CA/Browser Forum

Guidelines For The Issuance And Management Of Extended Validation Certificates

Guidelines for the Issuance and Management of Extended Validation Certificates

This version 1.5.~~6~~ 7 represents the Extended Validation Guidelines, as adopted by the CA/Browser Forum as of Ballot1~~47~~51, passed by the Forum on 2~~85~~ ~~June~~ September 2015.

The Guidelines describe an integrated set of technologies, protocols, identity proofing, lifecycle management, and auditing practices specifying the minimum requirements that must be met in order to issue and maintain Extended Validation Certificates ("EV Certificates") concerning an organization. Subject Organization information from valid EV Certificates can then be used in a special manner by certain relying-party software applications (e.g., browser software) in order to provide users with a trustworthy confirmation of the identity of the entity that controls the Web site or other services they are accessing. Although initially intended for use in establishing Web-based data communication conduits via TLS/SSL protocols, extensions are envisioned for S/MIME, time-stamping, VoIP, IM, Web services, etc.

The primary purposes of Extended Validation Certificates are to: 1) identify the legal entity that controls a Web or service site, and 2) enable encrypted communications with that site. The secondary purposes include significantly enhancing cybersecurity by helping establish the legitimacy of an organization claiming to operate a Web site, and providing a vehicle that can be used to assist in addressing problems related to distributing malware, phishing, identity theft, and diverse forms of online fraud.

Notice to Readers

The Guidelines for the Issuance and Management of Extended Validation Certificates present criteria established by the CA/Browser Forum for use by certification authorities when issuing, maintaining, and revoking certain digital certificates for use in Internet Web site commerce. These Guidelines may be revised from time to time, as appropriate, in accordance with procedures adopted by the CA/Browser Forum. Questions or suggestions concerning these guidelines may be directed to the CA/Browser Forum at questions@cabforum.org.

The CA/Browser Forum

The CA/Browser Forum is a voluntary open organization of certification authorities and suppliers of Internet browsers and other relying-party software applications. Membership is listed at https://cabforum.org/members/.

Document History

Ver.	Ballot	Description	Adopted	Effective*
1.4.0	72	Reorganize EV Documents	29 May 2012	29 May 2012
1.4.1	75	NameConstraints Criticality Flag	8 June 2012	8 June 2012
1.4.2	101	EV 11.10.2 Accountants	31 May 2013	31 May 2013
1.4.3	104	Domain verification for EV Certificates	9 July 2013	9 July 2013
1.4.4	113	Revision to QIIS in EV Guidelines	13 Jan 2014	13 Jan 2014
1.4.5	114	Improvements to the EV Definitions	28 Jan 2014	28 Jan 2014
1.4.6	119	Remove "OfIncorporation" from OID descriptions in EVG 9.2.5	24 Mar 2014	24 Mar 2014
1.4.7	120	Affiliate Authority to Verify Domain	5 June 2014	5 June 2014
1.4.8	124	Business Entity Clarification	5 June 2014	5 June 2014
1.4.9	127	Verification of Name, Title and Agency	17 July 2014	17 July 2014
1.5.0	126	Operational Existence	24 July 2014	24 July 2014
1.5.1	131	Verified Method of Communication	12 Sept 2014	12 Sept 2014
1.5.2	123	Reuse of Information	16 Oct. 2014	16 Oct. 2014
1.5.3	144	Validation rules for .onion names	18 Feb. 2015	18 Feb. 2015
1.5.4	146	Convert Baseline Requirements to RFC 3647 Framework	16 Apr. 2015	16 Apr. 2015
1.5.5	145	Operational Existence for Government Entities	5 Mar. 2015	5 Mar. 2015
1.5.6	147	Attorney-Accountant Letter Changes	25 June 2015	25 June 2015
1.5.7	151	Addition of Optional OIDs for Indicating Level of Validation	28 Sept 2015	28 Sept 2015

Implementers' Note: Version 1.3 of these EV Guidelines was published on 20 November 2010 and supplemented through May 2012 when version 1.4 was published. ETSI TS 102 042 and ETSI TR 101 564 Technical Report: Guidance on ETSI TS 102 042 for Issuing Extended Validation Certificates for Auditors and CSPs reference version 1.3 of these EV Guidelines, and ETSI Draft EN 319 411-1 references version 1.4. Version 1.4.5 of Webtrust® For Certification Authorities – Extended Validation Audit Criteria references version 1.4.5 of these EV Guidelines. As illustrated in the Document History table above, the CA/Browser Forum continues to improve relevant industry guidelines, including this document, the Baseline Requirements, and the Network and Certificate System Security Requirements. We encourage all CAs to conform to each revision on the date specified without awaiting a corresponding update to an applicable audit criterion. In the event of a conflict between an existing audit criterion and a guideline revision, we will communicate with the audit community and attempt to resolve any uncertainty. We will respond to implementation questions directed to questions@cabforum.org. Our coordination with compliance auditors will continue as we develop guideline revision cycles that harmonize with the revision cycles for audit criteria, the compliance auditing periods and cycles of CAs, and the CA/Browser Forum's guideline implementation dates.

TABLE OF CONTENTS

1. Scope 1

2. Purpose 1

2.1. Purpose of EV Certificates 1

2.1.1. Primary Purposes 1

2.1.2. Secondary Purposes 1

2.1.3. Excluded Purposes 1

3. References 2

4. Definitions 2

5. Abbreviations and Acronyms 5

6. Conventions 5

7. Certificate Warranties and Representations 6

7.1. EV Certificate Warranties 6

7.2. By the Applicant 6

8. Community and Applicability 6

8.1. Issuance of EV Certificates 6

8.2. EV Policies 7

8.2.1. Implementation 7

8.2.2. Disclosure 7

8.3. Commitment to Comply with Recommendations 7

8.4. Insurance 7

8.5. Obtaining EV Certificates 8

8.5.1. General 8

8.5.2. Private Organization Subjects 8

8.5.3. Government Entity Subjects 8

8.5.4. Business Entity Subjects 8

8.5.5. Non-Commercial Entity Subjects 9

9. EV Certificate Content and Profile 9

9.1. Issuer Information 9

9.2. Subject Information 9

9.2.1. Subject Organization Name Field 9

9.2.2. Subject Alternative Name Extension 10

9.2.3. Subject Common Name Field 10

9.2.4. Subject Business Category Field 10

9.2.5. Subject Jurisdiction of Incorporation or Registration Field 10

9.2.6. Subject Registration Number Field 11

9.2.7. Subject Physical Address of Place of Business Field 11

9.2.8. Other Subject Attributes 11

9.3. Certificate Policy Identification 11

9.3.1. EV Certificate Policy Identification Requirements 11

9.3.2. EV Subscriber Certificates 11

9.3.3. Root CA Certificates 12

9.3.4. EV Subordinate CA Certificates 12
9.3.5. Subscriber Certificates 12
9.4. Maximum Validity Period For EV Certificate 12
9.5. Subscriber Public Key 12
9.6. Certificate Serial Number 12
9.7. Additional Technical Requirements for EV Certificates 12
10. EV Certificate Request Requirements 13
10.1. General Requirements 13
10.1.1. Documentation Requirements 13
10.1.2. Role Requirements 13
10.2. EV Certificate Request Requirements 13
10.3. Requirements for Subscriber Agreement and Terms of Use 13
11. Verification Requirements ..... 14~~13~~
11.1. General Overview ..... 14~~13~~
11.1.1. Verification Requirements – Overview 14
11.1.2. Acceptable Methods of Verification – Overview 14
11.2. Verification of Applicant's Legal Existence and Identity 14
11.2.1. Verification Requirements 14
11.2.2. Acceptable Method of Verification 15
11.3. Verification of Applicant's Legal Existence and Identity – Assumed Name 17
11.3.1. Verification Requirements 17
11.3.2. Acceptable Method of Verification ..... 18~~17~~
11.4. Verification of Applicant's Physical Existence 18
11.4.1. Address of Applicant's Place of Business 18
11.5. Verified Method of Communication 19
11.5.1. Verification Requirements 19
11.5.2. Acceptable Methods of Verification 19
11.6. Verification of Applicant's Operational Existence 19
11.6.1. Verification Requirements 19
11.6.2. Acceptable Methods of Verification 19
11.7. Verification of Applicant's Domain Name 20
11.7.1. Verification Requirements 20
11.8. Verification of Name, Title, and Authority of Contract Signer and Certificate Approver 20
11.8.1. Verification Requirements 20
11.8.2. Acceptable Methods of Verification – Name, Title and Agency 20
11.8.3. Acceptable Methods of Verification – Authority 21
11.8.4. Pre-Authorized Certificate Approver 22
11.9. Verification of Signature on Subscriber Agreement and EV Certificate Requests 22
11.9.1. Verification Requirements 22
11.9.2. Acceptable Methods of Signature Verification 23
11.10. Verification of Approval of EV Certificate Request 23
11.10.1. Verification Requirements 23
11.10.2. Acceptable Methods of Verification 23
11.11. Verification of Certain Information Sources 23
11.11.1. Verified Legal Opinion 23
11.11.2. Verified Accountant Letter 24

11.11.3. Face-to-Face Validation 25
11.11.4. Independent Confirmation From Applicant 25
11.11.5. Qualified Independent Information Source 27
11.11.6. Qualified Government Information Source 27
11.11.7. Qualified Government Tax Information Source 27

11.12. Other Verification Requirements 27
11.12.1. High Risk Status 27
11.12.2. Denied Lists and Other Legal Black Lists 27
11.12.3. Parent/Subsidiary/Affiliate Relationship 28

11.13. Final Cross-Correlation and Due Diligence 28

11.14. Requirements for Re-use of Existing Documentation 29
11.14.1. Validation For Existing Subscribers 29
11.14.2. Re-issuance Requests 29
11.14.3. Age of Validated Data 29

12. Certificate Issuance by a Root CA 30

13. Certificate Revocation and Status Checking 30

14. Employee and third party issues 30

14.1. Trustworthiness and Competence 30
14.1.1. Identity and Background Verification 30
14.1.2. Training and Skills Level 31
14.1.3. Separation of Duties 31

14.2. Delegation of Functions to Registration Authorities and Subcontractors 31
14.2.1. General 31
14.2.2. Enterprise RAs 31
14.2.3. Guidelines Compliance Obligation 32
14.2.4. Allocation of Liability 32

15. Data Records 32

16. Data Security 32

17. Audit 32

17.1. Eligible Audit Schemes 32

17.2. Audit Period 32

17.3. Audit Record 32

17.4. Pre-Issuance Readiness Audit 32

17.5. Regular Self Audits 33

17.6. Auditor Qualification 33

17.7. Root CA Key Pair Generation 33

18. Liability and Indemnification 33

Appendix A - User Agent Verification (Normative) 34

Appendix B - Sample Attorney Opinions Confirming Specified Information 35

Appendix C - Sample Accountant Letters Confirming Specified Information 37

Appendix D - Country-Specific Interpretative Guidelines (Normative) **40**

Appendix E - Sample Contract Signer's Representation/Warranty (Informative) **42**

Appendix F – Issuance of Certificates for .onion Domain Names **43**

1. Scope

These Guidelines for the issuance and management of Extended Validation Certificates describe certain of the minimum requirements that a Certification Authority must meet in order to issue Extended Validation Certificates. Subject Organization information from Valid EV Certificates may be displayed in a special manner by certain relying-party software applications (e.g., browser software) in order to provide users with a trustworthy confirmation of the identity of the entity that controls the Web site they are accessing. These Guidelines incorporate the Baseline Requirements established by the CA/Browser Forum by reference. A copy of the Baseline Requirements is available on the CA/Browser Forum's website at www.cabforum.org.

These Guidelines address the basic issue of validating Subject identity information in EV Certificates and some related matters. They do not address all of the related matters, such as certain technical and operational ones. This version of the Guidelines addresses only requirements for EV Certificates intended to be used for SSL/TLS authentication on the Internet and for code signing. Similar requirements for S/MIME, time-stamping, VoIP, IM, Web services, etc. may be covered in future versions.

These Guidelines do not address the verification of information, or the issuance, use, maintenance, or revocation of EV Certificates by enterprises that operate their own Public Key Infrastructure for internal purposes only, where its Root CA Certificate is not distributed by any Application Software Supplier.

2. Purpose

2.1. Purpose of EV Certificates

EV Certificates are intended for establishing Web-based data communication conduits via the TLS/SSL protocols and for verifying the authenticity of executable code.

2.1.1. Primary Purposes

The primary purposes of an EV Certificate are to:

(1) **Identify the legal entity that controls a Web site:** Provide a reasonable assurance to the user of an Internet browser that the Web site the user is accessing is controlled by a specific legal entity identified in the EV Certificate by name, address of Place of Business, Jurisdiction of Incorporation or Registration and Registration Number or other disambiguating information; and

(2) **Enable encrypted communications with a Web site:** Facilitate the exchange of encryption keys in order to enable the encrypted communication of information over the Internet between the user of an Internet browser and a Web site.

2.1.2. Secondary Purposes

The secondary purposes of an EV Certificate are to help establish the legitimacy of a business claiming to operate a Web site or distribute executable code, and to provide a vehicle that can be used to assist in addressing problems related to phishing, malware, and other forms of online identity fraud. By providing more reliable third-party verified identity and address information regarding the business, EV Certificates may help to:

(1) Make it more difficult to mount phishing and other online identity fraud attacks using Certificates;

(2) Assist companies that may be the target of phishing attacks or online identity fraud by providing them with a tool to better identify themselves to users; and

(3) Assist law enforcement organizations in their investigations of phishing and other online identity fraud, including where appropriate, contacting, investigating, or taking legal action against the Subject.

2.1.3. Excluded Purposes

EV Certificates focus only on the identity of the Subject named in the Certificate, and not on the behavior of the Subject. As such, an EV Certificate is ***not*** intended to provide any assurances, or otherwise represent or warrant:

(1) That the Subject named in the EV Certificate is actively engaged in doing business;

(2) That the Subject named in the EV Certificate complies with applicable laws;

(3) That the Subject named in the EV Certificate is trustworthy, honest, or reputable in its business dealings; or

(4) That it is "safe" to do business with the Subject named in the EV Certificate.

3. References

See Baseline Requirements, which are available at www.cabforum.org.

4. Definitions

Capitalized Terms are defined in the Baseline Requirements except where provided below:

Accounting Practitioner: A certified public accountant, chartered accountant, or a person with an equivalent license within the country of the Applicant's Jurisdiction of Incorporation or Registration or any jurisdiction where the Applicant maintains an office or physical facility; provided that an accounting standards body in the jurisdiction maintains full (not "suspended" or "associate") membership status with the International Federation of Accountants.

Baseline Requirements: The Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates as published by the CA/Browser Forum and any amendments to such document.

Business Entity: Any entity that is not a Private Organization, Government Entity, or Non-Commercial Entity as defined herein. Examples include, but are not limited to, general partnerships, unincorporated associations, sole proprietorships, etc.

Certificate Approver: A natural person who is either the Applicant, employed by the Applicant, or an authorized agent who has express authority to represent the Applicant to (i) act as a Certificate Requester and to authorize other employees or third parties to act as a Certificate Requester, and (ii) to approve EV Certificate Requests submitted by other Certificate Requesters.

Certificate Requester: A natural person who is either the Applicant, employed by the Applicant, an authorized agent who has express authority to represent the Applicant, or a third party (such as an ISP or hosting company) that completes and submits an EV Certificate Request on behalf of the Applicant.

Confirmation Request: An appropriate out-of-band communication requesting verification or confirmation of the particular fact at issue.

Confirming Person: A position within an Applicant's organization that confirms the particular fact at issue.

Contract Signer: A natural person who is either the Applicant, employed by the Applicant, or an authorized agent who has express authority to represent the Applicant, and who has authority on behalf of the Applicant to sign Subscriber Agreements.

Demand Deposit Account: A deposit account held at a bank or other financial institution, the funds deposited in which are payable on demand. The primary purpose of demand accounts is to facilitate cashless payments by means of check, bank draft, direct debit, electronic funds transfer, etc. Usage varies among countries, but a demand deposit account is commonly known as a share draft account, a current account, or a checking account.

Enterprise EV Certificate: An EV Certificate that an Enterprise RA authorizes the CA to issue at third and higher domain levels.

Enterprise EV RA: An RA that is authorized by the CA to authorize the CA to issue EV Certificates at third and higher domain levels.

EV Authority: A source other than the Certificate Approver, through which verification occurs that the Certificate Approver is expressly authorized by the Applicant, as of the date of the EV Certificate Request, to take the Request actions described in these Guidelines.

EV Certificate: A certificate that contains subject information specified in these Guidelines and that has been validated in accordance with these Guidelines.

EV Certificate Beneficiaries: Persons to whom the CA and its Root CA make specified EV Certificate Warranties.

EV Certificate Renewal: The process whereby an Applicant who has a valid unexpired and non-revoked EV Certificate makes an application, to the CA that issued the original certificate, for a newly issued EV Certificate for the same organizational name and Domain Name prior to the expiration of the Applicant's existing EV Certificate but with a new 'valid to' date beyond the expiry of the current EV Certificate.

EV Certificate Reissuance: The process whereby an Applicant who has a valid unexpired and non-revoked EV Certificate makes an application, to the CA that issued the original certificate, for a newly issued EV Certificate for the same organizational name and Domain Name prior to the expiration of the Applicant's existing EV Certificate but with a 'valid to' date that matches that of the current EV Certificate.

EV Certificate Request: A request from an Applicant to the CA requesting that the CA issue an EV Certificate to the Applicant, which request is validly authorized by the Applicant and signed by the Applicant Representative.

EV Certificate Warranties: In conjunction with the CA issuing an EV Certificate, the CA and its Root CA, during the period when the EV Certificate is Valid, promise that the CA has followed the requirements of these Guidelines and the CA's EV Policies in issuing the EV Certificate and in verifying the accuracy of the information contained in the EV Certificate.

EV OID: An identifying number, in the form of an "object identifier," that is included in the *certificatePolicies* field of a certificate that: (i) indicates which CA policy statement relates to that certificate, and (ii) is either the CA/Browser Forum EV policy identifier or a policy identifier that, by pre-agreement with one or more Application Software Supplier, marks the certificate as being an EV Certificate.

EV Policies: Auditable EV Certificate practices, policies and procedures, such as a certification practice statement and certificate policy, that are developed, implemented, and enforced by the CA and its Root CA.

EV Processes: The keys, software, processes, and procedures by which the CA verifies Certificate Data under this Guideline, issues EV Certificates, maintains a Repository, and revokes EV Certificates.

Extended Validation Certificate: See EV Certificate.

Government Agency: In the context of a Private Organization, the government agency in the Jurisdiction of Incorporation under whose authority the legal existence of Private Organizations is established (e.g., the government agency that issued the Certificate of Incorporation). In the context of Business Entities, the government agency in the jurisdiction of operation that registers business entities. In the case of a Government Entity, the entity that enacts law, regulations, or decrees establishing the legal existence of Government Entities.

Guidelines: This document.

Incorporating Agency: In the context of a Private Organization, the government agency in the Jurisdiction of Incorporation under whose authority the legal existence of the entity is registered (e.g., the government agency that issues certificates of formation or incorporation). In the context of a Government Entity, the entity that enacts law, regulations, or decrees establishing the legal existence of Government Entities.

Independent Confirmation From Applicant: Confirmation of a particular fact received by the CA pursuant to the provisions of the Guidelines or binding upon the Applicant.

Individual: A natural person.

International Organization: An organization founded by a constituent document, e.g., a charter, treaty, convention or similar document, signed by, or on behalf of, a minimum of two Sovereign State governments.

Jurisdiction of Incorporation: In the context of a Private Organization, the country and (where applicable) the state or province or locality where the organization's legal existence was established by a filing with (or an act of) an appropriate government agency or entity (e.g., where it was incorporated). In the context of a Government Entity, the country and (where applicable) the state or province where the Entity's legal existence was created by law.

Jurisdiction of Registration: In the case of a Business Entity, the state, province, or locality where the organization has registered its business presence by means of filings by a Principal Individual involved in the business.

Latin Notary: A person with legal training whose commission under applicable law not only includes authority to authenticate the execution of a signature on a document but also responsibility for the correctness and content of the document. A Latin Notary is sometimes referred to as a Civil Law Notary.

Legal Existence: A Private Organization, Government Entity, or Business Entity has Legal Existence if it has been validly formed and not otherwise terminated, dissolved, or abandoned.

Legal Practitioner: A person who is either a lawyer or a Latin Notary as described in these Guidelines and competent to render an opinion on factual claims of the Applicant.

Maximum Validity Period: 1. The maximum time period for which the issued EV Certificate is valid. 2. The maximum period after validation by the CA that certain Applicant information may be relied upon in issuing an EV Certificate pursuant to these Guidelines.

Notary: A person whose commission under applicable law includes authority to authenticate the execution of a signature on a document.

Place of Business: The location of any facility (such as a factory, retail store, warehouse, etc) where the Applicant's business is conducted.

Principal Individual: An individual of a Private Organization, Government Entity, or Business Entity that is either an owner, partner, managing member, director, or officer, as identified by their title of employment, or an employee, contractor or agent authorized by such entity or organization to conduct business related to the request, issuance, and use of EV Certificates.

Private Organization: A non-governmental legal entity (whether ownership interests are privately held or publicly traded) whose existence was created by a filing with (or an act of) the Incorporating Agency or equivalent in its Jurisdiction of Incorporation.

Qualified Auditor: An independent public accounting firm that meets the auditing qualification requirements specified in Section 17.6 of these Guidelines.

Qualified Government Information Source: A database maintained by a Government Entity (e.g. SEC filings) that meets the requirements of Section 11.11.6.

Qualified Government Tax Information Source: A Qualified Governmental Information Source that specifically contains tax information relating to Private Organizations, Business Entities, or Individuals.

Qualified Independent Information Source: A regularly-updated and current, publicly available, database designed for the purpose of accurately providing the information for which it is consulted, and which is generally recognized as a dependable source of such information.

Registration Agency: A Governmental Agency that registers business information in connection with an entity's business formation or authorization to conduct business under a license, charter or other certification. A Registration Agency MAY include, but is not limited to (i) a State Department of Corporations or a Secretary of State; (ii) a licensing agency, such as a State Department of Insurance; or (iii) a chartering agency, such as a state office or department of financial regulation, banking or finance, or a federal agency such as the Office of the Comptroller of the Currency or Office of Thrift Supervision.

Registered Agent: An individual or entity that is: (i) authorized by the Applicant to receive service of process and business communications on behalf of the Applicant; and (ii) listed in the official records of the Applicant's Jurisdiction of Incorporation as acting in the role specified in (i) above.

Registered Office: The official address of a company, as recorded with the Incorporating Agency, to which official documents are sent and at which legal notices are received.

Registration Number: The unique number assigned to a Private Organization by the Incorporating Agency in such entity's Jurisdiction of Incorporation.

Regulated Financial Institution: A financial institution that is regulated, supervised, and examined by governmental, national, state or provincial, or local authorities.

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

Signing Authority: One or more Certificate Approvers designated to act on behalf of the Applicant.

Superior Government Entity: Based on the structure of government in a political subdivision, the Government Entity or Entities that have the ability to manage, direct and control the activities of the Applicant.

Suspect code: Code that contains malicious functionality or serious vulnerabilities, including spyware, malware and other code that installs without the user's consent and/or resists its own removal, and code that can be exploited in ways not intended by its designers to compromise the trustworthiness of the platforms on which it executes.

Translator: An individual or Business Entity that possesses the requisite knowledge and expertise to accurately translate the words of a document written in one language to the native language of the CA.

Verified Accountant Letter: A document meeting the requirements specified in Section 11.11.2 of these Guidelines

Verified Legal Opinion: A document meeting the requirements specified in Section 11.11.1 of these Guidelines.

Verified Method of Communication: The use of a telephone number, a fax number, an email address, or postal delivery address, confirmed by the CA in accordance with Section 11.5 of the Guidelines as a reliable way of communicating with the Applicant.

Verified Professional Letter: A Verified Accountant Letter or Verified Legal Opinion.

WebTrust EV Program: The additional audit procedures specified for CAs that issue EV Certificates by the AICPA/CICA to be used in conjunction with its WebTrust Program for Certification Authorities.

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

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

5. Abbreviations and Acronyms

Abbreviations and Acronyms are defined in the Baseline Requirements except as otherwise defined herein:

BIPM	International Bureau of Weights and Measures
BIS	(US Government) Bureau of Industry and Security
CEO	Chief Executive Officer
CFO	Chief Financial Officer
CIO	Chief Information Officer
CISO	Chief Information Security Officer
COO	Chief Operating Officer
CPA	Chartered Professional Accountant
CSO	Chief Security Officer
EV	Extended Validation
gTLD	Generic Top-Level Domain
IFAC	International Federation of Accountants
IRS	Internal Revenue Service
ISP	Internet Service Provider
QGIS	Qualified Government Information Source
QTIS	Qualified Government Tax Information Source
QIIS	Qualified Independent Information Source
SEC	(US Government) Securities and Exchange Commission
UTC(k)	National realization of Coordinated Universal Time

6. Conventions

Terms not otherwise defined in these Guidelines shall be as defined in applicable agreements, user manuals, certification practice statements (CPS), and certificate policies (CP) of the CA issuing EV Certificates.

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

7. Certificate Warranties and Representations

7.1. EV Certificate Warranties

When the CA issues an EV Certificate, the CA and its Root CA represent and warrant to the Certificate Beneficiaries listed in Section 9.6.1 of the Baseline Requirements, during the period when the EV Certificate is Valid, that the CA has followed the requirements of these Guidelines and its EV Policies in issuing and managing the EV Certificate and in verifying the accuracy of the information contained in the EV Certificate. The EV Certificate Warranties specifically include, but are not limited to, the following:

(A) **Legal Existence:** The CA has confirmed with the Incorporating or Registration Agency in the Subject's Jurisdiction of Incorporation or Registration that, as of the date the EV Certificate was issued, the Subject named in the EV Certificate legally exists as a valid organization or entity in the Jurisdiction of Incorporation or Registration;

(B) **Identity:** The CA has confirmed that, as of the date the EV Certificate was issued, the legal name of the Subject named in the EV Certificate matches the name on the official government records of the Incorporating or Registration Agency in the Subject's Jurisdiction of Incorporation or Registration, and if an assumed name is also included, that the assumed name is properly registered by the Subject in the jurisdiction of its Place of Business;

(C) **Right to Use Domain Name:** The CA has taken all steps reasonably necessary to verify that, as of the date the EV Certificate was issued, the Subject named in the EV Certificate has the right to use all the Domain Name(s) listed in the EV Certificate;

(D) **Authorization for EV Certificate:** The CA has taken all steps reasonably necessary to verify that the Subject named in the EV Certificate has authorized the issuance of the EV Certificate;

(E) **Accuracy of Information:** The CA has taken all steps reasonably necessary to verify that all of the other information in the EV Certificate is accurate, as of the date the EV Certificate was issued;

(F) **Subscriber Agreement:** The Subject named in the EV Certificate has entered into a legally valid and enforceable Subscriber Agreement with the CA that satisfies the requirements of these Guidelines or, if they are affiliated, the Applicant Representative has acknowledged and accepted the Terms of Use;

(G) **Status:** The CA will follow the requirements of these Guidelines and maintain a 24 x 7 online-accessible Repository with current information regarding the status of the EV Certificate as Valid or revoked; and

(H) **Revocation:** The CA will follow the requirements of these Guidelines and revoke the EV Certificate for any of the revocation reasons specified in these Guidelines.

7.2. By the Applicant

EV Certificate Applicants make the commitments and warranties set forth in Section 9.6.3 of the Baseline Requirements for the benefit of the CA and Certificate Beneficiaries.

8. Community and Applicability

8.1. Issuance of EV Certificates

The CA MAY issue EV Certificates, provided that the CA and its Root CA satisfy the requirements in these Guidelines and the Baseline Requirements.

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

8.2. EV Policies

8.2.1. Implementation

Each CA MUST develop, implement, enforce, display prominently on its Web site, and periodically update as necessary its own auditable EV Certificate practices, policies and procedures, such as a Certification Practice Statement (CPS) and Certificate Policy (CP) that:

(A) Implement the requirements of these Guidelines as they are revised from time-to-time;

(B) Implement the requirements of (i) the then-current WebTrust Program for CAs, and (ii) the then-current WebTrust EV Program or ETSI TS 102 042; and

(C) Specify the CA's and its Root CA's entire root certificate hierarchy including all roots that its EV Certificates depend on for proof of those EV Certificates' authenticity.

8.2.2. Disclosure

Each CA MUST publicly disclose their EV Policies through an appropriate and readily accessible online means that is available on a 24x7 basis. The CA is also REQUIRED to publicly disclose its CA business practices as required by both WebTrust for CAs and ETSI TS 102 042. The disclosures MUST be structured in accordance with either RFC 2527 or RFC 3647.

8.3. Commitment to Comply with Recommendations

Each CA SHALL publicly give effect to these Guidelines and represent that they will adhere to the latest published version by incorporating them into their respective EV Policies, using a clause such as the following (which must include a link to the official version of these Guidelines):

> [Name of CA] conforms to the current version of the CA/Browser Forum Guidelines for Issuance and Management of Extended Validation Certificates published at http://www.cabforum.org. In the event of any inconsistency between this document and those Guidelines, those Guidelines take precedence over this document.

In addition, the CA MUST include (directly or by reference) the applicable requirements of these Guidelines in all contracts with Subordinate CAs, RAs, Enterprise RAs, and subcontractors that involve or relate to the issuance or maintenance of EV Certificates. The CA MUST enforce compliance with such terms.

8.4. Insurance

Each CA SHALL maintain the following insurance related to their respective performance and obligations under these Guidelines:

(A) Commercial General Liability insurance (occurrence form) with policy limits of at least two million US dollars in coverage; and

(B) Professional Liability/Errors and Omissions insurance, with policy limits of at least five million US dollars in coverage, and including coverage for (i) claims for damages arising out of an act, error, or omission, unintentional breach of contract, or neglect in issuing or maintaining EV Certificates, and (ii) claims for damages arising out of infringement of the proprietary rights of any third party (excluding copyright, and trademark infringement), and invasion of privacy and advertising injury.

Such insurance MUST be with a company rated no less than A- as to Policy Holder's Rating in the current edition of Best's Insurance Guide (or with an association of companies each of the members of which are so rated).

A CA MAY self-insure for liabilities that arise from such party's performance and obligations under these Guidelines provided that it has at least five hundred million US dollars in liquid assets based on audited financial statements in the past twelve months, and a quick ratio (ratio of liquid assets to current liabilities) of not less than 1.0.

8.5. Obtaining EV Certificates

8.5.1. General

The CA MAY only issue EV Certificates to Applicants that meet the Private Organization, Government Entity, Business Entity and Non-Commercial Entity requirements specified below.

8.5.2. Private Organization Subjects

An Applicant qualifies as a Private Organization if:

(1) The entity's legal existence is created or recognized by a by a filing with (or an act of) the Incorporating or Registration Agency in its Jurisdiction of Incorporation or Registration (e.g., by issuance of a certificate of incorporation, registration number, etc.) or created or recognized by a Government Agency (e.g. under a charter, treaty, convention, or equivalent recognition instrument);

(2) The entity designated with the Incorporating or Registration Agency a Registered Agent, a Registered Office (as required under the laws of the Jurisdiction of Incorporation or Registration), or an equivalent facility;

(3) The entity is not designated on the records of the Incorporating or Registration Agency by labels such as "inactive," "invalid," "not current," or the equivalent;

(4) The entity has a verifiable physical existence and business presence;

(5) The entity's Jurisdiction of Incorporation, Registration, Charter, or License, and/or its Place of Business is not in any country where the CA is prohibited from doing business or issuing a certificate by the laws of the CA's jurisdiction; and

(6) The entity is not listed on any government denial list or prohibited list (e.g., trade embargo) under the laws of the CA's jurisdiction.

8.5.3. Government Entity Subjects

An Applicant qualifies as a Government Entity if:

(1) The entity's legal existence was established by the political subdivision in which the entity operates;

(2) The entity is not in any country where the CA is prohibited from doing business or issuing a certificate by the laws of the CA's jurisdiction; and

(3) The entity is not listed on any government denial list or prohibited list (e.g., trade embargo) under the laws of the CA's jurisdiction.

8.5.4. Business Entity Subjects

An Applicant qualifies as a Business Entity if:

(1) The entity is a legally recognized entity that filed certain forms with a Registration Agency in its jurisdiction, the Registration Agency issued or approved the entity's charter, certificate, or license, and the entity's existence can be verified with that Registration Agency;

(2) The entity has a verifiable physical existence and business presence;

(3) At least one Principal Individual associated with the entity is identified and validated by the CA;

(4) The identified Principal Individual attests to the representations made in the Subscriber Agreement;

(5) the CA verifies the entity's use of any assumed name used to represent the entity pursuant to the requirements of Section 11.3 herein;

(6) The entity and the identified Principal Individual associated with the entity are not located or residing in any country where the CA is prohibited from doing business or issuing a certificate by the laws of the CA's jurisdiction; and

(7) The entity and the identified Principal Individual associated with the entity are not listed on any government denial list or prohibited list (e.g., trade embargo) under the laws of the CA's jurisdiction.

8.5.5. Non-Commercial Entity Subjects

An Applicant qualifies as a Non-Commercial Entity if:

(A) The Applicant is an International Organization Entity, created under a charter, treaty, convention or equivalent instrument that was signed by, or on behalf of, more than one country's government. The CA/Browser Forum may publish a listing of Applicants who qualify as an International Organization for EV eligibility; and

(B) The Applicant is not headquartered in any country where the CA is prohibited from doing business or issuing a certificate by the laws of the CA's jurisdiction; and

(C) The Applicant is not listed on any government denial list or prohibited list (e.g., trade embargo) under the laws of the CA's jurisdiction.

Subsidiary organizations or agencies of an entity that qualifies as a Non-Commercial Entity also qualifies for EV Certificates as a Non-Commercial Entity.

9. EV Certificate Content and Profile

This section sets forth minimum requirements for the content of the EV Certificate as they relate to the identity of the CA and the Subject of the EV Certificate.

9.1. Issuer Information

Issuer Information listed in an EV Certificate MUST comply with Section 7.1.4.1 of the Baseline Requirements.

9.2. Subject Information

Subject to the requirements of these Guidelines, the EV Certificate and certificates issued to Subordinate CAs that are not controlled by the same entity as the CA MUST include the following information about the Subject organization in the fields listed:

9.2.1. Subject Organization Name Field

Certificate field: subject:organizationName (OID 2.5.4.10)

Required/Optional: Required

Contents: This field MUST contain the Subject's full legal organization name as listed in the official records of the Incorporating or Registration Agency in the Subject's Jurisdiction of Incorporation or Registration or as otherwise verified by the CA as provided herein. A CA MAY abbreviate the organization prefixes or suffixes in the organization name, e.g., if the official record shows "Company Name Incorporated" the CA MAY include "Company Name, Inc."

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

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

If the combination of names or the organization name by itself exceeds 64 characters, the CA MAY abbreviate parts of the organization name, and/or omit non-material words in the organization name in such a way that the text in this field does not exceed the 64-character limit; provided that the CA checks this field in accordance with section 11.12.1 and a Relying Party will not be misled into thinking that they are dealing with a different organization. In cases where this is not possible, the CA MUST NOT issue the EV Certificate.

9.2.2. Subject Alternative Name Extension

Certificate field: subjectAltName:dNSName

Required/Optional: Required

Contents: This extension MUST contain one or more host Domain Name(s) owned or controlled by the Subject and to be associated with the Subject's server. Such server MAY be owned and operated by the Subject or another entity (e.g., a hosting service). Wildcard certificates are not allowed for EV Certificates.

9.2.3. Subject Common Name Field

Certificate field: subject:commonName (OID: 2.5.4.3)

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

Contents: If present, this field MUST contain a single Domain Name(s) owned or controlled by the Subject and to be associated with the Subject's server. Such server MAY be owned and operated by the Subject or another entity (e.g., a hosting service). Wildcard certificates are not allowed for EV Certificates except as permitted under Appendix F.

9.2.4. Subject Business Category Field

Certificate field: *subject:businessCategory* (OID: 2.5.4.15)

Required/Optional: Required

Contents: This field MUST contain one of the following strings: "Private Organization", "Government Entity", "Business Entity", or "Non-Commercial Entity" depending upon whether the Subject qualifies under the terms of Section 8.5.2, 8.5.3, 8.5.4 or 8.5.5 of these Guidelines, respectively.

9.2.5. Subject Jurisdiction of Incorporation or Registration Field

Certificate fields:

Locality (if required):

subject:jurisdictionLocalityName (OID: 1.3.6.1.4.1.311.60.2.1.1)

ASN.1 - X520LocalityName as specified in RFC 5280

State or province (if required):

subject:jurisdictionStateOrProvinceName (OID: 1.3.6.1.4.1.311.60.2.1.2)

ASN.1 - X520StateOrProvinceName as specified in RFC 5280

Country:

subject:jurisdictionCountryName (OID: 1.3.6.1.4.1.311.60.2.1.3)

ASN.1 – *X520countryName* as specified in RFC 5280

Required/Optional: Required

Contents: These fields MUST NOT contain information that is not relevant to the level of the Incorporating Agency or Registration Agency. For example, the Jurisdiction of Incorporation for an Incorporating Agency or Jurisdiction of Registration for a Registration Agency that operates at the country level MUST include the country information but MUST NOT include the state or province or locality information. Similarly, the jurisdiction for the applicable Incorporating Agency or Registration Agency at the state or province level MUST include both country and state or province information, but MUST NOT include locality information. And, the jurisdiction for the applicable Incorporating Agency or Registration Agency at the locality level MUST include the country and state or province information, where the state or province regulates the registration of the entities at the locality level, as well as the locality information. Country information MUST be specified using the applicable ISO country code. State or province or locality information (where

applicable) for the Subject's Jurisdiction of Incorporation or Registration MUST be specified using the full name of the applicable jurisdiction.

9.2.6. Subject Registration Number Field

Certificate field: Subject:serialNumber (OID: 2.5.4.5)

Required/Optional: Required

Contents: For Private Organizations, this field MUST contain the Registration (or similar) Number assigned to the Subject by the Incorporating or Registration Agency in its Jurisdiction of Incorporation or Registration, as appropriate. If the Jurisdiction of Incorporation or Registration does not provide a Registration Number, then the date of Incorporation or Registration SHALL be entered into this field in any one of the common date formats.

For Government Entities that do not have a Registration Number or readily verifiable date of creation, the CA SHALL enter appropriate language to indicate that the Subject is a Government Entity.

For Business Entities, the Registration Number that was received by the Business Entity upon government registration SHALL be entered in this field. For those Business Entities that register with an Incorporating Agency or Registration Agency in a jurisdiction that does not issue numbers pursuant to government registration, the date of the registration SHALL be entered into this field in any one of the common date formats.

9.2.7. Subject Physical Address of Place of Business Field

Certificate fields:

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

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

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

Country: subject:countryName (OID: 2.5.4.6)

Postal code: subject:postalCode (OID: 2.5.4.17)

Required/Optional: City, state, and country – Required; Street and postal code – Optional

Contents: This field MUST contain the address of the physical location of the Subject's Place of Business.

9.2.8. Other Subject Attributes

All other optional attributes, when present within the subject field, MUST contain information that has been verified by the CA. CAs SHALL NOT include Fully-Qualified Domain Names in Subject attributes except as specified in Sections 9.2.1 and SHALL NOT include any Subject Organization Information except as specified in Section 9.2. Optional subfields within the Subject field MUST either contain information verified by the CA or MUST be left empty. Metadata such as '.', '-', and ' ' characters, and/or any other indication that the field is empty, absent or incomplete, MUST not be used.

9.3. Certificate Policy Identification

9.3.1. EV Certificate Policy Identification Requirements

This section sets forth minimum requirements for the contents of EV Certificates as they relate to the identification of EV Certificate Policy.

9.3.2. EV Subscriber Certificates

Each EV Certificate issued by the CA to a Subscriber MUST contain a policy identifier that is either defined by these Guidelines or the CA in the certificate's certificatePolicies extension that: (i) indicates which CA policy statement relates to that Certificate, (ii) asserts the CA's adherence to and compliance with these Guidelines, and (iii) ~~,~~ is either the CA/Browser Forum's EV policy identifier or a policy identifier that, by pre-agreement with the Application Software Supplier, marks the Certificate as being an EV Certificate.

The following Certificate Policy identifier is the CA/Browser Forum's EV policy identifier:

{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) ev-guidelines (1) } (2.23.140.1.1), if the Certificate complies with these Guidelines.

9.3.3. Root CA Certificates

The Application Software Supplier identifies Root CAs that are approved to issue EV Certificates by storing EV policy identifiers in metadata associated with Root CA Certificates.

9.3.4. EV Subordinate CA Certificates

(1) Certificates issued to Subordinate CAs that are not controlled by the issuing CA MUST contain one or more policy identifiers defined by the issuing CA that explicitly identify the EV Policies that are implemented by the Subordinate CA.

(2) Certificates issued to Subordinate CAs that are controlled by the Root CA MAY contain the special anyPolicy identifier (OID: 2.5.29.32.0).

9.3.5. Subscriber Certificates

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

9.4. Maximum Validity Period For EV Certificate

The validity period for an EV Certificate SHALL NOT exceed twenty seven months. It is RECOMMENDED that EV Subscriber Certificates have a maximum validity period of twelve months.

9.5. Subscriber Public Key

The requirements in Section 6.1.1.3 of the Baseline requirements apply equally to EV Certificates.

9.6. Certificate Serial Number

The requirements in Section 7.1 of the Baseline requirements apply equally to EV Certificates.

9.7. Additional Technical Requirements for EV Certificates

All provisions of the Baseline Requirements concerning Minimum Cryptographic Algorithms, Key Sizes, and Certificate Extensions apply to EV Certificates with the following exceptions:

1) If a Subordinate CA Certificates is issued to a Subordinate CA not controlled by the entity that controls the Root CA, the policy identifiers in the certificatePolicies extension MUST include the CA's Extended Validation policy identifier. Otherwise, it MAY contain the anyPolicy identifier.

2) The following fields MUST be present if the Subordinate CA is not controlled by the entity that controls the Root CA.

certificatePolicies:policyQualifiers:policyQualifierId

- id-qt 1 [RFC 5280]

certificatePolicies:policyQualifiers:qualifier:cPSuri

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

3) The certificatePolicies extension in EV Certificates issued to Subscribers MUST include the following:

certificatePolicies:policyIdentifier (Required)

- The Issuer's EV policy identifier

certificatePolicies:policyQualifiers:policyQualifierId (Required)

- id-qt 1 [RFC 5280]

certificatePolicies:policyQualifiers:qualifier:cPSuri (Required)

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

4) The cRLDistribution Point extension MUST be present in Subscriber Certificates if the certificate does not specify OCSP responder locations in an authorityInformationAccess extension.

10. EV Certificate Request Requirements

10.1. General Requirements

10.1.1. Documentation Requirements

The documentation requirements in Section 4.1.2 of the Baseline requirements apply equally to EV Certificates.

10.1.2. Role Requirements

The following Applicant roles are required for the issuance of an EV Certificate.

(1) **Certificate Requester:** The EV Certificate Request MUST be submitted by an authorized Certificate Requester. A Certificate Requester is a natural person who is either the Applicant, employed by the Applicant, an authorized agent who has express authority to represent the Applicant, or a third party (such as an ISP or hosting company) that completes and submits an EV Certificate Request on behalf of the Applicant.

(2) **Certificate Approver:** The EV Certificate Request MUST be approved by an authorized Certificate Approver. A Certificate Approver is a natural person who is either the Applicant, employed by the Applicant, or an authorized agent who has express authority to represent the Applicant to (i) act as a Certificate Requester and to authorize other employees or third parties to act as a Certificate Requester, and (ii) to approve EV Certificate Requests submitted by other Certificate Requesters.

(3) **Contract Signer:** A Subscriber Agreement applicable to the requested EV Certificate MUST be signed by an authorized Contract Signer. A Contract Signer is a natural person who is either the Applicant, employed by the Applicant, or an authorized agent who has express authority to represent the Applicant, and who has authority on behalf of the Applicant to sign Subscriber Agreements.

(4) **Applicant Representative**: In the case where the CA and the Subscriber are affiliated, Terms of Use applicable to the requested EV Certificate MUST be acknowledged and agreed to by an authorized Applicant Representative. An Applicant Representative is a natural person who is either the Applicant, employed by the Applicant, or an authorized agent who has express authority to represent the Applicant, and who has authority on behalf of the Applicant to acknowledge and agree to the Terms of Use.

The Applicant MAY authorize one individual to occupy two or more of these roles. The Applicant MAY authorize more than one individual to occupy any of these roles.

10.2. EV Certificate Request Requirements

The Certificate Request requirements in Section 4.1.2 of the Baseline Requirements apply equally to EV Certificates subject to the additional more stringent ageing and updating requirement of Section 11.14 of these Guidelines.

10.3. Requirements for Subscriber Agreement and Terms of Use

Section 9.6.3 of the Baseline Requirements applies equally to EV Certificates. In cases where the Certificate Request does not contain all necessary information about the Applicant, the CA MUST additionally confirm the data with the Certificate Approver or Contract Signer rather than the Certificate Requester.

11. Verification Requirements

11.1. General Overview

This part of the Guidelines sets forth Verification Requirements and Acceptable Methods of Verification for each such Requirement.

11.1.1. Verification Requirements – Overview

Before issuing an EV Certificate, the CA MUST ensure that all Subject organization information to be included in the EV Certificate conforms to the requirements of, and is verified in accordance with, these Guidelines and matches the information confirmed and documented by the CA pursuant to its verification processes. Such verification processes are intended to accomplish the following:

(1) Verify Applicant's existence and identity, including;

(A) Verify the Applicant's legal existence and identity (as more fully set forth in Section 11.2 herein),

(B) Verify the Applicant's physical existence (business presence at a physical address), and

(C) Verify the Applicant's operational existence (business activity).

(2) Verify the Applicant is a registered holder, or has control, of the Domain Name(s) to be included in the EV Certificate;

(3) Verify a reliable means of communication with the entity to be named as the Subject in the Certificate;

(4) Verify the Applicant's authorization for the EV Certificate, including;

(A) Verify the name, title, and authority of the Contract Signer, Certificate Approver, and Certificate Requester,

(B) Verify that a Contract Signer signed the Subscriber Agreement or that a duly authorized Applicant Representative acknowledged and agreed to the Terms of Use; and

(C) Verify that a Certificate Approver has signed or otherwise approved the EV Certificate Request.

11.1.2. Acceptable Methods of Verification – Overview

As a general rule, the CA is responsible for taking all verification steps reasonably necessary to satisfy each of the Verification Requirements set forth in the subsections below. The Acceptable Methods of Verification set forth in each of Sections 11.2 through 11.14 (which usually include alternatives) are considered to be the minimum acceptable level of verification required of the CA. In all cases, however, the CA is responsible for taking any additional verification steps that may be reasonably necessary under the circumstances to satisfy the applicable Verification Requirement.

11.2. Verification of Applicant's Legal Existence and Identity

11.2.1. Verification Requirements

To verify the Applicant's legal existence and identity, the CA MUST do the following.

(1) **Private Organization Subjects**

(A) **Legal Existence:** Verify that the Applicant is a legally recognized entity, in existence and validly formed (e.g., incorporated) with the Incorporating or Registration Agency in the Applicant's Jurisdiction of Incorporation or Registration, and not designated on the records of the Incorporating or Registration Agency by labels such as "inactive", "invalid", "not current", or the equivalent.

(B) **Organization Name:** Verify that the Applicant's formal legal name as recorded with the Incorporating or Registration Agency in the Applicant's Jurisdiction of Incorporation or Registration matches the Applicant's name in the EV Certificate Request.

(C) **Registration Number:** Obtain the specific Registration Number assigned to the Applicant by the Incorporating or Registration Agency in the Applicant's Jurisdiction of Incorporation or Registration. Where the Incorporating or Registration Agency does not assign a Registration Number, the CA SHALL obtain the Applicant's date of Incorporation or Registration.

(D) **Registered Agent:** Obtain the identity and address of the Applicant's Registered Agent or Registered Office (as applicable in the Applicant's Jurisdiction of Incorporation or Registration).

(2) **Government Entity Subjects**

(A) **Legal Existence:** Verify that the Applicant is a legally recognized Government Entity, in existence in the political subdivision in which such Government Entity operates.

(B) **Entity Name:** Verify that the Applicant's formal legal name matches the Applicant's name in the EV Certificate Request.

(C) **Registration Number:** The CA MUST attempt to obtain the Applicant's date of incorporation, registration, or formation, or the identifier for the legislative act that created the Government Entity. In circumstances where this information is not available, the CA MUST enter appropriate language to indicate that the Subject is a Government Entity.

(3) **Business Entity Subjects**

(A) **Legal Existence:** Verify that the Applicant is engaged in business under the name submitted by the Applicant in the Application.

(B) **Organization Name:** Verify that the Applicant's formal legal name as recognized by the Registration Authority in the Applicant's Jurisdiction of Registration matches the Applicant's name in the EV Certificate Request.

(C) **Registration Number:** Attempt to obtain the specific unique Registration Number assigned to the Applicant by the Registration Agency in the Applicant's Jurisdiction of Registration. Where the Registration Agency does not assign a Registration Number, the CA SHALL obtain the Applicant's date of Registration.

(D) **Principal Individual:** Verify the identity of the identified Principal Individual.

(4) **Non-Commercial Entity Subjects (International Organizations)**

(A) **Legal Existence:** Verify that the Applicant is a legally recognized International Organization Entity.

(B) **Entity Name:** Verify that the Applicant's formal legal name matches the Applicant's name in the EV Certificate Request.

(C) **Registration Number:** The CA MUST attempt to obtain the Applicant's date of formation, or the identifier for the legislative act that created the International Organization Entity. In circumstances where this information is not available, the CA MUST enter appropriate language to indicate that the Subject is an International Organization Entity.

11.2.2. Acceptable Method of Verification

(1) **Private Organization Subjects:** Unless verified under subsection (6), all items listed in Section 11.2.1(1) MUST be verified directly with, or obtained directly from, the Incorporating or Registration Agency in the Applicant's Jurisdiction of Incorporation or Registration. Such verification MAY be through use of a Qualified Government Information Source operated by, or on behalf of, the Incorporating or Registration Agency, or by direct contact with the Incorporating or Registration Agency in person or via mail, e-mail, Web address, or telephone, using an address or phone number obtained directly from the Qualified Government Information Source, Incorporating or Registration Agency, or from a Qualified Independent Information Source.

(2) **Government Entity Subjects:** Unless verified under subsection (6), all items listed in Section 11.2.1(2) MUST either be verified directly with, or obtained directly from, one of the following: (i) a Qualified Government Information Source in the political subdivision in which such Government Entity operates; (ii) a superior governing Government Entity in the same political subdivision as the Applicant (e.g. a Secretary of State may verify the legal existence of a specific State Department), or (iii) from a judge that is an active member of the federal, state or local judiciary within that political subdivision.

Any communication from a judge SHALL be verified in the same manner as is used for verifying factual assertions that are asserted by an Attorney as set forth in Section 11.11.1.

Such verification MAY be by direct contact with the appropriate Government Entity in person or via mail, e-mail, Web address, or telephone, using an address or phone number obtained from a Qualified Independent Information Source.

(3) **Business Entity Subjects:** Unless verified under subsection (6), items listed in Section 11.2.1(3) (A) through (C) above, MUST be verified directly with, or obtained directly from, the Registration Agency in the Applicant's Jurisdiction of Registration. Such verification MAY be performed by means of a Qualified Government Information Source, a Qualified Governmental Tax Information Source, or by direct contact with the Registration Agency in person or via mail, e-mail, Web address, or telephone, using an address or phone number obtained directly from the Qualified Government Information Source, Qualified Governmental Tax Information Source or Registration Agency, or from a Qualified Independent Information Source. In addition, the CA MUST validate a Principal Individual associated with the Business Entity pursuant to the requirements in subsection (4), below.

(4) **Principal Individual:** A Principal Individual associated with the Business Entity MUST be validated in a face-to-face setting. The CA MAY rely upon a face-to-face validation of the Principal Individual performed by the Registration Agency, provided that the CA has evaluated the validation procedure and concluded that it satisfies the requirements of the Guidelines for face-to-face validation procedures. Where no face-to-face validation was conducted by the Registration Agency, or the Registration Agency's face-to-face validation procedure does not satisfy the requirements of the Guidelines, the CA SHALL perform face-to-face validation.

(A) **Face-To-Face Validation:** The face-to-face validation MUST be conducted before either an employee of the CA, a Latin Notary, a Notary (or equivalent in the Applicant's jurisdiction), a Lawyer, or Accountant (Third-Party Validator). The Principal Individual(s) MUST present the following documentation (Vetting Documents) directly to the Third-Party Validator:

(i) A Personal Statement that includes the following information:

1. Full name or names by which a person is, or has been, known (including all other names used);

2. Residential Address at which he/she can be located;

3. Date of birth; and

4. An affirmation that all of the information contained in the Certificate Request is true and correct.

(ii) A current signed government-issued identification document that includes a photo of the Individual and is signed by the Individual such as:

1. A passport;

2. A driver's license;

3. A personal identification card;

4. A concealed weapons permit; or

5. A military ID.

(iii) At least two secondary documentary evidences to establish his/her identity that include the name of the Individual, one of which MUST be from a financial institution.

1. Acceptable financial institution documents include:

a. A major credit card, provided that it contains an expiration date and it has not expired'

b. A debit card from a regulated financial institution, provided that it contains an expiration date and it has not expired,

c. A mortgage statement from a recognizable lender that is less than six months old,

d. A bank statement from a regulated financial institution that is less than six months old.

2. Acceptable non-financial documents include:

a. Recent original utility bills or certificates from a utility company confirming the arrangement to pay for the services at a fixed address (not a mobile/cellular telephone bill),

b. A copy of a statement for payment of a lease, provided that the statement is dated within the past six months,

c. A certified copy of a birth certificate,

d. A local authority tax bill for the current year,

e. A certified copy of a court order, such as a divorce certificate, annulment papers, or adoption papers.

The Third-Party Validator performing the face-to-face validation MUST:

(i) Attest to the signing of the Personal Statement and the identity of the signer; and

(ii) Identify the original Vetting Documents used to perform the identification. In addition, the Third-Party Validator MUST attest on a copy of the current signed government-issued photo identification document that it is a full, true, and accurate reproduction of the original.

(B) **Verification of Third-Party Validator:** The CA MUST independently verify that the Third-Party Validator is a legally-qualified Latin Notary or Notary (or legal equivalent in the Applicant's jurisdiction), lawyer, or accountant in the jurisdiction of the Individual's residency, and that the Third-Party Validator actually did perform the services and did attest to the signature of the Individual.

(C) **Cross-checking of Information:** The CA MUST obtain the signed and attested Personal Statement together with the attested copy of the current signed government-issued photo identification document. The CA MUST review the documentation to determine that the information is consistent, matches the information in the application, and identifies the Individual. The CA MAY rely on electronic copies of this documentation, provided that:

(i) the CA confirms their authenticity (not improperly modified when compared with the underlying original) with the Third-Party Validator; and

(ii) electronic copies of similar kinds of documents are recognized as legal substitutes for originals under the laws of the CA's jurisdiction.

(5) **Non-Commercial Entity Subjects (International Organization):** Unless verified under subsection (6), all items listed in Section 11.2.1(4) MUST be verified either:

(A) With reference to the constituent document under which the International Organization was formed; or

(B) Directly with a signatory country's government in which the CA is permitted to do business. Such verification may be obtained from an appropriate government agency or from the laws of that country, or by verifying that the country's government has a mission to represent it at the International Organization; or

(C) Directly against any current list of qualified entities that the CA/Browser Forum may maintain at www.cabforum.org.

(D) In cases where the International Organization applying for the EV Certificate is an organ or agency - including a non-governmental organization of a verified International Organization, then the CA may verify the International Organization Applicant directly with the verified umbrella International Organization of which the Applicant is an organ or agency.

(6) The CA may rely on a Verified Professional Letter to establish the Applicant's information listed in (1)-(5) above if (i) the Verified Professional Letter includes a copy of supporting documentation used to establish the Applicant's legal existence, such as a certificate of registration, articles of incorporation, operating agreement, statute, or regulatory act, and (ii) the CA confirms the Applicant's organization name specified in the Verified Professional Letter with a QIIS or QGIS.

11.3. Verification of Applicant's Legal Existence and Identity – Assumed Name

11.3.1. Verification Requirements

If, in addition to the Applicant's formal legal name, as recorded with the applicable Incorporating Agency or Registration Agency in the Applicant's Jurisdiction of Incorporation or Registration, the Applicant's identity, as asserted in the EV Certificate, is to contain any assumed name (also known as "doing business as", "DBA", or "d/b/a" in the US, and "trading as" in the UK) under which the Applicant conducts business, the CA MUST verify that: (i) the Applicant has registered its use of the assumed name with the appropriate government agency for such filings in the jurisdiction of its Place of Business (as verified in accordance with these Guidelines), and (ii) that such filing continues to be valid.

11.3.2. Acceptable Method of Verification

To verify any assumed name under which the Applicant conducts business:

(1) The CA MAY verify the assumed name through use of a Qualified Government Information Source operated by, or on behalf of, an appropriate government agency in the jurisdiction of the Applicant's Place of Business, or by direct contact with such government agency in person or via mail, e-mail, Web address, or telephone; or

(2) The CA MAY verify the assumed name through use of a Qualified Independent Information Source provided that the QIIS has verified the assumed name with the appropriate government agency.

(3) The CA MAY rely on a Verified Professional Letter that indicates the assumed name under which the Applicant conducts business, the government agency with which the assumed name is registered, and that such filing continues to be valid.

11.4. Verification of Applicant's Physical Existence

11.4.1. Address of Applicant's Place of Business

(1) **Verification Requirements:** To verify the Applicant's physical existence and business presence, the CA MUST verify that the physical address provided by the Applicant is an address where the Applicant or a Parent/Subsidiary Company conducts business operations (not, for example, a mail drop or P.O. box, or 'care of' (C/O) address, such as an address for an agent of the Organization), and is the address of the Applicant's Place of Business.

(2) **Acceptable Methods of Verification**

(A) **Place of Business in the Country of Incorporation or Registration**

(i) For Applicants whose Place of Business is in the same country as the Applicant's Jurisdiction of Incorporation or Registration and whose Place of Business is NOT the same as that indicated in the relevant Qualified Government Information Source used in Section 11.2 to verify legal existence:

(1) For Applicants listed at the same Place of Business address in the current version of either at least one QGIS (other than that used to verify legal existence), QIIS or QTIS, the CA MUST confirm that the Applicant's address, as listed in the EV Certificate Request, is a valid business address for the Applicant or a Parent/Subsidiary Company by reference to such QGIS, QIIS, or QTIS, and MAY rely on the Applicant's representation that such address is its Place of Business;

(2) For Applicants who are not listed at the same Place of Business address in the current version of either at least one QIIS or QTIS, the CA MUST confirm that the address provided by the Applicant in the EV Certificate Request is the Applicant's or a Parent/Subsidiary Company's business address, by obtaining documentation of a site visit to the business address, which MUST be performed by a reliable individual or firm. The documentation of the site visit MUST:

(a) Verify that the Applicant's business is located at the exact address stated in the EV Certificate Request (e.g., via permanent signage, employee confirmation, etc.),

(b) Identify the type of facility (e.g., office in a commercial building, private residence, storefront, etc.) and whether it appears to be a permanent business location,

(c) Indicate whether there is a permanent sign (that cannot be moved) that identifies the Applicant,

(d) Indicate whether there is evidence that the Applicant is conducting ongoing business activities at the site (not that it is just, for example, a mail drop, P.O. box, etc.), and

(e) Include one or more photos of (i) the exterior of the site (showing signage indicating the Applicant's name, if present, and showing the street address if possible), and (ii) the interior reception area or workspace.

(2) For all Applicants, the CA MAY alternatively rely on a Verified Professional Letter that indicates the address of the Applicant's or a Parent/Subsidiary Company's Place of Business and that business operations are conducted there.

(3) For Government Entity Applicants, the CA MAY rely on the address contained in the records of the QGIS in the Applicant's jurisdiction.

(4) For Applicants whose Place of Business is in the same country as the Applicant's Jurisdiction of Incorporation or Registration and where the QGIS used in Section 11.2 to verify legal existence contains a business address for the Applicant, the CA MAY rely on the address in the QGIS to confirm the Applicant's or a Parent/Subsidiary Company's address as listed in the EV Certificate Request, and MAY rely on the Applicant's representation that such address is its Place of Business.

(B) **Place of Business not in the Country of Incorporation or Registration:** The CA MUST rely on a Verified Professional Letter that indicates the address of the Applicant's Place of Business and that business operations are conducted there.

11.5. Verified Method of Communication

11.5.1. Verification Requirements

To assist in communicating with the Applicant and confirming that the Applicant is aware of and approves issuance, the CA MUST verify a telephone number, fax number, email address, or postal delivery address as a Verified Method of Communication with the Applicant.

11.5.2. Acceptable Methods of Verification

To verify a Verified Method of Communication with the Applicant, the CA MUST:

(A) Verify that the Verified Method of Communication belongs to the Applicant, or a Parent/Subsidiary or Affiliate of the Applicant, by matching it with one of the Applicant's Parent/Subsidiary or Affiliate's Places of Business in: (i) records provided by the applicable phone company; (ii) a QGIS, QTIS, or QIIS; or (iii) a Verified Professional Letter; and

(B) Confirm the Verified Method of Communication by using it to obtain an affirmative response sufficient to enable a reasonable person to conclude that the Applicant, or a Parent/Subsidiary or Affiliate of Applicant, can be contacted reliably by using the Verified Method of Communication.

11.6. Verification of Applicant's Operational Existence

11.6.1. Verification Requirements

The CA MUST verify that the Applicant has the ability to engage in business by verifying the Applicant's, or Affiliate/Parent/Subsidiary Company's, operational existence. The CA MAY rely on its verification of a Government Entity's legal existence under Section 11.2 as verification of a Government Entity's operational existence.

11.6.2. Acceptable Methods of Verification

To verify the Applicant's ability to engage in business, the CA MUST verify the operational existence of the Applicant, or its Affiliate/Parent/Subsidiary Company, by:

(1) Verifying that the Applicant, Affiliate, Parent Company, or Subsidiary Company has been in existence for at least three years, as indicated by the records of an Incorporating Agency or Registration Agency;

(2) Verifying that the Applicant, Affiliate, Parent Company, or Subsidiary Company is listed in either a current QIIS or QTIS;

(3) Verifying that the Applicant, Affiliate, Parent Company, or Subsidiary Company has an active current Demand Deposit Account with a Regulated Financial Institution by receiving authenticated documentation of the Applicant's, Affiliate's, Parent Company's, or Subsidiary Company's Demand Deposit Account directly from a Regulated Financial Institution; or

(4) Relying on a Verified Professional Letter to the effect that the Applicant has an active current Demand Deposit Account with a Regulated Financial Institution.

11.7. Verification of Applicant's Domain Name

11.7.1. Verification Requirements

(1) For each Fully-Qualified Domain Name listed in a Certificate, other than a Domain Name with .onion in the right-most label of the Domain Name, the CA SHALL confirm that, as of the date the Certificate was issued, the Applicant (or the Applicant's Parent Company, Subsidiary Company, or Affiliate, collectively referred to as "Applicant" for the purposes of this section) either is the Domain Name Registrant or has control over the FQDN using a procedure specified in Section 3.2.2.4 of the Baseline Requirements, except that a CA MAY NOT verify a domain using the procedure described subsection 3.2.2.4(7). For a Certificate issued to a Domain Name with .onion in the right-most label of the Domain Name, the CA SHALL confirm that, as of the date the Certificate was issued, the Applicant's control over the .onion Domain Name in accordance with Appendix F.

(2) **Mixed Character Set Domain Names:** EV Certificates MAY include Domain Names containing mixed character sets only in compliance with the rules set forth by the domain registrar. The CA MUST visually compare any Domain Names with mixed character sets with known high risk domains. If a similarity is found, then the EV Certificate Request MUST be flagged as High Risk. The CA must perform reasonably appropriate additional authentication and verification to be certain beyond reasonable doubt that the Applicant and the target in question are the same organization.

11.8. Verification of Name, Title, and Authority of Contract Signer and Certificate Approver

11.8.1. Verification Requirements

For both the Contract Signer and the Certificate Approver, the CA MUST verify the following.

(1) **Name, Title and Agency:** The CA MUST verify the name and title of the Contract Signer and the Certificate Approver, as applicable. The CA MUST also verify that the Contract Signer and the Certificate Approver are agents representing the Applicant.

(2) **Signing Authority of Contract Signer:** The CA MUST verify that the Contract Signer is authorized by the Applicant to enter into the Subscriber Agreement (and any other relevant contractual obligations) on behalf of the Applicant, including a contract that designates one or more Certificate Approvers on behalf of the Applicant.

(3) **EV Authority of Certificate Approver:** The CA MUST verify, through a source other than the Certificate Approver him- or herself, that the Certificate Approver is expressly authorized by the Applicant to do the following, as of the date of the EV Certificate Request:

(A) Submit, and, if applicable, authorize a Certificate Requester to submit, the EV Certificate Request on behalf of the Applicant; and

(B) Provide, and, if applicable, authorize a Certificate Requester to provide, the information requested from the Applicant by the CA for issuance of the EV Certificate; and

(C) Approve EV Certificate Requests submitted by a Certificate Requester.

11.8.2. Acceptable Methods of Verification – Name, Title and Agency

Acceptable methods of verification of the name, title, and agency status of the Contract Signer and the Certificate Approver include the following.

(1) **Name and Title:** The CA MAY verify the name and title of the Contract Signer and the Certificate Approver by any appropriate method designed to provide reasonable assurance that a person claiming to act in such a role is in fact the named person designated to act in such role**.**

(2) **Agency:** The CA MAY verify the agency of the Contract Signer and the Certificate Approver by:

(A) Contacting the Applicant using a Verified Method of Communication for the Applicant, and obtaining confirmation that the Contract Signer and/or the Certificate Approver, as applicable, is an employee;

(B) Obtaining an Independent Confirmation From the Applicant (as described in Section 11.11.4), or a Verified Professional Letter verifying that the Contract Signer and/or the Certificate Approver, as applicable, is either an employee or has otherwise been appointed as an agent of the Applicant; or

(C) Obtaining confirmation from a QIIS or QGIS that the Contract Signer and/or Certificate Approver is an employee of the Applicant.

The CA MAY also verify the agency of the Certificate Approver via a certification from the Contract Signer (including in a contract between the CA and the Applicant signed by the Contract Signer), provided that the employment or agency status and Signing Authority of the Contract Signer has been verified.

11.8.3. Acceptable Methods of Verification – Authority

Acceptable methods of verification of the Signing Authority of the Contract Signer, and the EV Authority of the Certificate Approver, as applicable, include:

(1) **Verified Professional Letter:** The Signing Authority of the Contract Signer, and/or the EV Authority of the Certificate Approver, MAY be verified by reliance on a Verified Professional Letter;

(2) **Corporate Resolution:** The Signing Authority of the Contract Signer, and/or the EV Authority of the Certificate Approver, MAY be verified by reliance on a properly authenticated corporate resolution that confirms that the person has been granted such Signing Authority, provided that such resolution is (i) certified by the appropriate corporate officer (e.g., secretary), and (ii) the CA can reliably verify that the certification was validly signed by such person, and that such person does have the requisite authority to provide such certification;

(3) **Independent Confirmation from Applicant:** The Signing Authority of the Contract Signer, and/or the EV Authority of the Certificate Approver, MAY be verified by obtaining an Independent Confirmation from the Applicant (as described in Section 11.11.4);

(4) **Contract between CA and Applicant:** The EV Authority of the Certificate Approver MAY be verified by reliance on a contract between the CA and the Applicant that designates the Certificate Approver with such EV Authority, provided that the contract is signed by the Contract Signer and provided that the agency and Signing Authority of the Contract Signer have been verified;

(5) **Prior Equivalent Authority:** The signing authority of the Contract Signer, and/or the EV authority of the Certificate Approver, MAY be verified by relying on a demonstration of Prior Equivalent Authority.

(A) Prior Equivalent Authority of a Contract Signer MAY be relied upon for confirmation or verification of the signing authority of the Contract Signer when the Contract Signer has executed a binding contract between the CA and the Applicant with a legally valid and enforceable seal or handwritten signature and only when the contract was executed more than 90 days prior to the EV Certificate application. The CA MUST record sufficient details of the previous agreement to correctly identify it and associate it with the EV application. Such details MAY include any of the following:

(i) Agreement title,

(ii) Date of Contract Signer's signature,

(iii) Contract reference number, and

(iv) Filing location.

(B) Prior Equivalent Authority of a Certificate Approver MAY be relied upon for confirmation or verification of the EV Authority of the Certificate Approver when the Certificate Approver has performed one or more of the following:

(i) Under contract to the CA, has served (or is serving) as an Enterprise RA for the Applicant, or

(ii) Has participated in the approval of one or more certificate requests, for certificates issued by the CA and which are currently and verifiably in use by the Applicant. In this case the CA MUST have contacted the Certificate Approver by phone at a previously validated phone number or have accepted a signed and notarized letter approving the certificate request.

(6) **QIIS or QGIS**: The Signing Authority of the Contract Signer, and/or the EV Authority of the Certificate Approver, MAY be verified by a QIIS or QGIS that identifies the Contract Signer and/or the Certificate Approver as a corporate officer, sole proprietor, or other senior official of the Applicant.

(7) **Contract Signer's Representation/Warranty:** Provided that the CA verifies that the Contract Signer is an employee or agent of the Applicant, the CA MAY rely on the signing authority of the Contract Signer by obtaining a duly executed representation or warranty from the Contract Signer that includes the following acknowledgments:

(A) That the Applicant authorizes the Contract Signer to sign the Subscriber Agreement on the Applicant's behalf,

(B) That the Subscriber Agreement is a legally valid and enforceable agreement,

(C) That, upon execution of the Subscriber Agreement, the Applicant will be bound by all of its terms and conditions,

(D) That serious consequences attach to the misuse of an EV certificate, and

(E) The contract signer has the authority to obtain the digital equivalent of a corporate seal, stamp or officer's signature to establish the authenticity of the company's Web site.

Note: An example of an acceptable representation/warranty appears in Appendix E.

11.8.4. Pre-Authorized Certificate Approver

Where the CA and Applicant contemplate the submission of multiple future EV Certificate Requests, then, after the CA:

(1) Has verified the name and title of the Contract Signer and that he/she is an employee or agent of the Applicant; and

(2) Has verified the Signing Authority of such Contract Signer in accordance with one of the procedures in Section 11.8.3.

The CA and the Applicant MAY enter into a written agreement, signed by the Contract Signer on behalf of the Applicant, whereby, for a specified term, the Applicant expressly authorizes one or more Certificate Approver(s) designated in such agreement to exercise EV Authority with respect to each future EV Certificate Request submitted on behalf of the Applicant and properly authenticated as originating with, or otherwise being approved by, such Certificate Approver(s).

Such an agreement MUST provide that the Applicant shall be obligated under the Subscriber Agreement for all EV Certificates issued at the request of, or approved by, such Certificate Approver(s) until such EV Authority is revoked, and MUST include mutually agreed-upon provisions for (i) authenticating the Certificate Approver when EV Certificate Requests are approved, (ii) periodic re-confirmation of the EV Authority of the Certificate Approver, (iii) secure procedures by which the Applicant can notify the CA that the EV Authority of any such Certificate Approver is revoked, and (iv) such other appropriate precautions as are reasonably necessary.

11.9. Verification of Signature on Subscriber Agreement and EV Certificate Requests

Both the Subscriber Agreement and each non-pre-authorized EV Certificate Request MUST be signed. The Subscriber Agreement MUST be signed by an authorized Contract Signer. The EV Certificate Request MUST be signed by the Certificate Requester submitting the document, unless the Certificate Request has been pre-authorized in line with Section 11.8.4 of these Guidelines. If the Certificate Requester is not also an authorized Certificate Approver, then an authorized Certificate Approver MUST independently approve the EV Certificate Request. In all cases, applicable signatures MUST be a legally valid and contain an enforceable seal or handwritten signature (for a paper Subscriber Agreement and/or EV Certificate Request), or a legally valid and enforceable electronic signature (for an electronic Subscriber Agreement and/or EV Certificate Request), that binds the Applicant to the terms of each respective document.

11.9.1. Verification Requirements

(1) **Signature:** The CA MUST authenticate the signature of the Contract Signer on the Subscriber Agreement and the signature of the Certificate Requester on each EV Certificate Request in a manner that makes it reasonably certain that the person named as the signer in the applicable document is, in fact, the person who signed the document on behalf of the Applicant.

(2) **Approval Alternative:** In cases where an EV Certificate Request is signed and submitted by a Certificate Requester who does not also function as a Certificate Approver, approval and adoption of the EV Certificate

Request by a Certificate Approver in accordance with the requirements of Section 11.10 can substitute for authentication of the signature of the Certificate Requester on such EV Certificate Request.

11.9.2. Acceptable Methods of Signature Verification

Acceptable methods of authenticating the signature of the Certificate Requester or Contract Signer include the following:

(1) Contacting the Applicant using a Verified Method of Communication for the Applicant, for the attention of the Certificate Requester or Contract Signer, as applicable, followed by a response from someone who identifies themselves as such person confirming that he/she did sign the applicable document on behalf of the Applicant;

(2) A letter mailed to the Applicant's or Agent's address, as verified through independent means in accordance with these Guidelines, for the attention of the Certificate Requester or Contract Signer, as applicable, followed by a response through a Verified Method of Communication from someone who identifies themselves as such person confirming that he/she did sign the applicable document on behalf of the Applicant;

(3) Use of a signature process that establishes the name and title of the signer in a secure manner, such as through use of an appropriately secure login process that identifies the signer before signing, or through use of a digital signature made with reference to an appropriately verified certificate; or

(4) Notarization by a notary, provided that the CA independently verifies that such notary is a legally qualified notary in the jurisdiction of the Certificate Requester or Contract Signer.

11.10. Verification of Approval of EV Certificate Request

11.10.1. Verification Requirements

In cases where an EV Certificate Request is submitted by a Certificate Requester, before the CA issues the requested EV Certificate, the CA MUST verify that an authorized Certificate Approver reviewed and approved the EV Certificate Request.

11.10.2. Acceptable Methods of Verification

Acceptable methods of verifying the Certificate Approver's approval of an EV Certificate Request include:

(1) Contacting the Certificate Approver using a Verified Method of Communication for the Applicant and obtaining oral or written confirmation that the Certificate Approver has reviewed and approved the EV Certificate Request;

(2) Notifying the Certificate Approver that one or more new EV Certificate Requests are available for review and approval at a designated access-controlled and secure Web site, followed by a login by, and an indication of approval from, the Certificate Approver in the manner required by the Web site; or

(3) Verifying the signature of the Certificate Approver on the EV Certificate Request in accordance with Section 11.9 of these Guidelines.

11.11. Verification of Certain Information Sources

11.11.1. Verified Legal Opinion

(1) **Verification Requirements:** Before relying on a legal opinion submitted to the CA, the CA MUST verify that such legal opinion meets the following requirements:

(A) **Status of Author:** The CA MUST verify that the legal opinion is authored by an independent legal practitioner retained by and representing the Applicant (or an in-house legal practitioner employed by the Applicant) (Legal Practitioner) who is either:

(i) A lawyer (or solicitor, barrister, advocate, or equivalent) licensed to practice law in the country of the Applicant's Jurisdiction of Incorporation or Registration or any jurisdiction where the Applicant maintains an office or physical facility, or

(ii) A notary that is a member of the International Union of Latin Notaries, and is licensed to practice in the country of the Applicant's Jurisdiction of Incorporation or Registration or any jurisdiction where the Applicant maintains an office or physical facility (and that such jurisdiction recognizes the role of the Latin Notary);

(B) **Basis of Opinion:** The CA MUST verify that the Legal Practitioner is acting on behalf of the Applicant and that the conclusions of the Verified Legal Opinion are based on the Legal Practitioner's stated familiarity with the relevant facts and the exercise of the Legal Practitioner's professional judgment and expertise;

(C) **Authenticity:** The CA MUST confirm the authenticity of the Verified Legal Opinion.

(2) **Acceptable Methods of Verification:** Acceptable methods of establishing the foregoing requirements for a Verified Legal Opinion are:

(A) **Status of Author:** The CA MUST verify the professional status of the author of the legal opinion by directly contacting the authority responsible for registering or licensing such Legal Practitioner(s) in the applicable jurisdiction;

(B) **Basis of Opinion:** The text of the legal opinion MUST make it clear that the Legal Practitioner is acting on behalf of the Applicant and that the conclusions of the legal opinion are based on the Legal Practitioner's stated familiarity with the relevant facts and the exercise of the practitioner's professional judgment and expertise. The legal opinion MAY also include disclaimers and other limitations customary in the Legal Practitioner's jurisdiction, provided that the scope of the disclaimed responsibility is not so great as to eliminate any substantial risk (financial, professional, and/or reputational) to the Legal Practitioner, should the legal opinion prove to be erroneous. An acceptable form of legal opinion is attached as Appendix B;

(C) **Authenticity:** To confirm the authenticity of the legal opinion, the CA MUST make a telephone call or send a copy of the legal opinion back to the Legal Practitioner at the address, phone number, facsimile, or (if available) e-mail address for the Legal Practitioner listed with the authority responsible for registering or licensing such Legal Practitioner, and obtain confirmation from the Legal Practitioner or the Legal Practitioner's assistant that the legal opinion is authentic. If a phone number is not available from the licensing authority, the CA MAY use the number listed for the Legal Practitioner in records provided by the applicable phone company, QGIS, or QIIS.

In circumstances where the opinion is digitally signed, in a manner that confirms the authenticity of the document and the identity of the signer, as verified by the CA in Section 11.11.1(2)(A), no further verification of authenticity is required.

11.11.2. Verified Accountant Letter

(1) **Verification Requirements:** Before relying on an accountant letter submitted to the CA, the CA MUST verify that such accountant letter meets the following requirements:

(A) **Status of Author:** The CA MUST verify that the accountant letter is authored by an Accounting Practitioner retained or employed by the Applicant and licensed within the country of the Applicant's Jurisdiction of Incorporation, Jurisdiction of Registration, or country where the Applicant maintains an office or physical facility. Verification of license MUST be through the member organization or regulatory organization in the Accounting Practitioner's country or jurisdiction that is appropriate to contact when verifying an accountant's license to practice in that country or jurisdiction. Such country or jurisdiction must have an accounting standards body that maintains full membership status with the International Federation of Accountants.

(B) **Basis of Opinion:** The CA MUST verify that the Accounting Practitioner is acting on behalf of the Applicant and that the conclusions of the Verified Accountant Letter are based on the Accounting Practitioner's stated familiarity with the relevant facts and the exercise of the Accounting Practitioner's professional judgment and expertise;

(C) **Authenticity:** The CA MUST confirm the authenticity of the Verified Accountant Letter.

(2) **Acceptable Methods of Verification:** Acceptable methods of establishing the foregoing requirements for a Verified Accountant Letter are listed here.

(A) **Status of Author:** The CA MUST verify the professional status of the author of the accountant letter by directly contacting the authority responsible for registering or licensing such Accounting Practitioners in the applicable jurisdiction.

(B) **Basis of Opinion:** The text of the Verified Accountant Letter MUST make clear that the Accounting Practitioner is acting on behalf of the Applicant and that the information in the letter is based on the Accounting Practitioner's stated familiarity with the relevant facts and the exercise of the practitioner's professional judgment and expertise. The Verified Accountant Letter MAY also include disclaimers and other limitations customary in the Accounting Practitioner's jurisdiction, provided that the scope of the disclaimed responsibility is not so great as to eliminate any substantial risk (financial, professional, and/or reputational) to the Accounting Practitioner, should the Verified Accountant Letter prove to be erroneous. Acceptable forms of Verified Accountant Letter are attached as Appendix C.

(C) **Authenticity:** To confirm the authenticity of the accountant's opinion, the CA MUST make a telephone call or send a copy of the Verified Accountant Letter back to the Accounting Practitioner at the address, phone number, facsimile, or (if available) e-mail address for the Accounting Practitioner listed with the authority responsible for registering or licensing such Accounting Practitioners and obtain confirmation from the Accounting Practitioner or the Accounting Practitioner's assistant that the accountant letter is authentic. If a phone number is not available from the licensing authority, the CA MAY use the number listed for the Accountant in records provided by the applicable phone company, QGIS, or QIIS.

In circumstances where the opinion is digitally signed, in a manner that confirms the authenticity of the document and the identity of the signer, as verified by the CA in Section 11.11.2(2)(A), no further verification of authenticity is required.

11.11.3. Face-to-Face Validation

(1) **Verification Requirements:** Before relying on face-to-face vetting documents submitted to the CA, the CA MUST verify that the Third-Party Validator meets the following requirements:

(A) **Qualification of Third-Party Validator:** The CA MUST independently verify that the Third-Party Validator is a legally-qualified Latin Notary or Notary (or legal equivalent in the Applicant's jurisdiction), Lawyer, or Accountant in the jurisdiction of the individual's residency;

(B) **Document Chain of Custody:** The CA MUST verify that the Third-Party Validator viewed the Vetting Documents in a face-to-face meeting with the individual being validated;

(C) **Verification of Attestation:** If the Third-Party Validator is not a Latin Notary, then the CA MUST confirm the authenticity of the attestation and vetting documents.

(2) **Acceptable Methods of Verification:** Acceptable methods of establishing the foregoing requirements for vetting documents are:

(A) **Qualification of Third-Party Validator:** The CA MUST verify the professional status of the Third-Party Validator by directly contacting the authority responsible for registering or licensing such Third-Party Validators in the applicable jurisdiction;

(B) **Document Chain of Custody:** The Third-Party Validator MUST submit a statement to the CA which attests that they obtained the Vetting Documents submitted to the CA for the individual during a face-to-face meeting with the individual;

(C) **Verification of Attestation:** If the Third-Party Validator is not a Latin Notary, then the CA MUST confirm the authenticity of the vetting documents received from the Third-Party Validator. The CA MUST make a telephone call to the Third-Party Validator and obtain confirmation from them or their assistant that they performed the face-to-face validation. The CA MAY rely upon self-reported information obtained from the Third-Party Validator for the sole purpose of performing this verification process. In circumstances where the attestation is digitally signed, in a manner that confirms the authenticity of the documents, and the identity of the signer as verified by the CA in Section 11.11.3(1)(A), no further verification of authenticity is required.

11.11.4. Independent Confirmation From Applicant

An Independent Confirmation from the Applicant is a confirmation of a particular fact (e.g., confirmation of the employee or agency status of a Contract Signer or Certificate Approver, confirmation of the EV Authority of a Certificate Approver, etc.) that is:

(A) Received by the CA from a Confirming Person (someone other than the person who is the subject of the inquiry) that has the appropriate authority to confirm such a fact, and who represents that he/she has confirmed such fact;

(B) Received by the CA in a manner that authenticates and verifies the source of the confirmation; and

(C) Binding on the Applicant.

An Independent Confirmation from the Applicant MAY be obtained via the following procedure:

(1) **Confirmation Request:** The CA MUST initiate a Confirmation Request via an appropriate out-of-band communication, requesting verification or confirmation of the particular fact at issue as follows:

(A) **Addressee:** The Confirmation Request MUST be directed to:

(i) A position within the Applicant's organization that qualifies as a Confirming Person (e.g., Secretary, President, CEO, CFO, COO, CIO, CSO, Director, etc.) and is identified by name and title in a current QGIS, QIIS, QTIS, Verified Legal Opinion, Verified Accountant Letter, or by contacting the Applicant using a Verified Method of Communication; or

(ii) The Applicant's Registered Agent or Registered Office in the Jurisdiction of Incorporation as listed in the official records of the Incorporating Agency, with instructions that it be forwarded to an appropriate Confirming Person; or

(iii) A named individual verified to be in the direct line of management above the Contract Signer or Certificate Approver by contacting the Applicant's Human Resources Department by phone or mail (at the phone number or address for the Applicant's Place of Business, verified in accordance with these Guidelines).

(B) **Means of Communication:** The Confirmation Request MUST be directed to the Confirming Person in a manner reasonably likely to reach such person. The following options are acceptable:

(i) By paper mail addressed to the Confirming Person at:

(1) The address of the Applicant's Place of Business as verified by the CA in accordance with these Guidelines, or

(2) The business address for such Confirming Person specified in a current QGIS, QTIS, QIIS, Verified Professional Letter, or

(3) The address of the Applicant's Registered Agent or Registered Office listed in the official records of the Jurisdiction of Incorporation, or

(ii) By e-mail addressed to the Confirming Person at the business e-mail address for such person listed in a current QGIS, QTIS, QIIS, Verified Legal Opinion, or Verified Accountant Letter; or

(iii) By telephone call to the Confirming Person, where such person is contacted by calling the main phone number of the Applicant's Place of Business (verified in accordance with these Guidelines) and asking to speak to such person, and a person taking the call identifies him- or herself as such person; or

(iv) By facsimile to the Confirming Person at the Place of Business. The facsimile number must be listed in a current QGIS, QTIS, QIIS, Verified Legal Opinion, or Verified Accountant Letter. The cover page must be clearly addressed to the Confirming Person.

(2) **Confirmation Response:** The CA MUST receive a response to the Confirmation Request from a Confirming Person that confirms the particular fact at issue. Such response MAY be provided to the CA by telephone, by e-mail, or by paper mail, so long as the CA can reliably verify that it was provided by a Confirming Person in response to the Confirmation Request.

(3) The CA MAY rely on a verified Confirming Person to confirm their own contact information: email address, telephone number, and facsimile number. The CA MAY rely on this verified contact information for future correspondence with the Confirming Person if:

(A) The domain of the e-mail address is owned by the Applicant and is the Confirming Person's own e-mail address and not a group e-mail alias;

(B) The Confirming Person's telephone/fax number is verified by the CA to be a telephone number that is part of the organization's telephone system, and is not the personal phone number for the person.

11.11.5. Qualified Independent Information Source

A Qualified Independent Information Source (QIIS) is a regularly-updated and publicly available database that is generally recognized as a dependable source for certain information. A database qualifies as a QIIS if the CA determines that:

(1) Industries other than the certificate industry rely on the database for accurate location, contact, or other information; and

(2) The database provider updates its data on at least an annual basis.

The CA SHALL use a documented process to check the accuracy of the database and ensure its data is acceptable, including reviewing the database provider's terms of use. The CA SHALL NOT use any data in a QIIS that the CA knows is (i) self-reported and (ii) not verified by the QIIS as accurate. Databases in which the CA or its owners or affiliated companies maintain a controlling interest, or in which any Registration Authorities or subcontractors to whom the CA has outsourced any portion of the vetting process (or their owners or affiliated companies) maintain any ownership or beneficial interest, do not qualify as a QIIS.

11.11.6. Qualified Government Information Source

A Qualified Government Information Source (QGIS) is a regularly-updated and current, publicly available, database designed for the purpose of accurately providing the information for which it is consulted, and which is generally recognized as a dependable source of such information provided that it is maintained by a Government Entity, the reporting of data is required by law, and false or misleading reporting is punishable with criminal or civil penalties. Nothing in these Guidelines shall prohibit the use of third-party vendors to obtain the information from the Government Entity provided that the third party obtains the information directly from the Government Entity.

11.11.7. Qualified Government Tax Information Source

A Qualified Government Tax Information Source is a Qualified Government Information Source that specifically contains tax information relating to Private Organizations, Business Entities or Individuals (e.g., the IRS in the United States).

11.12. Other Verification Requirements

11.12.1. High Risk Status

The High Risk Certificate requirements of Section 4.2.1 of the Baseline Requirements apply equally to EV Certificates.

11.12.2. Denied Lists and Other Legal Black Lists

(1) **Verification Requirements:** The CA MUST verify whether the Applicant, the Contract Signer, the Certificate Approver, the Applicant's Jurisdiction of Incorporation, Registration, or Place of Business:

(A) Is identified on any government denied list, list of prohibited persons, or other list that prohibits doing business with such organization or person under the laws of the country of the CA's jurisdiction(s) of operation; or

(B) Has its Jurisdiction of Incorporation, Registration, or Place of Business in any country with which the laws of the CA's jurisdiction prohibit doing business.

The CA MUST NOT issue any EV Certificate to the Applicant if either the Applicant, the Contract Signer, or Certificate Approver or if the Applicant's Jurisdiction of Incorporation or Registration or Place of Business is on any such list.

(2) **Acceptable Methods of Verification:** The CA MUST take reasonable steps to verify with the following lists and regulations:

(A) If the CA has operations in the U.S., the CA MUST take reasonable steps to verify with the following US Government denied lists and regulations:

(i) BIS Denied Persons List - http://www.bis.doc.gov/dpl/thedeniallist.asp

(ii) BIS Denied Entities List - http://www.bis.doc.gov/Entities/Default.htm

(iii) US Treasury Department List of Specially Designated Nationals and Blocked Persons - http://www.treas.gov/ofac/t11sdn.pdf

(iv) US Government export regulations

(B) If the CA has operations in any other country, the CA MUST take reasonable steps to verify with all equivalent denied lists and export regulations (if any) in such other country.

11.12.3. Parent/Subsidiary/Affiliate Relationship

A CA verifying an Applicant using information of the Applicant's Parent, Subsidiary, or Affiliate, when allowed under section 11.4.1, 11.5, 11.6.1, or 11.7.1, MUST verify the Applicant's relationship to the Parent, Subsidiary, or Affiliate. Acceptable methods of verifying the Applicant's relationship to the Parent, Subsidiary, or Affiliate include the following:

(1) QIIS or QGIS: The relationship between the Applicant and the Parent, Subsidiary, or Affiliate is identified in a QIIS or QGIS;

(2) Independent Confirmation from the Parent, Subsidiary, or Affiliate: A CA MAY verify the relationship between an Applicant and a Parent, Subsidiary, or Affiliate by obtaining an Independent Confirmation from the appropriate Parent, Subsidiary, or Affiliate (as described in Section 11.11.4);

(3) Contract between CA and Parent, Subsidiary, or Affiliate: A CA MAY verify the relationship between an Applicant and a Parent, Subsidiary, or Affiliate by relying on a contract between the CA and the Parent, Subsidiary, or Affiliate that designates the Certificate Approver with such EV Authority, provided that the contract is signed by the Contract Signer and provided that the agency and Signing Authority of the Contract Signer have been verified;

(4) Verified Professional Letter: A CA MAY verify the relationship between an Applicant and a Parent, Subsidiary, or Affiliate by relying on a Verified Professional Letter; or

(5) Corporate Resolution: A CA MAY verify the relationship between an Applicant and a Subsidiary by relying on a properly authenticated corporate resolution that approves creation of the Subsidiary or the Applicant, provided that such resolution is (i) certified by the appropriate corporate officer (e.g., secretary), and (ii) the CA can reliably verify that the certification was validly signed by such person, and that such person does have the requisite authority to provide such certification.

11.13. Final Cross-Correlation and Due Diligence

Except for Enterprise EV Certificates:

(1) The results of the verification processes and procedures outlined in these Guidelines are intended to be viewed both individually and as a group. Thus, after all of the verification processes and procedures are completed, the CA MUST have a person who is not responsible for the collection of information review all of the information and documentation assembled in support of the EV Certificate application and look for discrepancies or other details requiring further explanation.

(2) The CA MUST obtain and document further explanation or clarification from the Applicant, Certificate Approver, Certificate Requester, Qualified Independent Information Sources, and/or other sources of information, as necessary, to resolve those discrepancies or details that require further explanation.

(3) The CA MUST refrain from issuing an EV Certificate until the entire corpus of information and documentation assembled in support of the EV Certificate Request is such that issuance of the EV Certificate will not communicate factual information that the CA knows, or the exercise of due diligence should discover from the assembled information and documentation, to be inaccurate,. If satisfactory explanation and/or additional documentation are not received within a reasonable time, the CA MUST decline the EV Certificate Request and SHOULD notify the Applicant accordingly.

(4) In the case where some or all of the documentation used to support the application is in a language other than the CA's normal operating language, the CA or its Affiliate MUST perform the requirements of this Final Cross-Correlation and Due Diligence section using employees under its control and having appropriate training, experience, and judgment in confirming organizational identification and authorization and fulfilling all qualification requirements contained in Section 14.1 of these Guidelines. When employees under the control of the CA do not possess the language skills necessary to perform the Final Cross-Correlation and Due Diligence a CA MAY:

(A) Rely on language translations of the relevant portions of the documentation, provided that the translations are received from a Translator; or

(B) When the CA has utilized the services of an RA, the CA MAY rely on the language skills of the RA to perform the Final Cross-Correlation and Due Diligence, provided that the RA complies with Section 11.13, Subsections (1), (2) and (3). Notwithstanding the foregoing, prior to issuing the EV Certificate, the CA MUST review the work completed by the RA and determine that all requirements have been met; or

(C) When the CA has utilized the services of an RA, the CA MAY rely on the RA to perform the Final Cross-Correlation and Due Diligence, provided that the RA complies with this section and is subjected to the Audit Requirements of Sections 17.5 and 17.6.

In the case of Enterprise EV Certificates to be issued in compliance with the requirements of Section 14.2 of these Guidelines, the Enterprise RA MAY perform the requirements of this Final Cross-Correlation and Due Diligence section.

11.14. Requirements for Re-use of Existing Documentation

For each EV Certificate Request, including requests to renew existing EV Certificates, the CA MUST perform all authentication and verification tasks required by these Guidelines to ensure that the request is properly authorized by the Applicant and that the information in the EV Certificate is still accurate and valid. This section sets forth the age limitations on for the use of documentation collected by the CA.

11.14.1. Validation For Existing Subscribers

If an Applicant has a currently valid EV Certificate issued by the CA, a CA MAY rely on its prior authentication and verification of:

(1) The Principal Individual verified under Section 11.2.2 (4) if the individual is the same person as verified by the CA in connection with the Applicant's previously issued and currently valid EV Certificate;

(2) The Applicant's Place of Business under Section 11.4.1;

(3) The Applicant's Verified Method of Communication required by Section 11.5 but still MUST perform the verification required by section 11.5.2(B);

(4) The Applicant's Operational Existence under Section 11.6;

(5) The Name, Title, Agency and Authority of the Contract Signer, and Certificate Approver, under Section 11.8; and

(6) The Applicant's right to use the specified Domain Name under Section 11.7, provided that the CA verifies that the WHOIS record still shows the same registrant as when the CA verified the specified Domain Name for the initial EV Certificate.

11.14.2. Re-issuance Requests

A CA may rely on a previously verified certificate request to issue a replacement certificate, so long as the certificate being referenced was not revoked due to fraud or other illegal conduct, if:

(1) The expiration date of the replacement certificate is the same as the expiration date of the EV Certificate that is being replaced, and

(2) The Subject Information of the Certificate is the same as the Subject in the EV Certificate that is being replaced.

11.14.3. Age of Validated Data

(1) Except for reissuance of an EV Certificate under Section 11.14.2 and except when permitted otherwise in Section 11.14.1, the age of all data used to support issuance of an EV Certificate (before revalidation is required) SHALL NOT exceed the following limits:

(A) Legal existence and identity – thirteen months;

(B) Assumed name – thirteen months;

(C) Address of Place of Business – thirteen months;

(D) Verified Method of Communication – thirteen months;

(E) Operational existence – thirteen months;

(F) Domain Name – thirteen months;

(G) Name, Title, Agency, and Authority – thirteen months, unless a contract between the CA and the Applicant specifies a different term, in which case, the term specified in such contract controls. For example, the contract MAY include the perpetual assignment of EV roles until revoked by the Applicant or CA, or until the contract expires or is terminated.

(2) The thirteen-month period set forth above SHALL begin to run on the date the information was collected by the CA.

(3) The CA MAY reuse a previously submitted EV Certificate Request, Subscriber Agreement, or Terms of Use, including use of a single EV Certificate Request in support of multiple EV Certificates containing the same Subject to the extent permitted under Sections 11.9 and 11.10.

(4) The CA MUST repeat the verification process required in these Guidelines for any information obtained outside the time limits specified above except when permitted otherwise under section 11.14.1.

12. Certificate Issuance by a Root CA

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

Root CA Private Keys MUST NOT be used to sign EV Certificates.

13. Certificate Revocation and Status Checking

The requirements in Section 4.9 of the Baseline Requirements apply equally to EV Certificates. However, CAs MUST ensure that CRLs for an EV Certificate chain can be downloaded in no more than three (3) seconds over an analog telephone line under normal network conditions.

14. Employee and third party issues

14.1. Trustworthiness and Competence

14.1.1. Identity and Background Verification

Prior to the commencement of employment of any person by the CA for engagement in the EV Processes, whether as an employee, agent, or an independent contractor of the CA, the CA MUST:

(1) **Verify the Identity of Such Person:** Verification of identity MUST be performed through:

(A) The personal (physical) presence of such person before trusted persons who perform human resource or security functions, and

(B) The verification of well-recognized forms of government-issued photo identification (e.g., passports and/or drivers licenses);

and

(2) **Verify the Trustworthiness of Such Person:** Verification of trustworthiness SHALL include background checks, which address at least the following, or their equivalent:

(A) Confirmation of previous employment,

(B) Check of professional references;

(C) Confirmation of the highest or most-relevant educational qualification obtained;

(D) Search of criminal records (local, state or provincial, and national) where allowed by the jurisdiction in which the person will be employed;

and

(3) In the case of employees already in the employ of the CA at the time of adoption of these Guidelines whose identity and background has not previously been verified as set forth above, the CA SHALL conduct such verification within three months of the date of adoption of these Guidelines.

14.1.2. Training and Skills Level

The requirements in Section 5.3.3 of the Baseline Requirements apply equally to EV Certificates and these Guidelines. The required internal examination must relate to the EV Certificate validation criteria outlined in these Guidelines.

14.1.3. Separation of Duties

(1) The CA MUST enforce rigorous control procedures for the separation of validation duties to ensure that no one person can single-handedly validate and authorize the issuance of an EV Certificate. The Final Cross-Correlation and Due Diligence steps, as outlined in Section 11.13, MAY be performed by one of the persons. For example, one Validation Specialist MAY review and verify all the Applicant information and a second Validation Specialist MAY approve issuance of the EV Certificate.

(2) Such controls MUST be auditable.

14.2. Delegation of Functions to Registration Authorities and Subcontractors

14.2.1. General

The CA MAY delegate the performance of all or any part of a requirement of these Guidelines to an Affiliate or a Registration Authority (RA) or subcontractor, provided that the process employed by the CA fulfills all of the requirements of Section 11.13. Affiliates and/or RAs must comply with the qualification requirements of Section 14.1 of these Guidelines.

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

14.2.2. Enterprise RAs

The CA MAY contractually authorize the Subject of a specified Valid EV Certificate to perform the RA function and authorize the CA to issue additional EV Certificates at third and higher domain levels that are contained within the domain of the original EV Certificate (also known as an Enterprise EV Certificate). In such case, the Subject SHALL be considered an Enterprise RA, and the following requirements SHALL apply:

(1) An Enterprise RA SHALL NOT authorize the CA to issue an Enterprise EV Certificate at the third or higher domain levels to any Subject other than the Enterprise RA or a business that is owned or directly controlled by the Enterprise RA;

(2) In all cases, the Subject of an Enterprise EV Certificate MUST be an organization verified by the CA in accordance with these Guidelines;

(3) The CA MUST impose these limitations as a contractual requirement with the Enterprise RA and monitor compliance by the Enterprise RA;

(4) The Final Cross-Correlation and Due Diligence requirements of Section 11.13 of these Guidelines MAY be performed by a single person representing the Enterprise RA; and

(5) The audit requirements of Section 17.1 of these Guidelines SHALL apply to the Enterprise RA, except in the case where the CA maintains control over the Root CA Private Key or Subordinate CA Private Key used to issue the Enterprise EV Certificates, in which case, the Enterprise RA MAY be exempted from the audit requirements.

14.2.3. Guidelines Compliance Obligation

In all cases, the CA MUST contractually obligate each Affiliate, RA, subcontractor, and Enterprise RA to comply with all applicable requirements in these Guidelines and to perform them as required of the CA itself. The CA SHALL enforce these obligations and internally audit each Affiliate's, RA's, subcontractor's, and Enterprise RA's compliance with these Requirements on an annual basis.

14.2.4. Allocation of Liability

As specified in Section 9.8 of the Baseline Requirements.

15. Data Records

As specified in Section 5.4 of the Baseline Requirements.

16. Data Security

As specified in Section 5 of the Baseline Requirements. In addition, systems used to process and approve EV Certificate Requests MUST require actions by at least two trusted persons before creating an EV Certificate.

17. Audit

17.1. Eligible Audit Schemes

A CA issuing EV Certificates SHALL undergo an audit in accordance with one of the following schemes:

(i) WebTrust Program for CAs audit and WebTrust EV Program audit, or

(ii) ETSI TS 102 042 audit.

If the CA is a Government Entity, an audit of the CA by the appropriate internal government auditing agency is acceptable in lieu of the audits specified above, provided that such internal government auditing agency publicly certifies in writing that its audit addresses the criteria specified in one of the above audit schemes and certifies that the government CA has successfully passed the audit.

EV audits MUST cover all CA obligations under these Guidelines regardless of whether they are performed directly by the CA or delegated to an RA or subcontractor.

17.2. Audit Period

CAs issuing EV Certificates MUST undergo an annual audit that meets the criteria of Section 17.1.

17.3. Audit Record

CAs SHOULD make its audit report publicly available no later than three months after the end of the audit period. If there is a delay greater than three months and if so requested by an Application Software Supplier, the CA MUST provide an explanatory letter signed by its auditor.

17.4. Pre-Issuance Readiness Audit

(1) If the CA has a currently valid WebTrust Seal of Assurance for CAs, then, before issuing EV Certificates, the CA and its Root CA MUST successfully complete a point-in-time readiness assessment audit against the WebTrust EV Program.

(2) If the CA has a currently valid ETSI 102 042 audit, then, before issuing EV Certificates, the CA and its Root CA MUST successfully complete a point-in-time readiness assessment audit against ETSI TS 102 042.

(3) If the CA does not have a currently valid WebTrust Seal of Assurance for CAs or an ETSI 102 042 audit, then, before issuing EV Certificates, the CA and its Root CA MUST successfully complete either: (i) a point-in-time readiness assessment audit against the WebTrust for CA Program, or (ii) a point-in-time readiness assessment audit against the WebTrust EV Program, or an ETSI TS 102 042 audit.

The CA MUST complete any required point-in-time readiness assessment no earlier than twelve (12) months prior to issuing an EV Certificate. The CA MUST undergo a complete audit under such scheme within ninety (90) days of issuing the first EV Certificate.

17.5. Regular Self Audits

During the period in which it issues EV Certificates, the CA MUST strictly control its service quality by performing ongoing self audits against a randomly selected sample of at least three percent of the EV Certificates it has issued in the period beginning immediately after the last sample was taken. For all EV Certificates where the Final Cross-Correlation and Due Diligence requirements of Section 11.13 of these Guidelines is performed by an RA, the CA MUST strictly control its service quality by performing ongoing self audits against a randomly selected sample of at least six percent of the EV Certificates it has issued in the period beginning immediately after the last sample was taken.

17.6. Auditor Qualification

A Qualified Auditor (as defined in Section 8.2 of the Baseline Requirements) MUST perform the CA's audit.

17.7. Root CA Key Pair Generation

All requirements in Section 6.1.1.1 of the Baseline Requirements apply equally to EV Certificates. However, for Root CA Key Pairs generated after the release of these Guidelines, the Root CA Key Pair generation ceremony MUST be witnessed by the CA's Qualified Auditor in order to observe the process and the controls over the integrity and confidentiality of the Root CA Key Pairs produced. The Qualified Auditor MUST then issue a report opining that the CA, during its Root CA Key Pair and Certificate generation process:

(1) Documented its Root CA key generation and protection procedures in its Certificate Policy, and its Certification Practices Statement;

(2) Included appropriate detail in its Root Key Generation Script;

(3) Maintained effective controls to provide reasonable assurance that the Root CA key pair was generated and protected in conformity with the procedures described in its CP/CPS and with its Root Key Generation Script;

(4) Performed, during the Root CA key generation process, all the procedures required by its Root Key Generation Script.

18. Liability and Indemnification

CAs MAY limit their liability as described in Section 9.8 of the Baseline Requirements except that a CA MAY NOT limit its liability to Subscribers or Relying Parties for legally recognized and provable claims to a monetary amount less than two thousand US dollars per Subscriber or Relying Party per EV Certificate.

A CA's indemnification obligations and a Root CA's obligations with respect to subordinate CAs are set forth in Section 9.9 of the Baseline Requirements.

Appendix A - User Agent Verification (Normative)

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

Appendix B - Sample Attorney Opinions Confirming Specified Information (Informative)

[Law Firm Letterhead]

[Date]

To:	***[Name of Issuing Certification Authority]*** ***[Address / fax number of Issuing CA – may be sent by fax or email attachment]***
Re:	**EV Certificate Request No. _____** ***[CA Reference Number]***
Client:	***[Exact company name of Client – see footnote 1]***
Client Representative:	***[Exact name of Client Representative who signed the Application – see footnote 2]***
Application Date:	***[Insert date of Client's Application to the Issuing CA,]***

This firm represents *[exact company name of Client]*[1] ("Client"), who has submitted the Application to you dated as of the Application Date shown above ("Application"). We have been asked by our Client to present you with our opinion as stated in this letter.

[Insert customary preliminary matters for opinion letters in your jurisdiction.]

On this basis, we hereby offer the following opinion:

1. That [exact company name of Client] ("Company") is a duly formed [corporation, LLC, etc.] that is "active," "valid," "current," or the equivalent under the laws of the state/province of [name of governing jurisdiction where Client is incorporated or registered] and is not under any legal disability known to the author of this letter.

2. That Company conducts business under the assumed name or "DBA"*[assumed name of the Applicant]* and has registered such name with the appropriate government agency in the jurisdiction of its place of business below.

3. That *[name of Client's Representative]*[2] has authority to act on behalf of Company to: [*select as appropriate*] (a) provide the information about Company required for issuance of the EV Certificates as contained in the attached Application, (b) request one or more EV Certificates and to designate other persons to request EV Certificates, and (c) agree to the relevant contractual obligations contained in the Subscriber Agreement on behalf of Company.

4. That Company has a physical presence and its place of business is at the following location:

_____

_____

_____

[1] Note: This must be the Client's exact corporate name, as registered with the relevant Incorporating Agency in the Client's Jurisdiction of Incorporation. This is the name that will be included in the EV Certificate.

[2] Note: If necessary to establish the Client Representative's actual authority, you may rely on a Power of Attorney from an officer of Client who has authority to delegate the authority to the Client Representative.

5. That Company can be contacted at its stated place of business at the following telephone number:

_____

6. That Company has an active current Demand Deposit Account with a regulated financial institution.

7. That Company has the right to use the following Domain Name in identifying itself on the Internet:

_____

[Insert customary limitations and disclaimers for opinion letters in your jurisdiction.

[Name and signature]

[Jurisdiction(s) in which attorney / Latin notary is admitted to practice][3]

cc: [Send copy to Client*]*

[3] Note: This letter may be issued by in-house counsel for the Client so long as permitted by the rules of your jurisdiction.

Appendix C - Sample Accountant Letters Confirming Specified Information

(Informative)

It is acceptable for professional accountants to provide letters that address specified matters. The letters would be provided in accordance with the professional standards in the jurisdiction in which the accountant practices.

Two examples of the letter that might be prepared by an accountant in the United States and in Canada follow:

UNITED STATES

To the [Certification Authority] and Management of [Client]:

We have performed the procedures enumerated below, which were agreed to by the Managements of Client, solely to assist you in evaluating the company's application for an Extended Validation (EV) Certificate, dated....., 20..... This agreed-upon procedures engagement was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. The sufficiency of these procedures is solely the responsibility of those parties specified in this report. Consequently, we make no representation regarding the sufficiency of the procedures described below either for the purpose for which this report has been requested or for any other purpose.

Specified Information:	**Procedure:** **(Note 1: These are illustrative of the procedures that would be undertaken and are designed to meet the needs of the Certification Authorities issuing Extended Validation Certificates)**	**Results:** **(Note 2: If you are unavailable to perform any of the stated procedure, this should be noted in this column. Any exceptions should be noted in a separate paragraph below)**
Legal Name - 123456 Delaware corporation	Agree legal name to permanent audit file information (If audit has been completed).	Legal name on the application agrees with the information contained in our permanent file with respect to Client. (If there is no permanent file, state this fact)
Doing business as - "Name"	Agree name to government data base of business names	The name "Name" is registered with the (name of database to which the name was agreed)
Physical location - "Address Information"	Visit the location at the address	Site visit completed at Address
Business Phone Number - 555 999 9999	Phone the number provided and confirm that it was answered by the named organization	Phoned Business Number and noted that it was answered with the Doing Business As name. This would provided by the receptionist

Bank Account – “Bank Name”, “Account Number”	Request a letter directly from “the Bank” confirming the existence of the account for the benefit of “the Client”	Received letter directly from “the Bank” confirming the existence of the account for the benefit of “the Client”
The corporate officers are "NAMED" (verified officer)	Agree Names to annual shareholders meeting minutes (Note - not required to personally know the officers)	Agreed Names listed as corporate officers on the application to minute books maintained by the Client
Name of application signer and approver	Obtain letter from verified Officer confirming the names of the application signer and approver	Obtained letter from the President confirming the names of the duly authorized names of the application signer and approver as they appear in the application

We were not engaged to and did not conduct an examination, the objective of which would be the expression of an opinion on the Application for Extended Validation Certificate. Accordingly, we do not express such an opinion. Had we performed additional procedures, other matters might have come to our attention that would have been reported to you.

This report is intended solely for the information and use of the Certification Authority and managements of Client, and is not intended to be and should not be used by anyone other than these specified parties.

[Signature]

[Date]

CANADA

To: [Name of Certification Authority]

Re: Client Limited [Applicant]

As specifically agreed, I/we have performed the following procedures in connection with the above company's application for an Extended Validation (EV) Certificate, dated ....., 20.... with respect to the following specified information contained in the application

Specified Information:	**Procedure:** **(Note 1: These are illustrative of the procedures that would be undertaken and are designed to meet the needs of the Certification Authorities issuing Extended Validation Certificates)**	**Results:** **(Note 2: If you are unavailable to perform any of the stated procedure, this should be noted in this column. Any exceptions should be noted in a separate paragraph below)**

Legal Name - 123456 Ontario limited	Agree legal name to permanent audit file information (If audit has been completed)	Legal name on the application agrees with the information contained in our permanent file with respect to Client. (If there is no permanent file, state this fact)
Doing business as - "Name"	Agree name to government data base of business names	The name “Name” is registered with the (name of database to which the name was agreed)
Physical location - "Address Information"	Visit the location at the address	Site visit completed at Address
Business Phone Number - 555 999 9999	Phone the number provided and confirm that it was answered by the named organization	Phoned Business Number and noted that it was answered with the Doing Business As name. This would provided by the receptionist
Bank Account – “Bank Name”, “Account Number”	Request a letter directly from “the Bank” confirming the existence of the account for the benefit of “the Client”	Received letter directly from “the Bank” confirming the existence of the account for the benefit of “the Client”
The corporate officers are "NAMED" (verified officer)	Agree Names to annual shareholders meeting minutes (Note - not required to personally know the officers)	Agreed Names listed as corporate officers on the application to minute books maintained by the Client
Name of application signer and approver	Obtain letter from verified Officer confirming the names of the application signer and approver	Obtained letter from the President confirming the names of the duly authorized names of the application signer and approver as they appear in the application

As a result of applying the above procedures, I/we found [no / the following] exceptions [list of exceptions]. However, these procedures do not constitute an audit of the company's application for an EV Certificate, and therefore I express no opinion on the application dated ....., 20.....

This letter is for use solely in connection with the application for an Extended Validation Certificate by [Client] dated ....., 20.....

City

(signed) .....

Appendix D - Country-Specific Interpretative Guidelines (Normative)

NOTE: This appendix provides alternative interpretations of the EV Guidelines for countries that have a language, cultural, technical, or legal reason for deviating from a strict interpretation of the EV Guidelines. More specific information for particular countries may be added to this appendix in the future.

1. Organization Names

(1) Non-Latin Organization Name

Where an EV Applicant's organization name is not registered with a QGIS in *Latin* characters and the Applicant's foreign character organization name and registration have been verified with a QGIS in accordance with these Guidelines, a CA MAY include a Latin character organization name in the EV Certificate. In such a case, the CA MUST follow the procedures laid down in this section.

(2) Romanized Names

In order to include a transliteration/Romanization of the registered name, the Romanization MUST be verified by the CA using a system officially recognized by the Government in the Applicant's Jurisdiction of Incorporation.

If the CA can not rely on a transliteration/Romanization of the registered name using a system officially recognized by the Government in the Applicant's Jurisdiction of Incorporation, then it MUST rely on one of the options below, in order of preference:

(A) A system recognized by the International Organization for Standardization (ISO);

(B) A system recognized by the United Nations; or

(C) A Lawyer's Opinion or Accountant's Letter confirming the proper Romanization of the registered name.

(3) Translated Name

In order to include a Latin character name in the EV certificate that is not a direct Romanization of the registered name (e.g. an English Name) the CA MUST verify that the Latin character name is:

(A) Included in the Articles of Incorporation (or equivalent document) filed as part of the organization registration; or

(B) Recognized by a QTIS in the Applicant's Jurisdiction of Incorporation as the Applicant's recognized name for tax filings; or

(C) Confirmed with a QIIS to be the name associated with the registered organization; or

(D) Confirmed by a Verified Legal Opinion or Accountant's Letter to be a translated trading name associated with the registered organization.

Country-Specific Procedures

D-1. Japan

As interpretation of the procedures set out above:

1. Organization Names

(A) The Revised Hepburn method of Romanization, as well as Kunrei-shiki and Nihon-shiki methods described in ISO 3602, are acceptable for Japanese Romanizations.

(B) The CA MAY verify the Romanized transliteration, language translation (e.g. English name), or other recognized Roman-letter substitute of the Applicant's formal legal name with either a QIIS, Verified Legal Opinion, or Verified Accountant Letter.

(C) The CA MAY use the Financial Services Agency to verify a Romanized, translated, or other recognized Roman-letter substitute name. When used, the CA MUST verify that the translated English is recorded in the audited Financial Statements.

(D) When relying on Articles of Incorporation to verify a Romanized, translated, or other recognized Roman-letter substitute name, the Articles of Incorporation MUST be accompanied either: by a document, signed with the original Japanese Corporate Stamp, that proves that the Articles of Incorporation are authentic and current, or by a Verified Legal Opinion or a Verified Accountant Letter. The CA MUST verify the authenticity of the Corporate Stamp.

(E) A Romanized, translated, or other recognized Roman-lettered substitute name confirmed in accordance with this Appendix D-1 stored in the ROBINS database operated by JIPDEC MAY be relied upon by a CA for determining the allowed organization name during any issuance or renewal process of an EV Certificate without the need to re-perform the above procedures.

2. Accounting Practitioner

In Japan:

(A) Accounting Practitioner includes either a certified public accountant (公認会計士 - Konin-kaikei-shi) or a licensed tax accountant (税理士 – Zei-ri-shi).

(B) The CA MUST verify the professional status of the Accounting Practitioner through direct contact with the relevant local member association that is affiliated with either the Japanese Institute of Certified Public Accountants (http://www.hp.jicpa.or.jp), the Japan Federation of Certified Tax Accountant's Associations (http://www.nichizeiren.or.jp), or any other authoritative source recognized by the Japanese Ministry of Finance (http://www.mof.go.jp) as providing the current registration status of such professionals.

3. Legal Practitioner

In Japan:

(A) Legal Practitioner includes any of the following:

a licensed lawyer (弁護士 - Ben-go-shi),

a judicial scrivener (司法書士 - Shiho-sho-shi lawyer), an administrative solicitor (行政書士 - Gyosei-sho-shi Lawyer), or a notary public (公証人 - Ko-sho-nin).

For purposes of the EV Guidelines, a Japanese Notary Public is considered equivalent to a Latin Notary.

(B) The CA MUST verify the professional status of the Legal Practitioner by direct contact through the relevant local member association that is affiliated with one of the following national associations:

the Japan Federation of Bar Associations (http://www.nichibenren.or.jp),

the Japan Federation of Shiho-Shoshi Lawyer's Associations (http://www.shiho-shoshi.or.jp),

the Japan Federation of Administrative Solicitors (http://www.gyosei.or.jp),

the Japan National Notaries Association (http://www.koshonin.gr.jp), or

any other authoritative source recognized by the Japanese Ministry of Justice (http://www.moj.go.jp) as providing the current registration status of such professionals.

Appendix E - Sample Contract Signer's Representation/Warranty (Informative)

A CA may rely on the Contract Signer's authority to enter into the Subscriber Agreement using a representation/warranty executed by the Contract Signer. An example of an acceptable warranty is as follows:

> [CA] and Applicant are entering into a legally valid and enforceable Subscriber Agreement that creates extensive obligations on Applicant. An EV Certificate serves as a form of digital identity for Applicant. The loss or misuse of this identity can result in great harm to the Applicant. By signing this Subscriber Agreement, the contract signer acknowledges that they have the authority to obtain the digital equivalent of a company stamp, seal, or (where applicable) officer's signature to establish the authenticity of the company's website, and that [Applicant name] is responsible for all uses of its EV Certificate. By signing this Agreement on behalf of [Applicant name], the contract signer represents that the contract signer (i) is acting as an authorized representative of [Applicant name], (ii) is expressly authorized by [Applicant name] to sign Subscriber Agreements and approve EV Certificate requests on Applicant's behalf, and (iii) has confirmed Applicant's right to use the domain(s) to be included in EV Certificates.

Appendix F – Issuance of Certificates for .onion Domain Names

A CA may issue an EV Certificate with .onion in the right-most label of the Domain Name provided that issuance complies with the requirements set forth in this Appendix: 1. CAB Forum Tor Service Descriptor Hash extension (2.23.140.1.31) The CAB Forum has created an extension of the TBSCertificate for use in conveying hashes of keys related to .onion addresses. The Tor Service Descriptor Hash extension has the following format:

cabf-TorServiceDescriptor OBJECT IDENTIFIER ::= { 2.23.140.1.31 }

TorServiceDescriptorSyntax ::=

SEQUENCE (1..MAX) of TorServiceDescriptorHash

TorServiceDescriptorHash:: = SEQUENCE {

onionURI	UTF8String
algorithm	AlgorithmIdentifier
subjectPublicKeyHash	BIT STRING

}

Where the AlgorithmIdentifier is a hashing algorithm (defined in RFC 6234) performed over the DER-encoding of an ASN.1 SubjectPublicKey of the .onion service and SubjectPublicKeyHash is the hash output.

2. The CA MUST verify the Applicant's control over the .onion Domain Name using one of the following:

a. The CA MAY verify the Applicant's control over the .onion service by posting a specific value at a well-known URL under RFC5785.

b. The CA MAY verify the Applicant's control over the .onion service by having the Applicant provide a Certificate Request signed using the .onion public key if the Attributes section of the certificationRequestInfo contains:

(i) A caSigningNonce attribute that (1) contains a single value with at least 64-bits of entropy, (2) is generated by the CA, and (3) delivered to the Applicant through a Verified Method of Communication and (ii) An applicantSigningNonce attribute that (1) contains a single value with at least 64-bits of entropy and (2) is generated by the Applicant.

The signing nonce attributes have the following format:

caSigningNonce ATTRIBUTE ::= {

WITH SYNTAX	OCTET STRING
EQUALITY MATCHING RULE	octetStringMatch

SINGLE VALUE TRUE
ID { cabf-caSigningNonce }

}

cabf-caSigningNonce OBJECT IDENTIFIER ::= { cabf 41 }

applicantSigningNonce ATTRIBUTE ::= {

WITH SYNTAX OCTET STRING
EQUALITY MATCHING RULE octetStringMatch
SINGLE VALUE TRUE
ID { cabf-applicantSigningNonce }

}

cabf-applicantSigningNonce OBJECT IDENTIFIER ::= { cabf 42 }

4. Each Certificate that includes a Domain Name where .onion is in the right-most label of the Domain Name MUST conform to the requirements of these Guidelines, including the content requirements in Section 7.1 of the Baseline Requirements, except that the CA MAY include a wildcard character in the Subject Alternative Name Extension and Subject Common Name Field as the left-most character in the .onion Domain Name provided inclusion of the wildcard character complies with Section 3.2.2.6 of the Baseline Requirements.

5. CAs MUST NOT issue a Certificate that includes a Domain Name where .onion is in the right-most label of the Domain Name with a validity period longer than 15 months. Despite Section 7.1.4.2.1 of the Baseline Requirements deprecating the use of Internal Names, a CA MAY issue a Certificate containing an .onion name with an expiration date later than 1 November 2015 after (and only if) .onion is officially recognized by the IESG as a reserved TLD.

6. On or before May 1, 2015, each CA MUST revoke all Certificates issued with the Subject Alternative Name extension or Common Name field that includes a Domain Name where .onion is in the right-most label of the Domain Name unless the Certificate was issued in compliance with this Appendix F.