

1
2
3 **CA/Browser Forum**
4

5
6
7
8
9
10
11 **Baseline Requirements**
12 **for the**
13 **Issuance and Management**
14 **of**
15 **Publicly-Trusted Certificates**
16

17 Copyright © 2011, The CA / Browser Forum, all rights reserved.

18 Verbatim copying and distribution of this entire document is permitted in any medium without royalty, provided this
19 notice is preserved.

20 Upon request, the CA / Browser Forum may grant permission to make a translation of this document into a language
21 other than English. In such circumstance, copyright in the translation remains with the CA / Browser Forum. In the
22 event that a discrepancy arises between interpretations of a translated version and the original English version, the
23 original English version shall govern. A translated version of the document must prominently display the following
24 statement in the language of the translation:-

25 'Copyright © 2011 The CA / Browser Forum, all rights reserved.

26 This document is a translation of the original English version. In the event that a discrepancy arises between
27 interpretations of this version and the original English version, the original English version shall govern.'

28 A request to make a translated version of this document should be submitted to questions@cabforum.org.
29

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 September 2011 is as follows:

Certification Authorities

- A-Trust GmbH
- AC Camerfirma SA
- Buypass AS
- Certum
- Comodo CA Ltd
- Cybertrust
- D-TRUST GmbH
- DanID A/S
- DigiCert, Inc.
- Digidentity BV
- 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
- Logius PKIoverheid
- Network Solutions, LLC
- QuoVadis Ltd.
- RSA Security, Inc.
- SECOM Trust Systems CO., Ltd.
- Skaitmeninio sertifikavimo centras (SSC)
- StartCom Certification Authority
- SwissSign AG
- Symantec Corporation
- T-Systems Enterprise Services GmbH.
- TC TrustCenter GmbH
- Thawte, Inc.
- TÜRKTRUST
- Trustis Limited
- Trustwave
- TWCA
- 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 AICPA/CICA WebTrust for Certification Authorities 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	7
2.	Purpose	7
3.	References	7
4.	Definitions	8
5.	Abbreviations and Acronyms	11
6.	Conventions	11
7.	Certificate Warranties and Representations	11
7.1	By the CA	11
7.1.1	Certificate Beneficiaries	12
7.1.2	Certificate Warranties	12
7.2	By the Applicant	13
8.	Community and Applicability	13
8.1	Compliance	13
8.2	Certificate Policies	13
8.2.1	Implementation	13
8.2.2	Disclosure	13
8.3	Commitment to Comply	13
8.4	Trust model	13
9.	Certificate Content and Profile	14
9.1	Issuer Information	14
9.1.1	Issuer Common Name Field	14
9.1.2	Issuer Domain Component Field	14
9.1.3	Issuer Organization Name Field	14
9.1.4	Issuer Country Name Field	14
9.2	Subject Information	14
9.2.1	Subject Alternative Name Extension	14
9.2.2	Subject Common Name Field	15
9.2.3	Subject Domain Component Field	15
9.2.4	Subject Organization Name Field	15
9.2.5	Subject Country Name Field	15
9.2.6	Other Subject Attributes	16
9.3	Certificate Policy Identification	16
9.3.1	Reserved Certificate Policy Identifiers	16
9.3.2	Root CA Certificates	16
9.3.3	Subordinate CA Certificates	16
9.3.4	Subscriber Certificates	17
9.4	Validity Period	17
9.5	Subscriber Public Key	17
9.6	Certificate Serial Number	17
9.7	Additional Technical Requirements	17
10.	Certificate Application	17
10.1	Documentation Requirements	17
10.2	Certificate Request	18
10.2.1	General	18
10.2.2	Request and Certification	18
10.2.3	Information Requirements	18
10.2.4	Subscriber Private Key	18
10.3	Subscriber and Terms of Use Agreement	18
10.3.1	General	18
10.3.2	Agreement Requirements	19
11.	Verification Practices	19
11.1	Authorization by Domain Name Registrant	19
11.2	Verification of Subject Identity Information	20
11.2.1	Identity	20

11.2.2	DBA/Tradename.....	21
11.2.3	Authenticity of Certificate Request	21
11.2.4	Verification of Individual Applicant.....	21
11.2.5	Verification of Country.....	21
11.3	Age of Certificate Data.....	21
11.4	Denied List	22
11.5	High Risk Requests	22
11.6	Data Source Accuracy	22
12.	Certificate Issuance by a Root CA	22
13.	Certificate Revocation and Status Checking	23
13.1	Revocation.....	23
13.1.1	Revocation Request	23
13.1.2	Certificate Problem Reporting	23
13.1.3	Investigation	23
13.1.4	Response.....	23
13.1.5	Reasons for Revocation	23
13.2	Certificate Status Checking	24
13.2.1	Mechanisms	24
13.2.2	Repository.....	24
13.2.3	Response Time.....	25
13.2.4	Deletion of Entries	25
13.2.5	OCSP Signing.....	25
14.	Employees and Third Parties.....	25
14.1	Trustworthiness and Competence.....	25
14.1.1	Identity and Background Verification.....	25
14.1.2	Training and Skill Level	25
14.2	Delegation of Functions.....	25
14.2.1	General.....	25
14.2.2	Compliance Obligation	26
14.2.3	Allocation of Liability	26
14.2.4	Enterprise RAs.....	26
15.	Data Records	26
15.1	Documentation and Event Logging	26
15.2	Events and Actions	26
15.3	Retention	27
15.3.1	Audit Log Retention	27
15.3.2	Documentation Retention	27
16.	Data Security	27
16.1	Objectives.....	27
16.2	Risk Assessment.....	28
16.3	Security Plan.....	28
16.4	Business Continuity.....	28
16.5	System Security	29
16.6	Private Key Protection.....	29
17.	Audit.....	29
17.1	Eligible Audit Schemes	29
17.2	Audit Period.....	29
17.3	Audit Report	29
17.4	Pre-Issuance Readiness Audit.....	30
17.5	Audit of Delegated Functions	30
17.6	Auditor Qualifications	30
17.7	Key Generation Ceremony	31
17.8	Regular Quality Assessment Self Audits	31
18.	Liability and Indemnification	31
18.1	Liability to Subscribers and Relying Parties.....	31
18.2	Indemnification of Application Software Suppliers	32

18.3	Root CA Obligations	32
	Appendix A - Cryptographic Algorithm and Key Requirements (Normative).....	33
	Appendix B – Certificate Extensions (Normative).....	35
	Root CA Certificate	35
	Subordinate CA Certificate.....	35
	Subscriber Certificate	36
	Appendix C - User Agent Verification (Normative)	37

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 to issue Publicly Trusted Certificates. Except where explicitly stated otherwise, these requirements apply only to relevant events that occur on or after the Effective Date.

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. In particular, it is expected that a future version will contain more formal and comprehensive audit requirements for delegated functions.

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, et 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 2.0, AICPA/CICA, available at <http://www.webtrust.org/homepage-documents/item49945.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, 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.

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.

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

Domain Namespace: The set of all possible Domain Names that are subordinate to a single node in the Domain Name System.

Domain Name Registrant: Sometimes referred to as the "owner" of a Domain Name, but more properly the person(s) or entity(ies) registered with a Domain Name Registrar as having the right to control how a Domain Name

1 is used, such as the natural person or Legal Entity that is listed as the “Registrant” by WHOIS or the Domain Name
2 Registrar.

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

7 **Effective Date:** These Requirements come into force on [date specified in Motion adopting these Requirements.

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

10 **Expiry Date:** The “Not After” date in a Certificate that defines the end of a Certificate’s validity period.

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

13 **Government Entity:** A government-operated legal entity, agency, department, ministry, branch, or similar element
14 of the government of a country, or political subdivision within such country (such as a state, province, city, county,
15 etc.).

16 **Internal Server Name:** A Server Name (which may or may not include an Unregistered Domain Name) that is not
17 resolvable using the public DNS.

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

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

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

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

25 **Legal Entity:** An association, corporation, partnership, proprietorship, trust, government entity or other entity
26 with legal standing in a country’s legal system.

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

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

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

33 **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
34 Digital Signatures and/or to decrypt electronic records or files that were encrypted with the corresponding Public
35 Key.

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

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

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

44 **Qualified Auditor:** A natural person or Legal Entity that meets the requirements of Section 17.6 (Auditor
45 Qualifications).

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

2 **Registration Authority (RA):** Any Legal Entity that is responsible for identification and authentication of subjects
3 of Certificates, but is not a CA, and hence does not sign or issue Certificates. An RA may assist in the certificate
4 application process or revocation process or both. When “RA” is used as an adjective to describe a role or function,
5 it does not necessarily imply a separate body, but can be part of the CA.

6 **Reliable Method of Communication:** A method of communication, such as a postal/courier delivery address,
7 telephone number, or email address, that was verified using a source other than the Applicant Representative.

8 **Relying Party:** Any natural person or Legal Entity that relies on a Valid Certificate. An Application Software
9 Supplier is not considered a Relying Party when software distributed by such Supplier merely displays information
10 relating to a Certificate.

11 **Repository:** An online database containing publicly-disclosed PKI governance documents (such as Certificate
12 Policies and Certification Practice Statements) and Certificate status information, either in the form of a CRL or an
13 OCSP response.

14 **Requirements:** This document.

15 **Reserved IP Address:** An IPv4 or IPv6 address that the IANA has marked as reserved:
16 <http://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xml>
17 <http://www.iana.org/assignments/ipv6-address-space/ipv6-address-space.xml>
18

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

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

23 **Subject:** The natural person, device, system, unit, or Legal Entity identified in a Certificate as the Subject. The
24 Subject is either the Subscriber or a device under the control and operation of the Subscriber.

25 **Subject Identity Information:** Information that identifies the Certificate Subject. Subject Identity Information
26 does not include a domain name listed in the subjectAltName extension or the Subject commonName field.

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

29 **Subscriber:** A natural person or Legal Entity to whom a Certificate is issued and who is legally bound by a
30 Subscriber or Terms of Use Agreement.

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

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

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

38 **Unregistered Domain Name:** A Domain Name that is not a Registered Domain Name.

39 **Valid Certificate:** A Certificate that passes the validation procedure specified in RFC 5280.

40 **Validation Specialists:** Someone who performs the information verification duties specified by these
41 Requirements.

42 **Validity Period:** The period of time measured from the date when the Certificate is issued until the Expiry Date.

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

5. Abbreviations and Acronyms

1		
2	AICPA	American Institute of Certified Public Accountants
3	CA	Certification Authority
4	ccTLD	Country Code Top-Level Domain
5	CICA	Canadian Institute of Chartered Accountants
6	CP	Certificate Policy
7	CPS	Certification Practice Statement
8	CRL	Certificate Revocation List
9	DBA	Doing Business As
10	DNS	Domain Name System
11	FIPS	(US Government) Federal Information Processing Standard
12	FQDN	Fully Qualified Domain Name
13	IM	Instant Messaging
14	IANA	Internet Assigned Numbers Authority
15	ICANN	Internet Corporation for Assigned Names and Numbers
16	ISO	International Organization for Standardization
17	NIST	(US Government) National Institute of Standards and Technology
18	OCSP	Online Certificate Status Protocol
19	OID	Object Identifier
20	PKI	Public Key Infrastructure
21	RA	Registration Authority
22	S/MIME	Secure MIME (Multipurpose Internet Mail Extensions)
23	SSL	Secure Sockets Layer
24	TLD	Top-Level Domain
25	TLS	Transport Layer Security
26	VOIP	Voice Over Internet Protocol

6. Conventions

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

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

7. Certificate Warranties and Representations

7.1 By the CA

35 By issuing a Certificate, the CA makes the Certificate Warranties listed in Section 7.1.2 to the Certificate
36 Beneficiaries listed in 7.1.1.

1 **7.1.1 Certificate Beneficiaries**

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

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

7 **7.1.2 Certificate Warranties**

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

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

- 12 1. **Right to Use Domain Name or IP Address:** That, at the time of issuance, the CA (i) implemented a
13 procedure for verifying that the Applicant either had the right to use, or had control of, the Domain
14 Name(s) and IP address(es) listed in the Certificate's subject field and subjectAltName extension (or, only
15 in the case of Domain Names, was delegated such right or control by someone who had such right to use or
16 control); (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the
17 procedure in the CA's Certificate Policy and/or Certification Practice Statement;
- 18 2. **Authorization for Certificate:** That, at the time of issuance, the CA (i) implemented a procedure for
19 verifying that the Subject authorized the issuance of the Certificate and that the Applicant Representative is
20 authorized to request the Certificate on behalf of the Subject; (ii) followed the procedure when issuing the
21 Certificate; and (iii) accurately described the procedure in the CA's Certificate Policy and/or Certification
22 Practice Statement;
- 23 3. **Accuracy of Information:** That, at the time of issuance, the CA (i) implemented a procedure for verifying
24 the accuracy of all of the information contained in the Certificate (with the exception of the
25 subject:organizationalUnitName attribute); (ii) followed the procedure when issuing the Certificate; and
26 (iii) accurately described the procedure in the CA's Certificate Policy and/or Certification Practice
27 Statement;
- 28 4. **No Misleading Information:** That, at the time of issuance, the CA (i) implemented a procedure for
29 reducing the likelihood that the information contained in the Certificate's subject:organizationalUnitName
30 attribute would be misleading; (ii) followed the procedure when issuing the Certificate; and (iii) accurately
31 described the procedure in the CA's Certificate Policy and/or Certification Practice Statement;
- 32 5. **Identity of Applicant:** That, if the Certificate contains Subject Identity Information, the CA (i)
33 implemented a procedure to verify the identity of the Applicant in accordance with Sections 9.2.4 and 11.2;
34 (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in the
35 CA's Certificate Policy and/or Certification Practice Statement;
- 36 6. **Subscriber Agreement:** That, if the CA and Subscriber are not Affiliated, the Subscriber and CA are
37 parties to a legally valid and enforceable Subscriber Agreement that satisfies these Requirements, or, if the
38 CA and Subscriber are Affiliated, the Applicant Representative acknowledged and accepted the Terms of
39 Use;
- 40 7. **Status:** That the CA maintains a 24 x 7 publicly-accessible Repository with current information regarding
41 the status (valid or revoked) of all unexpired Certificates; and
- 42 8. **Revocation:** That the CA will revoke the Certificate for any of the reasons specified in these
43 Requirements.

1 **7.2 By the Applicant**

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

5 **8. Community and Applicability**

6 **8.1 Compliance**

7 The CA SHALL at all times:

- 8 1. Issue Certificates and operate its PKI in accordance with all law applicable to its business and the
9 Certificates it issues in every jurisdiction in which it operates;
- 10 2. Comply with these Requirements;
- 11 3. Comply with the audit requirements set forth in Section 17; and
- 12 4. Be licensed as a CA in each jurisdiction where it operates, if licensing is required by the law of such
13 jurisdiction for the issuance of Certificates.

14 If a court or government body with jurisdiction over the activities covered by these Requirements determines that
15 the performance of any mandatory requirement is illegal, then such requirement is considered reformed to the
16 minimum extent necessary to make the requirement valid and legal. This applies only to operations or certificate
17 issuances that are subject to the laws of that jurisdiction. The parties involved SHALL notify the CA / Browser
18 Forum of the facts, circumstances, and law(s) involved, so that the CA/Browser Forum may revise these
19 Requirements accordingly.

20 **8.2 Certificate Policies**

21 **8.2.1 Implementation**

22 The CA SHALL develop, implement, enforce, and annually update a Certificate Policy and/or Certification Practice
23 Statement that describes in detail how the CA implements the latest version of these Requirements.

24 **8.2.2 Disclosure**

25 The CA SHALL publicly disclose its Certificate Policy and/or Certification Practice Statement through an
26 appropriate and readily accessible online means that is available on a 24x7 basis. The CA SHALL publicly disclose
27 its CA business practices to the extent required by the CA's selected audit scheme (see Section 17.1). The
28 disclosures MUST include all the material required by RFC 2527 or RFC 3647, and MUST be structured in
29 accordance with either RFC 2527 or RFC 3647.

30 **8.3 Commitment to Comply**

31 The CA SHALL publicly give effect to these Requirements and represent that it will adhere to the latest published
32 version. The CA MAY fulfill this requirement by incorporating these Requirements directly into its Certificate
33 Policy and/or Certification Practice Statements or by incorporating them by reference using a clause such as the
34 following (which MUST include a link to the official version of these Requirements):

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

39 **8.4 Trust model**

40 The CA SHALL disclose all Cross Certificates that identify the CA as the Subject, provided that the CA arranged
41 for or accepted the establishment of the trust relationship (i.e. the Cross Certificate at issue).

9. Certificate Content and Profile

9.1 Issuer Information

An Issuing CA SHALL populate the issuer field of each Certificate issued after the adoption of these Requirements in accordance with the following subsections.

9.1.1 Issuer Common Name Field

Certificate Field: issuer:commonName (OID 2.5.4.3)

Required/Optional: Optional

Contents: If present in a Certificate, the Common Name field MUST include a name that accurately identifies the Issuing CA.

9.1.2 Issuer Domain Component Field

Certificate Field: issuer:domainComponent (OID 0.9.2342.19200300.100.1.25)

Required/Optional: Optional.

Contents: If present in a Certificate, the Domain Component field MUST include all components of the Issuing CA's Registered Domain Name in ordered sequence, with the most significant component, closest to the root of the namespace, written last.

9.1.3 Issuer Organization Name Field

Certificate Field: issuer:organizationName (OID 2.5.4.10)

Required/Optional: Required

Contents: This field MUST contain the name (or abbreviation thereof), trademark, or other meaningful identifier for the CA, provided that they accurately identify the CA. The field MUST NOT contain a generic designation such as "Root" or "CA1".

9.1.4 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 3166-1 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 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.

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.

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

9 **9.2.2 Subject Common Name Field**

10 **Certificate Field:** subject:commonName (OID 2.5.4.3)

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

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

14 **9.2.3 Subject Domain Component Field**

15 **Certificate Field:** subject:domainComponent (OID 0.9.2342.19200300.100.1.25)

16 **Required/Optional:** Optional.

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

19 **9.2.4 Subject Organization Name Field**

20 **Certificate Fields:**

21 Organization name: organizationName (OID 2.5.4.10)

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

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

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

25 Country: subject:countryName (OID: 2.5.4.6)

26 Postal/Zip code: subject:postalCode (OID: 2.5.4.17)

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

32 **Contents:** If the organizationName field is present, the field MUST contain the Subject's name or DBA and the
33 required address fields MUST contain a location of the Subject as verified by the CA pursuant to Section 11.2. If the
34 Subject is a natural person, because Subject name attributes for individuals (e.g. givenName (2.5.4.42) and surname
35 (2.5.4.4)) are not broadly supported by application software, the CA MAY use the organizationName field to convey
36 the Subject's name or DBA.

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

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

42 **9.2.5 Subject Country Name Field**

43 **Certificate Field:** subject:countryName (OID: 2.5.4.6)

1 **Required/Optional:** Optional

2 **Contents:** If the subject:countryName field is present, then the CA SHALL verify the country associated with the
3 Subject in accordance with Section 11.2.5 and use its two-letter ISO 3166-1 country code.

4 **9.2.6 Other Subject Attributes**

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

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

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

16 **9.3 Certificate Policy Identification**

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

19 **9.3.1 Reserved Certificate Policy Identifiers**

20 The following Certificate Policy identifiers are reserved for use by CAs as an optional means of asserting
21 compliance with these Requirements as follows:

22 {joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) baseline-
23 requirements(2) domain-validated(1)} (2.23.140.1.2.1), if the Certificate complies with these Requirements
24 but lacks Subject Identity Information that is verified in accordance with Section 11.2.

25 If the Certificate asserts the policy identifier of 2.23.140.1.2.1, then it MUST NOT include organizationName,
26 streetAddress, localityName, stateOrProvinceName, or postalCode in the Subject field.

27 {joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) baseline-
28 requirements(2) subject-identity-validated(2)} (2.23.140.1.2.2), if the Certificate complies with these
29 Requirements and includes Subject Identity Information that is verified in accordance with Section 11.2.

30 If the Certificate asserts the policy identifier of 2.23.140.1.2.2, then it MUST also include organizationName,
31 localityName, stateOrProvinceName (if applicable), and countryName in the Subject field.

32 **9.3.2 Root CA Certificates**

33 A Root CA Certificate SHOULD NOT contain the certificatePolicies extension.

34 **9.3.3 Subordinate CA Certificates**

35 A Certificate issued after the Effective Date to a Subordinate CA that is not an Affiliate of the Issuing CA:

- 36 1. MUST include one or more explicit policy identifiers that indicates the Subordinate CA's
37 adherence to and compliance with these Requirements (i.e. either the CA/Browser Forum reserved
38 identifiers or identifiers defined by the CA in its Certificate Policy and/or Certification Practice
39 Statement) and
- 40 2. MUST NOT contain the “anyPolicy” identifier (2.5.29.32.0).

41 A Certificate issued after the Effective Date to a Subordinate CA that is an affiliate of the Issuing CA:

- 1 1. MAY include the CA/Browser Forum reserved identifiers or an identifier defined by the CA in its
2 Certificate Policy and/or Certification Practice Statement to indicate the Subordinate CA's
3 compliance with these Requirements and
- 4 2. MAY contain the "anyPolicy" identifier (2.5.29.32.0) in place of an explicit policy identifier.

5 A Subordinate CA SHALL represent, in its Certificate Policy and/or Certification Practice Statement, that all
6 Certificates containing a policy identifier indicating compliance with these Requirements are issued and managed in
7 accordance with these Requirements.

8 **9.3.4 Subscriber Certificates**

9 A Certificate issued to a Subscriber MUST contain one or more policy identifier(s), defined by the Issuing CA, in
10 the Certificate's certificatePolicies extension that indicates adherence to and compliance with these Requirements.
11 CAs complying with these Requirements MAY also assert one of the reserved policy OIDs in such Certificates.

12 The issuing CA SHALL document in its Certificate Policy or Certification Practice Statement that the Certificates it
13 issues containing the specified policy identifier(s) are managed in accordance with these Requirements.

14 **9.4 Validity Period**

15 Certificates issued after the Effective Date MUST have a Validity Period no greater than 60 months.

16 Except as provided for below, Certificates issued after 1 April 2015 MUST have a Validity Period no greater than
17 39 months.

18 Beyond 1 April 2015, CAs MAY continue to issue Certificates with a Validity Period greater than 39 months but not
19 greater than 60 months provided that the CA documents that the Certificate is for a system or software that:

- 20 (a) was in use prior to the Effective Date;
- 21 (b) is currently in use by either the Applicant or a substantial number of Relying Parties;
- 22 (c) fails to operate if the Validity Period is shorter than 60 months;
- 23 (d) does not contain known security risks to Relying Parties; and
- 24 (e) is difficult to patch or replace without substantial economic outlay.

25 **9.5 Subscriber Public Key**

26 The CA SHALL reject a certificate request if the requested Public Key does not meet the requirements set forth in
27 Appendix A or if it has a known weak Private Key (such as a Debian weak key, see <http://wiki.debian.org/SSLkeys>).

28 **9.6 Certificate Serial Number**

29 CAs SHOULD generate non-sequential Certificate serial numbers that exhibit at least 20 bits of entropy.

30 **9.7 Additional Technical Requirements**

31 The CA SHALL meet the technical requirements set forth in Appendix A - Cryptographic Algorithm and Key
32 Requirements, and Appendix B - Certificate Extensions, and Appendix C - User Agent Verification.

33 **10. Certificate Application**

34 **10.1 Documentation Requirements**

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

- 36 1. A certificate request, which may be electronic; and

2. An executed Subscriber or Terms of Use Agreement, which may be electronic.
- The CA SHOULD obtain any additional documentation the CA determines necessary to meet these Requirements.

10.2 Certificate Request

10.2.1 General

Prior to the issuance of a Certificate, the CA SHALL 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 and/or Certification Practice Statement. In cases where the certificate request does not contain all the necessary information about the Applicant, the CA SHALL 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 MUST include, but not be limited to, at least one Fully-Qualified Domain Name or IP address to be included in the Certificate's SubjectAltName extension.

10.2.4 Subscriber Private Key

Parties other than the Subscriber SHALL NOT archive the Subscriber Private Key.

If the CA or any of its designated RAs generated the Private Key on behalf of the Subscriber, then the CA SHALL encrypt the Private Key for transport to the Subscriber.

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

10.3 Subscriber and Terms of Use Agreement

10.3.1 General

Prior to the issuance of a Certificate, the CA SHALL obtain, for the express benefit of the CA and the Certificate Beneficiaries, either:

1. The Applicant's agreement to the Subscriber Agreement with the CA, or
2. The Applicant's agreement to the Terms of Use agreement.

The CA SHALL implement a process to ensure that each Subscriber or Terms of Use Agreement is legally enforceable against the Applicant. In either case, the Agreement MUST apply to the Certificate to be issued pursuant to the certificate request. The CA MAY use an electronic or "click-through" Agreement provided that the CA has determined that such agreements are legally enforceable. A separate Agreement MAY be used for each certificate request, or a single Agreement MAY be used to cover multiple future certificate requests and the resulting

1 Certificates, so long as each Certificate that the CA issues to the Applicant is clearly covered by that Subscriber or
2 Terms of Use Agreement.

3 **10.3.2 Agreement Requirements**

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

- 7 1. **Accuracy of Information:** An obligation and warranty to provide accurate and complete information at all
8 times to the CA, both in the certificate request and as otherwise requested by the CA in connection with the
9 issuance of the Certificate(s) to be supplied by the CA;
- 10 2. **Protection of Private Key:** An obligation and warranty by the Applicant to take all reasonable measures
11 to maintain sole control of, keep confidential, and properly protect at all times the Private Key that
12 corresponds to the Public Key to be included in the requested Certificate(s) (and any associated activation
13 data or device, e.g. password or token);
- 14 3. **Acceptance of Certificate:** An obligation and warranty that the Subscriber will review and verify the
15 Certificate contents for accuracy;
- 16 4. **Use of Certificate:** An obligation and warranty to install the Certificate only on servers that are accessible
17 at the subjectAltName(s) listed in the Certificate, and to use the Certificate solely in compliance with all
18 applicable laws and solely in accordance with the Subscriber or Terms of Use Agreement;
- 19 5. **Reporting and Revocation:** An obligation and warranty to promptly cease using a Certificate and its
20 associated Private Key, and promptly request the CA to revoke the Certificate, in the event that: (a) any
21 information in the Certificate is, or becomes, incorrect or inaccurate, or (b) there is any actual or suspected
22 misuse or compromise of the Subscriber's Private Key associated with the Public Key included in the
23 Certificate;
- 24 6. **Termination of Use of Certificate:** An obligation and warranty to promptly cease all use of the Private
25 Key corresponding to the Public Key included in the Certificate upon revocation of that Certificate for
26 reasons of Key Compromise.
- 27 7. **Responsiveness:** An obligation to respond to the CA's instructions concerning Key Compromise or
28 Certificate misuse within a specified time period.
- 29 8. **Acknowledgment and Acceptance:** An acknowledgment and acceptance that the CA is entitled to revoke
30 the certificate immediately if the Applicant were to violate the terms of the Subscriber or Terms of Use
31 Agreement or if the CA discovers that the Certificate is being used to enable criminal activities such as
32 phishing attacks, fraud, or the distribution of malware.

33 **11. Verification Practices**

34 **11.1 Authorization by Domain Name Registrant**

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

39 If the CA relies on a confirmation of the right to use or control the Registered Domain Name(s) from a Domain
40 Name Registrar, and the top-level Domain is a two-letter country code (ccTLD), the CA SHALL obtain the
41 confirmation directly from the Domain Name Registrar for the Domain Name level to which the rules of the ccTLD
42 apply. For example, if the requested FQDN is www.mysite.users.example.co.uk, then the CA SHALL obtain
43 confirmation from the Domain Name Registrant of the Domain Name example.co.uk, because applications for
44 Domain Names immediately subordinate to .co.uk are governed by the rules of the .uk registry.

1 If the CA uses the Internet mail system to confirm that the Applicant has authorization from the Domain Name
2 Registrant to obtain a Certificate for the requested Fully-Qualified Domain Name, the CA SHALL use a mail system
3 address formed in one of the following ways:

- 4 1. Supplied by the Domain Name Registrar;
- 5 2. Taken from the Domain Name Registrant's "registrant", "technical", or "administrative" contact
6 information, as it appears in the Domain's WHOIS record; or;
- 7 3. By pre-pending a local part to a Domain Name as follows:
 - 8 a. Local part - One of the following: 'admin', 'administrator', 'webmaster', 'hostmaster', or
9 'postmaster'; and
 - 10 b. Domain Name – Formed by pruning zero or more components from the Registered Domain Name
11 or the requested Fully-Qualified Domain Name.

12 If the Domain Name Registrant has used a private, anonymous, or proxy registration service, and the CA relies upon
13 a Domain Authorization as an alternative to the foregoing, the Domain Authorization MUST be received directly
14 from the private, anonymous, or proxy registration service identified in the WHOIS record for the Registered
15 Domain Name. The document MUST contain the letterhead of the private, anonymous, or proxy registration
16 service, the signature of the General Manager, or equivalent, or an authorized representative of such officer, dated
17 on or after the certificate request date, and the Fully-Qualified Domain Name(s) to be included in the Certificate. If
18 the WHOIS record identifies the private, anonymous, or proxy registration service as the Domain Name Registrant,
19 then the Domain Authorization MUST contain a statement granting the Applicant the right to use the Fully-
20 Qualified Domain Name in a Certificate. The CA SHALL contact the private, anonymous, or proxy registration
21 service directly, using contact information obtained from a reliable, independent, third-party data source, and obtain
22 confirmation from the Domain Name Registrant that the Domain Authorization is authentic.

23 **11.2 Verification of Subject Identity Information**

24 If the Applicant requests a Certificate that will contain Subject Identity Information comprised only of the
25 countryName field, then the CA SHALL verify the country associated with the Subject using a verification process
26 meeting the requirements of Section 11.2.5 and that is described in the CA's Certificate Policy and/or Certification
27 Practice Statement. If the Applicant requests a Certificate that will contain the countryName field and other Subject
28 Identity Information, then the CA SHALL verify the identity of the Applicant, and the authenticity of the Applicant
29 Representative's certificate request using a verification process meeting the requirements of this Section 11.2 and
30 that is described in the CA's Certificate Policy and/or Certification Practice Statement. The CA SHALL inspect any
31 document relied upon under this Section for alteration or falsification.

32 **11.2.1 Identity**

33 If the Subject Identity Information is to include the name or address of an organization, the CA SHALL verify the
34 identity and address of the organization and that the address is the Applicant's address of existence or operation.
35 The CA SHALL verify the identity and address of the Applicant using documentation provided by, or through
36 communication with, at least one of the following:

- 37 1. A government agency in the jurisdiction of the Applicant's legal creation, existence, or recognition;
- 38 2. A third party database that is periodically updated, which the CA has evaluated in accordance with Section
39 11.6;
- 40 3. A site visit by the CA or a third party who is acting as an agent for the CA; or
- 41 4. An Attestation Letter.

42 The CA MAY use the same documentation or communication described in 1 through 4 above to verify both the
43 Applicant's identity and address.

44 Alternatively, the CA MAY verify the address of the Applicant (but not the identity of the Applicant) using a utility
45 bill, bank statement, credit card statement, government-issued tax document, or other form of identification that
46 meets the requirements of Section 11.6.

1 **11.2.2 DBA/Tradename**

2 If the Subject Identity Information is to include a DBA or tradename, the CA SHALL verify the Applicant’s right to
3 use the DBA/tradename using at least one of the following:

- 4 1. Documentation provided by, or communication with, a government agency in the jurisdiction of the
5 Applicant’s legal creation, existence, or recognition;
- 6 2. Documentation or communication provided by a third party source that meets the requirements of Section
7 11.6;
- 8 3. Communication with a government agency responsible for the management of such DBAs or tradenames;
- 9 4. An Attestation Letter accompanied by documentary support that meets the requirements of Section 11.6; or
- 10 5. A utility bill, bank statement, credit card statement, government-issued tax document, or other form of
11 identification that meets the requirements of Section 11.6.

12 **11.2.3 Authenticity of Certificate Request**

13 If the Applicant for a Certificate containing Subject Identity Information is an organization, the CA SHALL use a
14 Reliable Method of Communication to verify the authenticity of the Applicant Representative’s certificate request.

15 The CA MAY use the sources listed in section 11.2.1 to verify the Reliable Method of Communication. Provided
16 that the CA uses a Reliable Method of Communication, the CA MAY establish the authenticity of the certificate
17 request directly with the Applicant Representative or with an authoritative source within the Applicant’s
18 organization, such as the Applicant’s main business offices, corporate offices, human resource offices, information
19 technology offices, or other department that the CA deems appropriate.

20 In addition, the CA SHALL establish a process that allows an Applicant to specify the individuals who may request
21 Certificates. If an Applicant specifies, in writing, the individuals who may request a Certificate, then the CA
22 SHALL NOT accept any certificate requests that are outside this specification. The CA SHALL provide an
23 Applicant with a list of its authorized certificate requesters upon the Applicant’s verified written request.

24 **11.2.4 Verification of Individual Applicant**

25 If an Applicant subject to this Section 11.2 is a natural person, then the CA SHALL verify the Applicant’s name,
26 Applicant’s address, and the authenticity of the certificate request.

27 The CA SHALL verify the Applicant’s name using a legible copy, which discernibly shows the Applicant’s face, of
28 at least one currently valid government-issued photo ID (passport, drivers license, military ID, national ID, or
29 equivalent document type). The CA SHALL inspect the copy for any indication of alteration or falsification.

30 The CA SHALL verify the Applicant’s address using a form of identification that meets Section 11.6, such as a
31 government ID, utility bill, or bank or credit card statement. The CA MAY rely on the same government-issued ID
32 that was used to verify the Applicant’s name.

33 The CA SHALL verify the certificate request with the Applicant using a Reliable Method of Communication.

34 **11.2.5 Verification of Country**

35 If the subject:countryName field is present, then the CA SHALL verify the country associated with the Subject
36 using one of the following: (a) the IP Address range assignment by country for either (i) the web site’s IP address, as
37 indicated by the DNS record for the web site or (ii) the Applicant’s IP address; (b) the ccTLD of the requested
38 Domain Name; (c) information provided by the Domain Name Registrar; or (d) a method identified in Section
39 11.2.1. The CA SHOULD implement a process to screen proxy servers in order to prevent reliance upon IP
40 addresses assigned in countries other than where the Applicant is actually located.

41 **11.3 Age of Certificate Data**

42 Section 9.4 limits the validity period of Subscriber Certificates. The CA SHALL NOT use any data or document to
43 validate a certificate request if the data or document was obtained more than thirty-nine (39) months prior to the
44 Certificates’ issuance.

1 **11.4 *Denied List***

2 In accordance with Section 15.3.2, the CA SHALL maintain an internal database of all previously revoked
3 Certificates and previously rejected certificate requests due to suspected phishing or other fraudulent usage or
4 concerns. The CA SHALL use this information to identify subsequent suspicious certificate requests.

5 **11.5 *High Risk Requests***

6 The CA SHALL identify high risk certificate requests, and conduct such additional verification activity, and take
7 such additional precautions, as are reasonably necessary to ensure that such requests are properly verified under
8 these Requirements.

9 The CA MAY identify high risk requests by checking appropriate lists of organization names that are most
10 commonly targeted in phishing and other fraudulent schemes, and by automatically flagging certificate requests that
11 match these lists for further scrutiny before issuance. Examples of such lists include: internal databases maintained
12 by the CA that include previously revoked Certificates and previously rejected certificate requests due to suspected
13 phishing or other fraudulent usage.

14 The CA SHALL use information identified by the CA’s high-risk criteria to flag suspicious certificate requests. The
15 CA SHALL follow a documented procedure for performing additional verification of any certificate request flagged
16 as suspicious or high risk.

17 **11.6 *Data Source Accuracy***

18 Before relying on a data source to verify Subject Identity Information, the CA SHALL evaluate the data source’s
19 accuracy and reliability. The CA SHALL NOT use a data source to verify Subject Identity Information if the CA’s
20 evaluation determines that the data source is not reasonably accurate or reliable.

21 **12. Certificate Issuance by a Root CA**

22 Certificate issuance by the Root CA SHALL require an individual authorized by the CA (i.e. the CA system
23 operator, system officer, or PKI administrator) to deliberately issue a direct command in order for the Root CA to
24 perform a certificate signing operation.

25 Root CA Private Keys MUST NOT be used to sign Certificates except in the following cases:

- 26 1. Self-signed Certificates to represent the Root CA itself;
- 27 2. Certificates for Subordinate CAs and Cross Certificates;
- 28 3. Certificates for infrastructure purposes (e.g. administrative role certificates, internal CA operational device
29 certificates, and OCSP Response verification Certificates);
- 30 4. Certificates issued solely for the purpose of testing products with Certificates issued by a Root CA; and
- 31 5. Subscriber Certificates, provided that:
- 32 a. The Root CA uses a 1024-bit RSA signing key that was created prior to the Effective Date;
- 33 b. The Applicant’s application was deployed prior to the Effective Date;
- 34 c. The Applicant’s application is in active use by the Applicant or the CA uses a documented
35 process to establish that the Certificate’s use is required by a substantial number of Relying
36 Parties;
- 37 d. The CA follows a documented process to determine that the Applicant’s application poses no
38 known security risks to Relying Parties; and
- 39 e. The CA documents that the Applicant’s application cannot be patched or replaced without
40 substantial economic outlay.

13. Certificate Revocation and Status Checking

13.1 Revocation

13.1.1 Revocation Request

The CA SHALL 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 SHALL maintain a continuous 24x7 ability to accept and respond to revocation requests and related inquiries.

13.1.2 Certificate Problem Reporting

The CA SHALL 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 SHALL publicly disclose the instructions through a readily accessible online means.

13.1.3 Investigation

The CA SHALL 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 entity making the complaint (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.

13.1.4 Response

The CA SHALL 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.

13.1.5 Reasons for Revocation

The CA SHALL revoke a Certificate within 24 hours if one or more of the following occurs:

1. The Subscriber requests in writing that the CA revoke the Certificate;
2. The Subscriber notifies the CA that the original certificate request was not authorized and does not retroactively grant authorization;
3. The CA obtains 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 is made aware that a Subscriber has violated one or more of its material obligations under the Subscriber or Terms of Use Agreement;
5. The CA is made 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 is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name;

- 1 7. The CA is made aware of a material change in the information contained in the Certificate;
- 2 8. The CA is made aware that the Certificate was not issued in accordance with these Requirements or the
- 3 CA's Certificate Policy or Certification Practice Statement;
- 4 9. The CA determines that any of the information appearing in the Certificate is inaccurate or misleading;
- 5 10. The CA ceases operations for any reason and has not made arrangements for another CA to provide
- 6 revocation support for the Certificate;
- 7 11. The CA's right to issue Certificates under these Requirements expires or is revoked or terminated, unless
- 8 the CA has made arrangements to continue maintaining the CRL/OCSP Repository;
- 9 12. The CA is made aware of a possible compromise of the Private Key of the Subordinate CA used for issuing
- 10 the Certificate;
- 11 13. Revocation is required by the CA's Certificate Policy and/or Certification Practice Statement; or
- 12 14. The technical content or format of the Certificate presents an unacceptable risk to Application Software
- 13 Suppliers or Relying Parties (e.g. the CA/Browser Forum might determine that a deprecated
- 14 cryptographic/signature algorithm or key size presents an unacceptable risk and that such Certificates
- 15 should be revoked and replaced by CAs within a given period of time).

16 **13.2 Certificate Status Checking**

17 **13.2.1 Mechanisms**

18 The CA SHALL make revocation information for Subordinate Certificates and Subscriber Certificates available in
19 accordance with Appendix B.

20 If the Subscriber Certificate is for a high-traffic FQDN, the CA MAY rely on stapling, in accordance with
21 [RFC4366], to distribute its OCSP responses. In this case, the CA SHALL ensure that the Subscriber "staples" the
22 OCSP response for the Certificate in its TLS handshake. The CA SHALL enforce this requirement on the
23 Subscriber either contractually, through the Subscriber or Terms of Use Agreement, or by technical review measures
24 implement by the CA.

25 **13.2.2 Repository**

26 The CA SHALL maintain an online 24x7 Repository that application software can use to automatically check the
27 current status of all unexpired Certificates issued by the CA.

28 For the status of Subscriber Certificates:

- 29 1. If the CA publishes a CRL, then the CA SHALL update and reissue CRLs at least once every seven days,
30 and the value of the nextUpdate field MUST NOT be more than ten days beyond the value of the
31 thisUpdate field; and
- 32 2. The CA SHALL update information provided via an Online Certificate Status Protocol at least every four
33 days. OCSP responses from this service MUST have a maximum expiration time of ten days.

34 For the status of Subordinate CA Certificates:

- 35 1. The CA SHALL update and reissue CRLs at least (i) once every twelve months and (ii) within 24 hours
36 after revoking a Subordinate CA Certificate, and the value of the nextUpdate field MUST NOT be more
37 than twelve months beyond the value of the thisUpdate field; and
- 38 2. The CA SHALL update information provided via an Online Certificate Status Protocol at least (i) every
39 twelve months and (ii) within 24 hours after revoking a Subordinate CA Certificate.

40 Effective 1 January 2013, the CA SHALL support an OCSP capability using the GET method for Certificates issued
41 in accordance with these Requirements.

13.2.3 Response Time

The CA SHALL operate and maintain its CRL and OCSP capability with resources sufficient to provide a response time of ten seconds or less under normal operating conditions.

13.2.4 Deletion of Entries

Revocation entries on a CRL or OCSP Response MUST NOT be removed until after the Expiry Date of the revoked Certificate.

13.2.5 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.

14. Employees and Third Parties

14.1 *Trustworthiness and Competence*

14.1.1 Identity and Background Verification

Prior to the engagement of any person in the Certificate Management Process, whether as an employee, agent, or an independent contractor of the CA, the CA SHALL verify the identity and trustworthiness of such person.

14.1.2 Training and Skill Level

The CA SHALL 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 and/or Certification Practice Statement), common threats to the information verification process (including phishing and other social engineering tactics), and these Requirements.

The CA SHALL 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 SHALL maintain skill levels consistent with the CA's training and performance programs.

The CA SHALL document that each Validation Specialist possesses the skills required by a task before allowing the Validation Specialist to perform that task.

The CA SHALL require all Validation Specialists to pass an examination provided by the CA on the information verification requirements outlined in these Requirements.

14.2 *Delegation of Functions*

14.2.1 General

The CA MAY delegate the performance of all, or any part, of Section 11 of these Requirements to a Delegated Third Party, provided that the process as a whole fulfills all of the requirements of Section 11.

Before the CA authorizes a Delegated Third Party to perform a delegated function, the CA SHALL contractually require the Delegated Third Party to:

- 1) Meet the qualification requirements of Section 14.1, when applicable to the delegated function;
- 2) Retain documentation in accordance with Section 15.3.2;

- 1 3) Abide by the other provisions of these Requirements that are applicable to the delegated function; and
2 4) Comply with (a) the CA’s Certificate Policy/Certification Practice Statement or (b) the Delegated Third
3 Party’s practice statement that the CA has verified complies with these Requirements.

4 The CA SHALL verify that the Delegated Third Party’s personnel involved in the issuance of a Certificate meet the
5 training and skills requirements of Section 14 and the document retention and event logging requirements of Section
6 15.

7 **14.2.2 Compliance Obligation**

8 The CA SHALL internally audit each Delegated Third Party’s compliance with these Requirements on an annual
9 basis.

10 **14.2.3 Allocation of Liability**

11 For delegated tasks, the CA and any Delegated Third Party MAY allocate liability between themselves contractually
12 as they determine, but the CA SHALL remain fully responsible for the performance of all parties in accordance with
13 these Requirements, as if the tasks had not been delegated.

14 **14.2.4 Enterprise RAs**

15 The CA MAY designate an Enterprise RA to verify certificate requests from the Enterprise RA’s own organization.

16 The CA SHALL NOT accept certificate requests authorized by an Enterprise RA unless the following requirements
17 are satisfied:

- 18 1. The CA SHALL confirm that the requested Fully-Qualified Domain Name(s) are within the Enterprise
19 RA’s verified Domain Namespace (see Section 7.1.2 para 1).
20 2. If the certificate request includes a Subject name of a type other than a Fully-Qualified Domain Name, the
21 CA SHALL confirm that the name is either that of the delegated enterprise, or an Affiliate of the delegated
22 enterprise, or that the delegated enterprise is an agent of the named Subject. For example, the CA SHALL
23 NOT issue a Certificate containing the Subject name “XYZ Co.” on the authority of Enterprise RA “ABC
24 Co.”, unless the two companies are affiliated (see Section 11.1) or “ABC Co.” is the agent of “XYZ Co.”.
25 This requirement applies regardless of whether the accompanying requested Subject FQDN falls within the
26 Domain Namespace of ABC Co.’s Registered Domain Name.

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

29 **15. Data Records**

30 **15.1 Documentation and Event Logging**

31 The CA and each Delegated Third Party SHALL record details of the actions taken to process a certificate request
32 and to issue a Certificate, including all information generated and documentation received in connection with the
33 certificate request; the time and date; and the personnel involved. The CA SHALL make these records available to
34 its Qualified Auditor as proof of the CA’s compliance with these Requirements.

35 **15.2 Events and Actions**

36 The CA SHALL record at least the following events:

- 37 1. CA key lifecycle management events, including:
38 a. Key generation, backup, storage, recovery, archival, and destruction; and
39 b. Cryptographic device lifecycle management events.
40 2. CA and Subscriber Certificate lifecycle management events, including:

- 1 a. Certificate requests, renewal, and re-key requests, and revocation;
- 2 b. All verification activities stipulated in these Requirements and the CA's Certification Practice
- 3 Statement;
- 4 c. Date, time, phone number used, persons spoken to, and end results of verification telephone calls;
- 5 d. Acceptance and rejection of certificate requests;
- 6 e. Issuance of Certificates; and
- 7 f. Generation of Certificate Revocation Lists and OCSP entries.
- 8 3. Security events, including:
 - 9 a. Successful and unsuccessful PKI system access attempts;
 - 10 b. PKI and security system actions performed;
 - 11 c. Security profile changes;
 - 12 d. System crashes, hardware failures, and other anomalies;
 - 13 e. Firewall and router activities; and
 - 14 f. Entries to and exits from the CA facility.

15 Log entries MUST include the following elements:

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

19 **15.3 Retention**

20 **15.3.1 Audit Log Retention**

21 The CA SHALL retain any audit logs generated after the Effective Date for at least seven years. The CA SHALL
22 make these audit logs available to its Qualified Auditor upon request.

23 **15.3.2 Documentation Retention**

24 The CA SHALL retain all documentation relating to certificate requests and the verification thereof, and all
25 Certificates and revocation thereof, for at least seven years after any Certificate based on that documentation ceases
26 to be valid.

27 **16. Data Security**

28 **16.1 Objectives**

29 The CA SHALL develop, implement, and maintain a comprehensive security program designed to:

- 30 1. Protect the confidentiality, integrity, and availability of Certificate Data and Certificate Management
- 31 Processes;
- 32 2. Protect against anticipated threats or hazards to the confidentiality, integrity, and availability of the
- 33 Certificate Data and Certificate Management Processes;
- 34 3. Protect against unauthorized or unlawful access, use, disclosure, alteration, or destruction of any Certificate
- 35 Data or Certificate Management Processes;
- 36 4. Protect against accidental loss or destruction of, or damage to, any Certificate Data or Certificate
- 37 Management Processes; and

1 5. Comply with all other security requirements applicable to the CA by law.

2 **16.2 Risk Assessment**

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

- 4 1. Identifies foreseeable internal and external threats that could result in unauthorized access, disclosure,
5 misuse, alteration, or destruction of any Certificate Data or Certificate Management Processes;
- 6 2. Assesses the likelihood and potential damage of these threats, taking into consideration the sensitivity of
7 the Certificate Data and Certificate Management Processes; and
- 8 3. Assesses the sufficiency of the policies, procedures, information systems, technology, and other
9 arrangements that the CA has in place to counter such threats.

10 **16.3 Security Plan**

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

19 **16.4 Business Continuity**

20 In addition, the CA SHALL document a business continuity and disaster recovery procedures designed to notify and
21 reasonably protect Application Software Suppliers, Subscribers, and Relying Parties in the event of a disaster,
22 security compromise, or business failure. The CA is not required to publicly disclose its business continuity plans
23 but SHALL make the business continuity plan and security plan of Section 15.3 available to the CA's auditors upon
24 request. The CA SHALL annually test, review, and update these procedures.

25 The business continuity plan MUST include:

- 26 1. The conditions for activating the plan,
- 27 2. Emergency procedures,
- 28 3. Fallback procedures,
- 29 4. Resumption procedures,
- 30 5. A maintenance schedule for the plan;
- 31 6. Awareness and education requirements;
- 32 7. The responsibilities of the individuals;
- 33 8. Recovery time objective (RTO);
- 34 9. Regular testing of contingency plans.
- 35 10. The CA's plan to maintain or restore the CA's business operations in a timely manner following
36 interruption to or failure of critical business processes
- 37 11. A requirement to store critical cryptographic materials (i.e., secure cryptographic device and activation
38 materials) at an alternate location;
- 39 12. What constitutes an acceptable system outage and recovery time
- 40 13. How frequently backup copies of essential business information and software are taken;
- 41 14. The distance of recovery facilities to the CA's main site; and
- 42 15. Procedures for securing its facility to the extent possible during the period of time following a disaster and
43 prior to restoring a secure environment either at the original or a remote site.

1 **16.5 System Security**¹

2 The Certificate Management Process MUST include:

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

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

10 **16.6 Private Key Protection**

11 The CA SHALL protect its Private Key in a system or device that has been validated as meeting at least FIPS 140
12 level 3 or an appropriate Common Criteria Protection Profile or Security Target, EAL 4 (or higher), which includes
13 requirements to protect the Private Key and other assets against known threats. The CA SHALL implement physical
14 and logical safeguards to prevent unauthorized certificate issuance. Protection of the Private Key outside the
15 validated system or device specified above MUST consist of physical security, encryption, or a combination of both,
16 implemented in a manner that prevents disclosure of the Private Key. The CA SHALL encrypt its Private Key with
17 an algorithm and key-length that, according to the state of the art, are capable of withstanding cryptanalytic attacks
18 for the residual life of the encrypted key or key part. The Private Key SHALL be backed up, stored, and recovered
19 only by personnel in trusted roles using, at least, dual control in a physically secured environment.

20 **17. Audit**

21 **17.1 Eligible Audit Schemes**

22 The CA SHALL undergo an audit in accordance with one of the following schemes:

- 23 1. WebTrust for Certification Authorities v2.0 or later;
- 24 2. A national scheme that audits conformance to ETSI TS 101 456 v1.2.1 or later;
- 25 3. A national scheme that audits conformance to ETSI TS 102 042 V1.1.1 or later;
- 26 4. A scheme that audits conformance to ISO 21188:2006, completed by a Qualified Auditor; or
- 27 5. If a Government CA is required by its Certificate Policy to use a different internal audit scheme, it may use
28 such scheme provided that: (a) the audit either (i) encompasses all requirements of one of the above
29 schemes or (ii) consists of comparable criteria that are available for public review, and (b) the audit is
30 performed by a Qualified Auditor, who is separate from the CA and who meets the requirements of Section
31 17.6.

32 **17.2 Audit Period**

33 The period during which the CA issues Certificates SHALL be divided into an unbroken sequence of audit periods.
34 An audit period MUST NOT exceed one year in duration.

35 **17.3 Audit Report**

36 The CA SHALL make the Audit Report publicly available. The CA is not required to make publicly available any
37 general audit findings that do not impact the overall audit opinion. For both government and commercial CAs, the
38 CA SHOULD make its Audit Report publicly available no later than three months after the end of the audit period.

¹ The CA/Browser Forum will enact additional security requirements after the adoption of v1.0 of the Requirements.

1 In the event of a delay greater than three months, and if so requested by an Application Software Supplier, the CA
2 SHALL provide an explanatory letter signed by the Qualified Auditor.

3 **17.4 Pre-Issuance Readiness Audit**

4 If the CA has a currently valid Audit Report indicating compliance with an audit scheme listed in Section 17.1, then
5 no pre-issuance readiness assessment is necessary.

6 If the CA does not have a currently valid Audit Report indicating compliance with one of the audit schemes listed in
7 Section 17.1, then, before issuing Publicly-Trusted Certificates, the CA SHALL successfully complete a point-in-
8 time readiness assessment performed in accordance with applicable standards under one of the audit schemes listed
9 in Section 17.1. The point-in-time readiness assessment SHALL be completed no earlier than twelve (12) months
10 prior to issuing Publicly-Trusted Certificates and SHALL be followed by a complete audit under such scheme
11 within ninety (90) days of issuing the first Publicly-Trusted Certificate.

12 **17.5 Audit of Delegated Functions**

13 If a Delegated Third Party is not currently audited in accordance with Section 17 and is not an Enterprise RA, then
14 prior to certificate issuance the CA SHALL ensure that the domain control validation process required under Section
15 11.1 has been properly performed by the Delegated Third Party by either (1) using an out-of-band mechanism
16 involving at least one human who is acting either on behalf of the CA or on behalf of the Delegated Third Party to
17 confirm the authenticity of the certificate request or the information supporting the certificate request or (2)
18 performing the domain control validation process itself.

19 If the CA is not using one of the above procedures and the Delegated Third Party is not an Enterprise RA, then the
20 CA SHALL obtain an audit report, issued under the auditing standards that underlie the accepted audit schemes
21 found in Section 17.1, that provides an opinion whether the Delegated Third Party's performance complies with
22 either the Delegated Third Party's practice statement or the CA's Certificate Policy and/or Certification Practice
23 Statement. If the opinion is that the Delegated Third Party does not comply, then the CA SHALL not allow the
24 Delegated Third Party to continue performing delegated functions.

25 The audit period for the Delegated Third Party SHALL NOT exceed one year (ideally aligned with the CA's audit).
26 However, if the CA or Delegated Third Party is under the operation, control, or supervision of a Government Entity
27 and the audit scheme is completed over multiple years, then the annual audit MUST cover at least the core controls
28 that are required to be audited annually by such scheme plus that portion of all non-core controls that are allowed to
29 be conducted less frequently, but in no case may any non-core control be audited less often than once every three
30 years.

31 **17.6 Auditor Qualifications**

32 The CA's audit SHALL be performed by a Qualified Auditor. A Qualified Auditor means a natural person, Legal
33 Entity, or group of natural persons or Legal Entities that collectively possess the following qualifications and skills:
34

- 35 1. Independence from the subject of the audit;
- 36 2. The ability to conduct an audit that addresses the criteria specified in an Eligible Audit Scheme;
- 37 3. Employs individuals who have proficiency in examining Public Key Infrastructure technology, information
38 security tools and techniques, information technology and security auditing, and the third-party attestation
39 function;
- 40 4. Certified, accredited, licensed, or otherwise assessed as meeting the qualification requirements of auditors
41 under the audit scheme;
- 42 5. Bound by law, government regulation, or professional code of ethics; and
- 43 6. Except in the case of an Internal Government Auditing Agency, maintains Professional Liability/Errors &
44 Omissions insurance with policy limits of at least one million US dollars in coverage.

17.7 Key Generation Ceremony

For Root CA Key Pairs created after the Effective Date that are either (i) used as Root CA Key Pairs or (ii) Key Pairs generated for a subordinate CA that is not the operator of the Root CA or an Affiliate of the Root CA, the CA SHALL:

1. prepare and follow a Key Generation Script,
2. have a Qualified Auditor witness the Root CA Key Pair generation process or record a video of the entire Root CA Key Pair generation process, and
3. have a Qualified Auditor issue a report opining that the CA followed its key ceremony during its Key and Certificate generation process and the controls used to ensure the integrity and confidentiality of the Key Pair.

For other CA Key Pairs created after the Effective Date that are for the operator of the Root CA or an Affiliate of the Root CA, the CA SHOULD:

1. prepare and follow a Key Generation Script and
2. have a Qualified Auditor witness the Root CA Key Pair generation process or record a video of the entire Root CA Key Pair generation process.

In all cases, the CA SHALL:

1. generate the keys in a physically secured environment as described in the CA's Certificate Policy and/or Certification Practice Statement;
2. generate the CA keys using personnel in trusted roles under the principles of multiple person control and split knowledge;
3. generate the CA keys within cryptographic modules meeting the applicable technical and business requirements as disclosed in the CA's Certificate Policy and/or Certification Practice Statement;
4. log its CA key generation activities; and
5. maintain effective controls to provide reasonable assurance that the Private Key was generated and protected in conformance with the procedures described in its Certificate Policy and/or Certification Practice Statement and (if applicable) its Key Generation Script.

17.8 Regular Quality Assessment Self Audits

During the period in which the CA issues Certificates, the CA SHALL 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 Delegated Third Parties that undergo an annual audit that meets the criteria specified in Section 16.3, the CA SHALL strictly control the service quality of Certificates issued or containing information verified by a Delegated Third Party by having a Validation Specialist employed by the CA perform ongoing quarterly audits against a randomly selected sample of at least the greater of one certificate or three percent of the Certificates verified by the Delegated Third Party in the period beginning immediately after the last sample was taken. The CA SHALL review each Delegated Third Party's practices and procedures to ensure that the Delegated Third Party is in compliance with these Requirements and the relevant Certificate Policy and/or Certification Practice Statement.

18. Liability and Indemnification

18.1 Liability to Subscribers and Relying Parties

If the CA has issued and managed the Certificate in compliance with these Requirements and its Certificate Policy and/or 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 and/or Certification Practice Statement. If the CA has not issued or managed the Certificate

1 in compliance with these Requirements and its Certificate Policy and/or Certification Practice Statement, the CA
2 MAY seek to limit its liability to the Subscriber and to Relying Parties, regardless of the cause of action or legal
3 theory involved, for any and all claims, losses or damages suffered as a result of the use or reliance on such
4 Certificate by any appropriate means that the CA desires. If the CA chooses to limit its liability for Certificates that
5 are not issued or managed in compliance with these Requirements or its Certificate Policy and/or Certification
6 Practice Statement, then the CA SHALL include the limitations on liability in the CA's Certificate Policy and/or
7 Certification Practice Statement.

8 **18.2 Indemnification of Application Software Suppliers**

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

22 **18.3 Root CA Obligations**

23 The Root CA SHALL be responsible for the performance and warranties of the Subordinate CA, for the Subordinate
24 CA's compliance with these Requirements, and for all liabilities and indemnification obligations of the Subordinate
25 CA under these Requirements, as if the Root CA were the Subordinate CA issuing the Certificates.

26

1

2 **Appendix A - Cryptographic Algorithm and Key Requirements** 3 **(Normative)**

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

5 **(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), SHA-1, SHA-256, SHA-384 or SHA-512	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

6

7 **(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-256, SHA-384 or SHA-512	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

8

9 **(3) Subscriber Certificates**

	Validity period <u>ending</u> on or before 31 Dec 2013	Validity period <u>ending</u> 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

10

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

13 ** A Root CA Certificate issued prior to 31 Dec. 2010 with an RSA key size less than 2048 bits MAY still serve as
14 a trust anchor for Subscriber Certificates issued in accordance with these Requirements .

1 **Appendix B – Certificate Extensions (Normative)**

2 This appendix specifies the requirements for Certificate extensions for Certificates generated after the Effective
3 Date.

4 **Root CA Certificate**

5 Root Certificates MUST be of type X.509 v3.

6 **A. basicConstraints**

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

9 **B. keyUsage**

10 This extension MUST be present and MUST be marked critical. Bit positions for keyCertSign and
11 cRLSign MUST be set. If the Root CA Private Key is used for signing OCSP responses, then the
12 digitalSignature bit MUST be set.

13 **C. certificatePolicies**

14 This extension SHOULD NOT be present.

15 **D. extendedKeyUsage**

16 This extension MUST NOT be present.

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

18 **Subordinate CA Certificate**

19 Subordinate CA Certificates MUST be of type X.509 v3.

20 **A. certificatePolicies**

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

22 certificatePolicies:policyIdentifier (Required)

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

25 certificatePolicies:policyQualifiers:policyQualifierId (Optional)

- 26 • id-qt 1 [RFC 5280].

27 certificatePolicies:policyQualifiers:qualifier:cPSuri (Optional)

- 28 • HTTP URL for the Root CA's Certificate Policies, Certification Practice Statement, Relying Party
29 Agreement, or other pointer to online policy information provided by the CA.

30 **B. cRLDistributionPoints**

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

33 **C. authorityInformationAccess**

34 With the exception of stapling, which is noted below, this extension MUST be present. It MUST NOT be
35 marked critical, and it MUST contain the HTTP URL of the Issuing CA's OCSP responder (accessMethod
36 = 1.3.6.1.5.5.7.48.1). It SHOULD also contain the HTTP URL of the Issuing CA's certificate
37 (accessMethod = 1.3.6.1.5.5.7.48.2). See Section 13.2.1 for details.

38 The HTTP URL of the Issuing CA's OCSP responder MAY be omitted, provided that the Subscriber
39 "staples" the OCSP response for the Certificate in its TLS handshakes [RFC4366].

1 **D. basicConstraints**

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

4 **E. keyUsage**

5 This extension **MUST** be present and **MUST** be marked critical. Bit positions for `keyCertSign` and
6 `cRLSign` **MUST** be set. If the Subordinate CA Private Key is used for signing OCSP responses, then the
7 `digitalSignature` bit **MUST** be set.

8 All other fields and extensions **MUST** be set in accordance to RFC 5280.

9 **Subscriber Certificate**

10 **A. certificatePolicies**

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

12 `certificatePolicies:policyIdentifier` (Required)

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

15 The following extensions **MAY** be present:

16 `certificatePolicies:policyQualifiers:policyQualifierId` (Recommended)

- 17 • `id-qt 1` [RFC 5280].

18 `certificatePolicies:policyQualifiers:qualifier:cPSuri` (Optional)

- 19 • HTTP URL for the Subordinate CA's Certification Practice Statement, Relying Party Agreement
20 or other pointer to online information provided by the CA.

21 **B. cRLDistributionPoints**

22 This extension **MAY** be present. If present, it **MUST NOT** be marked critical, and it **MUST** contain the
23 HTTP URL of the CA's CRL service. See Section 13.2.1 for details.

24 **C. authorityInformationAccess**

25 With the exception of stapling, which is noted below, this extension **MUST** be present. It **MUST NOT** be
26 marked critical, and it **MUST** contain the HTTP URL of the Issuing CA's OCSP responder (`accessMethod`
27 = 1.3.6.1.5.5.7.48.1). It **SHOULD** also contain the HTTP URL of the Issuing CA's certificate
28 (`accessMethod` = 1.3.6.1.5.5.7.48.2). See Section 13.2.1 for details.

29 The HTTP URL of the Issuing CA's OCSP responder **MAY** be omitted provided that the Subscriber
30 "staples" OCSP responses for the Certificate in its TLS handshakes [RFC4366].

31 **D. basicConstraints (optional)**

32 If present, the `cA` field **MUST** be set false.

33 **E. keyUsage (optional)**

34 If present, bit positions for `keyCertSign` and `cRLSign` **MUST NOT** be set.

35 **F. extKeyUsage (required)**

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

38 All other fields and extensions **MUST** be set in accordance to RFC 5280.

1 **Appendix C - User Agent Verification (Normative)**

2 The CA SHALL host test Web pages that allow Application Software Suppliers to test their software with
3 Subscriber Certificates that chain up to each publicly trusted Root Certificate. At a minimum, the CA SHALL host
4 separate Web pages using Subscriber Certificates that are (i) valid, (ii) revoked, and (iii) expired.

5