, ST=Name of State, C=ET
Validity Period	M	NA	Generalized Time (2 Years)
Subject Distinguished Name	M	NA	CN=FirstNameMiddleNameLastName NID= [This attribute should be populated with the SHA256 hash of National ID] OID= [This attribute should be populated with the

			SHA256 hash of Organizational ID] O= Organization Name O= Organizational Unit Name ST=Name of State C=ET
Subject Public Key Information	M	NA	RSA 2048
X.509 V3 extensions			
Field	**Mandatory/ Optional**	**Critical/ Non critical**	**Note**
Authority Key Identifier	Mandatory	Non critical	Issuing CA Subject Key Identifier
Subject Key Identifier	Mandatory	Non critical	Subject Key Identifier
Key usage	Mandatory	Critical	digitalSignature, nonrepudiation
Certificate policies	Mandatory	Non critical	Policy OID , Policy Qualifier
Subject Alternative Name	Optional	Non critical	E=username@organization_domain.com
Basic Constraints	Optional	Non critical	Subject Type=End Entity Path Length Constraint=None
Extended Key Usage	Optional	Non critical	emailProtection
CRL Distribution Points	Mandatory	Non critical	URL pointing to CRL Distribution
Authority Information Access	Mandatory	Non critical	OCSP locator URL, URL pointing to CA Issuer Certificate

Table 49.End User Encryption Certificate (Organizational Use)

9. Reference CRL Profiles

9.1. Root CA CRL

Field	Critical/ Non critical	Note
Version		Version 2
Issuer Signature Algorithm		SHA256WithRSA
Issuer Distinguished Name		CN= National Root CA , O=INSA ,ST=Name of State, C=ET
thisUpdate		Generalized Time
nextUpdate		Generalized Time
Revoked certificates list		
CRL extensions		
CRL Number	Non critical	
Authority Key Identifier	Non critical	
Reason Code	Non critical	

Table 50.Root CA CRL

9.2. Subordinate CA CRL

Field	Critical/ Non critical	Note
Version		Version 2
Issuer Signature Algorithm		SHA256WithRSA
Issuer Distinguished Name		CN= Certificate Provider Name , O=Organization ,OU=Organizational Unit , ST=Name of State, C=ET
thisUpdate		Generalized Time
nextUpdate		Generalized Time
Revoked certificates list		
CRL extensions		

CRL Number	Non critical	
Authority Key Identifier	Non critical	
Reason Code	Non critical	

Table 51.Subordinate CA CRL

10. 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

10.1. Cryptography Algorithms

Supported Cryptographic Algorithms	
Asymmetric Algorithms	RSA , Diffie-Hellman , ECMQV, DSA, KCDSA, ECDSA, ECDH, Edwardes(x25519,Ed25519)
Symmetric Algorithms	AES, AES-GCM,Camellia,CAST,RIPEMD160 HMAC
Hash/Message digest	SHA-1,SHA-2(224,256,384,512 bit),HAS-160

Table 52.Cryptography Algorithms

10.2. Supported APIs

Supported APIs	
APIs	PKCS#11 , OpenSSL , Java(JCA/JCE) , Microsoft CAPI and CNG

Table 53.Supported APIs

10.3. Application Pre-requisites

1. As a prerequisite, the applications need to establish a trust anchor. The trust anchor for Ethiopian PKI would be National Root Certificate Authority of Ethiopia (INSA) 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 3 certificate or both Class 2 and Class 3 – depending upon the level of assurance required.
3. Applications should be able to determine the prospective certification path. Since Ethiopian PKI has limited number of CAs and with no cross certification, the CA certificates are easily obtainable manually. Applications also may download the issuer's 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 if applicable)

10.4. 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 National Root Certificate Authority (INSA)

   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

10.5. 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,

11. Application Owner Guidelines

These Guidelines are intended for Application Owners for planning implementation of Digital Certificate facility in their 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 Certificates which is suitable for them.

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

3 Application owners shall not impose the requirements of any additional Digital Certificate fields or private key storage requirements other than those mentioned in the Guidelines issued by National Root CA (INSA).

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

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