X.509v3, ITU-T Recommendation X.509 (2005) | ISO/IEC 9594-8:2005, Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks.

4. Definitions

Affiliate: A corporation, partnership, joint venture or other entity controlling, controlled by, or under common control with another entity, or an agency, department, political subdivision, or any entity operating under the direct control of a Government Entity.

Applicant: The natural person or Legal Entity that applies for (or seeks renewal of) a Certificate. Once the Certificate issues, the Applicant is referred to as the Subscriber. For Certificates issued to devices, the Applicant is the entity that controls or operates the device named in the Certificate, even if the device is sending the actual certificate request.

Applicant Representative: A natural person or human sponsor who is either the Applicant, employed by the Applicant, or an authorized agent who has express authority to represent the Applicant: (i) who signs and submits, or approves a certificate request on behalf of the Applicant, and/or (ii) who signs and submits a Subscriber Agreement on behalf of the Applicant, and/or (iii) who acknowledges and agrees to the Certificate Terms of Use on behalf of the Applicant when the Applicant is an Affiliate of the CA.

Application Software Supplier: A supplier of Internet browser software or other relying-party application software that displays or uses Certificates and incorporates Root Certificates.

Attestation Letter: A letter attesting that Subject Information is correct written by an accountant, lawyer, government official, or other reliable third party customarily relied upon for such information.

Audit Report: A report from a Qualified Auditor stating the Qualified Auditor’s opinion on whether an entity’s processes and controls comply with the mandatory provisions of these Requirements.

Certificate: An electronic document that uses a digital signature to bind a public key and an identity.

Certificate Data: Certificate requests and data related thereto (whether obtained from the Applicant or otherwise) in the CA’s possession or control or to which the CA has access.

Certificate Management Process: Processes, practices, and procedures associated with the use of keys, software, and hardware, by which the CA verifies Certificate Data, issues Certificates, maintains a Repository, and revokes Certificates.

Certificate Policy: A set of rules that indicates the applicability of a named Certificate to a particular community and/or PKI implementation with common security requirements.

Certificate Problem Report: Complaint of suspected Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, or inappropriate conduct related to Certificates.

Certificate Revocation List: A regularly updated time-stamped list of revoked Certificates that is created and digitally signed by the CA that issued the Certificates.

Certification Authority: An organization that is responsible for the creation, issuance, revocation, and management of Certificates. The term applies equally to both Roots CAs and Subordinate CAs.

Certification Practice Statement: One of several documents forming the governance framework in which Certificates are created, issued, managed, and used.

Country: Either a member of the United Nations OR a geographic region recognized as a sovereign nation by at least two UN member nations.

Cross Certificate: A certificate that is used to establish a trust relationship between two Root CAs.

Delegated Third Party: A natural person or Legal Entity that is not the CA but is authorized by the CA to assist in the Certificate Management Process by performing or fulfilling one or more of the CA requirements found herein.

Domain Authorization: Correspondence or other documentation provided by a Domain Name Registrant attesting to the authority of an Applicant to request a Certificate for a specific Domain Namespace.

9.2 Subject Information

By issuing the Certificate, the CA represents that it followed the procedure set forth in its Certificate Policy and/or Certification Practice Statement to verify that, as of the Certificate's issuance date, all of the Subject Information was accurate. CAs SHALL NOT include a Domain Name in a Subject attribute except as specified in Sections 9.2.1 and 9.2.2 below.

9.2.1 Subject Alternative Name Extension

Certificate Field: extensions:subjectAltName

Required/Optional: Required

Contents: This extension MUST contain at least one entry. Each entry MUST be either a dNSName containing the Fully-Qualified Domain Name or an iPAddress containing the IP address of a server. The CA MUST confirm that the Applicant controls the Fully-Qualified Domain Name or IP address or has been granted the right to use it by the Domain Name Registrant or IP address assignee, as appropriate.

Wildcard FQDNs are permitted.

As of the Effective Date of these Requirements, prior to the issuance of a Certificate with a subjectAlternativeName extension or Subject commonName field containing a Reserved IP Address or Internal Server Name, the CA SHALL notify the Applicant that the use of such Certificates has been deprecated by the CA / Browser Forum and that the practice will be eliminated by October 2016. Also as of the Effective Date, the CA SHALL NOT issue a certificate with an Expiry Date later than 1 November 2015 with a subjectAlternativeName extension or Subject commonName field containing a Reserved IP Address or Internal Server Name. Effective 1 October 2016, CAs SHALL revoke all unexpired Certificates whose subjectAlternativeName extension or Subject commonName field contains a Reserved IP Address or Internal Server Name.

9.2.2 Subject Common Name Field

Certificate Field: subject:commonName (OID 2.5.4.3)

Required/Optional: Deprecated (Discouraged, but not prohibited)

Contents: If present, this field MUST contain a single IP address or Fully-Qualified Domain Name that is one of the values contained in the Certificate's subjectAltName extension (see Section 9.2.1).

9.2.3 Subject Domain Component Field

Certificate Field: subject:domainComponent (OID 0.9.2342.19200300.100.1.25)

Required/Optional: Optional.

Contents: If present, this field MUST contain all components of the subject's Registered Domain Name in ordered sequence, with the most significant component, closest to the root of the namespace, written last.

9.2.4 Subject Distinguished ~~Organization~~ Name Fields

a. **Certificate Fields:** ~~Organization name:~~ subject:organizationName (OID 2.5.4.10)

Optional.

Contents: If present, the subject:organizationName field MUST contain either the Subject's name or DBA as verified under Section 11.2. The CA may include information in this field that differs slightly from the verified name, such as common variations or abbreviations, provided that the CA documents the difference and any abbreviations used are locally accepted abbreviations; e.g., if the official record shows "Company Name Incorporated", the CA MAY use "Company Name Inc." or "Company Name". Because Subject name attributes for individuals (e.g. givenName (2.5.4.42) and surname (2.5.4.4)) are not broadly supported by application software, the CA MAY use the subject:organizationName field to convey a natural person Subject's name or DBA.

b. **Certificate Field:** Number and street: subject:streetAddress (OID: 2.5.4.9)

Optional if the subject:organizationName field is present.

Prohibited if the subject:organizationName field is absent.

Contents: If present, the subject:streetAddress field MUST contain the Subject's street address information as verified under Section 11.2.

c. **Certificate Field**~~City or town~~: subject:localityName (OID: 2.5.4.7)

Required if the subject:organizationName field is present and the subject:stateOrProvinceName field is absent.

Optional if the subject:organizationName and subject:stateOrProvinceName fields are present.

Prohibited if the subject:organizationName field is absent.

Contents: If present, the subject:localityName field MUST contain the Subject's locality information as verified under Section 11.2. If the subject:countryName field specifies the ISO 3166-1 user-assigned code of XX in accordance with Section 9.2.5, the localityName field MAY contain the Subject's locality and/or state or province information as verified under Section 11.2.

d. **Certificate Field:** ~~State or province (where applicable):~~ subject:stateOrProvinceName (OID: 2.5.4.8):

Required if the subject:organizationName field is present and subject:localityName field is absent.

Optional if subject:organizationName and subject:localityName fields are present.

Prohibited if the subject:organizationName field is absent.

Contents: If present, the subject:stateOrProvinceName field MUST contain the Subject's state or province information as verified under Section 11.2. If the subject:countryName field specifies the ISO 3166-1 user-assigned code of XX in accordance with Section 9.2.5, the subject:stateOrProvinceName field MAY contain the full name of the Subject's country information as verified under Section 11.2.5.

~~Country: subject:countryName (OID: 2.5.4.6)~~

e. **Certificate Field:** ~~Postal/Zip code:~~ subject:postalCode (OID: 2.5.4.17)

Optional if the subject:organizationName field is present.

Prohibited if the subject:organizationName field is absent.

Contents: If present, the subject:postalCode field MUST contain the Subject's zip or postal information as verified under Section 11.2

~~**Required/Optional:** The organization name is OPTIONAL. If organization name is present, then localityName, stateOrProvinceName (where applicable), and countryName are REQUIRED and streetAddress and postalCode are OPTIONAL. If organization name is absent, then the Certificate MUST NOT contain a streetAddress, localityName, stateOrProvinceName, or postalCode attribute. The CA MAY include the Subject's countryName field without including other Subject Identity Information pursuant to Section 9.2.5.~~

~~**Contents:** If the organizationName field is present, the field MUST contain the Subject's name or DBA and the required address fields MUST contain a location of the Subject as verified by the CA pursuant to Section 11.2. If the Subject is a natural person, because Subject name attributes for individuals (e.g. givenName (2.5.4.42) and surname (2.5.4.4)) are not broadly supported by application software, the CA MAY use the organizationName field to convey the Subject's name or DBA.~~

~~If the fields include discrepancies that the CA considers minor, such as common variations and abbreviations, then the CA SHALL document the discrepancy and SHALL use locally accepted abbreviations when abbreviating the organization name, e.g., if the official record shows "Company Name Incorporated", the CA MAY include "Company Name, Inc."~~

~~The organizationName field may include a verified DBA or tradename of the Subject.~~

9.2.5 Subject Country Name Field

Certificate Field: subject:countryName (OID: 2.5.4.6)

~~**Required/Optional:** Optional~~

Required if the subject:organizationName field is present.

Optional if the subject:organizationName field is absent.

Contents: If the ~~subject:countryName field is present, then the CA SHALL verify the country associated with the Subject in accordance with Section 11.2.5 and use its two-letter ISO 3166-1 country code.~~ subject:organizationName field is present, the subject:countryName MUST contain the two-letter ISO 3166-1 country code associated with the location of the Subject verified under Section 11.2. If the subject:organizationName field is absent, the subject:countryName field MAY contain the two-letter ISO 3166-1 country code associated with the Subject as verified in accordance with Section 11.2.5. If a Country is not represented by an official ISO 3166-1 country code, the CA MAY specify the ISO 3166-1 user-assigned code of XX indicating that an official ISO 3166-1 alpha-2 code has not been assigned.

9.2.6 ~~Other~~ Subject Organizational Unit Field~~Attributes~~

~~With the exception of the subject:organizationalUnitName (OU) attribute, optional attributes, when present within the subject field, MUST contain information that has been verified by the CA. Metadata such as '.', '-', and ' ' (i.e. space) characters, and/or any other indication that the value is absent, incomplete, or not applicable, SHALL NOT be used.~~

Certificate Field: subject:organizationalUnitName

Optional.

~~CAs SHALL NOT include Fully-Qualified Domain Names in Subject attributes except as specified in Sections 9.2.1 and 9.2.2, above.~~

The CA SHALL implement a process that prevents an OU attribute from including a name, DBA, tradename, trademark, address, location, or other text that refers to a specific natural person or Legal Entity unless the CA has verified this information in accordance with Section 11.2 and the Certificate also contains subject:organizationName, subject:localityName, and subject:countryName attributes, also verified in accordance with Section 11.2.

9.2.7 Other Subject Attributes

All other optional attributes, when present within the subject field, MUST contain information that has been verified by the CA. Optional attributes MUST NOT contain metadata such as '.', '-', and ' ' (i.e. space) characters, and/or any other indication that the value is absent, incomplete, or not applicable.

9.3 Certificate Policy Identification

This section describes the content requirements for the Root CA, Subordinate CA, and Subscriber Certificates, as they relate to the identification of Certificate Policy.