CA/Browser Forum

Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates

Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates

Version 1.0, as adopted by the CA/Browser Forum on nn aaa nnnn.

These Baseline Requirements describe an integrated set of technologies, protocols, identity-proofing, lifecycle management, and auditing requirements that are necessary (but not sufficient) for the issuance and management of Publicly-Trusted Certificates; Certificates that are trusted by virtue of the fact that their corresponding Root Certificate is distributed in widely-available application software. The Requirements are not mandatory for Certification Authorities unless and until they become adopted and enforced by relying –party Application Software Suppliers.

Notice to Readers

This version of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates present criteria established by the CA/Browser Forum for use by Certification Authorities when issuing, maintaining, and revoking publicly-trusted Certificates. The Requirements may be revised from time to time, as appropriate, in accordance with procedures adopted by the CA/Browser Forum. Because one of the primary beneficiaries of these Requirements is the end user, the Forum openly invites anyone to make recommendations and suggestions by email to the CA/Browser Forum at questions@cabforum.org. The Forum members value all input, regardless of source, and will seriously consider all such input.

The CA/Browser Forum

The CA/Browser Forum is a voluntary organization of Certification Authorities and suppliers of Internet browser and other relying-party software applications. Membership as of aaa nnnn is as follows:

Certification Authorities

- A-Trust GmbH
- AC Camerfirma SA
- Buypass AS
- Certum
- Comodo CA Ltd
- D-TRUST GmbH
- DanID A/S
- DigiCert, Inc.
- DigiNotar
- Echoworx Corporation
- Entrust, Inc.
- GeoTrust, Inc.
- Getronics PinkRoccade
- GlobalSign
- GoDaddy.com, Inc.
- IdenTrust, Inc.
- ipsCA, IPS Certification Authority s.l.
- Izenpe S.A.
- Japan Certification Services, Inc.
- Kamu Sertifikasyon Merkezi
- Keynectis
- Network Solutions, LLC
- QuoVadis Ltd.
- RSA Security, Inc.
- SECOM Trust Systems CO., Ltd.
- Skaitmeninio sertifikavimo centras (SSC)
- StartCom Certification Authority
- SwissSign AG
- T-Systems Enterprise Services GmbH.
- TC TrustCenter GmbH
- Thawte, Inc.
- Trustis Limited
- Trustwave
- TWCA
- VeriSign, Inc.
- Verizon
- Wells Fargo Bank, N.A.

Relying-Party Application Software Suppliers

- Apple
- Google Inc.
- KDE
- Microsoft Corporation
- Opera Software ASA
- Research in Motion Limited
- The Mozilla Foundation

Other groups that have participated in the development of these Requirements include the WebTrust task force and ETSI ESI. Participation by such groups does not imply their endorsement, recommendation, or approval of the final product.

TABLE OF CONTENTS

1. Scope

The Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates describe a subset of the requirements that a Certification Authority must meet in order [031] ~~for~~ to issue ~~its Certificates to be~~ Publicly Trusted Certificates.

These Requirements do not address all of the issues relevant to the issuance and management of Publicly-Trusted Certificates. The CA/Browser Forum may update the Requirements from time to time, in order to address both existing and emerging threats to online security.

This version of the Requirements only addresses Certificates intended to be used for authenticating servers accessible through the Internet. Similar requirements for code signing, S/MIME, time-stamping, VoIP, IM, Web services, etc. may be covered in future versions.

These Requirements do not address the issuance, or management of Certificates by enterprises that operate their own Public Key Infrastructure for internal purposes only, and for which the Root Certificate is not distributed by any Application Software Supplier.

2. Purpose

The primary goal of these Requirements is to enable efficient and secure electronic communication, while addressing user concerns about the trustworthiness of Certificates. The Requirements also serve to inform users and help them to make informed decisions when relying on Certificates.

3. References

ETSI TS 102 042 V2.1.1, Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates.

FIPS 140-2, Federal Information Processing Standards Publication - Security Requirements For Cryptographic Modules, Information Technology Laboratory, National Institute of Standards and Technology, May 25, 2001.

ISO 21188:2006, Public key infrastructure for financial services -- Practices and policy framework.

RFC2119, Request for Comments: 2119, Key words for use in RFCs to Indicate Requirement Levels, Bradner, March 1997.

RFC2527, Request for Comments: 2527, Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework, Chokhani, et al, March 1999.

RFC2560, Request for Comments: 2560, X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP M. Myers et al, June 1999.

RFC3647, Request for Comments: 3647, Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework, Chokhani et al, November 2003.

RFC4366, Request for Comments: 4366, Transport Layer Security (TLS) Extensions, Blake-Wilson et al, April 2006.

RFC5019, Request for Comments: 5019, The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environments, A. Deacon at al, September 2007.

RFC5280, Request for Comments: 5280, Internet X.509 Public Key Infrastructure: Certificate and Certificate Revocation List (CRL) Profile, Cooper et al, May 2008.

WebTrust, WebTrust Program for Certification Authorities Version 1.0, AICPA/CICA, available at http://www.webtrust.org/homepage-documents/item27839.aspx

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[052], or an entity operating under the supervision of a Government Entity.

Applicant: The entity that applies for (or seeks renewal of) a Certificate.

Applicant Representative: A natural person 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.

Appropriate Independent Supervisory Government Auditing Agency: The auditing body for Government CAs that are legally required to use an internal audit scheme.

Attestation Letter: A letter attesting that Subject Information is correct.

[006]**Audit Criteria:** The requirements described in this document and any requirements that an entity must follow in order to satisfy the audit scheme selected under section 16.1

[006]**Audit Report:** A statement or report issued by a Qualified Auditor that clearly states the entity's compliance with the Audit Criteria.

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.

[055]**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.

[055]~~**Certification Process:** Keys, software, processes, and procedures by which the CA verifies Certificate Data, issues Certificates, maintains a Repository, and revokes Certificates.~~

[053]~~**Country:** A Sovereign State as defined by these Requirements~~.

Domain Authorization: Correspondence or other documentation provided by the Domain Name Registrant, as indicated by WHOIS or through the Domain Name Registrar, attesting to the authority of an Applicant to request a certificate with an FQDN located within the Domain Namespace for that Registered Domain Name.

Domain Name: The label assigned to a node in the Internet Domain Name System.

Domain Namespace: The logical branch under the node defined by a Domain Name within which subordinate Domain Names, subdomains, and FQDNs may be created, assigned, allocated, registered, or controlled.

Domain Name Registrant: Sometimes referred to as the "owner" of a Domain Name, but more properly the person or entity registered with a Domain Name Registrar as having the right to control how a Domain Name is used, and who is indicated as the "Registrant" by WHOIS or the Domain Name Registrar.

Domain Name Registrar: A person or entity that registers Domain Names under the auspices of or by agreement with: the Internet Corporation for Assigned Names and Numbers (ICANN), a national Domain Name authority/registry, or a Network Information Center (including their affiliates, contractors, delegates, successors, or assigns).

Enterprise Certificate: A Certificate whose issuance is authorized by an Enterprise RA.

Enterprise RA: An employee or agent of an organization unaffiliated with the CA who authorizes issuance of Certificates to that organization.

Fully-Qualified Domain Name: A Domain Name that includes the labels of all superior nodes in the Internet Domain Name System.

Issuing CA: In relation to a particular Certificate, the CA that issued the Certificate. This could be either a Root CA or a Subordinate CA.

[007]**Independent Audit:** An audit that is performed by a Qualified Auditor and that determines an entity's compliance with these Requirements and one or more of the audit schemes listed in Section 16.1.

Key Compromise: A Private Key is said to be compromised if it has been disclosed to an unauthorized person, an unauthorized person has had access to it, or there exists a practical technique by which an unauthorized person may discover its value.

Key Pair: The Private Key and its associated Public Key.

Object Identifier: A unique alphanumeric or numeric identifier registered under the International Organization for Standardization's applicable standard for a specific object or object class.

OCSP Responder: An online server operated under the authority of the CA and connected to its Repository for processing Certificate status requests. See also, Online Certificate Status Protocol.

Online Certificate Status Protocol: An online Certificate-checking protocol that enables relying-party application software to determine the status of an identified Certificate. See also OCSP Responder.

Private Key: The key of a Key Pair that is kept secret by the holder of the Key Pair, and that is used to create Digital Signatures and/or to decrypt electronic records or files that were encrypted with the corresponding Public Key.

Public Key: The key of a Key Pair that may be publicly disclosed by the holder of the corresponding Private Key and that is used by a Relying Party to verify Digital Signatures created with the holder's corresponding Private Key and/or to encrypt messages so that they can be decrypted only with the holder's corresponding Private Key.

Public Key Infrastructure: A set of hardware, software, people, procedures, rules, policies, and obligations used to facilitate the trustworthy creation, issuance, management, and use of Certificates and keys based on Public Key Cryptography.

Publicly-Trusted Certificate: A Certificate that is accepted by virtue of the fact that its corresponding Root Certificate is distributed as a trust anchor in widely-available application software.

[007]**Qualified Auditor:** The Qualified Independent Auditing Organization or, for government entities, the Appropriate Independent Supervisory Government Auditing Agency that meets the requirements of Section 16.4.

Qualified Independent Auditing Organization: An independent public accounting firm that meets the auditing qualification requirements specified in these Requirements.

Registered Domain Name: A Domain Name that has been registered with a Domain Name Registrar.

[008]**Registration Authority (RA):** Any entity that is responsible for identification and authentication of subjects of certificates, but is not a CA, and hence does not sign or issue certificates. An RA may assist in the certificate application process or revocation process or both. When "RA" is used as an adjective to describe a role or function, it does not necessarily imply a separate body, but can be part of the CA.

Relying Party: Any person (individual or entity) that relies on a Valid Certificate. An Application Software Supplier is not considered a Relying Party when software distributed by such Supplier merely displays information relating to a Certificate.

Repository: An online database of Certificate status information, either in the form of a CRL or an OCSP response.

Requirements: This document.

Reserved IP Address - An IP address that has been reserved for a special purpose by one of RFC 1918, 3330, 3513, 3927, 4193, 4291, or 5735.

Root CA: The top level Certification Authority whose Root Certificate is distributed by Application Software Suppliers and that issues Subordinate CA Certificates.

Root Certificate: The self-signed Certificate issued by the Root CA to identify itself and to facilitate verification of Certificates issued to its Subordinate CAs.

Root Key Generation Script: A documented plan of procedures for the generation of the Root CA Key Pair**.**

[053]~~**Sovereign State:** A state, or country, that administers its own government, and is not dependent upon, or subject to, another power.~~

Subject: The entity identified by a Certificate.

Subject Identity Information: Information that identifies the Certificate Subject.

Subordinate CA: A Certification Authority whose Certificate is signed by the Root CA, or another Subordinate CA.

Subscriber: An entity (organization, individual, etc.) that is legally bound by a Subscriber Agreement.

Subscriber Agreement: An agreement between the CA and the Applicant that specifies the rights and responsibilities of the parties.

Terms of Use: Provisions regarding the safekeeping and acceptable uses of a Certificate issued in accordance with these Requirements when the Applicant is an Affiliate of the CA.

Trustworthy System: Computer hardware, software, and procedures that are: reasonably secure from intrusion and misuse; provide a reasonable level of availability, reliability, and correct operation; are reasonably suited to performing their intended functions; and enforce the applicable security policy.

Valid Certificate: A Certificate that has not expired and has not been revoked.

Validation Specialists: Personnel performing the information verification duties specified by these Requirements.

WebTrust Program for CAs: The then-current version of the AICPA/CICA WebTrust Program for Certification Authorities.

WebTrust Seal of Assurance: An affirmation of compliance resulting from the WebTrust Program for CAs.

Wildcard Certificate: A Certificate containing an asterisk (*) in the left-most position of any of the Subject Fully-Qualified Domain Names contained in the Certificate.

5. Abbreviations and Acronyms

AICPA	American Institute of Certified Public Accountants
CA	Certification Authority
ccTLD	Country Code Top-Level Domain
CICA	Canadian Institute of Chartered Accountants
CP	Certificate Policy
CPA	Chartered Professional Accountant
CPS	Certification Practice Statement

CRL	Certificate Revocation List
DBA	Doing Business As
DNS	Domain Name System
FIPS	(US Government) Federal Information Processing Standard
FQDN	Fully Qualified Domain Name
IM	Instant Messaging
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
ISO	International Organization for Standardization
NIST	(US Government) National Institute of Standards and Technology
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PKI	Public Key Infrastructure
RA	Registration Authority
S/MIME	Secure MIME (Multipurpose Internet Mail Extensions)
SSL	Secure Sockets Layer
TLD	Top-Level Domain
TLS	Transport Layer Security
VOIP	Voice Over Internet Protocol

6. Conventions

Terms not otherwise defined in these Requirements shall be as defined in applicable agreements, user manuals, Certificate Policies and Certification Practice Statements, of the CA.

The key words "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in these Requirements shall be interpreted in accordance with RFC 2119.

7. Certificate Warranties and Representations

7.1 By the CA

By issuing a Certificate, the CA makes the Certificate Warranties listed below to the Certificate Beneficiaries listed below.

7.1.1 Certificate Beneficiaries

Certificate Beneficiaries include, but are not limited to, the following:

1. The Subscriber party to the Subscriber Agreement for the Certificate;
2. All Application Software Suppliers with whom the Root CA has entered into a contract for inclusion of its Root Certificate in software distributed by such Application Software Supplier; and
3. All Relying Parties who reasonably rely on the Certificate when it is a Valid Certificate.

7.1.2 Certificate Warranties

The CA represents and warrants to the Certificate Beneficiaries that, during the period when the Certificate is valid, the CA has complied with these Requirements and its Certificate Policy [010] and/or ~~and~~ Certification Practice Statement in issuing and managing the Certificate.

The Certificate Warranties specifically include, but are not limited to, the following:

1. **Right to Use Domain Name or IP Address:** That, at the time of issuance, the CA: operated an effective procedure for verifying that the Applicant either had the right to use, or had control of, the Domain Name(s) and IP address(es) listed in the Certificate's subject field and subjectAltName extension, or (in the case of Domain Names) had been delegated such right or control by someone who had; the effective procedure was followed; and the same effective procedure was accurately described in the CA's Certificate Policy [010] and/or Certification Practice Statement;
2. **Authorization for Certificate:** That, at the time of issuance, the CA: operated an effective procedure for verifying that the Applicant authorized the issuance of the Certificate; the effective procedure was followed; and the same effective procedure was accurately described in the CA's Certificate Policy [010] and/or ~~and~~ Certification Practice Statement;
3. **Accuracy of Information:** That, at the time of issuance, the CA: operated an effective procedure for verifying that all of the information contained in the Certificate (with the exception of the subject:organizationalUnitName attribute) was true and accurate; the effective procedure was followed; and the same effective procedure was accurately described in the CA's Certificate Policy [010] and/or Certification Practice Statement;
4. **No Misleading Information:** That, at the time of issuance, the CA: operated an effective procedure for verifying that none of the information contained in the Certificate's subject:organizationalUnitName attribute was misleading; the effective procedure was followed; and the same effective procedure was accurately described in the CA's Certificate Policy [010] and/or ~~and~~ Certification Practice Statement;
5. **Identity of Applicant:** That, if the Certificate contains Subject Identity Information, the CA: operated an effective procedure for verifying the identity of the Applicant and the Applicant Representative; the effective procedure was followed; and the same effective procedure was accurately described in the CA's Certificate Policy [010] and/or ~~and~~ Certification Practice Statement;
6. **Subscriber Agreement:** That the Subscriber is party to a legally valid and enforceable Subscriber Agreement with the CA that satisfies these Requirements;
7. **Status:** That the CA will maintain a 24 x 7 online-accessible Repository with current information regarding the status of all unexpired Certificates as valid or revoked; and
8. **Revocation:** That the CA will revoke the Certificate for any of the reasons specified in these Requirements.

7.2 By the Applicant

The CA SHALL require, as part of the Subscriber Agreement, that the Applicant make the commitments and warranties set forth in Section 10.3.2 of these Requirements, for the benefit of the CA and the Certificate Beneficiaries.

8. Community and Applicability

8.1 Compliance

The CA MUST at all times:

1. Comply with all law applicable to its business and the Certificates it issues in each jurisdiction where it operates;
2. Comply with these Requirements;

3. Comply with the audit requirements set forth in Section 16; and

4. Be licensed as a CA in each jurisdiction where it operates, if licensing is required by the law of such jurisdiction for the issuance of Certificates.

8.2 Certificate Policies

8.2.1 Implementation

The CA MUST develop, implement, enforce, display prominently on its Web site, and periodically update as necessary its policies and practices, including its Certificate Policy [010] and/or ~~and~~ Certification Practice Statement, that implement these Requirements as they may be revised from time-to-time.

8.2.2 Disclosure

The CA MUST publicly disclose its policies and practices through an appropriate and readily accessible online means that is available on a 24x7 basis. The CA is also REQUIRED to publicly disclose its CA business practices such as are required to be publicly disclosed by the audit scheme (see Section 16.1). The disclosures MUST include all the material required by RFC 2527 and RFC 3647, and MUST be structured in accordance with either RFC 2527 or RFC 3647.

8.3 Commitment to Comply

The CA MUST publicly give effect to these Requirements and represent that it will adhere to the latest published version by incorporating them directly into its Certification Practice Statements, or by reference using a clause such as the following (which MUST include a link to the official version of these Requirements):

> [Name of CA] conforms to the current version of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates published at http://www.cabforum.org. In the event of any inconsistency between this document and those Requirements, those Requirements take precedence over this document.

8.4 Trust model

The CA MUST disclose the identities of all issuers of Certificates that identify the CA as the Subject.

9. Certificate Content and Profile

9.1 Issuer Information

For Root CA, Subordinate CA and Subscriber Certificates created after the adoption of these Requirements, the Issuing CA MUST populate the issuer field in accordance with the following subsections.

9.1.1 Issuer Common Name Field

Certificate Field: issuer:commonName (OID 2.5.4.3)

Required/Optional: Required

Contents: This field MUST contain a meaningful name to identify the Certificate issuer.

9.1.2 Issuer Organization Name Field

Certificate Field: issuer:organizationName (OID 2.5.4.10)

Required/Optional: Required

Contents: This field MUST contain the issuer's full legal organization name as listed in the official records of its Incorporating or Registration Agency [012] at the time when the Certificate is created. Prefixes or suffixes in the organization name MAY be abbreviated, e.g., if the official record shows "Company Name, Incorporated" the CA MAY use "Company Name, Inc."

When abbreviating a full legal name as allowed by this subsection, the CA MUST use abbreviations that are not misleading in its Jurisdiction of Incorporation or Registration.

In addition, an assumed name or DBA name used by the issuer MAY be included at the beginning of this field, provided that it is followed by the full legal organization name in parenthesis.

If the combination of names or the organization name by itself exceeds 64 characters, the CA MAY abbreviate parts of the organization name, and/or omit non-material words in the organization name in such a way that the text in this field does not exceed the 64-character limit; provided that a Relying Party will not be misled into thinking that they are dealing with a different organization. In cases where this is not possible, the CA MUST NOT issue the Certificate.

9.1.3 Issuer Country Name Field

Certificate Field: issuer:countryName (OID 2.5.4.6)

Required/Optional: Required

Contents: This field MUST contain the two-letter ISO country code for the country in which the issuer's place of business is located.

9.2 Subject Information

By issuing the Certificate, the CA represents that it has taken the steps set forth in its Certification Practice Statement to verify that all of the Subject information is accurate, as of the date the Certificate was issued.

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 server MUST either be owned and operated by, or for the benefit of, the Applicant or by a related entity (e.g., a hosting service). The Applicant MUST control the Fully-Qualified Domain Name or IP address or have been granted the right to use it by the Domain Name Registrant or IP address assignee, as appropriate.

Wildcard FQDNs are permitted.

Effective 1 June 2012, no CA SHALL issue a certificate with a validity date beyond 1 June 2015 that contains a Reserved IP Address or Domain Name that is not resolvable through the public DNS. On 1 June 2015, CAs MUST revoke any unexpired certificate that includes a Reserved IP Address or Domain Name not resolvable through the public DNS.

9.2.2 Subject Common Name Field

Certificate Field: subject:commonName (OID 2.5.4.3)

Required/Optional: Deprecated

Contents: If present, this field MUST contain a single 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 Organization Name Field

Certificate fields:

Organization name: organizationName (OID 2.5.4.10)

Number and street: subject:streetAddress (OID: 2.5.4.9)

City or town: subject:localityName (OID: 2.5.4.7)

State or province (where applicable): subject:stateOrProvinceName (OID: 2.5.4.8)

Country: subject:countryName (OID: 2.5.4.6)

Postal code: subject:postalCode (OID: 2.5.4.17)

Required/Optional: Organization name is OPTIONAL. If organization name is present, then city, state (where applicable), and country are REQUIRED and street and postal code are OPTIONAL. If organization name is absent, then the other attributes MUST also be absent.

Contents: If present, the organizationName field MUST contain the identified Subject's name or DBA and the other required fields MUST contain the verified information of the Subject's location. The CA MAY abbreviate the organization prefixes or suffixes in the organization name, e.g., if the official record shows "Company Name Incorporated", the CA MAY include "Company Name, Inc." The CA MUST use generally accepted abbreviations. The CA MAY use a tradename or DBA name provided that:

1. The DBA or tradename is verified by the CA as belonging to the Subject; and
2. use of the DBA or tradename will not mislead a Relying Party into thinking that they are dealing with a different organization.

If the Subject is a natural person, the CA MAY use the organizationName field to convey the Subject's name or DBA until such time that the Subject name attributes for Individuals (e.g. givenName (2.5.4.42) and surname (2.5.4.4)) become broadly supported in application software.

9.2.4 Other Subject Attributes

With the exception of the subject:organizationalUnitName attribute, optional attributes within the subject field MUST contain information that has been verified by the CA. Otherwise, optional attributes MUST be omitted. 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.

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

The CA SHALL NOT include misleading information in the subject:organizationalUnitName attribute. Information SHALL be considered misleading if it contains any of the following:

1. Any Subscriber name and/or address information, including DBA or tradename information (unless the Certificate also contains verified subject:organizationName, subject:localityName (OID: 2.5.4.7), and subject:countryName attributes),
2. A well-known trademark that is not commonly associated with the Subscriber,
3. Any information that the CA knows, or has reason to believe, is associated with an entity other than the Subscriber or the Subscriber's Parent/Subsidiary/Affiliate, or
4. Any information that the CA knows or reasonably believes contains inaccuracies.

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.

9.3.1 Root CA Certificates

A Root CA Certificate SHOULD NOT contain the certificatePolicies extension.

9.3.2 Subordinate CA Certificates

A Certificate issued to a Subordinate CA that is not an Affiliate of the Issuing CA MUST contain one or more explicit policy identifier(s) defined by the Issuing CA that indicates adherence to and compliance with these Requirements. The Issuing CA MUST document in its Certificate Policy or Certification Practice Statement that the Certificates it issues containing the specified policy identifier(s) are managed in accordance with these Requirements. The Certificate MUST NOT contain the "anyPolicy" identifier (2.5.29.32.0).

A Certificate issued to a Subordinate CA that is an Affiliate of the Root CA MAY contain the special "anyPolicy" identifier (2.5.29.32.0) in place of an explicit policy identifier.

9.3.3 Subscriber Certificates

A Certificate issued to a Subscriber MUST contain one or more policy identifier(s), defined by the Issuing CA, in the Certificate's certificatePolicies extension that indicates adherence to and compliance with these Requirements. The issuing CA MUST document in its Certificate Policy or Certification Practice Statement that the Certificates it issues containing the specified policy identifier(s) are managed in accordance with these Requirements.

9.4 Validity Period

The validity period of a Subscriber Certificate MUST NOT exceed sixty months. The Issuing CA MUST comply with the requirements of Section 11.3, and the Certificates it issues MUST conform to the requirements of Appendix A, throughout their validity period.

9.5 Subject Public Key

The CA SHALL take all practical steps to ensure that the requested Public Key is not a known weak key (such as a Debian weak key, see http://wiki.debian.org/SSLkeys). The CA SHALL reject all such requests.

9.6 Certificate Serial Number

It is RECOMMENDED that the CA implement an unpredictable scheme that exhibits at least 20 bits of entropy for assigning Certificate serial numbers.

9.7 Additional Technical Requirements

See Appendix A - Cryptographic Algorithm and Key Requirements~~Appendix A – Cryptographic Algorithm and Key Requirements~~, and Appendix B – Certificate Extensions~~Appendix B – Certificate Extensions~~, and Appendix C – User Agent Verification.

10. Certificate Application

10.1 Documentation Requirements

Prior to the issuance of a Certificate, the CA MUST obtain from the Applicant the following documentation:

1. A Certificate Request, which may be electronic;
2. A Subscriber Agreement, which may be electronic; and
3. Such additional documentation as the CA requires from the Applicant to satisfy its obligations under these Requirements.

10.2 Certificate Request

10.2.1 General

Prior to the issuance of a Certificate, the CA MUST obtain from the Applicant a Certificate Request in a form prescribed by the CA and that complies with these Requirements. One Certificate Request MAY suffice for multiple Certificates to be issued to the same Applicant, subject to the aging and updating requirement in Section 11.3, provided that each Certificate is supported by a valid, current Certificate Request signed by the appropriate Applicant Representative on behalf of the Applicant. The Certificate Request MAY be made, submitted and/or signed electronically.

10.2.2 Request and Certification

The Certificate Request MUST contain a request from, or on behalf of, the Applicant for the issuance of a Certificate, and a certification by, or on behalf of, the Applicant that all of the information contained therein is correct.

10.2.3 Information Requirements

The Certificate Request MAY include all factual information about the Applicant to be included in the Certificate, and such additional information as is necessary for the CA to obtain from the Applicant in order to comply with these Requirements and the CA's Certificate Policy [010] and/or ~~and~~ Certification Practice Statement. In cases where the Certificate Request does not contain all the necessary information about the Applicant, the CA MUST obtain the remaining information from the Applicant or, having obtained it from a reliable, independent, third-party data source, confirm it with the Applicant.

Applicant information SHALL include, but not be limited to, the Fully-Qualified Domain Name(s) and/or IP addresses to be included in the Certificate SubjectAltName extension.

10.2.4 Subscriber Private Key

The CA and its RAs SHALL NOT archive the Subscriber Private Key.

If the CA, or any of its designated RAs were to generate a Private Key on behalf of the Subscriber, then the CA MUST encrypt the Private Key for transport to the Subscriber.

If the CA, or any of its designated RAs were to become aware that a Subscriber's Private Key had been communicated to any person or organization not affiliated with the Subscriber, then the CA MUST revoke any certificates that include the Public Key corresponding to the Private Key that has been communicated.

10.3 Subscriber Agreement

10.3.1 General

Prior to the issuance of a Certificate, the CA MUST obtain the Applicant's agreement to a Subscriber Agreement with the CA for the express benefit of the CA and the Certificate Beneficiaries. The Subscriber Agreement MUST be legally enforceable against the Applicant. The CA MAY use an electronic or "click-through" Subscriber Agreement provided that the CA has determined that such agreements are legally enforceable. A separate Subscriber Agreement MAY be used for each Certificate Request, or a single Subscriber Agreement MAY be used to cover multiple future Certificate Requests and the resulting Certificates, provided that each Certificate is clearly covered by a valid Subscriber Agreement.

10.3.2 Agreement Requirements

The Subscriber Agreement MUST contain provisions imposing on the Applicant itself (or made by the Applicant on behalf of its principal or agent under a subcontractor or hosting service relationship) the following obligations and warranties:

1. **Accuracy of Information:** An obligation and warranty to provide accurate and complete information at all times to the CA, both in the Certificate Request and as otherwise requested by the CA in connection with the issuance of the Certificate(s) to be supplied by the CA;
2. **Protection of Private Key:** An obligation and warranty by the Applicant to take all reasonable measures to maintain sole control of, keep confidential, and properly protect at all times the Private Key that corresponds to the Public Key to be included in the requested Certificate(s) (and any associated activation data or device, e.g. password or token);
3. **Acceptance of Certificate:** An obligation and warranty that the Certificate will not be used until the Certificate has been reviewed and verified for accuracy;

4. **Use of Certificate:** An obligation and warranty to install the Certificate only on servers that are accessible at the subjectAltName(s) listed in the Certificate, and to use the Certificate solely in compliance with all applicable laws and solely in accordance with the Subscriber Agreement;

5. **Reporting and Revocation:** An obligation and warranty to promptly cease using a Certificate and its associated Private Key, and promptly request the CA to revoke the Certificate, in the event that: (a) any information in the Certificate is, or becomes, incorrect or inaccurate, or (b) there is any actual or suspected misuse or compromise of the Subscriber's Private Key associated with the Public Key included in the Certificate;

6. **Termination of Use of Certificate:** An obligation and warranty to promptly cease all use of the Private Key corresponding to the Public Key included in the Certificate upon revocation of that Certificate for reasons of Key Compromise.

7. **Responsiveness:** An obligation to respond to the CA's instructions concerning Key Compromise or Certificate misuse within a specified time period.

8. **Acknowledgment and Acceptance:** An acknowledgment and acceptance that the CA is entitled to revoke the certificate immediately if the Applicant were to violate the terms of the Subscriber Agreement or if the CA discovers that the certificate is being used to enable criminal activities such as phishing attacks, fraud, or the distribution of malware.

11. Verification Practices

11.1 Authorization by Domain Name Registrant

The CA [050]or RA MUST confirm that, as of the date the Certificate was issued, the Applicant either had the right to use, or had control of, the Fully-Qualified Domain Name(s) and/or IP address(es) listed in the Certificate, or was authorized by a person having such right or control (e.g. under a Principal-Agent or Licensor-Licensee relationship) to obtain a Certificate containing the Fully-Qualified Domain Name(s) and/or IP address(es).

If the CA [050]or RA relies on a confirmation of the right to use or control the Registered Domain Name(s) from a Domain Name Registrar, and the top-level Domain is a two-letter country code (ccTLD), the CA [050]or RA MUST obtain the confirmation directly from the Domain Name Registrar for the Domain Name level specified by the rules of ~~-~~the ccTLD. For example, if the requested FQDN is www.mysite.users.example.co.uk, then the CA [050]or RA must obtain confirmation from the Domain Name Registrant of the Domain Name example.co.uk.

If the CA [050]or RA uses the Internet mail system to confirm that the Applicant has authorization from the Domain Name Registrant to obtain a Certificate for the requested Fully-Qualified Domain Name, the CA [050]or RA MUST use a mail system address formed in one of the following ways:

1. Supplied by the Domain Name Registrar;

2. Taken from the Domain Name Registrant's "registrant", "technical", or "administrative" contact information, as it appears in the Domain's WHOIS record; or;

3. By prepending a local part to a Domain Name as follows:

    a. Local part - One of the following: 'admin', 'administrator', 'webmaster', 'hostmaster', or 'postmaster'; and

    b. Domain Name – Formed by pruning zero or more components from the Registered Domain Name or the requested Fully-Qualified Domain Name.

If the Domain Name Registrant has used a private, anonymous, or proxy registration service, and the CA [050]or RA relies upon a Domain Authorization as an alternative to the foregoing, the Domain Authorization MUST be received directly from the private, anonymous, or proxy registration service identified in the WHOIS record for the Registered Domain Name. The document MUST contain the letterhead of the private, anonymous, or proxy registration service, the signature of the General Manager, or equivalent, or an authorized representative of such officer, dated on or after the Certificate Request date, and the Fully-Qualified Domain Name(s) to be included in the Certificate. If the WHOIS record identifies the private, anonymous, or proxy registration service as the Domain

Name Registrant, then the Domain Authorization MUST contain a statement granting the Applicant the right to use the Fully-Qualified Domain Name in a Certificate. The CA [050]or RA MUST contact the private, anonymous, or proxy registration service directly, using contact information obtained from a reliable, independent, third-party data source, and obtain confirmation from the Domain Name Registrant that the Domain Authorization is authentic.

11.2 Verification of Subject Identity Information

If the Applicant requests a Certificate that will contain Subject Identity Information, the CA [050]or RA MUST verify the identity of the Applicant and Applicant's relationship to the Applicant Representative using a verification process meeting the requirements of this Section 11.2, and that is described in the CA's Certificate Policy and/or Certification Practice Statement.

11.2.1 Identity

If the [001] Subject Identity Information is to include the name or address of an ~~Applicant is an~~ organization, the CA or RA MUST verify the identity and address of the Applicant using documentation provided by, or through communication with, at least one of the following:

1. A government agency in the jurisdiction of the Applicant's legal creation, existence, or recognition;
2. A reliable third party database that is periodically updated; or
3. An Attestation Letter that the CA or RA has confirmed was written by an accountant, lawyer, government official, or other reliable third party customarily relied upon for such information.

The CA MAY exercise professional judgment in accepting minor discrepancies, such as common variations and abbreviations.

11.2.2 Verification of a DBA/Tradename

If the Subject Identity Information is to include a DBA or tradename, the CA or RA MUST verify the Applicant's right to use the DBA/tradename using at least one of the following:

1. Documentation or communication provided by a reliable third party source;
2. Communication with a government agency responsible for the management of such DBAs or tradenames; or
3. An Attestation Letter accompanied by reliable documentary support. The CA or RA MUST confirm that the Attestation Letter was written by an accountant, lawyer, government official, or another reliable third party that is customarily relied upon for such information.

11.2.3 Authenticity of Certificate Request

If the Applicant for a Certificate containing Subject Identity Information is an organization, the CA or RA MUST use a reliable means of communication to verify that the request from the Applicant Representative was the authentic request of the Applicant.

The CA or RA MUST communicate reliably with the Applicant or Applicant Representative using means established by reference to a reliable third party source (i.e. a source other than solely the Applicant Representative). The same sources listed in section 11.2.1 MAY be used to identify the Applicant Representative and contact information for the Applicant or Applicant Representative. Contact information includes a postal/courier delivery address, telephone number, or email address for the Applicant's main business office, corporate office, human resource office, information technology office, or other appropriate department obtained from a reliable third party source.

If communication with an authoritative source within the Applicant's organization is necessary to establish or verify the Applicant Representative's information, then the CA or RA MUST communicate with the authoritative source using means that reasonably ensure:

1. The identity of the authoritative source; and
2. Reliable communication with the authoritative source.

The identity of the source MAY be established by telephone, postal mail/courier, facsimile, email, or other authenticated communication with the Applicant's main business offices, corporate offices, human resource offices, information technology offices, or other appropriate department. Contact information provided by the Applicant is not considered a means of establishing reliable communication unless the CA or RA first verifies the contact information with a third party source. The authoritative source within an organization may be the same individual as the Applicant Representative, provided that identity, contact information, and reliable communication have been established as described above.

In addition, the CA or RA MUST establish a process that allows an Applicant to limit the number or identity of individuals who may request Certificates. If an Applicant specifies, in writing, the number or identity of individuals who may request a Certificate, then the CA or RA MUST NOT accept any Certificate Requests that are outside this specification. The CA or RA MUST provide the Applicant with a list of its authorized Certificate Requesters upon the Applicant's verified written request.

11.2.4 Verification of Individual Applicant

If an Applicant subject to this Section 11.2 is an Individual, then the CA or RA MUST verify the Applicant's name, address, and telephone number.

1. The CA or RA MUST verify the Applicant's name using a legible copy, which discernibly shows the Applicant's face, of at least one currently valid government-issued photo ID (passport, drivers license, military ID, national ID, or equivalent document type). The CA or RA MUST inspect the copy for any indication of alteration or falsification.
2. The CA or RA MUST verify the Applicant's address using a reliable form of identification, such as a government ID, utility bill, or bank or credit card statement. The CA or RA MAY rely on the same government-issued ID that was used to verify the Applicant's name.
3. The CA or RA MUST verify the Applicant's telephone number using either a reliable third party source or a telephone bill. The CA [050]or RA must use the verified telephone number to verify the Applicant's certificate request.

11.3 Age of Certificate Data

Section 9.4 limits the validity period of Subscriber Certificates. If, at any time during the validity period of a Subscriber Certificate, more than thirty-nine months elapses since the CA [050]or RA verified any part of its Certificate Data, then the CA MUST revoke the Certificate.

11.4 Denied List

In accordance with Section 14.3.2, the CA MUST maintain an internal database of all previously revoked Certificates and previously rejected Certificate Requests due to suspected phishing or other fraudulent usage or concerns. This information SHOULD be used to identify subsequent suspicious Certificate Requests.

11.5 High Risk Status

The CA [050]or RA MUST endeavor to identify High Risk Certificate Requests, and conduct such additional verification activity, and take such additional precautions, as are reasonably necessary to ensure that such requests are properly verified under these Requirements.

The CA [050]or RA MAY identify High Risk Requests by checking appropriate lists of organization names that are most commonly targeted in phishing and other fraudulent schemes, and by automatically flagging Certificate Requests that match these lists for further scrutiny before issuance. Examples of such lists include:

~~1. Lists of phishing targets published by the Anti-Phishing Work Group (APWG); and~~ [054]

~~2.~~1. Internal databases maintained by the CA [050]or RA that include previously revoked Certificates and previously rejected Certificate Requests due to suspected phishing or other fraudulent usage. The information MUST then be used to flag suspicious Certificate Requests. If a Request is flagged as a High Risk Request, the CA [050]or RA MUST perform reasonably appropriate additional authentication and verification.

12. Certificate Status Checking and Revocation

12.1 Certificate Status Checking

12.1.1 Repository

The CA MUST maintain an online 24x7 Repository, using which, application software can automatically check the current status of all unexpired Certificates issued by the CA.

For the status of Subscriber Certificates, or Subordinate CA Certificates issued to entities that are not Affiliates of the Issuing CA:

1. In the case of revocation information provided in the form of a CRL, the CA MUST update and reissue the CRL at least once every seven days, and the value of the nextUpdate field SHALL NOT be more than ten days beyond the value of the thisUpdate field; or
2. In the case of revocation information provided via the Online Certificate Status Protocol, the CA MUST update the service at least every four days. OCSP responses from this service MUST have a maximum expiration time of ten days.

For the status of Subordinate CA Certificates issued to entities that are Affiliates of the Issuing CA:

1. In the case of revocation information provided in the form of a CRL, the CA MUST update and reissue the CRL at least once every twelve months, and the value of the nextUpdate field SHALL NOT be more than twelve months beyond the value of the thisUpdate field; or
2. In the case of revocation information provided via the Online Certificate Status Protocol, the CA MUST update the service at least every twelve months. OCSP responses from this service MUST have a maximum expiration time of twelve months.

The CA MUST support an OCSP capability using the GET method for Certificates issued after these Requirements have been adopted.

12.1.2 Response Time

The CA MUST operate and maintain its CRL and/or OCSP capability with resources sufficient to provide a commercially reasonable response time for the number of queries generated by all of the Certificates issued by the CA.

12.1.3 Deletion of Entries

Revocation entries on a CRL or OCSP MUST NOT be removed until after the expiration date of the revoked Certificate.

12.1.4 OCSP Signing

OCSP responses MUST conform to RFC2560 and/or RFC5019. OCSP responses MUST either:

1. Be signed by the CA that issued the Certificates whose revocation status is being checked, or
2. Be signed by an OCSP Responder whose Certificate is signed by the CA that issued the Certificate whose revocation status is being checked.

In the latter case, the OCSP signing Certificate MUST contain an extension of type id-pkix-ocsp-nocheck, as defined by RFC2560.

12.1.5 Root CA CRL

Certificates issued by a Root CA MUST include the CrlDistributionPoints extension. The URL contained in the CDP extension MUST be publicly accessible.

12.2 Revocation

12.2.1 Revocation Request

The CA MUST provide a process for Subscribers to request revocation of their own Certificates. The process MUST be described in the CA's Certificate Policy or Certification Practice Statement. The CA MUST maintain a continuous 24x7 ability to accept and respond to revocation requests and related inquiries.

12.2.2 Certificate Problem Reporting

The CA MUST provide Subscribers, Relying Parties, Application Software Suppliers, and other third parties with clear instructions for reporting suspected Private Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, inappropriate conduct, or any other matter related to Certificates. The CA MUST publicly disclose the instructions through a readily accessible online means.

12.2.3 Investigation

The CA MUST begin investigation of a Certificate Problem Report within twenty-four hours of receipt, and decide whether revocation or other appropriate action is warranted based on at least the following criteria:

1. The nature of the alleged problem;
2. The number of Certificate Problem Reports received about a particular Certificate or Subscriber;
3. The type of the complainants (for example, a complaint from a law enforcement official that a Web site is engaged in illegal activities should carry more weight than a complaint from a consumer alleging that she didn't receive the goods she ordered); and
4. Relevant legislation.

12.2.4 Response

The CA MUST maintain a continuous 24x7 ability to respond internally to a high-priority Certificate Problem Report, and where appropriate, forward such a complaint to law enforcement authorities, and/or revoke a Certificate that is the subject of such a complaint.

12.2.5 Reasons for Revocation

The CA MUST revoke a Certificate that it has issued for any of the following reasons:

1. The Subscriber requests revocation of its Certificate;
2. The Subscriber indicates that the original Certificate Request was not authorized and does not retroactively grant authorization;
3. The CA obtains reasonable evidence that the Subscriber's Private Key (corresponding to the Public Key in the Certificate) has suffered a Key Compromise, or that the Certificate has otherwise been misused (also see Section 10.2.4);
4. The CA receives notice, or otherwise becomes aware, that a Subscriber has violated one or more of its material obligations under the Subscriber Agreement;
5. The CA receives notice, or otherwise becomes aware, of any circumstance indicating that use of a Fully-Qualified Domain Name or IP address in the Certificate is no longer legally permitted (e.g. a court or arbitrator has revoked a Domain Name Registrant's right to use the Domain Name, a relevant licensing or services agreement between the Domain Name Registrant and the Applicant has terminated, or the Domain Name Registrant has failed to renew the Domain Name);
6. The CA receives notice, or otherwise becomes aware, that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name;
7. The CA receives notice, or otherwise becomes aware, of a material change in the information contained in the Certificate;

8. A determination, in the CA's sole discretion, that the Certificate was not issued in accordance with these Requirements or the CA's Certificate Policy or Certification Practice Statement;
9. The CA determines that any of the information appearing in the Certificate is inaccurate or misleading;
10. The CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate;
11. The CA's right to issue Certificates under these Requirements expires or is revoked or terminated, unless the CA has made arrangements to continue maintaining the CRL/OCSP Repository;
12. The Private Key of the CA's Root Certificate used for issuing the Certificate is suspected to have been compromised; or
13. Such additional revocation reasons as the CA publishes in its Certificate Policy [010] and/or ~~and~~ Certification Practice Statement.

13. Employees and Third Parties

13.1 Trustworthiness and Competence

13.1.1 Identity and Background Verification

Prior to the commencement of employment of any person ~~by the CA~~engaged ~~for engagement~~ in the Certificate~~ion~~ [055]Management Process, whether as an employee, agent, or an independent contractor of the CA [035] or RA, the ~~CA~~ employer MUST verify the identity of such person.

13.1.2 Training and Skill Level

The [035] ~~CA~~ employer MUST provide all personnel performing information verification duties with skills-training that covers basic Public Key Infrastructure knowledge, authentication and vetting policies and procedures (including the CA's Certificate Policy [010] and/or ~~and~~ Certification Practice Statement), common threats to the information verification process (including phishing and other social engineering tactics), and these Requirements.

The [035] ~~CA~~ employer MUST maintain records of such training and ensure that personnel entrusted with Validation Specialist duties maintain a skill level that enables them to perform such duties satisfactorily.

Validation Specialists engaged in Certificate issuance MUST maintain skill levels consistent with the ~~CA's~~ employer's training and performance programs.

The ~~CA~~ employer MUST ensure that its Validation Specialists possess the skills required by each task before granting the privilege to perform that task.

The ~~CA~~ employer MUST require all Validation Specialists to pass an internal examination on the information verification requirements outlined in these Requirements.

13.2 Delegation of Functions

13.2.1 General

The CA MAY delegate the performance of all, or any part, of these Requirements to an Affiliate, RA, Enterprise RA, or subcontractor, provided that the process as a whole fulfills all of the requirements of Section 11. Affiliates, RAs, Enterprise RAs, and subcontractors MUST comply with the qualification requirements of Section 13.1, as applicable to their function within the Certificat~~ion~~e [055] Management Process. Prior to delegating functions to an RA or sub CA that is not operated by the CA, the CA MUST review, evaluate and determine that the entity's practice statement complies with these Requirements.

13.2.2 Compliance Obligation

The CA MUST contractually oblige its RAs, Enterprise RAs, [21]Affiliates, and subcontractors to comply with all applicable parts of these Requirements. The CA MUST take the steps reasonably necessary to ensure that the other

parties honor these obligations. For RAs and sub CAs that are not operated by the CA, the CA MUST review each RA's or sub CA's independent audit report prior to processing certificate requests from the RA or issuing a certificate to the sub CA.

13.2.3 Allocation of Liability

In delegating tasks, the CA, its Subordinate CAs, Affiliates, RAs, Enterprise RAs, and subcontractors (as applicable) MAY allocate liability between themselves contractually as they determine, but the CA SHALL remain fully responsible for the performance of all parties in accordance with these Requirements, as if the tasks had not been delegated.

13.2.4 Enterprise RAs

The CA MAY designate an Enterprise RA to verify Certificate Requests from the Enterprise RA's own organization.

The CA SHALL NOT accept Certificate Requests authorized by an Enterprise RA unless the following requirements are satisfied:

1. The CA SHALL confirm that the requested Fully-Qualified Domain Name(s) are within the Enterprise RA's verified Domain Namespace (see Section 7.1.2 para 1).
2. If the Certificate Request includes a Subject name of a type other than a Fully-Qualified Domain Name, the CA MUST confirm that the name is either that of the Enterprise RA, or an Affiliate of the Enterprise RA, or that the Enterprise RA is an agent of the named Subject. For example, the CA SHALL NOT issue a Certificate containing the Subject name "XYZ Co." on the authority of Enterprise RA "ABC Co.", unless the two companies are affiliated (see Section 11.1) or "ABC Co." is the agent of "XYZ Co". This requirement applies regardless of whether the accompanying requested Subject FQDN falls within the Domain Namespace of ABC Co.'s Registered Domain Name.

The CA MUST impose these limitations as a contractual requirement on the Enterprise RA and monitor compliance by the Enterprise RA.

14. Data Records

14.1 Documentation and Event Logging

The CA, its RAs, Enterprise RAs, and subcontractors MUST record details of every action taken to process a Certificate Request and to issue a Certificate, including: all information generated, and documentation received in connection with the Certificate Request; the time and date; and the personnel involved. These records MUST be available as auditable proof of the CA's practices.

14.2 Events and Actions

The foregoing record requirements include, but are not limited to, an obligation to record the following events:

1. CA key lifecycle management events, including:
    a. Key generation, backup, storage, recovery, archival, and destruction; and
    b. Cryptographic device lifecycle management events.
2. CA and Subscriber Certificate lifecycle management events, including:
    a. Certificate Requests, renewal, and re-key requests, and revocation;
    b. All verification activities stipulated in these Requirements and the CA's Certification Practice Statement;
    c. Date, time, phone number used, persons spoken to, and end results of verification telephone calls;
    d. Acceptance and rejection of Certificate Requests;

e. Issuance of Certificates; and

f. Generation of Certificate Revocation Lists and OCSP entries.

3. Security events, including:

a. Successful and unsuccessful PKI system access attempts;

b. PKI and security system actions performed;

c. Security profile changes;

d. System crashes, hardware failures, and other anomalies;

e. Firewall and router activities; and

f. Entries to and exits from the CA facility.

Log entries MUST include the following elements:

1. Date and time of entry;
2. Identity of the person making the journal entry; and
3. Description of the entry.

14.3 Retention

14.3.1 Audit Log Retention

The CA's audit logs MUST be retained for at least seven years, and MUST be made available to the auditor upon request.

14.3.2 Documentation Retention

The CA, its RAs and Enterprise RAs MUST retain all documentation relating to all Certificate Requests and verification thereof, and all Certificates and revocation thereof, for at least seven years after any Certificate based on that documentation ceases to be valid.

15. Data Security

15.1 Objectives

The CA MUST develop, implement, and maintain a comprehensive security program reasonably designed to:

1. Protect the confidentiality, integrity, and availability of Certificate Data and Certificate[055] Management ~~ion~~ Processes;
2. Protect against any anticipated threats or hazards to the confidentiality, integrity, and availability of the Certificate Data and Certificate [055]Management ~~ion~~ Processes;
3. Protect against unauthorized or unlawful access, use, disclosure, alteration, or destruction of any Certificate Data or Certificate [055] Management ~~ion~~ Processes;
4. Protect against accidental loss or destruction of, or damage to, any Certificate Data or Certificate [055] Management~~ion~~ Processes; and
5. Comply with all other security requirements applicable to the CA by law.

15.2 Risk Assessment

The CA's security program MUST include an annual Risk Assessment that:

1. Identifies reasonably foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any Certificate Data or Certificate [055] Management ~~ion~~ Processes;

2. Assesses the likelihood and potential damage of these threats, taking into consideration the sensitivity of the Certificate Data and Certificate [055] Management~~ion~~ Processes; and

3. Assesses the sufficiency of the policies, procedures, information systems, technology, and other arrangements that the CA has in place to counter such threats.

15.3 Security Plan

Based on the Risk Assessment, the CA MUST develop, implement, and maintain a Security Plan consisting of security procedures, measures, and products designed to achieve the objectives set forth above and to reasonably manage and control the risks identified during the Risk Assessment, commensurate with the sensitivity of the Certificate Data and Certificate Management ~~ion~~ Processes. The Security Plan SHALL include administrative, organizational, technical, and physical safeguards appropriate to the sensitivity of the Certificate Data and Certificate Management ~~ion~~ Processes. The Security Plan SHALL also take into account then-available technology and the cost of implementing the specific measures, and MUST implement a reasonable level of security appropriate to the harm that might result from a breach of security and the nature of the data to be protected.

15.4 Business Continuity

In addition, the CA MUST establish and document business continuity and disaster recovery procedures that notify and reasonably protect Application Software Suppliers, Subscribers, and Relying Parties in the event of a disaster, security compromise, or business failure. The CA is not required to publicly disclose these plans but MUST make the plans available to the CA's auditors upon request. The CA must review and update these procedures annually.

15.5 [055]~~Private Key Protection~~System Security

The Certificate Management Process SHALL consist of:

- physical security and environmental controls to prevent equipment tampering;
- system integrity controls, including configuration management, integrity maintenance of trusted code, and malware detection/prevention;
- network security and firewall management, including port restrictions and IP address filtering;
- user management, separate trusted-role assignments, education, awareness, and training; and
- logical access controls, activity logging, and inactivity time-outs to provide individual accountability.

The CA SHALL enforce multi-factor authentication for all accounts capable of directly causing certificate issuance.

15.6 Private Key Protection

The CA MUST protect its Private Key by housing it in a FIPS 140-1 level 3 (or equivalent or higher) cryptographic module.

~~15.6~~15.7 Root CA Private Key Use

Root CA Private Keys MUST NOT be used directly to sign Subscriber Certificates. Root CA Private Keys MAY be used to sign Certificates for the following purposes:

1. Self-signed Certificates to represent the Root CA itself.
2. Certificates for Subordinate CAs;

3. Certificates for infrastructure purpose (e.g. – OCSP Response verification Certificates);
4. Certificates issued solely for the purpose of testing products with Certificates issued by a Root CA.

16. Audit Requirements

16.1 Eligible Audit Schemes

Eligible ~~Audit~~ audit schemes include:

1. WebTrust for Certification Authorities v1.0 or later;
2. ETSI TS 101 456 v1.2.1 or later;
3. ETSI TS 102 042 V1.1.1 or later;
4. ISO 21188:2006, completed by either a licensed WebTrust for CAs auditor, or an audit authority operating according to the laws and policies for assessors in the jurisdiction of the CA; or
5. If a Government CA is legally required to use a different internal audit scheme, it may use such scheme provided that: (a) the audit encompasses all requirements of one of the above schemes, and (b) the audit is performed by an Appropriate Internal Supervisory Government Auditing Agency, separate from the CA, that meets the requirements of Section 16.4.

16.2 Pre-Issuance Readiness Audit

If the CA has a currently valid [004]~~unqualified~~ [006]~~audit~~ Audit ~~opinion~~ Report indicating compliance with ~~the~~ an audit scheme~~s~~ listed in Section 16.1, then no pre-issuance readiness assessment is necessary.

If the CA does not have a currently valid [004]~~unqualified a~~[006]Audit ~~opinion~~ Report indicating compliance with one of the audit schemes listed in Section 16.1, then, before issuing Certificates, the CA MUST successfully complete a point-in-time readiness assessment performed in accordance with applicable standards under one of the audit schemes listed in Section 16.1.

16.3 Annual Independent Audit

At least once every eleven to thirteen months following the previous independent audit (in order to accommodate an auditor's schedule), the CA MUST be independently examined for compliance with the requirements of one of the eligible audit schemes listed in Section 16.1.

Such audits MUST cover all audit requirements regardless of whether they are performed directly by a Qualified Independent Auditing Organization on the CA, subordinate CA, RA, Affiliate, or subcontractor, or by the CA's independent auditing group [007 – needs explanation] on subordinate CAs, RAs, Affiliates, or subcontractors.

Because of the limited powers that may be delegated to an Enterprise RA, and the oversight required of the CA (see Section 13.2.4), Enterprise RAs MAY be excluded from this requirement. However, Enterprise RAs SHALL comply with the documentation retention requirements of Section 14.3.2.

The audit period SHALL NOT exceed one year. However, if the CA is under the operation, control, or supervision of a Government Entity and the audit scheme is conducted pursuant to Section 16 over multiple years, then the annual audit must cover at least the core controls that are required to be audited annually by such scheme plus that portion of all non-core controls that are allowed to be conducted less frequently, but in no case may any non-core control be audited less often than once every three years.

The[006] ~~a~~Audit ~~r~~Report MUST be made publicly available. For both government and commercial CAs, the CA SHOULD make its ~~audit~~ Audit ~~report~~ Report publicly available no later than three months after the end of the audit period. In the event of a delay greater than three months, and if so requested by an Application Software Supplier, the CA MUST provide an explanatory letter signed by the Qualified Auditor~~its auditor~~.

16.4 Auditor Qualifications

The audit MUST be performed by a [029] Qualified Auditor~~Qualified Independent Auditing Organization or Appropriate Internal Supervisory Government Auditing Agency~~. A Qualified ~~Independent Auditing Organization or Appropriate Internal Supervisory Government Auditing Agency~~ Auditor means an entity that:

1. Produces a documented commitment to maintaining its impartiality and independence [029]and is bound by law, government regulation, or professional code of ethics to render an honest and objective judgment regarding the CA or RA;
2. Publicly certifies in writing that its audits address the criteria specified in one of the schemes listed in section 16.1;
3. Employs individuals during the audit who have proficiency in examining Public Key Infrastructure technology, information security tools and techniques, information technology and security auditing, and the third-party attestation function, and be currently licensed or certified to perform the audit in accordance with the scheme selected; and
4. Is licensed, certified, or registered ~~a member of the American Institute of Certified Public Accountants, the Canadian Institute of Chartered Accountants, the Institute of Chartered Accountants in England and Wales, or an equivalent~~ [029] with a recognized ~~professional auditing organization affiliated directly or indirectly with an international professional auditing organization such as the International Federation of Accountants (IFAC)~~ accrediting body that requires that audits be completed under defined standards, including the possession of certain skill sets, quality assurance measures (such as peer review), competency testing, standards with respect to proper assignment of staff to engagements, and requirements for continuing professional education.~~; and~~ [029]
5. (Except in the case of an Appropriate Internal Supervisory Government Auditing Agency) Is an independent accounting firm currently licensed or certified to perform the audit in accordance with the scheme selected and maintains Professional Liability/Errors & Omissions insurance, with policy limits of at least one million US dollars in coverage.

16.5 Key Generation Ceremony

[002] A CA generating a new Key Pair for use in a Root Certificate or Subordinate CA certificate SHOULD have a Qualified Auditor witness the key generation ceremony. This requirement does not apply if the Subordinate CA is an Affiliate of the Root CA issuing the Subordinate CA certificate. The CA's Qualified Auditor SHOULD observe the key generation process and the controls used to ensure the integrity and confidentiality of the Key Pair. ~~For Root CAs and CAs that operate subordinate to unaffiliated Root CAs, whose Key Pairs are generated after the adoption of these Requirements, the CA's Qualified Auditor SHOULD witness the key generation ceremony in order to observe the process and the controls over the integrity and confidentiality of the Key Pair.~~ The Qualified Auditor MUST then issue a report opining that the CA, during its Key and Certificate generation process:

1. Documented its Key Pair generation and protection procedures in its Certificate Policy, and its Certification Practice Statement;
2. Included appropriate detail in its procedures for generating the Key Pair;
3. Maintained effective controls to provide reasonable assurance that the Private Key was generated and protected in conformance with the procedures described in its Certificate Policy [010] and/or ~~and~~ Certification Practice Statement and its Root Key Generation Script; and
4. Performed, during the Root Key generation process, all the procedures required by its Root Key Generation Script.

A video of the entire key generation ceremony SHOULD be recorded for auditing purposes.

16.6 Regular Self Audits

During the period in which it issues Certificates, the CA MUST monitor adherence to its Certificate Policy, Certification Practice Statement and these Requirements and strictly control its service quality by performing self audits on at least a quarterly basis against a randomly selected sample of the greater of~~,~~ one certificate or at least

three percent of the Certificates issued by it during the period commencing immediately after the previous self-audit sample was taken. Except for RAs,~~,~~ [020] Subordinate ~~Sub-~~CAs, or Affiliates that undergo an annual audit that meets the criteria specified in Section 16.3, the CA MUST strictly control its service quality of Certificates issued or containing information verified by a RA, [020] Subordinate ~~Sub-~~CA, or Affiliate by [037]having a Validation Specialist employed by the CA ~~performing~~ perform ongoing quarterly audits against a randomly selected sample of the greater of one certificate or at least three percent of the Certificates issued by the RA, [020] Subordinate ~~sub-~~CA, or Affiliate in the period beginning immediately after the last sample was taken. [037 and 047] The CA's internal audit MUST verify that each Subordinate CA, RA, and Affiliate who has responsibilities under these requirements (by delegation or otherwise) is in compliance with these Requirement and the relevant Certificate Policy and/or Certification Practice Statement.

17. Liability and Indemnification

17.1 Liability to Subscribers and Relying Parties

In cases where the CA has issued and managed the Certificate in compliance with these Requirements and its Certificate Policy [010] and/or ~~and-~~Certification Practice Statement, the CA MAY disclaim liability to the Certificate Beneficiaries or any other third parties for any losses suffered as a result of use or reliance on such Certificate beyond those specified in the CA's Certificate Policy [010] and/or ~~and-~~Certification Practice Statement. In cases where the CA has not issued or managed the Certificate in complete compliance with these Requirements and its Certificate Policy [010] and/or ~~and-~~Certification Practice Statement, the CA MAY seek to limit its liability to the Subscriber and to Relying Parties, regardless of the cause of action or legal theory involved, for any and all claims, losses or damages suffered as a result of the use or reliance on such Certificate by any appropriate means that the CA desires, provided that all such purported limitations on the CA's liability MUST also be specified in the CA's Certificate Policy [010] and/or ~~and-~~Certification Practice Statement.

17.2 Indemnification of Application Software Suppliers

Notwithstanding any limitations on its liability to Subscribers and Relying Parties, the CA understands and acknowledges that the Application Software Suppliers who have a Root Certificate distribution agreement in place with the Root CA do not assume any obligation or potential liability of the CA under these Requirements or that otherwise might exist because of the issuance or maintenance of Certificates or reliance thereon by Relying Parties or others. Thus, the CA SHALL defend, indemnify, and hold harmless each Application Software Supplier for any and all claims, damages, and losses suffered by such Application Software Supplier related to a Certificate issued by the CA, regardless of the cause of action or legal theory involved. This shall not apply, however, to any claim, damages, or loss suffered by such Application Software Supplier related to a Certificate issued by the CA where such claim, damage, or loss was directly caused by such Application Software Supplier's software displaying as not trustworthy a Certificate that is still valid, or displaying as trustworthy: (1) a Certificate that has expired, or (2) a Certificate that has been revoked (but only in cases where the revocation status is currently available from the CA online, and the application software either failed to check such status or ignored an indication of revoked status).

17.3 Root CA Obligations

[018] ~~In cases where the Subordinate CA is not an Affiliate of the entity that controls the Root CA, t~~[019] The Root CA SHALL be responsible for the performance and warranties of the Subordinate CA, for the Subordinate CA's compliance with these Requirements, and for all liabilities and indemnification obligations of the Subordinate CA under these Requirements, as if the Root CA were the Subordinate CA issuing the Certificates.

18. Privacy and Confidentiality

The CA MUST comply with all applicable privacy, confidential information, and trade-secret laws and regulations, as well as its published privacy policy, in the collection, use, retention, and disclosure of non-public information as part of its Certificate [055] Management ~~ion-~~Processes.

1

Appendix A - Cryptographic Algorithm and Key Requirements (Normative)

Certificates SHALL meet the following requirements for algorithm type and key size.

(1) Root CA Certificates

	Validity period beginning on or before 31 Dec 2010	Validity period beginning after 31 Dec 2010
Digest algorithm	MD5 (NOT RECOMMENDED), or, SHA-1	SHA-1*, SHA-256, SHA-384 or SHA-512
Minimum RSA modulus size (bits)	2048**	2048
ECC curve	NIST P-256, P-384, or P-521	NIST P-256, P-384, or P-521

(2) Subordinate CA Certificates

	Validity period beginning on or before 31 Dec 2010 and ending on or before 31 Dec 2013	Validity period beginning after 31 Dec 2010 or ending after 31 Dec 2013
Digest algorithm	SHA-1	SHA-1*, SHA-256, SHA-384 or SHA-512
Minimum RSA modulus size (bits)	1024	2048
ECC curve	NIST P-256, P-384, or P-521	NIST P-256, P-384, or P-521

(3) Subscriber Certificates

	Validity period ending on or before 31 Dec 2013	Validity period ending after 31 Dec 2013
Digest algorithm	SHA1*, SHA-256, SHA-384 or SHA-512	SHA1*, SHA-256, SHA-384 or SHA-512
Minimum RSA modulus size (bits)	1024	2048
ECC curve	NIST P-256, P-384, or P-521	NIST P-256, P-384, or P-521

* SHA-1 MAY be used until SHA-256 is supported widely by browsers used by a substantial portion of relying-parties worldwide.

** A Subscriber Certificate MAY, in addition, chain to a Root CA certificate with an RSA key whose size is less than 2048 bits.

1

2

Appendix B – Certificate Extensions (Normative)

This appendix specifies the requirements for Certificates extensions.

Root CA Certificate

Root Certificates MUST be of type X.509 v3.

A. basicConstraints

This extension MUST appear as a critical extension. The cA field MUST be set true. The pathLenConstraint field SHOULD NOT be present.

B. keyUsage

This extension MUST be present and MUST be marked critical. Bit positions for keyCertSign and cRLSign MUST be set. All other bit positions SHOULD NOT be set.

C. certificatePolicies

This extension SHOULD NOT be present.

D. extendedKeyUsage

This extension MUST NOT be present.

All other fields and extensions SHALL be set in accordance to RFC 5280.

Subordinate CA Certificate

Subordiante CA Certificates MUST be of type X.509 v3.

A. certificatePolicies

This extension MUST be present and SHOULD NOT be marked critical.

certificatePolicies:policyIdentifier (Required)

The following fields MUST be present if the Subordinate CA is not an Affiliate of the entity that controls the Root CA.

certificatePolicies:policyQualifiers:policyQualifierId

- id-qt 1 [RFC 5280].

certificatePolicies:policyQualifiers:qualifier:cPSuri

- HTTP URL for the Root CA's Certification Practice Statement.

B. cRLDistributionPoints

This extension MUST be present and MUST NOT be marked critical. It MUST contain the HTTP URL of the CA's CRL service.

C. authorityInformationAccess

With the exception of one uncommon circumstance, which is noted below, this extension MUST be present. It MUST NOT be marked critical, and it MUST contain the HTTP URL of the Issuing CA's OCSP responder (accessMethod = 1.3.6.1.5.5.7.48.1). It MAY also contain the HTTP URL of the Issuing CA's certificate (accessMethod = 1.3.6.1.5.5.7.48.2). See Section 12.1.1 for details.

The HTTP URL of the Issuing CA's OCSP responder MAY be omitted, provided all the Subscriber Certificates issued by the Subordinate CA are for high-traffic FQDNs. In this case, the CA MUST ensure that the Subscriber "staples" the OCSP response for the Certificate in its TLS handshakes [RFC4366].

D. basicConstraints

This extension MUST be present and MUST be marked critical. The cA field MUST be set true. The pathLenConstraint field MAY be present.

E. keyUsage

This extension MUST be present and MUST be marked critical. Bit positions for keyCertSign and cRLSign MUST be set. All other bit positions MUST NOT be set.

All other fields and extensions SHALL be set in accordance to RFC 5280.

Subscriber Certificate

A. certificatePolicies

This extension MUST be present and SHOULD NOT be marked critical.

certificatePolicies:policyIdentifier (Required)

- A Policy Identifier, defined by the issuing CA, that indicates a Certificate Policy asserting the issuing CA's adherence to and compliance with these Requirements.

certificatePolicies:policyQualifiers:policyQualifierId (Required)

- id-qt 1 [RFC 5280].

certificatePolicies:policyQualifiers:qualifier:cPSuri (Required)

- HTTP URL for the Subordinate CA's Certification Practice Statement.

B. cRLDistributionPoints

If the certificate does not specify an OCSP responder location in an authorityInformationAccess extension, then this extension MUST be present. Otherwise, this extension SHOULD be present. If present, it MUST NOT be marked critical, and it MUST contain the HTTP URL of the CA's CRL service. See Section 12.1.1 for details.

C. authorityInformationAccess

With the exception of one uncommon circumstance, which is noted below, this extension MUST be present. It MUST NOT be marked critical, and it MUST contain the HTTP URL of the Issuing CA's OCSP responder (accessMethod = 1.3.6.1.5.5.7.48.1). It MAY also contain the HTTP URL of the Issuing CA's certificate (accessMethod = 1.3.6.1.5.5.7.48.2). See Section 12.1.1 for details.

The HTTP URL of the Issuing CA's OCSP responder MAY be omitted provided the Certificate is for a high-traffic FQDNs. In this case, the Issuing CA MUST ensure that the Subscriber "staples" OCSP responses for the Certificate in its TLS handshakes [RFC4366].

D. basicConstraints (optional)

If present, the cA field MUST be set false.

E. keyUsage (optional)

If present, bit positions for keyCertSign, cRLSign and nonRepudiation MUST NOT be set.

F. extKeyUsage (required)

Either the value id-kp-serverAuth [RFC5280] or id-kp-clientAuth [RFC5280] or both values MUST be present. id-kp-emailProtection [RFC5280] MAY be present. Other values SHOULD NOT be present.

All other fields and extensions SHALL be set in accordance to RFC 5280.

Appendix C - User Agent Verification (Normative)

The CA MUST host test Web pages that allow Application Software Suppliers to test their software. At a minimum, the CA MUST host separate Web pages using Certificates that are (i) valid, (ii) revoked, and (iii) expired.