

# **CA/BROWSER FORUM**

## **GUIDELINES FOR THE ISSUANCE AND MANAGEMENT OF EXTENDED VALIDATION CERTIFICATES**

Copyright © 2007-2008, The CA / Browser Forum, all rights reserved.

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

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

'Copyright © 2007-2008 The CA / Browser Forum, all rights reserved.

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

A request to make a translated version of these guidelines should be submitted to [questions@cabforum.org](mailto:questions@cabforum.org).



# **Guidelines for the Issuance and Management of Extended Validation Certificates**

Version 1.1, as adopted by the CA/Browser Forum on 10 April 2008

## **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 website commerce. These Guidelines may be revised from time to time, as appropriate, in accordance with procedures adopted by the CA/Browser Forum. Questions concerning these guidelines or suggestions may be directed to the CA/Browser Forum at [questions@cabforum.org](mailto:questions@cabforum.org).

## **The CA/Browser Forum**

The CA/Browser Forum is a voluntary open organization of certification authorities and suppliers of Internet browser software and other applications. Membership as of April 2008 is as follows:

### **Certification Authorities**

- A-Trust GmbH
- Certum
- Comodo CA Ltd
- DigiCert, Inc.
- DigiNotar
- Echoworx Corporation
- Entrust, Inc.
- GeoTrust Inc.
- Getronics PinkRoccade
- GlobalSign
- GoDaddy.com, Inc.
- IdenTrust, Inc.
- ipsCA, IPS Certification Authority s.l.
- Izenpe S.A.
- Network Solutions, LLC
- QuoVadis Ltd.
- RSA Security, Inc.
- SECOM Trust Systems CO., Ltd
- Skaitmeninio sertifikavimo centras
- SwissSign
- TC TrustCenter GmbH
- TDC Certification Authority
- Thawte, Inc.
- Trustis Limited
- Trustwave
- VeriSign, Inc.
- Verizon
- Wells Fargo Bank, N.A.

### **Internet Browser Software Suppliers**

- KDE
- Microsoft Corporation
- Opera Software ASA
- The Mozilla Foundation

Other groups that have participated in the process of developing these Guidelines include members of the Information Security Committee of the American Bar Association Section of Science & Technology Law, and WebTrust for CA. Participation by such groups does not imply their endorsement, recommendation or approval of the final product.



## TABLE OF CONTENTS

	<u>Page</u>
<b><u>A. INTRODUCTION.....</u></b>	<b><u>1</u></b>
1. Introduction.....	1
(a) General.....	1
(b) Scope.....	1
(c) Guidelines Issuing Authority .....	1
(d) Revisions to Guidelines .....	2
<b><u>B. BASIC CONCEPT OF THE EV CERTIFICATE .....</u></b>	<b><u>2</u></b>
2. Purpose of EV Certificates.....	2
(a) Primary Purposes .....	2
(b) Secondary Purposes .....	2
(c) Excluded Purposes .....	3
3. EV Certificate Warranties and Representations .....	3
(a) By the CA and Root CA .....	3
(b) By the Subscriber.....	5
<b><u>C. COMMUNITY AND APPLICABILITY.....</u></b>	<b><u>5</u></b>
4. Issuance of EV Certificates.....	5
(a) Compliance .....	5
(b) EV Policies.....	5
(c) Insurance .....	6
(d) Audit Requirements .....	7
5. Obtaining EV Certificates.....	7
(a) General.....	7
(b) Private Organization Subjects.....	7
(c) Government Entity Subjects .....	7
(d) Business Entities .....	8
(d) Non-Commercial Entity Subjects .....	8
<b><u>D. EV CERTIFICATE CONTENT AND PROFILE.....</u></b>	<b><u>9</u></b>
6. EV Certificate Content Requirements .....	9
(a) Subject Organization Information.....	9

7.	EV Certificate Policy Identification Requirements .....	12
	(a) EV Subscriber Certificates.....	12
	(b) EV Subordinate CA Certificates.....	12
	(c) Root CA Certificates.....	12
8.	Maximum Validity Period .....	12
	(a) For EV Certificate.....	12
	(b) For Validated Data.....	12
9.	Other Technical Requirements for EV Certificates .....	13
<b>E.</b>	<b><u>EV CERTIFICATE REQUEST REQUIREMENTS .....</u></b>	<b>13</b>
10.	General Requirements.....	13
	(a) Documentation Requirements.....	13
	(b) Role Requirements.....	13
11.	EV Certificate Request Requirements .....	14
	(a) General.....	14
	(b) Request and Certification.....	14
	(c) Information Requirements .....	14
12.	Subscriber Agreement Requirements .....	15
	(a) General.....	15
	(b) Agreement Requirements.....	16
<b>F.</b>	<b><u>INFORMATION VERIFICATION REQUIREMENTS.....</u></b>	<b>16</b>
13.	General Overview .....	16
	(a) Verification Requirements – Overview .....	16
	(b) Acceptable Methods of Verification – Overview .....	17
14.	Verification of Applicant’s Legal Existence and Identity .....	17
	(a) Verification Requirements .....	17
	(b) Acceptable Method of Verification .....	19
15.	Verification of Applicant’s Legal Existence and Identity – Assumed Name.....	22
	(a) Verification Requirements .....	22
	(b) Acceptable Method of Verification .....	22
16.	Verification of Applicant’s Physical Existence .....	22
	(a) Address of Applicant’s Place of Business .....	22
	(b) Telephone Number for Applicant’s Place of Business .....	24
17.	Verification of Applicant’s Operational Existence.....	25

	(a)	Verification Requirements .....	25
	(b)	Acceptable Methods of Verification.....	25
18.		Verification of Applicant’s Domain Name.....	25
	(a)	Verification Requirements .....	25
	(b)	Acceptable Methods of Verification.....	25
19.		Verification of Name, Title and Authority of Contract Signer & Certificate Approver .....	27
	(a)	Verification Requirements .....	27
	(b)	Acceptable Methods of Verification – Name, Title, and Agency.....	28
	(c)	Acceptable Methods of Verification - Authorization .....	29
	(d)	Pre-Authorized Certificate Approver.....	30
20.		Verification of Signature on Subscriber Agreement and EV Certificate Requests .....	31
	(a)	Verification Requirements .....	31
	(b)	Acceptable Methods of Signature Verification.....	31
21.		Verification of Approval of EV Certificate Request .....	32
	(a)	Verification Requirements .....	32
	(b)	Acceptable Methods of Verification.....	32
22.		Verification of Certain Information Sources .....	32
	(a)	Verified Legal Opinion.....	32
	(b)	Verified Accountant Letter .....	33
	(c)	Face-to-face validation.....	35
	(d)	Independent Confirmation From Applicant.....	35
	(e)	Qualified Independent Information Sources (QIIS) .....	37
	(f)	Qualified Government Information Sources (QGIS).....	38
	(g)	Qualified Government Tax Information Sources (QGTIS).....	38
23.		Other Verification Requirements.....	38
	(a)	High Risk Status .....	38
	(b)	Denied Lists and Other Legal Black Lists .....	39

24.	Final Cross-Correlation and Due Diligence.....	39
25.	Certificate Renewal Verification Requirements .....	40
<b>G.</b>	<b><u>CERTIFICATE STATUS CHECKING AND REVOCATION ISSUES.....</u></b>	<b>41</b>
26.	EV Certificate Status Checking .....	41
	(a) Repository .....	41
	(b) Reasonable User Experience.....	41
	(c) Response Time.....	41
	(d) Deletion of Entries .....	42
27.	EV Certificate Revocation .....	42
	(a) Revocation Guidelines and Capability.....	42
	(b) Revocation Events .....	42
28.	EV Certificate Problem Reporting and Response Capability .....	43
	(a) Reporting.....	43
	(b) Investigation.....	43
	(c) Response .....	43
<b>H.</b>	<b><u>EMPLOYEE AND THIRD PARTY ISSUES .....</u></b>	<b>43</b>
29.	Trustworthiness and Competence .....	43
	(a) Identity and Background Verification .....	43
	(b) Training and Skills Level.....	44
	(c) Separation of Duties.....	44
30.	Delegation of Functions to Registration Authorities and Subcontractors .....	45
	(a) General.....	45
	(b) Enterprise RAs .....	45
	(c) Guidelines Compliance Obligation.....	45
	(d) Responsibility .....	45
<b>I.</b>	<b><u>DATA AND RECORD ISSUES .....</u></b>	<b>46</b>
31.	Documentation and Audit Trail Requirements .....	46
32.	Document Retention .....	47
	(a) Audit Log Retention .....	47
	(b) Retention of Documentation .....	47
33.	Reuse and Updating Information and Documentation.....	47
	(a) Use of Documentation to Support Multiple EV Certificates .....	47
	(b) Use of Pre-Existing Information or Documentation .....	47

34.	Data Security.....	47
	(a) Objectives .....	47
	(b) Risk Assessment .....	48
	(c) Security Plan .....	48
	(d) Dual Access Control .....	48
<b>J.</b>	<b>COMPLIANCE.....</b>	<b>49</b>
35.	Audit Requirements .....	49
	(a) Pre-Issuance Readiness Audit.....	49
	(b) Regular Self Audits.....	49
	(c) Annual Independent Audit.....	49
	(d) Auditor Qualifications .....	50
	(e) Root Key Generation .....	50
<b>K.</b>	<b>OTHER CONTRACTUAL COMPLIANCE.....</b>	<b>51</b>
36.	Privacy/Confidentiality Issues .....	51
37.	Limitations on EV Certificate Liability .....	51
	(a) CA Liability .....	51
	(b) Root CA Indemnification.....	52
	<b>DEFINITIONS .....</b>	<b>53</b>
	<b>Appendix A — Minimum Cryptographic Algorithm and Key Sizes .....</b>	<b>60</b>
	<b>Appendix B — EV Certificates Required Certificate Extensions .....</b>	<b>61</b>
	<b>Appendix C — User Agent Verification .....</b>	<b>64</b>
	<b>Appendix D — Sample Form Legal Opinion Letter.....</b>	<b>65</b>
	<b>Appendix E — Sample Accountant Letters Confirming Specified Information.....</b>	<b>67</b>
	<b>Appendix F — Foreign organization name guidelines .....</b>	<b>71</b>
	<b>Appendix G — Code-Signing: Introduction .....</b>	<b>73</b>
	<b>Appendix H — Code-Signing: Requirements for Certification Authorities .....</b>	<b>77</b>
	<b>Appendix I — Code-Signing: Requirements for Timestamp Authorities .....</b>	<b>81</b>
	<b>Appendix J — Code-Signing: Requirements for Signing Authorities .....</b>	<b>82</b>



# GUIDELINES FOR THE ISSUANCE AND MANAGEMENT OF EXTENDED VALIDATION CERTIFICATES

## A. INTRODUCTION

### 1. Introduction

#### (a) General

These Guidelines for the issuance and management of Extended Validation Certificates (“Guidelines”) describe certain of the minimum requirements that a Certification Authority (CA) must meet in order to issue Extended Validation Certificates (“EV 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 website they are accessing.

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 such EV Certificates.

#### (b) Scope

These Guidelines address basic issues relating to the verification of information regarding Subjects named in EV Certificates and certain related matters.

These Guidelines do not address many of the other issues that must be addressed by the CA issuing EV Certificates, such as technical or operational issues.

This version of the Guidelines addresses only requirements for EV Certificates intended to be used for server-authentication SSL/TLS on the Internet. Similar requirements for client-authentication SSL/TLS, S/MIME, code-signing, 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 (PKI) for internal purposes only, where its Root CA Certificate is not distributed by any Application Software Vendor.

#### (c) Guidelines Issuing Authority

These Guidelines are issued by the CA/Browser Forum, and are available online at <http://www.cabforum.org>. Comments and questions regarding these

Guidelines may be addressed to the CA/Browser Forum at [questions@cabforum.org](mailto:questions@cabforum.org).

**(d) Revisions to Guidelines**

These Guidelines may be updated from time-to-time in accordance with the rules of the CA/Browser Forum. In the event the CA/Browser Forum decides to make significant changes to these Guidelines, notification of such changes will be posted at <http://www.cabforum.org> at least 30 days before they become effective. Minor changes will take effect on posting. A complete history of all revisions (including dates of changes) will be maintained on the site.

Unless otherwise stated in the revised version of the Guidelines, changes will apply only to EV Certificates issued after the effective date of a change. However, any renewal of an EV Certificate MUST comply with the Guidelines in effect as of the date of such renewal.

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this guidelines document are to be interpreted as described in RFC 2119.

**B. BASIC CONCEPT OF THE EV CERTIFICATE**

2. **Purpose of EV Certificates** EV Certificates are intended for use in establishing Web-based data communication conduits via TLS/SSL protocols.

(a) **Primary Purposes** The primary purposes of an EV Certificate are to:

- (1) **Identify the legal entity that controls a website** Provide a reasonable assurance to the user of an Internet browser that the website 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 website** 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 website.

(b) **Secondary Purposes** The secondary purposes of an EV Certificate are to help establish the legitimacy of a business claiming to operate a website, and to provide a vehicle that can be used to assist in addressing problems related to phishing and other forms of online identity fraud. By providing more reliable

third-party verified identity and address information regarding the owner of a website, EV Certificates may help to:

- (1) Make it more difficult to mount phishing and other online identity fraud attacks using SSL 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 and their legitimate websites to users; and
- (3) Assist law enforcement in investigations of phishing and other online identity fraud, including where appropriate, contacting, investigating, or taking legal action against the Subject.

(c) **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. **EV Certificate Warranties and Representations**

#### (a) **By the CA and Root CA**

When the CA issues an EV Certificate, the CA and its Root CA make the EV Certificate Warranties listed below to the EV Certificate Beneficiaries listed below:

- (1) **EV Certificate Beneficiaries** When the CA issues an EV Certificate, the CA and its Root CA make the EV Certificate Warranties listed below to the following persons (“EV Certificate Beneficiaries”):
  - (A) The Subscriber entering into the Subscriber Agreement for the EV Certificate;
  - (B) The Subject named in the EV Certificate;
  - (C) All Application Software Vendors with whom the CA or its Root CA has entered into a contract for inclusion of its Root Certificate in software distributed by such Application Software Vendors;
  - (D) All Relying Parties that actually rely on such EV Certificate during the period when it is Valid.

(2) EV Certificate Warranties When the CA issues an EV Certificate, the CA and its Root CA represent and warrant to the EV Certificate Beneficiaries, during the period when the EV Certificate is Valid, that the CA has followed the requirements of these Guidelines and its EV Policies (further described in Section 4(b)) in issuing the EV Certificate and in verifying the accuracy of the information contained in the EV Certificate (“EV Certificate Warranties”). 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 exclusive right to use 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;
- (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 upon the occurrence of any revocation event as specified in these Guidelines.

**(b) By the Subscriber**

The CA will require, as part of the Subscriber Agreement, that the Subscriber make the commitments and warranties set forth in the Subscriber Agreement Requirements section of these Guidelines, for the benefit of the CA and the EV Certificate Beneficiaries.

**C. COMMUNITY AND APPLICABILITY**

**4. Issuance of EV Certificates**

Any CA MAY issue EV Certificates, provided that, before the CA issues any EV Certificates, the CA and its Root CA satisfy the following requirements:

**(a) Compliance** The CA and its Root CA MUST at all times:

- (1) Comply with all law applicable to its business and the certificates it issues in each jurisdiction where it operates;
- (2) Comply with the requirements of these Guidelines;
- (3) Comply with the requirements of (i) the then-current WebTrust Program for CAs, and (ii) the then-current WebTrust EV Program, or an equivalent for both (i) and (ii) as approved by the CA/Browser Forum; and
- (4) Be licensed as a CA in each jurisdiction where it operates if licensing is required by the law of such jurisdiction for the issuance of EV Certificates.

**(b) EV Policies**

- (1) **Implementation** The CA and its Root CA MUST develop, implement, enforce, display prominently on its website, 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) (“EV Policies”) 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 an equivalent for both (i) and (ii) as approved by the CA/Browser Forum;
  - (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.

- (2) **Disclosure** The CA and its Root 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 such as are required for public disclosure by the WebTrust for CA requirements. The disclosures SHOULD be structured in accordance with either RFC 2527 or RFC 3647.
- (3) **Commitment to Comply with Guidelines** The CA and its Root CA MUST publicly give effect to these Guidelines and represent that they will adhere to them 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 (“Guidelines”) 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.

(c) **Insurance**

- (1) The CA and its Root CA MUST 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 \$2 million in coverage, and
  - (B) Professional Liability/Errors & Omissions insurance, with policy limits of at least \$5 million 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.
- (2) 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).
- (3) The CA and/or its Root CA MAY self-insure for liabilities that arise from such party's performance and obligations under these Guidelines provided that

it has at least \$500 million 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.

- (d) **Audit Requirements** The CA and its Root CA MUST satisfy the Audit Requirements set forth in the “Compliance” section (Section “J”) of these Guidelines.

## 5. **Obtaining EV Certificates**

- (a) **General** The CA MAY issue EV Certificates to Private Organizations, Government Entities, and Business Entities that satisfy the requirements specified below:

- (b) **Private Organization Subjects** The CA MAY issue EV Certificates to Private Organizations that satisfy the following requirements:

- (1) The Private Organization MUST be a legally recognized entity whose existence was created 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) or is an entity that is chartered by a state or federal regulatory agency;
- (2) The Private Organization MUST have designated with the Incorporating or Registration Agency either a Registered Agent, or a Registered Office (as required under the laws of the Jurisdiction of Incorporation or Registration) or an equivalent facility;
- (3) The Private Organization MUST NOT be designated on the records of the Incorporating or Registration Agency by labels such as “inactive,” “invalid,” “not current,” or the equivalent;
- (4) The Private organization MUST have a verifiable physical existence and business presence;
- (5) The Private Organization’s Jurisdiction of Incorporation, Registration, Charter, or License, and/or its Place of Business MUST NOT be 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 Private Organization MUST NOT be listed on any government denial list or prohibited list (e.g., trade embargo) under the laws of the CA’s jurisdiction.

- (c) **Government Entity Subjects** The CA MAY issue EV Certificates to Government Entities that satisfy the following requirements:

- (1) The legal existence of the Government Entity MUST be established by the political subdivision in which such Government Entity operates;

- (2) The Government Entity MUST NOT be 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 Government Entity MUST NOT be listed on any government denial list or prohibited list (e.g., trade embargo) under the laws of the CA's jurisdiction.
- (d) **Business Entities** The CA MAY issue EV Certificates to Business Entities who do not qualify under subsections (b) but that do satisfy the following requirements:
- (1) The Business Entity MUST be a legally recognized entity whose formation included the filing of certain forms with the Registration Agency in its Jurisdiction, the issuance or approval by such Registration Agency of a charter, certificate, or license, and whose existence can be verified with that Registration Agency;
  - (2) The Business Entity MUST have a verifiable physical existence and business presence;
  - (3) At least one Principal Individual associated with the Business Entity MUST be identified and validated;
  - (4) The identified Principal Individual MUST attest to the representations made in the Subscriber Agreement;
  - (5) Where the Business Entity represents itself under an assumed name, the CA MUST verify the Business Entity's use of the assumed name pursuant to the requirements of Section 15 herein;
  - (6) The Business Entity and the identified Principal Individual associated with the Business Entity MUST NOT be 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 Business Entity and the identified Principal Individual associated with the Business Entity MUST NOT be listed on any government denial list or prohibited list (e.g., trade embargo) under the laws of the CA's jurisdiction.
- (e) **Non-Commercial Entity Subjects** The CA MAY issue EV Certificates to Non-Commercial Entities who do not qualify under subsections (b), (c) and (d) but satisfy the following requirements:
- (1) **International Organization Entities**
    - (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 CABForum may publish a listing of International Organizations that have been approved for EV eligibility, and

- (B) The International Organization Entity MUST NOT be 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 International Organization Entity MUST NOT be 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 qualified international organizations may also qualify for EV certificates issued in accordance with these Guidelines.

#### **D. EV CERTIFICATE CONTENT AND PROFILE**

- 6. **EV Certificate Content Requirements** 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.

- (a) **Subject Organization 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 Root CA MUST include the following information about the Subject organization in the fields listed (“Subject Organization Information”):

- (1) **Organization name**

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 QGIS shows “\*Company Name\* Incorporated” the CA MAY include \*Company Name\*, Inc. The CA MUST use common abbreviations that are generally accepted in the Jurisdiction of Incorporation or Registration.

In addition, an assumed name or d/b/a 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 the full legal organization name and the assumed or d/b/a name exceeds 64 characters, as defined by RFC 3280, the CA SHOULD use only the full legal organization name in the certificate.

If the Organization name by itself exceeds 64 characters, the CA MAY abbreviate parts of organization name, and/or omit non-material words in the organization name in such a way that the name in the certificate does not

exceed the 64 character limit, and a Relying Party will not be misled into thinking they are dealing with a different Organization. In cases where this is not possible, the CA MUST NOT issue the EV certificate.

**(2) Domain name**

Certificate Field subject:commonName (OID 2.5.4.3) or  
SubjectAlternativeName:dNSName

Required/Optional Required

Contents This field MUST contain one or more host domain name(s) owned or controlled by the Subject and to be associated with 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.

**(3) Business Category**

Certificate Field subject:businessCategory (OID 2.5.4.15)

Required/Optional Required

Contents This field MUST contain one of the following strings: "V1.0, Clause 5.(b)", "V1.0, Clause 5.(c)", "V1.0, Clause 5.(d)" or "V1.0, Clause 5.(e)" depending whether the Subject qualifies under the terms of Section 5b, 5c, 5d or 5e of the Guidelines, respectively.

**(4) Jurisdiction of Incorporation or Registration**

Certificate Fields

Locality (if required):

subject:jurisdictionOfIncorporationLocalityName (OID  
1.3.6.1.4.1.311.60.2.1.1)

ASN.1 - X520LocalityName as specified in RFC 3280

State or province (if required):

subject:jurisdictionOfIncorporationStateOrProvinceName  
(OID 1.3.6.1.4.1.311.60.2.1.2)

ASN.1 - X520StateOrProvinceName as specified in RFC  
3280

Country:

subject:jurisdictionOfIncorporationCountryName (OID  
1.3.6.1.4.1.311.60.2.1.3)

ASN.1 - X520countryName as specified in RFC 3280

Required/Optional Required

Contents These fields MUST contain information only at and above the level of the Incorporating Agency or Registration Agency – e.g., the Jurisdiction of Incorporation for an Incorporating Agency or Jurisdiction of Registration for a Registration Agency at the country level would include country information but not state or province or locality information; the Jurisdiction of

Incorporation for the applicable Incorporating Agency or Registration Agency at the state or province level would include both country and state or province information, but not locality information; and so forth. Country information MUST be specified using the applicable ISO country code. State or province information, and locality information (where applicable), for the Subject's Jurisdiction of Incorporation or Registration MUST be specified using the full name of the applicable jurisdiction.

Compliance with European Union Qualified Certificates Standard In addition, CAs MAY include a qcStatements extension per RFC 3739. The OID for qcStatements:qcStatement:statementId is 1.3.6.1.4.1.311.60.2.1.

## **(5) Registration Number**

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 other 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.

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.

## **(6) Physical Address of Place of Business**

Certificate Fields

Number & street (optional)	subject:streetAddress (OID 2.5.4.9)
City or town	subject:localityName (OID 2.5.4.7)
State or province (if any)	subject:stateOrProvinceName (OID 2.5.4.8)
Country	subject:countryName (OID 2.5.4.6)
Postal code (optional)	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.

7. **EV Certificate Policy Identification Requirements** This section sets forth minimum requirements for the content of the EV Subscriber and non-Root CA Certificates as they relate to the identification of EV certificate policy:
- (a) **EV Subscriber Certificates** Each EV Certificate issued by the CA to a Subscriber MUST contain an OID defined by 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), by pre-agreement with the Application Software Vendor, marks the certificate as being an EV Certificate.
  - (b) **EV Subordinate CA Certificates**
    - (1) Certificates issued to Subordinate CAs that are not controlled by the issuing CA MUST contain one or more OIDs 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 OID (2.5.29.32.0).
  - (c) **Root CA Certificates** Root CA Certificates SHOULD NOT contain the certificatePolicies or extendedKeyUsage extensions.

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

## 8. **Maximum Validity Period**

- (a) **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.
- (b) **For Validated Data** The age of validated data used to support issuance of an EV Certificate (before revalidation is required) SHALL NOT exceed the following limits:
  - (1) Legal existence and identity – one year;
  - (2) Assumed name – one year;
  - (3) Address of Place of Business – one year, but thereafter data MAY be refreshed by checking a Qualified Independent Information Source, even where a site visit was originally required;
  - (4) Telephone number for Place of Business – one year;

- (5) Bank account verification – one year;
- (6) Domain name – one year;
- (7) Identity and authority of Certificate Approver – one year, unless a contract is in place between the CA and Applicant that specifies a different term, in which case, the term specified in such contract will control. For example, the contract MAY use terms that allow the assignment of roles that are perpetual until revoked, or until the contract expires or is terminated.

9. **Other Technical Requirements for EV Certificates** See Appendix A and Appendix B attached.

**E. EV CERTIFICATE REQUEST REQUIREMENTS**

**10. General Requirements**

- (a) **Documentation Requirements** Prior to the issuance of an EV Certificate, the CA MUST obtain from Applicant the following documentation, in compliance with the requirements of these Guidelines:
  - (1) EV Certificate Request
  - (2) Subscriber Agreement
  - (3) Such additional documentation as the CA requires from Applicant to satisfy its obligations under these Guidelines.
- (b) **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 Applicant, employed by Applicant, an authorized agent who has express authority to represent Applicant, or a third party (such as an ISP or hosting company) that completes and submits an EV Certificate Request on behalf of 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 Applicant, employed by Applicant, or an authorized agent who has express authority to represent 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 Applicant, employed by Applicant, or

an authorized agent who has express authority to represent Applicant, and who has authority on behalf of Applicant to sign Subscriber Agreements.

One person MAY be authorized by Applicant to fill one, two, or all three of these roles, provided that the Certificate Approver and Contract Signer are employees of Applicant. An Applicant MAY also authorize more than one person to fill each of these roles.

## **11. EV Certificate Request Requirements**

- (a) **General** Prior to the issuance of an EV Certificate, the CA MUST obtain from Applicant (via a Certificate Requester authorized to act on Applicant's behalf) a properly completed and signed EV Certificate Request in a form prescribed by the CA and that complies with these Guidelines. One EV Certificate Request MAY suffice for multiple EV Certificates to be issued to the same Applicant at the same time.
- (b) **Request and Certification** The EV Certificate Request MUST contain a request from, or on behalf of, Applicant for the issuance of an EV Certificate, and a certification by, or on behalf of, Applicant that all of the information contained therein is true and correct.
- (c) **Information Requirements** The EV Certificate Request MAY include all factual information about Applicant to be included in the EV Certificate, and such additional information as is necessary for the CA to obtain from Applicant in order to comply with these Guidelines and the CA's own policies. In cases where the EV Certificate Request does not contain all necessary information about Applicant, the CA MUST obtain the remaining information from either the Certificate Approver or Contract Signer or, having obtained it from a reliable source, confirm it with the Certificate Approver or Contract Signer.

Applicant information SHALL include, but not be limited to, the following information:

- (1) **Organization Name** Applicant's formal legal organization name to be included in the EV Certificate, as recorded with the Incorporating or Registration Agency in Applicant's Jurisdiction of Incorporation or Registration (for Private Organizations), or as specified in the law of the political subdivision in which the Government Entity operates (for Government Entities), or as registered with the government business Registration Agency (for Business Entities);
- (2) **Assumed Name (Optional)** Applicant's assumed name (e.g., d/b/a name) to be included in the EV Certificate, as recorded in the jurisdiction of Applicant's Place of Business, if requested by Applicant;
- (3) **Domain Name** Applicant's domain name(s) to be included in the EV Certificate;

- (4) Jurisdiction of Incorporation or Registration Applicant's Jurisdiction of Incorporation or Registration to be included in the EV Certificate, and consisting of:
  - (a) City or town (if any),
  - (b) State or province (if any), and
  - (c) Country.
- (5) Incorporating or Registration Agency The name of Applicant's Incorporating or Registration Agency;
- (6) Registration Number The Registration Number assigned to Applicant by the Incorporating or Registration Agency in Applicant's Jurisdiction of Incorporation or Registration and to be included in the EV Certificate. If the Incorporating or Registration Agency does not issue Registration numbers, then the date of Incorporation or Registration SHALL be collected.
- (7) Applicant Address The address of Applicant's Place of Business, including –
  - (a) Building number and street,
  - (b) City or town,
  - (c) State or province (if any),
  - (d) Country,
  - (e) Postal code (zip code), and
  - (f) Main telephone number.
- (8) Certificate Approver Name and contact information of the Certificate Approver submitting and signing, or that has authorized the Certificate Requester to submit and sign, the EV Certificate Application on behalf of Applicant; and
- (9) Certificate Requester Name and contact information of the Certificate Requester submitting the EV Certificate Request on behalf of Applicant, if other than the Certificate Approver.

## **12. Subscriber Agreement Requirements**

- (a) **General** Prior to the issuance of the EV Certificate, the CA MUST obtain Applicant's agreement to a legally enforceable Subscriber Agreement with the CA for the express benefit of Relying Parties and Application Software Vendors. The Subscriber Agreement MUST be signed by an authorized Contract Signer acting on behalf of Applicant in accordance with Section 20 of these Guidelines, and MUST apply to the EV Certificate to be issued pursuant to the EV Certificate Request. A separate Subscriber Agreement MAY be used for each EV Certificate Request, or a single Subscriber Agreement MAY be used to cover multiple future EV Certificate Requests and resulting EV Certificates, so long as each EV Certificate that the CA issues to Applicant is clearly covered by a Subscriber Agreement signed by an authorized Contract Signer acting on behalf of Applicant.

**(b) Agreement Requirements** The Subscriber Agreement MUST, at a minimum, specifically name both Applicant and the individual Contract Signer signing the Agreement on Applicant's behalf, and contain provisions imposing on Applicant the following obligations and warranties:

- (1) Accuracy of Information An obligation and warranty to provide accurate and complete information at all times to the CA, both in the EV Certificate Request and as otherwise requested by the CA in connection with the issuance of the EV Certificate(s) to be supplied by the CA;
- (2) Protection of Private Key An obligation and warranty by the subscriber or a subcontractor (e.g. hosting provider) to take all reasonable measures to maintain sole control of, keep confidential, and properly protect at all times the Private Key that corresponds to the Public Key to be included in the requested EV Certificate(s) (and any associated access information or device, e.g. password or token);
- (3) Acceptance of EV Certificate An obligation and warranty that it will not install and use the EV Certificate(s) until it has reviewed and verified the accuracy of the data in each EV Certificate;
- (4) Use of EV Certificate An obligation and warranty to install the EV Certificate only on the server accessible at a domain name listed on the EV Certificate, and to use the EV Certificate solely in compliance with all applicable laws, solely for authorized company business, and solely in accordance with the Subscriber Agreement;
- (5) Reporting and Revocation Upon Compromise An obligation and warranty to promptly cease using an EV Certificate and its associated Private Key, and promptly request the CA to revoke the EV Certificate, in the event that: (a) any information in the EV Certificate is or becomes incorrect or inaccurate, or (b) there is any actual or suspected misuse or compromise of the Subscriber's Private Key associated with the Public Key listed in the EV Certificate;
- (6) Termination of Use of EV Certificate An obligation and warranty to promptly cease all use of the Private Key corresponding to the Public Key listed in an EV Certificate upon expiration or revocation of that EV Certificate.

## **F. INFORMATION VERIFICATION REQUIREMENTS**

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

**(a) Verification Requirements – Overview** Before issuing an EV Certificate, the CA MUST ensure that all Subject organization information in the EV Certificate conforms to the requirements of, and has been 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 Applicant's legal existence and identity (as more fully set forth in Section 14 herein),
  - (b) Verify Applicant's physical existence (business presence at a physical address), and
  - (c) Verify Applicant's operational existence (business activity).
- (2) Verify Applicant is a registered holder, or has exclusive control, of the domain name to be included in the EV Certificate;
- (3) Verify 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 Contract Signer signed the Subscriber Agreement; and
  - (c) Verify that a Certificate Approver has signed or otherwise approved the EV Certificate Request.

**(b) 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 sections below. The Acceptable Methods of Verification set forth in each of Sections 14 through 25 below (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.

#### **14. Verification of Applicant's Legal Existence and Identity**

**(a) Verification Requirements** To verify Applicant's legal existence and identity, the CA MUST do the following:

- (1) Private Organizations
  - a. Legal Existence Verify that Applicant is a legally recognized entity, in existence and validly formed (e.g., incorporated) with the Incorporating or Registration Agency in 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 Applicant's formal legal name as recorded with the Incorporating or Registration Agency in Applicant's Jurisdiction of Incorporation or Registration matches Applicant's name in the EV Certificate Request.

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

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

## (2) Government Entities

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

b. Entity Name Verify that Applicant's formal legal name matches Applicant's name in the EV Certificate Request.

c. Registration Number The CA SHOULD obtain 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 Entities

a. Legal Existence Verify that Applicant is engaged in business under the name submitted by Applicant in the Application.

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

c. Registration Number Obtain the specific unique Registration Number assigned to Applicant by the Registration Agency in Applicant's Jurisdiction of Registration. Where the Registration Agency does not assign a Registration Number, the CA SHALL obtain Applicant's date of Registration.

d. Principal Individual Verify the identity of the identified Principal Individual.

## (4) Non-Commercial Entities (International Organization Entities)

a. Legal Existence Verify that Applicant is a legally recognized International Organization Entity.

b. Entity Name Verify that Applicant's formal legal name matches Applicant's name in the EV Certificate Request.

c. Registration Number The CA SHOULD obtain 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.

**(b) Acceptable Method of Verification**

- (1) Private Organizations: All items listed in subsection (a)(1) above MUST be verified directly with, or obtained directly from, the Incorporating or Registration Agency in 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 from a Qualified Independent Information Source.
  
- (2) Government Entities: All items listed in subsection (a)(2) above MUST either be verified directly with, or obtained directly from, one of the following: (i) a QGIS in the political subdivision in which such Government Entity operates; (ii) a superior governing Government Entity in the same political subdivision as 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, or (iv) an attorney representing the Government Entity.

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 22(a) below.

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 Entities: All items listed in subsection (a)(3) above, MUST be verified directly with, or obtained directly from, the Registration Agency in Applicant's Jurisdiction of Registration. Such verification MAY be through use 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 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 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;
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 drivers license;
3. A personal identification card;
4. A concealed weapons permit;
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.

Acceptable non-financial documents include:

1. 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).
2. A copy of a statement for a payment of a lease provided the statement is dated within the past six months.
3. A certified copy of a birth certificate.
4. A local authority tax bill for the current year.
5. 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:

1. Attest to the signing of the Personal Statement and the identity of the signer; and
2. 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) Cross-checking of Information: The CA MUST obtain the original 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.

(c) 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 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.

(5) Non-Commercial Entities (International Organization Entities):

All items listed in subsection 14(a)(4)(1) 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 CABForum may maintain at [www.cabforum.org](http://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 (NGO) 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.

## **15. Verification of Applicant's Legal Existence and Identity – Assumed Name**

(a) **Verification Requirements** If, in addition to Applicant's formal legal name as recorded with the applicable Incorporating Agency or Registration Agency in Applicant's Jurisdiction of Incorporation or Registration, 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 Applicant conducts business, the CA MUST verify that: (i) 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.

(b) **Acceptable Method of Verification** To verify any assumed name under which 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 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 Legal Opinion, or a Verified Accountant Letter that indicates the assumed name under which Applicant conducts business, the government agency with which the assumed name is registered, and that such filing continues to be valid.

## **16. Verification of Applicant's Physical Existence**

(a) **Address of Applicant's Place of Business**

- (1) **Verification Requirements** To verify Applicant's physical existence and business presence, the CA MUST verify that the physical address provided by Applicant is an address where Applicant or a Parent/Subsidiary Company conducts business operations (e.g., not a mail drop or P.O. box), and is the address of Applicant's Place of Business.

(2) Acceptable Methods of Verification To verify the address of Applicant's Place of Business:

(A) For Applicants whose Place of Business is in the same country as Applicant's Jurisdiction of Incorporation or Registration:

(1) For Applicants whose Place of Business is in the same country as Applicant's Jurisdiction of Incorporation or Registration:

(1) For Applicants listed at the same Place of Business address in the current version of either at least one Qualified Independent Information Source or a Qualified Governmental Tax Information Source, the CA MUST confirm that Applicant's address as listed in the EV Certificate Request is a valid business address for Applicant or a Parent/Subsidiary Company by reference to such Qualified Independent Information Sources or a Qualified Governmental Tax Information Source, and MAY rely on 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 Qualified Independent Information Source or a Qualified Governmental Tax Information Source, the CA MUST confirm that the address provided by Applicant in the EV Certificate Request is in fact 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 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 Applicant;

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

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

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

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

(B) For Applicants whose Place of Business is not in the same country as Applicant's Jurisdiction of Incorporation or Registration, the CA MUST rely on a Verified Legal Opinion that indicates the address of Applicant's Place of Business and that business operations are conducted there.

**(b) Telephone Number for Applicant's Place of Business**

- (1) Verification Requirements To further verify Applicant's physical existence and business presence, as well as to assist in confirming other verification requirements, the CA MUST verify that the telephone number provided by Applicant is a main phone number for Applicant's Place of Business.
- (2) Acceptable Methods of Verification To verify Applicant's telephone number, the CA MUST perform A and one of B, C, or D as listed below:
  - (A) Confirm Applicant's telephone number by calling it and obtaining an affirmative response sufficient to enable a reasonable person to conclude that Applicant is reachable by telephone at the number dialed; and
  - (B) Confirm that the telephone number provided by Applicant is listed as Applicant's or Parent/Subsidiary Company's telephone number for the verified address of its Place of Business in records provided by the applicable phone company, or, alternatively, in either at least one (1) Qualified Independent Information Source or a Qualified Governmental Tax Information Source; *or*
  - (C) During a site visit, the person who is conducting the site visit MUST confirm Applicant's or Parent/Subsidiary Company's main telephone number by calling it and obtaining an affirmative response sufficient to enable a reasonable person to conclude that Applicant is reachable by telephone at the number dialed. The CA MUST also confirm that Applicant's main telephone number is not a mobile phone; *or*
  - (D) Rely on a Verified Legal Opinion or a Verified Accountant Letter to the effect that Applicant's telephone number, as provided, is a main phone number for Applicant's Place of Business.
  - (E) For Government Entity Applicants, the CA MAY rely on the telephone number contained in the records of the QGIS in Applicant's Jurisdiction.

## **17. Verification of Applicant's Operational Existence**

- (a) **Verification Requirements** If Applicant has been in existence for less than three years, as indicated by the records of the Incorporating Agency or Registration Agency, and is not listed in either the current version of one Qualified Independent Information Source or a Qualified Governmental Tax Information Source, the CA MUST verify that Applicant has the ability to engage in business.
- (b) **Acceptable Methods of Verification** To verify Applicant's operational existence, the CA MUST perform one of the following:
- (1) Verify Applicant has an active current Demand Deposit Account with a Regulated Financial Institution. The CA MUST receive authenticated documentation directly from a Regulated Financial Institution verifying that Applicant has an active current Demand Deposit Account with the institution.
  - (2) Rely on a Verified Legal Opinion or a Verified Accountant Letter to the effect that Applicant has an active current Demand Deposit Account with a Regulated Financial Institution;

## **18. Verification of Applicant's Domain Name**

- (a) **Verification Requirements** To verify Applicant's registration, or exclusive control, of the domain name(s) to be listed in the EV Certificate, the CA MUST verify that each such domain name satisfies the following requirements:
- (1) The domain name is registered with an Internet Corporation for Assigned Names and Numbers (ICANN)-approved registrar or a registry listed by the Internet Assigned Numbers Authority (IANA);
  - (2) Domain registration information in the WHOIS database SHOULD be public and SHOULD show the name, physical address, and administrative contact information for the organization.  
  
For Government Entity Applicants, the CA MAY rely on the domain name listed for that entity in the records of the QGIS in Applicant's Jurisdiction to verify Domain Name.
  - (3) Applicant:
    - (A) is the registered holder of the domain name; or
    - (B) has been granted the exclusive right to use the domain name by the registered holder of the domain name;
  - (4) Applicant is aware of its registration or exclusive control of the domain name;

### **(b) Acceptable Methods of Verification**

- (1) **Applicant as Registered Holder** Acceptable methods by which the CA MAY verify that Applicant is the registered holder of the domain name include the following:

- (A) Performing a WHOIS inquiry on the Internet for the domain name supplied by Applicant, and obtaining a response indicating that Applicant or a Parent/Subsidiary Company is the entity registered to the domain name; or
  - (B) Communicating with the contact listed on the WHOIS record to confirm that Applicant is the registered holder of the domain name and having the contact update the WHOIS records to reflect the proper domain name registration. Confirmation that the registered owner of the domain name is a Parent/Subsidiary Company of Applicant, or a registered trading name of Applicant is sufficient to establish that Applicant is the registered owner of the domain name;
  - (C) In cases where domain registration information is private, and the domain registrar offers services to forward communication to the registered domain holder, the CA MAY contact Applicant through the domain registrar by e-mail or paper mail.
- (2) Applicant's Exclusive Right to Use In cases where Applicant is not the registered holder of the domain name, the CA MUST verify Applicant's exclusive right to use the domain name(s).

- (A) In cases where the registered domain holder can be contacted using information obtained from WHOIS, or through the domain registrar, the CA MUST obtain positive confirmation from the registered domain holder by paper mail, e-mail, telephone, or facsimile that Applicant has been granted the exclusive right to use the requested Fully Qualified Domain Name (FQDN).

If the Top-Level Domain is a generic top-level domain (gTLD) such as .com, .net, or .org in accordance with RFC 1591, the CA MUST obtain positive confirmation from the second-level domain registration holder. For example, if the requested FQDN is www1.www.example.com, the CA MUST obtain positive confirmation from the domain holder of example.com.

If the Top-Level Domain is a 2 letter Country Code Top-Level Domain (ccTLD), the CA MUST obtain positive confirmation from the domain holder at the appropriate domain level, based on the rules of the ccTLD. For example, if the requested FQDN is www.mysite.users.internet.co.uk, the CA MUST obtain positive confirmation from the domain holder of internet.co.uk.

In addition, the CA MUST verify Applicant's exclusive right to use the domain name using one of the following methods:

- (1) Relying on a Verified Legal Opinion to the effect that Applicant has the exclusive right to use the specified domain name in identifying itself on the Internet; or

- (2) Relying on a representation from the Contract Signer, or the Certificate Approver, if expressly so authorized in a mutually-agreed-upon contract.
- (B) In cases where the registered domain holder cannot be contacted, the CA MUST:
- (1) Rely on a Verified Legal Opinion to the effect that Applicant has the exclusive right to use the specified domain name in identifying itself on the Internet, and
  - (2) Rely on a representation from the Contract Signer, or the Certificate Approver, if expressly so authorized in a mutually-agreed-upon contract, coupled with a practical demonstration by Applicant establishing that it controls the domain name by making an agreed-upon change in information found online on a web page identified by a uniform resource identifier containing Applicant's FQDN;
- (3) Knowledge Acceptable methods by which the CA MAY verify Applicant is aware that it has exclusive control of the domain name include the following:
- (A) Relying on a Verified Legal Opinion to the effect that Applicant is aware that it has exclusive control of the domain name; or
  - (B) Obtaining a confirmation from the Contract Signer or Certificate Approver verifying that Applicant is aware that it has exclusive control of the domain name.
- (4) 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 Applicant and the target in question are the same organization.

## **19. Verification of Name, Title, and Authority of Contract Signer and Certificate Approver**

- (a) **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 Applicant.

- (2) Authorization of Contract Signer The CA MUST verify, through a source other than the Contract Signer, that the Contract Signer is expressly authorized by Applicant to enter into the Subscriber Agreement (and any other relevant contractual obligations) on behalf of Applicant, including a contract that designates one or more Certificate Approvers on behalf of Applicant (“Signing Authority”).
- (3) Authorization of Certificate Approver The CA MUST verify, through a source other than the Certificate Approver, that the Certificate Approver is expressly authorized by Applicant to do the following, as of the date of the EV Certificate Request (“EV Authority”):
- (a) Submit, and, if applicable, authorize a Certificate Requester to submit, the EV Certificate Request on behalf of Applicant; and
  - (b) Provide, and, if applicable, authorize a Certificate Requester to provide, the information requested from Applicant by the CA for issuance of the EV Certificate; and
  - (c) Approve EV Certificate Requests submitted by a Certificate Requester.
- (b) **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:
- (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 agency of the Contract Signer and the Certificate Approver by:
    - (A) Contacting Applicant’s Human Resources Department by phone or mail (at the phone number or address for Applicant’s Place of Business, verified in accordance with these Guidelines) and obtaining confirmation that the Contract Signer and/or the Certificate Approver, as applicable, is an employee; or
    - (B) Obtaining an Independent Confirmation From Applicant, or a Verified Legal Opinion (as described in Section 22 (a)), or a Verified Accountant Letter (as described in Section 22 (b)) 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 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 Applicant signed by the Contract Signer), provided that the employment or agency status and Signing Authority of the Contract Signer has been verified.

(c) **Acceptable Methods of Verification - Authorization** Acceptable methods of verification of the Signing Authority of the Contract Signer, and the EV Authority of the Certificate Approver, as applicable, include:

- (1) **Legal Opinion** The Signing Authority of the Contract Signer, and/or the EV Authority of the Certificate Approver, MAY be verified by reliance on a Verified Legal Opinion (as described in Section 22 (a));
- (2) **Accountant 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 Accountant Letter (as described in Section 22(b));
- (3) **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 (1) certified by the appropriate corporate officer (e.g., secretary), and (2) 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.
- (4) **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 Applicant.
- (5) **Contract between CA and Applicant** The EV Authority of the Certificate Approver MAY be verified by reliance on a contract between the CA and 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.
- (6) **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:

- (1) Agreement title
- (2) Date of Contract Signer's signature
- (3) Contract reference number
- (4) 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:

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

(2) Has participated in the approval of one or more SSL certificates issued by the CA, which are currently in use on public servers operated 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.

**(d) 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 Applicant, and

(2) Has verified the Signing Authority of such Contract Signer in accordance with one of the procedures in the preceding Subsection (c).

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

Such an agreement MUST provide that 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 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.

## **20. Verification of Signature on Subscriber Agreement and EV Certificate Requests**

Both the Subscriber Agreement and each 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. 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, the signature MUST be a legally valid and 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 Applicant to the terms of each respective document.

### **(a) 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 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 21 can substitute for authentication of the signature of the Certificate Requester on such EV Certificate Request.

### **(b) Acceptable Methods of Signature Verification** Acceptable methods of authenticating the signature of the Certificate Requester or Contract Signer include:

- (1) A phone call to Applicant's or Agent's phone number, as verified in accordance with these Guidelines, asking to speak to 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 Applicant.
- (2) A letter mailed to 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 phone or mail response from someone who identifies themselves as such person confirming that he/she did sign the applicable document on behalf of 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.

- (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;

## **21. Verification of Approval of EV Certificate Request**

- (a) **Verification Requirements** In cases where an EV Certificate Request is submitted by a Certificate Requester, before the CA MAY issue the requested EV Certificate, the CA MUST verify that an authorized Certificate Approver reviewed and approved the EV Certificate Request.
- (b) **Acceptable Methods of Verification** Acceptable methods of verifying the Certificate Approver's approval of an EV Certificate Request include:
  - (1) Contacting the Certificate Approver by phone or mail at a verified phone number or address for 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 website, followed by a login by, and an indication of approval from, the Certificate Approver in the manner required by the website; or
  - (3) Verifying the signature of the Certificate Requester on the EV Certificate Request in accordance with Section 20 of these Guidelines.

## **22. Verification of Certain Information Sources**

- (a) **Verified Legal Opinion**
  - (1) **Verification Requirements** Before relying on any legal opinion submitted to the CA, the CA MUST verify that such legal opinion meets the following requirements ("Verified Legal Opinion"):
    - (A) **Status of Author** The CA MUST verify that the legal opinion is authored by an independent legal practitioner retained by and representing Applicant (or an in-house legal practitioner employed by Applicant) (Legal Practitioner) who is either:
      - (i) A lawyer (or solicitor, barrister, advocate, or equivalent) licensed to practice law in the country of Applicant's Jurisdiction of Incorporation or Registration or any jurisdiction where 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 Applicant's Jurisdiction of Incorporation or Registration or any jurisdiction where 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 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 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 D.
- (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, a QGIS, or a 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 22(a)(2)(A), no further verification of authenticity is required.

**(b) Verified Accountant Letter**

- (1) Verification Requirements Before relying on any accountant letter submitted to the CA, the CA MUST verify that such accountant letter meets the following requirements ("Verified Accountant Letter"):

- (A) Status of Author The CA MUST verify that the accountant letter is authored by an independent professional accountant retained by and representing Applicant (or an in-house professional accountant employed by Applicant) (Accounting Practitioner) who is a certified public accountant, chartered accountant, or equivalent licensed by a full member of the International Federation of Accountants (IFAC) to practice accounting in the country of Applicant's Jurisdiction of Incorporation or Registration or any jurisdiction where Applicant maintains an office or physical facility;
  - (B) Basis of Opinion The CA MUST verify that the Accounting Practitioner is acting on behalf of 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:
- (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 accountant letter MUST make clear that the Accounting Practitioner is acting on behalf of Applicant and that the information in the accountant 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 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 accountant letter prove to be erroneous. Acceptable forms of accountant letter are attached as Appendix E.
  - (C) Authenticity To confirm the authenticity of the accountant's opinion, the CA MUST make a telephone call or send a copy of the 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, a QGIS, or a 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 22(b)(2)(A), no further verification of authenticity is required.

**(c) Face-to-face Validation**

- (1) **Verification Requirements** Before relying on any 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 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 22(c)(2)(A), no further verification of authenticity is required.

**(d) Independent Confirmation From Applicant** An “Independent Confirmation From Applicant” is a confirmation of a particular fact (e.g., knowledge of its

exclusive control of a domain name, 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:

- (i) Received by the CA from a person employed by Applicant (other than the person who is the subject of the inquiry) that has the appropriate authority to confirm such a fact (“Confirming Person”), and who represents that he/she has confirmed such fact;
- (ii) Received by the CA in a manner that authenticates and verifies the source of the confirmation; and
- (iii) Binding on Applicant.

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

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

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

- (i) A position within 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 Qualified Government Information Source (e.g., an SEC filing), a Qualified Independent Information Source, a Qualified Government Tax Information Source, a Verified Legal Opinion, a Verified Accountant Letter, or by contacting Applicant’s Human Resources Department by phone or mail (at the phone number or address for Applicant’s Place of Business, verified in accordance with these Guidelines); or
- (ii) 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 Applicant’s Human Resources Department by phone or mail (at the phone number or address for 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:
  - (a) The address of Applicant’s Place of Business as verified by the CA in accordance with these Guidelines; or

- (b) The business address for such Confirming Person specified in a current Qualified Government Information Source (e.g., an SEC filing), a Qualified Independent Information Source, a Qualified Government Tax Information Source, a Verified Legal Opinion, or a Verified Accountant Letter; or
  - (c) The address of 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 Qualified Government Information Source, a Qualified Government Tax Information Source, a Qualified Independent Information Source, a Verified Legal Opinion, or a Verified Accountant Letter; or
  - (iii) By telephone call to the Confirming Person, where such person is contacted by calling the main phone number of 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 himself 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 Qualified Government Information Source, a Qualified Independent Information Source, a Qualified Government Tax Information Source, a Verified Legal Opinion, or a 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.
- (e) **Qualified Independent Information Sources (QIIS)** 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. A commercial database is a QIIS if the following are true:
- (1) data it contains that will be relied upon has been independently verified by other independent information sources;
  - (2) the database distinguishes between self-reported data and data reported by independent information sources;
  - (3) the database provider identifies how frequently they update the information in their database;
  - (4) changes in the data that will be relied upon will be reflected in the database in no more than 12 months; and

- (5) the database provider uses authoritative sources independent of the subject, or multiple corroborated sources, to which the data pertains.

Databases in which the CA or its owners or affiliated companies maintain a controlling interest, or in which any Registration Authorities (RAs) 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. The CA SHOULD check the accuracy of the database and ensure its data is acceptable.

- (f) **Qualified Government Information Source (OGIS)** 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 they are 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.
- (g) **Qualified Government Tax Information Source (OGTIS)** A Qualified Governmental Information Source that specifically contains tax information relating to Private Organizations, Business Entities or Individuals (e.g. the I.R.S. in the United States).

### **23. Other Verification Requirements**

(a) **High Risk Status**

- (1) **Verification Requirements** The CA MUST seek to identify Applicants likely to be at a high risk of being targeted for fraudulent attacks (“High Risk Applicants”), and conduct such additional verification activity and take such additional precautions as are reasonably necessary to ensure that such Applicants are properly verified under these Guidelines.
- (2) **Acceptable Methods of Verification** The CA MAY identify High Risk Applicants by checking appropriate lists of organization names that are most commonly targeted in phishing and other fraudulent schemes, and automatically flagging EV Certificate Requests from Applicants named on these lists for further scrutiny before issuance. Examples of such lists include:
- (A) Lists of phishing targets published by the Anti-Phishing Work Group (APWG); and
  - (B) Internal databases maintained by the CA that include previously revoked EV Certificates and previously rejected EV Certificate Requests due to suspected phishing or other fraudulent usage.

The information SHOULD then be used to flag suspicious new EV Certificate Requests. If an Applicant is flagged as a High Risk Applicant, the CA MUST

perform reasonably appropriate additional authentication and verification to be certain beyond reasonable doubt that Applicant and the target in question are the same organization.

**(b) Denied Lists and Other Legal Black Lists**

- (1) Verification Requirements The CA MUST verify whether Applicant, the Contract Signer, the Certificate Approver, 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 SHOULD NOT issue any EV Certificate to Applicant if either Applicant, the Contract Signer, or Certificate Approver or if 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:

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:

- (A) BIS Denied Persons List - <http://www.bis.doc.gov/dpl/thedeniallist.asp>
  - (B) BIS Denied Entities List - <http://www.bis.doc.gov/Entities/Default.htm>
  - (C) US Treasury Department List of Specially Designated Nationals and Blocked Persons - <http://www.treas.gov/ofac/t11sdn.pdf>
  - (D) US Government export regulations
- (3) If the CA has operations in any other country, the CA SHOULD take reasonable steps to verify with all equivalent denied lists and export regulations (if any) in such other country.

**24. Final Cross-Correlation and Due Diligence**

Except for EV Subscriber Certificates approved by an Enterprise RA:

- (a) 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.

- (b) The CA MUST obtain and document further explanation or clarification from Applicant, Certificate Approver, Certificate Requester, Qualified Independent Information Sources, and/or other sources of information, as necessary, to resolve the discrepancies or details requiring further explanation.
- (c) The CA MUST refrain from issuing an EV Certificate until the entire corpus of information and documentation assembled in support of the EV Certificate is such that issuance of the EV Certificate will not communicate inaccurate factual information that the CA knows, or the exercise of due diligence should discover, from the assembled information and documentation. If satisfactory explanation and/or additional documentation are not received within a reasonable time, the CA SHOULD decline the EV Certificate Request and notify Applicant accordingly.
- (d) 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 29 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:
  - (i) Rely on language translations of the relevant portions of the documentation, provided that the translations are received from a Translator; or
  - (ii) When the CA has utilized the services of a RA, the CA MAY rely on the language skills of the RA to perform the Final Cross-Correlation and Due Diligence, provided the RA complies with Sections 24 (a)(b) and (c) above. 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
  - (iii) When the CA has utilized the services of a 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 24 and is subjected to the Audit Requirements of Sections 35 (b) and (c).

Furthermore, in the case of Enterprise EV Certificates to be issued in compliance with the requirements of Section 30 of these Guidelines, the Enterprise RA MAY perform the requirements of this Final Cross-Correlation and Due Diligence section.

## **25. Certificate Renewal Verification Requirements**

Before renewing an EV Certificate, the CA MUST perform all authentication and verification tasks required by these Guidelines to ensure that the renewal request is

properly authorized by Applicant and that the information in the EV Certificate is still accurate and valid.

## **G. CERTIFICATE STATUS CHECKING AND REVOCATION ISSUES**

### **26. EV Certificate Status Checking**

(a) **Repository** The CA MUST maintain an online 24x7 Repository mechanism whereby Internet browsers can automatically check online the current status of all certificates.

(1) For EV Certificates or Subordinate CA Certificates issued to entities not controlled by the entity that controls the Root CA:

(A) CRLs MUST be updated and reissued at least every seven days, and the nextUpdate field value SHALL NOT be more ten days; or

(B) OCSP. If the CA provides revocation information via an Online Certificate Status Protocol (OCSP) service, it MUST update that service at least every four days. OCSP responses from this service MUST have a maximum expiration time of ten days.

(2) For subordinate CA Certificates controlled by the Root CA:

(A) CRLs MUST be updated and reissued at least every twelve months, and the nextUpdate field value SHALL NOT be more twelve months; or

(B) OCSP. If the CA provides revocation information via an Online Certificate Status Protocol (OCSP) service, it MUST update that service at least every twelve months. OCSP responses from this service MUST have a maximum expiration time of twelve months..

It is strongly RECOMMENDED that all CAs support OCSP when a majority of deployed Web servers support the TLS 1.0 extension in accordance to RFC 3546, to return “stapled” OCSP responses to EV-enabled applications. CAs MUST support an OCSP capability for Subscriber Certificates that are issued after Dec 31, 2010.

(b) **Reasonable User Experience** In cases where the CA chooses to operate only a CRL capability, the CA MUST ensure all 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.

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

- (d) **Deletion of Entries** Revocation entries on a CRL or OCSP MUST NOT be removed until after the expiration date of the revoked EV Certificate.

## 27. **EV Certificate Revocation**

- (a) **Revocation Guidelines and Capability** The CA MUST publish clear guidelines for revoking EV Certificates as part of its EV Policies, and maintain a continuous 24x7 ability to accept and respond to revocation requests and related inquiries.
- (b) **Revocation Events** The CA MUST revoke an EV Certificate it has issued upon the occurrence of any of the following events:
- (1) The Subscriber requests revocation of its EV Certificate;
  - (2) The Subscriber indicates that the original EV Certificate Request was not authorized and does not retroactively grant authorization;
  - (3) The CA obtains reasonable evidence that the Subscriber's Private Key (corresponding to the Public Key in the EV Certificate) has been compromised, or that the EV Certificate has otherwise been misused;
  - (4) The CA receives notice or otherwise becomes aware that a Subscriber has violated one or more of its material obligations under the Subscriber Agreement;
  - (5) The CA receives notice or otherwise becomes aware that a court or arbitrator has revoked a Subscriber's right to use the domain name listed in the EV Certificate, or that the Subscriber has failed to renew its domain name;
  - (6) The CA receives notice or otherwise becomes aware of a material change in the information contained in the EV Certificate;
  - (7) A determination, in the CA's sole discretion, that the EV Certificate was not issued in accordance with the terms and conditions of these Guidelines or the CA's EV Policies;
  - (8) The CA determines that any of the information appearing in the EV Certificate is not accurate.
  - (9) The CA ceases operations for any reason and has not arranged for another EV CA to provide revocation support for the EV Certificate;
  - (10) The CA's right to issue EV Certificates under these Guidelines expires or is revoked or terminated, unless the CA makes arrangements to continue maintaining the CRL/OCSP Repository;
  - (11) The Private Key of the CA's Root Certificate used for issuing that EV Certificate is suspected to have been compromised;
  - (12) Such additional revocation events as the CA publishes in its EV Policies;  
or

- (13) The CA receives notice or otherwise becomes aware that a Subscriber has been added as a denied party or prohibited person to a blacklist, or is operating from a prohibited destination under the laws of the CA's jurisdiction of operation as described in Section 23 of these Guidelines.

## **28. EV Certificate Problem Reporting and Response Capability**

- (a) **Reporting** In addition to EV Certificate revocation, the CA MUST provide Subscribers, Relying Parties, Application Software Vendors, and other third parties with clear instructions for reporting complaints or suspected Private Key compromise, EV Certificate misuse, or other types of fraud, compromise, misuse, or inappropriate conduct related to EV Certificates ("Certificate Problem Reports"), and a 24x7 capability to accept and acknowledge such Reports.
- (b) **Investigation** CAs MUST begin investigation of all Certificate Problem Reports within twenty-four hours and decide whether revocation or other appropriate action is warranted based on at least the following criteria:
  - (i) The nature of the alleged problem;
  - (ii) The number of Certificate Problem Reports received about a particular EV Certificate or website;
  - (iii) The identity of the complainants (for example, complaints from a law enforcement official that a Web site is engaged in illegal activities carry more weight than a complaint from a consumer alleging that they didn't receive the goods they ordered); and
  - (iv) Relevant legislation.
- (c) **Response** The CA MUST also maintain a continuous 24x7 ability to internally respond to any high-priority Certificate Problem Report, and where appropriate, forward such complaints to law enforcement and/or revoke an EV Certificate that is the subject of such a complaint.

## **H. EMPLOYEE AND THIRD PARTY ISSUES**

### **29. Trustworthiness and Competence**

- (a) **Identity and Background Verification** Prior to the commencement of employment of any person by the CA for engagement in the EV Certificate process, 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 SHOULD 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 degree obtained,
  - (D) Search of criminal records (local, state or provincial, and national) where allowed by the jurisdiction where the person will be employed, and
- (3) In the case of employees of the CA at the time of the 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.

**(b) Training and Skills Level**

- (1) The CA MUST provide all personnel performing validation duties (“Validation Specialists”) with skills training that covers basic Public Key Infrastructure (PKI) knowledge, authentication and verification policies and procedures, common threats to the validation process including phishing and other social engineering tactics, and these Guidelines.
- (2) The CA MUST maintain records of such training and ensure that personnel entrusted with Validation Specialist duties meet a minimum skills requirement that enables them to perform such duties satisfactorily.
- (3) Validation Specialists engaged in EV Certificate issuance must maintain adequate skill levels in order to have issuance privilege, consistent with a CA’s training and performance programs.
- (4) The CA MUST ensure that its Validation Specialists qualify for each skill level required by the corresponding validation task before granting privilege to perform said task.
- (5) The CA MUST require all Validation Specialists to pass an internal examination on the EV Certificate validation criteria outlined in these Guidelines.

**(c) 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 due diligence steps, as outlined in Section 24, MAY be performed by one of the persons. For example, one Validation Specialist reviews and verifies all Applicant

information and a second Validation Specialist approves issuance of the EV Certificate.

(2) Such controls MUST be auditable.

### **30. Delegation of Functions to Registration Authorities and Subcontractors**

- (a) **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 24. Affiliates and/or RAs must comply with the qualification requirements of Section 29 of these Guidelines.
- (b) **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 “Enterprise EV Certificates”). In such case, the Subject SHALL be considered an Enterprise RA, and the following SHALL apply:
- (i) 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;
  - (ii) In all cases, the Subject of an Enterprise EV Certificate MUST be an organization verified by the CA in accordance with these Guidelines;
  - (iii) The CA MUST impose these limitations as a contractual requirement with the Enterprise RA and monitor compliance by the Enterprise RA;
  - (iv) The Final Cross-Correlation and Due Diligence requirements of Section 24 of these Guidelines MAY be performed by a single person representing the Enterprise RA; and
  - (v) The audit requirements in Section 35 of these Guidelines will not apply to the Enterprise RA if the CA maintains control over the root key or sub-root key used to issue the enterprise certificates, but the audit MUST cover the Enterprise RA in all other cases.
- (c) **Guidelines Compliance Obligation** In all cases, the CA MUST contractually obligate each such 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 MUST enforce compliance with such terms.
- (d) **Responsibility** In delegating tasks, the CA, its Affiliates, its RAs, Enterprise RAs, and subcontractors (as applicable) MAY allocate liability between themselves contractually as they determine, but the CA and its Root CA remain fully responsible for the performance of all parties in accordance with these Guidelines, as if the tasks had not been delegated.

## **I. DATA AND RECORD ISSUES**

### **31. Documentation and Audit Trail Requirements**

- (a) The CA MUST record in detail every action taken to process an EV Certificate Request and to issue an EV Certificate, including all information generated or received in connection with an EV Certificate Request, and every action taken to process the Request, including time, date, and personnel involved in the action. These records MUST be available as auditable proof of the CA's practices. The foregoing also applies to all Registration Authorities (RAs) and subcontractors as well.
  
- (b) The foregoing record requirements include, but are not limited to, an obligation to record the following events:
  - (i) CA key lifecycle management events, including:
    - (a) Key generation, backup, storage, recovery, archival, and destruction; and
    - (b) Cryptographic device lifecycle management events.
  - (ii) CA and Subscriber EV Certificate lifecycle management events, including:
    - (a) EV Certificate Requests, renewal and re-key requests, and revocation;
    - (b) All verification activities required by these Guidelines;
    - (c) Date, time, phone number used, persons spoken to, and end results of verification telephone calls;
    - (d) Acceptance and rejection of EV Certificate Requests;
    - (e) Issuance of EV Certificates; and
    - (f) Generation of EV Certificate Revocation Lists (CRLs); and OCSP entries.
  - (iii) Security events, including:
    - (a) Successful and unsuccessful PKI system access attempts;
    - (b) PKI and security system actions performed;
    - (c) Security profile changes;
    - (d) System crashes, hardware failures, and other anomalies;
    - (e) Firewall and router activities; and
    - (f) Entries to and exits from the CA facility.
  - (iv) Log entries MUST include the following elements:
    - (a) Date and time of entry;
    - (b) Identity of the person making the journal entry; and
    - (c) Description of entry.

### **32. Document Retention**

- (a) **Audit Log Retention** Audit logs MUST be available to independent auditors upon request. Audit logs SHOULD be retained for at least seven years.
- (b) **Retention of Documentation** The CA MUST retain all documentation relating to all EV Certificate Requests and verification thereof, and all EV Certificates and revocation thereof, for at least seven years after any EV Certificate based on that documentation ceases to be valid. In connection therewith, the CA MUST maintain current an internal database of all previously revoked EV Certificates and previously rejected EV Certificate Requests due to suspected phishing or other fraudulent usage or concerns. Such information SHOULD be used to flag suspicious EV Certificate Requests.

### **33. Reuse and Updating Information and Documentation**

- (a) **Use of Documentation to Support Multiple EV Certificates** The CA MAY issue multiple EV Certificates listing the same Subject and based on a single EV Certificate Request, subject to the aging and updating requirement in (b) below.
- (b) **Use of Pre-Existing Information or Documentation**
  - (1) Each EV Certificate issued by the CA MUST be supported by a valid current EV Certificate Request and a Subscriber Agreement signed by the appropriate Applicant Representative on behalf of Applicant.
  - (2) The age of information used by the CA to verify such an EV Certificate Request MUST NOT exceed the Maximum Validity Period for such information set forth in these Guidelines in Section 8, based on the earlier of the date the information was obtained (e.g., the date of a confirmation phone call) or the date the information was last updated by the source (e.g., if an online database was accessed by the CA on July 1, but contained data last updated by the vendor on February 1, then the date of information would be considered to be February 1).
  - (3) In the case of outdated information, the CA MUST repeat the verification processes required in these Guidelines.

### **34. Data Security**

- (a) **Objectives** The CA MUST develop, implement, and maintain a comprehensive Security Program reasonably designed to:
  - (1) Protect the confidentiality, integrity, and availability of: (i) all EV Certificate Requests and data related thereto (whether obtained from Applicant or otherwise) in CA's possession or control or to which CA has access ("EV Data"), and (ii) the keys, software, processes, and procedures by which the

CA verifies EV Data, issues EV Certificates, maintains a Repository, and revokes EV Certificates (“EV Processes”);

- (2) Protect against any anticipated threats or hazards to the confidentiality, integrity, and availability of the EV Data and EV Processes;
- (3) Protect against unauthorized or unlawful access, use, disclosure, alteration, or destruction of any EV Data or EV Processes;
- (4) Protect against accidental loss or destruction of, or damage to, any EV Data or EV Processes; and
- (5) Comply with all other security requirements applicable to the CA by law.

**(b) Risk Assessment** The CA’s Security Program MUST include regular risk assessments (“Risk Assessments”) that:

- (1) Identify reasonably foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any EV Data or EV Processes;
- (2) Assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of the EV Data and EV Processes; and
- (3) Assess the sufficiency of the policies, procedures, information systems, technology, and other arrangements that the CA has in place to control such risks.

**(c) Security Plan** Based on such Risk Assessment, the CA MUST develop, implement, and maintain a Security Plan consisting of security procedures, measures, and products designed to achieve the objectives set forth above and to reasonably manage and control the risks identified during the Risk Assessment, commensurate with the sensitivity of the EV Data and EV Processes, as well as the complexity and scope of the activities of the CA. Such Security Plan SHALL include administrative, organizational, technical, and physical safeguards appropriate to the size, complexity, nature, and scope of the CA’s business and the EV Data and EV Processes. Such Security Plan SHALL also take into account then-available technology and the cost of implementing the specific measures, and MUST implement a reasonable level of security appropriate to the harm that might result from a breach of security and the nature of the data to be protected.

**(d) Dual Access Control** The CA MUST ensure the system used to process and approve EV Certificate Requests requires actions by at least two trusted persons before the EV Certificate is created.

## J. COMPLIANCE

### 35. Audit Requirements

#### (a) Pre-Issuance Readiness Audit

- (1) If the CA has a currently valid WebTrust Seal of Assurance for CAs (or a currently valid unqualified opinion indicating compliance with equivalent audit procedures approved by the CA/Browser Forum), 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, or a point-in-time readiness assessment audit against equivalent audit procedures approved by the CA/Browser Forum.
- (2) If the CA does *not* have a currently valid WebTrust Seal of Assurance for CAs (or a currently valid unqualified opinion indicating compliance with equivalent audit procedures approved by the CA/Browser Forum), then before issuing EV Certificates the CA and its Root CA MUST successfully complete both: (i) a point-in-time readiness assessment audit against the WebTrust for CA Program, and (ii) a point-in-time readiness assessment audit against the WebTrust EV Program, or an equivalent for both (i) and (ii) as approved by the CA/Browser Forum.

(b) 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 24 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.

#### (c) Annual Independent Audit

- (1) During the period in which it issues EV Certificates, the CA and its Root CA MUST undergo and pass an annual (i) WebTrust Program for CAs audit and (ii) WebTrust EV Program audit, or an equivalent for both (i) and (ii) as approved by the CA/Browser Forum. Such 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.
- (2) Government CAs In cases where the CA is a government entity, an annual audit of the government CA by the appropriate internal government auditing agency is acceptable in lieu of the (i) WebTrust Program for CAs audit and (ii) WebTrust EV Program audit specified above, provided that such internal government auditing agency publicly certifies in writing that its audit addresses the criteria specified in the WebTrust Program for CAs and the

WebTrust EV Program, and certifies that the government CA has successfully passed the audit

- (3) For both government and commercial CAs, the audit report MUST be made publicly available

**(d) Auditor Qualifications** All audits required under these Guidelines MUST be performed by a Qualified Auditor. A Qualified Auditor MUST:

- (1) Be an independent public accounting firm that has proficiency in examining Public Key Infrastructure technology, information security tools and techniques, information technology and security auditing, and the third-party attestation function and be currently licensed to perform WebTrust for CA audits and WebTrust EV Program audits, or to perform such alternate equivalent audits approved by the CA/Browser Forum as will be performed; and
- (2) Be a member of the American Institute of Certified Public Accountants (AICPA), or a non-US equivalent that requires that audits be completed under defined standards that include the possession of certain skill sets, quality assurance measures such as peer review, competency testing, standards with respect to proper assignment of staff to engagements, and requirements for continuing professional education; and
- (3) Maintain Professional Liability/Errors & Omissions insurance, with policy limits of at least \$1 million in coverage.

**(e) Root Key Generation** For CA root keys generated after the release of these Guidelines, the CA's Qualified Auditor SHOULD witness the root key generation ceremony in order to observe the process and the controls over the integrity and confidentiality of the CA root keys produced. The Qualified Auditor MUST then issue a report opining that the CA, during its root key and certificate generation process:

- (1) Documented its Root CA key generation and protection procedures in its Certificate Policy, and its Certification Practices Statement, (CP and CPS);
- (2) Included appropriate detailed procedures and controls in a documented plan of procedures to be performed for the generation of the root certification authority key pair (the "Root Key Generation Script") for the Root CA;
- (3) Maintained effective controls to provide reasonable assurance that the Root CA was generated and protected in conformity with the procedures described in its CP/CPS and with its Root Key Generation Script; and
- (4) Performed, during the root key generation process, all the procedures required by its Root Key Generation Script.
- (5) A video of the entire key generation ceremony SHOULD be recorded for auditing purposes.

## **K. OTHER CONTRACTUAL COMPLIANCE**

### **36. Privacy/Confidentiality Issues**

The CA and its Root CA MUST comply with all applicable privacy, confidential information and trade secret laws and regulations, as well as its published privacy policy, in the collection, use, retention, and disclosure of non-public information as part of the EV Certificate vetting process.

### **37. Limitations on EV Certificate Liability**

#### **(a) CA Liability**

- (1) **Subscribers and Relying Parties** In cases where the CA has issued and managed the EV Certificate in compliance with these Guidelines and its EV Policies, the CA MAY disclaim liability to the EV Certificate Beneficiaries or any other third parties for any losses suffered as a result of use or reliance on such EV Certificate beyond those specified in the CA's EV Policies. In cases where the CA has *not* issued or managed the EV Certificate in complete compliance with these Guidelines and its EV Policies, the CA MAY seek to limit its liability to the Subscriber and to Relying Parties for any cause of action or legal theory involved for any and all claims, losses or damages suffered as a result of the use or reliance on such EV Certificate by any appropriate means that the CA desires, provided that all such purported limitations on the CA's liability MUST also be specified in the CA's EV Policies, and provided further that in no event SHALL the CA seek to limit its liability to Subscribers or Relying Parties for legally recognized and provable claims to a monetary amount less than \$2,000 per Subscriber or Relying Party per EV Certificate. The CA assumes all risk regarding whether its limitations of liability are legally enforceable.
- (2) **Indemnification of Application Software Vendors** Notwithstanding any limitations on its liability to Subscribers and Relying Parties, the CA (and its Root CA) understands and acknowledges that the Application Software Vendors who have a root certificate distribution agreement in place with the CA do not assume any obligation or potential liability of the CA under these Guidelines or that otherwise might exist because of the issuance or maintenance of EV Certificates or reliance thereon by Relying Parties or others. Thus, the CA (and its Root CA) SHALL defend, indemnify, and hold harmless each Application Software Vendor for any and all claims, damages, and losses suffered by such Application Software Vendor related to an EV Certificate issued by the CA, regardless of the cause of action or legal theory involved. This shall not apply, however, to any claim, damages, or loss suffered by such Application Software Vendor related to an EV Certificate issued by the CA where such claim, damage, or loss was directly caused by such Application Software Vendor's software displaying as not trustworthy an

EV Certificate that is still valid, or displaying as trustworthy: (1) an EV Certificate that has expired, or (2) an EV Certificate that has been revoked (but only in cases where the revocation status is currently available from the CA online, and the browser software either failed to check such status or ignored an indication of revoked status).

**(b) Root CA Indemnification** In cases where the Subordinate CA and the Root CA are different legal entities and the Root CA specifically enables the Subordinate CA to issue EV Subscriber Certificates, the Root CA SHALL also be responsible for the performance and warranties of the Subordinate CA, for the Subordinate CA's compliance with these Guidelines, and for all liabilities and indemnification obligations of the Subordinate CA under these Guidelines, as if the Root CA were the Subordinate CA issuing the EV Certificates.

For example, this Section SHALL NOT apply to cases where a Root CA "A", from a different legal entity, cross-certifies Root CA "B" to enable certificates issued by "B" to be trusted in older, non-EV-enabled browsers. The cross certificate issued by "A" to "B" does not enable EV according to these guidelines. Certificates issued by "B" are EV-enabled only when an EV-enabled browser can build a certificate chain to the root certificate of "B".

## DEFINITIONS

1. **Accounting Practitioner:** *[defined in Section 22(b)]*
2. **Affiliate of a CA:** A corporation, partnership, joint venture or other entity controlling, controlled by or under common control with a CA. As used in this definition, “control” (and its correlative meanings, “controlled by” and “under common control with”) means possession, directly or indirectly, of more than fifty percent (50%) of the voting shares of such entity or the power to direct the management and affairs of such entity.
3. **Applicant:** The Private Organization, Business Entity, or Government Entity that applies for (or seeks renewal of) an EV Certificate naming it as the Subject.
4. **Applicant Representative:** An individual person employed by Applicant: (i) who signs and submits, or approves an EV Certificate Request on behalf of an Applicant, and/or (ii) who signs and submits a Subscriber Agreement on behalf of an Applicant.
5. **Application Software Vendor:** A developer of Internet browser software or other software that displays or uses certificates and distributes root certificates, such as KDE, Microsoft Corporation, Mozilla Corporation, Opera Software ASA, and Red Hat, Inc.
6. **Business Entity:** Any entity that is neither a Private Organization nor a Government Entity as defined herein. Examples include general partnerships, unincorporated associations, and sole proprietorships.
7. **CA:** See Certification Authority.
8. **Certificate Approver:** *[defined in Section 10]*
9. **Certification Authority (CA):** An organization agreeing to be bound by these Guidelines that is responsible for the creation, issuance, revocation, and management of EV Certificates. Where the CA is also the Root CA, references to the CA will be synonymous with Root CA.
10. **Certificate Policy (CP):** A set of rules that indicates the applicability of a named certificate to a particular community and/or PKI implementation with common security requirements.
11. **Certificate Problem Report:** *[defined in Section 28(a)]*
12. **Certificate Requester:** *[defined in Section 10]*
13. **Certificate Revocation List (CRL):** A regularly updated time-stamped list of revoked or invalid EV Certificates that is created and digitally signed by the CA that issued the EV Certificates.
14. **Certification Practice Statement (CPS):** One of several documents providing the framework under which certificates are created, issued, managed and used.
15. **Confirmation Request:** *[defined in Section 21(b)]*

16. **Confirming Person:** [*defined in Section 22(d)*]
17. **Contract Signer:** [*defined in Section 10*]
18. **Country:** A Country shall mean a Sovereign State as defined in the Guidelines.
19. **CRL:** See Certificate Revocation List
20. **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.
21. **Enterprise EV Certificate:** An EV Certificate that an Enterprise RA authorizes the CA to issue at third and higher domain levels that are contained within the domain that was included in an original Valid EV Certificate issued to the Enterprise RA.
22. **Enterprise RA:** The Subject of a specified Valid EV Certificate that is authorized by the issuing CA 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 that was included in the original EV Certificate, in accordance with the requirements of these Guidelines.
23. **EV Authority:** [*defined in Section 19(a)*]
24. **EV Certificate:** A certificate that contains information specified in these Guidelines and that has been validated in accordance with these Guidelines.
25. **EV Certificate Beneficiaries:** [*defined in Section 3*]
26. **EV Certificate Request:** A request from an Applicant to the CA and requesting that the CA issue an EV Certificate to Applicant, which request is validly authorized by Applicant and signed by Applicant Representative.
27. **EV Certificate Warranties:** [*defined in Section 3*]
28. **EV Data:** [*defined in Section 34(a)(1)*]
29. **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) by pre-agreement with one or more Application Software Vendor, marks the certificate as being an EV Certificate.
30. **EV Policies:** [*defined in section 4*]
31. **EV Processes:** [*defined in Section 34(a)(1)*]
32. **Extended Validation Certificate:** See EV Certificate.
33. **Government Agency:** In the case of a Private Organization, the government agency in the Jurisdiction of Incorporation under whose authority the legal existence of the Private Organization was established (e.g., the government

- agency that issued the Certificate of Incorporation). In the case 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 enacted the law, regulation, or decree establishing the legal existence of the Government Entity.
34. **Government Entity:** A government-operated legal entity, agency, department, ministry, or similar element of the government of a country, or political subdivision within such country (such as a state, province, city, county, etc.).
  35. **Guidelines:** This document.
  36. **High Risk Applicants:** *[defined in Section 23(a)(1)]*
  37. **Incorporating Agency:** In the case of a Private Organization, the government agency in the Jurisdiction of Incorporation under whose authority the legal existence of the Private Organization was established (e.g., the government agency that issued the Certificate of Incorporation). In the case of a Government Entity, the entity that enacted the law, regulation, or decree establishing the legal existence of the Government Entity.
  38. **Independent Confirmation From Applicant:** *[defined in Section 22(d)]*
  39. **Individual:** A natural person.
  40. **International Organization:** An International Organization is an organization founded by a constituent document, e.g., charter, treaty, convention or similar document, signed by, or on behalf of, a minimum of two or more Sovereign State governments.
  41. **Jurisdiction of Incorporation:** In the case of a Private Organization, the country and (where applicable) the state or province 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 case of a Government Entity, the country and (where applicable) the state or province where the Entity's legal existence was created by law.
  42. **Jurisdiction of Registration:** In the case of a Business Entity, the state, province, locality where the organization has registered its business presence by filings by a Principal Individual involved in the business to verify its existence.
  43. **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.
  44. **Legal Practitioner:** *[defined in Section 22(a)]*
  45. **Maximum Validity Period:** (for verification information): *[defined in Section 8]*
  46. **Object Identifier (OID):** A unique alphanumeric/numeric identifier registered under the International Standards Organization's applicable standard for a specific object or object class.

47. **OCSP Responder:** An online software application operated under the authority of the CA and connected to the Repository to process EV Certificate status requests. See also, Online Certificate Status Protocol.
48. **OID:** See Object Identifier.
49. **Online Certificate Status Protocol (OCSP):** An online Certificate-checking protocol that enables Application Software to determine the status of an identified Certificate. See also OCSP Responder
50. **Parent Company:** A parent company is defined as a company that owns a majority of the Subsidiary Company and this can be verified by referencing a QIIS or from financial statement supplied by a registered Chartered Professional Accountant (CPA) or equivalent outside of the USA.
51. **Place of Business:** The location of any facility (such as a factory, retail store, warehouse, etc) where Applicant's business is conducted.
52. **Principal Individual(s):** Individuals of a Private Organization, Government Entity or Business Entity that are either owners, partners, managing members, directors or officers, 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.
53. **Private Key:** The key of a Key Pair that is kept secret by the holder of the Key Pair, and that is used to create Digital Signatures and/or to decrypt electronic records or files that were encrypted with the corresponding Public Key.
54. **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 in its Jurisdiction of Incorporation.
55. **Public Key:** The key of a Key Pair that MAY be publicly disclosed by the holder of the corresponding Private Key and that is used by a Relying Party to verify Digital Signatures created with the holder's corresponding Private Key and/or to encrypt messages so that they can be decrypted only with the holder's corresponding Private Key.
56. **Public Key Infrastructure (PKI):** A set of hardware, software, people, procedures, rules, policies, and obligations used to facilitate the trustworthy creation, issuance, management, and use of Certificates and keys based on Public Key Cryptography.
57. **Qualified Auditor:** *[defined in Section 35(d)]*
58. **Qualified Government Information Source (QGIS):** *[defined in Section 22(f)]*
59. **Qualified Government Tax Information Source (QGTIS):** *[defined in Section 22(g)]*
60. **Qualified Independent Information Source (QIIS):** *[defined in Section 22(e)]*

61. **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 Comptroller of Currency (OCC) or Office of Thrift Supervision (OTC).
62. **Registered Agent:** An individual or entity that is both:
- a. authorized by Applicant to receive service of process and business communications on behalf of Applicant; and
  - b. listed in the official records of Applicant's Jurisdiction of Incorporation as acting in the role specified in (a) above.
63. **Registered Office:** The official address of a company, as recorded with the Incorporating Agency, to which official documents are sent and legal notices received.
64. **Registration Number:** The unique number assigned to the Private Organization Applicant or Subject entity by the Incorporating Agency in such entity's Jurisdiction of Incorporation.
65. **Regulated Financial Institution:** A financial institution that is regulated, supervised, and examined by governmental, national, state or provincial, or local authorities having regulatory authority over such financial institution based on the governmental, national, state or provincial, or local laws under which such financial institution was organized and/or licensed.
66. **Relying Party:** Any person (individual or entity) that relies on a Valid EV Certificate. An Application Software Vendor is not considered a Relying Party when software distributed by such Vendor merely displays information regarding an EV Certificate.
67. **Repository:** An online database of EV Certificate status information, either in the form of a CRL or an OCSP responder.
68. **Risk Assessments:** *[defined in Section 34(b)]*
69. **Root CA:** The top level Certification Authority that issues the self-signed Root Certificate under which the CA issues EV Certificates.
70. **Root Certificate:** The self-signed certificate issued by the Root CA to identify itself and to facilitate signing of certificates identifying Subordinate CAs.
71. **Root Key:** The Private Key and its associated Public Key held by the Root CA.
72. **Root Key Generation Script:** *[defined in Section 36(e)(2)]*
73. **Security Plan:** *[defined in Section 34(c)]*
74. **Signing Authority:** *[defined in Section 19]*

75. **Sovereign State:** A Sovereign state is a state, or country, that administers its own government, and is not dependent upon, or subject to, another power.
76. **Subject:** The organization identified as the Subject in the Subject:organizationName field of an EV Certificate, whose identity is unambiguously bound to a Public Key also specified in the EV Certificate. An Applicant is also a Subject once the EV Certificate it requested is issued.
77. **Subject Organization Information:** *[defined in Section 6(a)]*
78. **Subordinate CA:** A Certification Authority whose certificates are signed by the Root CA, or another Subordinate CA. EV Certificates issued by a Subordinate CA will be valid if the appropriate EV OID(s) or the special anyPolicy OID are specified in the certificatePolicies extension of the certificates issued to it.
79. **Subscriber / Subscribing Organization:** The organization identified as the Subject in the Subject:organizationName field of an EV Certificate issued pursuant to these Guidelines, as qualified by the Jurisdiction of Incorporation information in the EV Certificate.
80. **Subscriber Agreement:** An agreement between the CA and the Subject named or to be named in an EV Certificate that specifies the rights and responsibilities of the parties, and that complies with the requirements of these Guidelines.
81. **Subsidiary Company:** A subsidiary company is defined as a company that is majority owned by Applicant as verified by referencing a QIIS or from financial statement supplied by a registered Chartered Professional Accountant (CPA) or equivalent outside of the USA.
82. **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 Applicant.
83. **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.
84. **Translator:** An individual or Business Entity that the CA has reason to believe 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.
85. **Trustworthy System:** Computer hardware, software, and procedures that are reasonably secure from intrusion and misuse; provide a reasonable level of availability, reliability, and correct operation; are reasonably suited to performing their intended functions; and enforce the applicable security policy.
86. **Valid:** An EV Certificate that has not expired and has not been revoked.
87. **Validation Specialists:** *[defined in Section 29(b)(1)]*
88. **Verified Accountant Letter:** *[defined in Section 22(b)].*

89. **Verified Legal Opinion:** *[defined in Section 22(a)].*
90. **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.
91. **WebTrust Program for CAs:** The then-current version of the AICPA/CICA WebTrust Program for Certification Authorities, available at <http://www.webtrust.org/certauth fin.htm>.
92. **WebTrust Seal of Assurance:** *[defined in Section 35(a)(1)]*

## Appendix A

### Minimum Cryptographic Algorithm and Key Sizes

#### 1. Root CA Certificates

	Certificate issued on or before 31 Dec 2010	Certificate issued after 31 Dec 2010
Digest algorithm	MD5 (NOT RECOMMENDED), SHA-1	SHA-1*, SHA-256, SHA-384 or SHA-512
RSA	2048 <sup>†</sup>	2048
ECC	NIST P-256	NIST P-256

#### 2. Subordinate CA Certificates

	Certificate issued on or before 31 Dec 2010	Certificate issued after 31 Dec 2010
Digest algorithm	SHA-1	SHA-1*, SHA-256, SHA-384 or SHA-512
RSA	1024	2048
ECC	NIST P-256	NIST P-256

#### 3. Subscriber Certificates

	Certificate issued on or before 31 Dec 2010	Certificate issued after 31 Dec 2010
Digest algorithm	SHA-1	SHA1*, SHA-256, SHA-384 or SHA-512
RSA	1024 or 2048 (Note: subscriber certificates containing a 1024 bit RSA key MUST expire on or before 31 Dec 2010)	2048
ECC	NIST P-256	NIST P-256

† An end-entity certificate MAY, in addition, chain to an EV-enabled 1024-bit RSA root CA certificate key.

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

## Appendix B

### EV Certificates Required Certificate Extensions

#### 1. Root CA Certificate

Root certificates generated after October 2006 MUST be X.509 v3.

##### (a) **basicConstraints**

If the certificate is v3 and is created after October 2006, this extension MUST appear as a critical extension in all CA certificates that contain Public Keys used to validate digital signatures on certificates. The `cA` field MUST be set true. The `pathLenConstraint` field SHOULD NOT be present.

##### (b) **keyUsage**

If the certificate is v3 and is created after October 2006, this extension MUST be present and MUST be marked critical. Bit positions for `keyCertSign` and `cRLSign` MUST be set. All other bit positions SHOULD NOT be set.

All other fields and extensions set in accordance to RFC 3280.

#### 2. Subordinate CA Certificate

##### (a) **certificatePolicies**

MUST be present and SHOULD NOT be marked critical. The set of policy identifiers MUST include the identifier for the CA's extended validation policy if the certificate is issued to a subordinate CA that is not controlled by the Root CA.

##### certificatePolicies:policyIdentifier (Required)

- anyPolicy if subordinate CA is controlled by Root CA
- explicit EV policy OID(s) if subordinate CA is not controlled by Root CA

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

##### certificatePolicies:policyQualifiers:policyQualifierId

- id-qt 2 [RFC 3280]

##### certificatePolicies:policyQualifiers:qualifier

- URI to the Certificate Practice Statement

**(b) cRLDistributionPoint**

MUST be present and MUST NOT be marked critical. If present, it MUST contain the HTTP URL of the CA's CRL service.

**(c) authorityInformationAccess**

SHOULD be present and MUST NOT be marked critical. SHALL contain the HTTP URL of the CA's OCSP responder (accessMethod = 1.3.6.1.5.5.7.48.1). An HTTP accessMethod MAY be included for the CA's certificate (accessMethod = 1.3.6.1.5.5.7.48.2).

**(d) basicConstraints**

This extension MUST appear as a critical extension in all CA certificates that contain Public Keys used to validate digital signatures on certificates. The cA field MUST be set true. The pathLenConstraint field MAY be present.

**(e) keyUsage**

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

All other fields and extensions set in accordance to RFC 3280.

**3. Subscriber Certificate**

**(a) certificate Policies**

MUST be present and SHOULD NOT be marked critical. The set of policyIdentifiers MUST include the identifier for the CA's extended validation policy.

certificatePolicies:policyIdentifier (Required)

- EV policy OID

certificatePolicies:policyQualifiers:policyQualifierId (Required)

- id-qt 2 [RFC 3280]

certificatePolicies:policyQualifiers:qualifier (Required)

- URI to the Certification Practice Statement

**(b) cRLDistributionPoint**

SHOULD be present and MUST NOT be marked critical. If present, it MUST contain the HTTP URL of the CA's CRL service. This extension MUST be present if the certificate does not specify OCSP responder

locations in an authorityInformationAccess extension. See section 26(b) for details.

**(c) authorityInformationAccess**

SHOULD be present and MUST NOT be marked critical. SHALL contain the HTTP URL of the CA's OCSP responder (accessMethod = 1.3.6.1.5.5.7.48.1). An HTTP accessMethod MAY be included for the CA's certificate (accessMethod = 1.3.6.1.5.5.7.48.2). This extension MUST be present if the certificate does not contain a cRLDistributionPoint extension. See section 26(b) for details.

**(d) basicConstraints (optional)**

If present, the cA field MUST be set false.

**(e) keyUsage (optional)**

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

All other fields and extensions set in accordance to RFC 3280.

**Appendix C**  
**User Agent Verification**

The CA MUST host test Web pages that allow Application Software Vendors to test their software. At a minimum, the CA MUST host separate Web pages using certificates that are (a) valid (b) revoked and (c) expired.

**Appendix D**  
**Sample Form Legal Opinion Letter**

[Law Firm Letterhead]

[Date]

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

This firm represents *[exact company name of Client]*<sup>1</sup> (“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 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]*<sup>2</sup> 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

<sup>1</sup> 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.

<sup>2</sup> 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.

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:

---

---

---

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 exclusive 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]<sup>3</sup>*

cc: *[Send copy to Client]*

---

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

## Appendix E

### Sample Accountant Letters Confirming Specified Information<sup>4</sup>

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.

<b>Specified Information:</b>	<b>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)</b>	<b>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)</b>
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)

<sup>4</sup> These are sample letters only and are subject to change. They have not been approved or endorsed by any professional accounting organization.

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

<b>Specified Information:</b>	<b>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)</b>	<b>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)</b>
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 F**

### **Foreign Organization Name Guidelines**

*NOTE: This appendix is only relevant to EV applications from countries that do not have Latin character organization name registrations. More specific information for particular countries may be added to this appendix in the future.*

#### **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 appendix.

#### **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 Standards Organization (ISO),
- (b) A system recognized by the United Nations or
- (c) A Lawyers Opinion confirming the Romanization of the registered name.

#### **3. English Name**

In order to include a Latin character name that is not a Romanization of the registered name in the EV certificate, 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 QGTIS 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 lawyer's opinion letter to be the trading name associated with the registered organization.

### **Country Specific Procedures**

#### **F-1. Japan**

In addition to the procedures set out above:

- (a) The Hepburn method of Romanization is acceptable for Japanese Romanizations.
- (b) The CA MAY verify the Romanized transliteration of Applicant's formal legal name with either a QIIS or a lawyer's opinion letter.
- (c) The CA MAY use the Financial Services Agency to verify an English Name. When used, the CA MUST verify that the English name is recorded in the audited Financial Statements filed with the Financial Services Agency.
- (d) When relying on Articles of Incorporation to verify an English 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 lawyer's opinion letter. The CA MUST verify the authenticity of the Corporate Stamp.

## Appendix G

### Code-signing: Introduction (Informative)

#### 1. Purpose

**(a) Purpose of Code Signing Certificates.** EV Code Signing Certificates are intended to be used to verify the identity of a holder of an EV code signing certificate (Subscriber) and the integrity of its code. They provide assurance to a user or platform provider that code verified with the certificate has not been modified from its original form and is distributed by the legal entity identified in the EV Code Signing Certificate by name, Place of Business address, Jurisdiction of Incorporation or Registration, and other information. EV Code Signing Certificates may help to establish the legitimacy of signed code, help to maintain the trustworthiness of software platforms, help users to make informed software choices, and limit the spread of malware.

No particular software object is identified by an EV Code-Signing Certificate, only its Subscriber is identified.

**(b) Excluded Purposes.** EV Code Signing Certificates focus only on assuring the identity of the Subscriber and that the signed code has not been modified from its original form. EV Code Signing Certificates are ***not*** intended to provide any other assurances, representations, or warranties. Specifically, EV Code Signing Certificates do not warrant that code is free from vulnerabilities, malware, bugs, or other problems. Like all EV Certificates, EV Code Signing Certificates do not warrant or represent that:

- i) the Subject named in the EV Code Signing Certificate is actively engaged in doing business;
- ii) the Subject named in the EV Code Signing Certificate complies with applicable laws;
- iii) the Subject named in the EV Code Signing Certificate is trustworthy, honest, or reputable in its business dealings; or
- iv) it is “safe” to install code distributed by the Subject named in the EV Code Signing Certificate.

#### 2. Environment

The code-signing environment includes the following actors:

**(a) Subscriber.** The Subscriber is the subject of the EV Code-Signing Certificate. It is the entity responsible for distributing the software. The Subscriber does not necessarily hold the copyright to the software.

**(b) Certification Authority.** The Certification Authority verifies the identity and other attributes of the Subscriber and issues a certificate containing the verified information and the Subscriber’s verified public key.

**(c) Timestamp Authority.** The Timestamp Authority timestamps data, thereby asserting that the data existed at the specified time.

**(d) Signing Authority.** The Signing Authority signs code on behalf of a Subscriber.

The Certification Authority, Timestamp Authority and Signing Authority are all governed by these Guidelines. The Timestamp Authority and the Signing Authority are optional components of the environment.

The Guidelines do not acknowledge gradations of assurance in code; they simply define one level of assurance.

### **3. EV indication**

Platforms may modify their behavior or user interface for code that validates correctly according to these Guidelines.

### **4. Life-cycle**

Code may be signed at any point in the development or distribution process, either by a software publisher or a user organization.

Signed code may be verified at any time, including during: download, unpacking, installation, reinstallation, or execution, or during a forensic investigation.

Subscribers may obtain an EV Code-Signing Certificate with a validity period not exceeding thirty-nine months. In the absence of time stamping, their code signatures will no longer be valid once their certificate has expired.

Timestamp Authorities and Signing Authorities may obtain an EV Timestamp Certificate or EV Code-Signing Certificate (respectively) with a validity period not exceeding one hundred and twenty three months.

Ordinarily, a code signature created by a Subscriber may be considered valid for a period of up to thirty-nine months. However, a code signature may be treated as valid for a period of up to one hundred and twenty three months by means of one of the following methods: the “timestamp” method or the “Signing Authority” method.

**(a) Timestamp method.** In this method, the Subscriber signs the code, appends its EV Code-Signing Certificate (whose expiration time is less than thirty-nine months in the future) and submits it to an EV Timestamp Authority to be time-stamped. The resulting package can be considered valid up to the expiration time

of the timestamp certificate (which may be up to one hundred and twenty three months in the future).

**(b) Signing Authority method.** In this method, the Subscriber submits the code, or a digest of the code, to an EV Signing Authority for signature. The resulting signature is valid up to the expiration time of the Signing Authority certificate (which may be up to one hundred and twenty three months in the future).

## **5. Revocation**

**(a) Revocation reasons.** Subscribers are expected to not intentionally include Suspect Code in their signed software. Intentionally signing Suspect Code is a violation of the terms of the Subscriber Agreement, and will likely result in revocation of an EV code signing certificate.

**(b) Revocation status information.** Certification Authorities are required to provide accurate and up-to-date revocation status information for at least one year following the expiration of the associated certificate.

**(c) Revocation processing.** Whenever practical, platforms should check the revocation status of the certificates that they rely upon. However, this is not always practical. This situation occurs, for instance, when signed code has to be loaded earlier in the boot sequence than the network communication stack.

In the timestamp model, the platform should deviate from the RFC 3280 certification path validation algorithm and check the revocation status, not only of the timestamp certificate, but also of the Subscriber's EV Code Signing Certificate at the time of reliance rather than at the time the time-stamp was applied.

In addition to checking revocation status, where practical, platforms should consult blacklists of suspect software.

**(d) Revocation consequences.** A certificate may have a one-to-one relationship with the software object that it verifies. In such cases, revocation of the certificate only invalidates the signature on the code that is suspect. If, on the other hand, a certificate has a one-to-many relationship with the software objects that it verifies, then revocation of the certificate invalidates the signatures on all those software objects, some of which may be perfectly sound.

## **6. Signature validation**

With the exception of revocation checking for time-stamped and expired certificates, platforms are expected to validate signed code in accordance with RFC 3280. When a platform encounters a certificate that fails to validate due to revocation, the platform should reject the code. When a platform encounters a certificate that fails to validate for

reasons other than revocation, the platform should treat the code as it would if it had been unsigned.

## **7. Private-key protection**

Code-signing keys are to be protected by a FIPS 140-2 level 2 (or equivalent) crypto module. Techniques that may be used to satisfy this requirement include:

- (a) Use of an HSM, verified by means of a manufacturer's certificate;
- (b) A hardware crypto module provided by the CA;
- (c) Contractual terms in the subscriber agreement requiring the Subscriber to protect the private key to a standard equivalent to FIPS 140-2 and with compliance being confirmed by means of an audit;

Cryptographic algorithms, key sizes and certificate life-times for both authorities and Subscribers are governed by the NIST key management guidelines.

## **Appendix H**

### **Code-signing: Requirements for Certification Authorities (Normative)**

#### **1. Subscriber verification**

The verification requirements of Sections 13 through 17 and 19 through 25 of the EV Guidelines SHALL be used to verify EV Code Signing Certificate requests. Section 18 of the EV Guidelines regarding validation of the Applicant's Domain Name SHALL NOT apply.

#### **2. Issuance**

An EV Code Signing Certificate SHALL be issued in accordance with the guidelines and policies of Section 4 of the EV Guidelines. Specifically, the Issuing CA and Root CA MUST follow the compliance requirements of 4(a), the EV policies of 4(b), the Insurance requirements of 4(c) and the audit requirements of 4(d). Certification Authorities meeting the requirements of Section 4 MAY issue EV Code Signing Certificates to Subscribers that meet the requirements of Section 5 of the EV Guidelines.

#### **3. Certificate Content**

EV Code Signing Certificates MUST meet the minimum content requirements of Section 6 and Appendix B of the EV Guidelines, except that the Domain Name SHALL be omitted and the keyUsage extension SHALL be set as follows:

##### **(a) keyUsage**

This extension MUST be present and MUST be marked critical. The bit position for digitalSignature MUST be set. All other bit positions SHOULD NOT be set.

The extended key usage certificate extension MUST be set as follows:

##### **(b) extKeyUsage**

This extension MUST be present and MUST be marked critical. The value `id-kp-codeSigning` MUST be present. Other values SHOULD NOT be present.

#### **4. EV Certificate Policy Requirements**

EV Code Signing Certificates, Subordinate CA Certificates, and Root CA Certificates MUST be governed by Section 7 of the EV Guidelines.

## **5. Maximum Validity Period**

The validity period for an EV Code Signing Certificate issued to a Subscriber MUST NOT exceed thirty-nine months. The validity period for an EV Code Signing Certificate issued to a Signing Authority that fully complies with these Guidelines MUST NOT exceed one hundred and twenty three months. The validity period for an EV Timestamp Certificate issued to a Timestamp Authority that fully complies with these Guidelines MUST NOT exceed one hundred and twenty three months. Appendix A and Appendix B.3 of the EV Guidelines SHALL apply.

## **6. Certificate Request Requirements**

EV Code Signing Certificates SHALL satisfy Sections 10, 11, and 12 of the EV Guidelines, except that 11(c)(3) regarding the Domain Name SHALL NOT apply. Additionally, section 12(b)(4) of the EV Guidelines SHALL NOT apply.

## **7. Certificate Status Checking and Revocation Issues**

EV Code Signing Certificates have the same requirements for Certificate Status Checking, Revocation terms, Certificate Problem Reporting and Response Capability as found in Sections 26, 27, and 28 of the EV Guidelines, except that 27(b)(5) shall not apply.

## **8. Employee and Third Party Issues**

The Certification Authority SHALL operate under the Trustworthiness and Competence and Delegation of Functions to Registration Authorities and Subcontractors obligations, duties, and requirements of Sections 29 and 30 of the EV Guidelines.

## **9. Data and Record Issues**

The CA SHALL operate under the Document and Auditing Trail, Document Retention, Reuse and Updating Information and Documentation, and Data Security requirements of Section 31-34 of the EV Guidelines. The CA SHALL abide by the Compliance guidelines and requirements of Section 35 of the EV Guidelines.

## **10. Signing key protection**

- (a) **Crypto module**. The CA SHALL ensure that the Subscriber's private key is generated, stored and used in a crypto module that meets or exceeds the requirements of FIPS 140-2 level 2.

Acceptable methods of satisfying this requirement include (but are not limited to) the following:

- (1) The CA ships a suitable hardware crypto module, with a preinstalled key pair, in the form of a smartcard or USB device or similar;
- (2) The Subscriber counter-signs certificate requests that can be verified by using a manufacturer's certificate indicating that the key is managed in a suitable hardware module;
- (3) The Subscriber provides a suitable IT audit indicating that its operating environment achieves a level of security at least equivalent to that of FIPS 140-2 level 2.

**11. Other Contractual Issues.** The Issuing CA and its Root CA **MUST** comply with the privacy terms as set forth in Section 36 of the EV Guidelines. Likewise, the CA **MUST** follow the guidelines regarding the Limitations on Liability and Indemnification as set forth in Section 37 of the EV Guidelines.

**12. Subscriber agreement.**

The Subscriber Agreement **MUST** impose upon the Subscriber an obligation and warranty:

- (a) To use the EV Code Signing Certificate only to sign code that complies with the requirements set forth in this Appendix and the applicable EV Guidelines;
- (b) To use the EV Code Signing Certificate solely in compliance with all applicable laws;
- (c) To use the EV Code Signing Certificate solely for authorized company business;
- (d) To use the EV Code Signing Certificate solely in accordance with the Subscriber Agreement;
- (e) To attest to the accuracy and currency of the information provided in certificate requests;
- (f) To not knowingly sign software that contains Suspect Code;
- (g) To inform the CA under any of the following circumstances:
  - (1) it is discovered (by whatever means) that code that has been signed is suspect;
  - (2) information in a certificate is or becomes invalid;
  - (3) the Subscriber discovers or suspects that a copy of its private key, or key-activation data, is no longer under its sole control.

### **13. Revocation**

The CA SHALL respond to all plausible notices that a signed software object containing Suspect Code verifies with a certificate that it has issued by setting the revocation status of that certificate to 'revoked'.

The CA SHALL, upon request, provide accurate and up-to-date revocation status information for a period not less than one year beyond expiry of the EV Code-Signing Certificate.

In the Subscriber Agreement, the CA MUST give notice that it will revoke certificates issued to Subscribers who use them to digitally sign Suspect Code.

## Appendix I

### Code-signing: Requirements for Timestamp Authorities (Normative)

#### 1. Timestamp requirements

An EV Timestamp Authority is NOT REQUIRED to validate in any way data submitted to it for time-stamping. It simply adds the time to the data that are presented to it, signs the result and append its own certificate.

An EV Timestamp Authority MUST protect its private key in a crypto module validated in accordance with FIPS 140-2 Level 2.

An EV Timestamp Authority MUST be synchronized with a publicly accepted time source in the jurisdiction of its operation, (e.g. NIST or Naval Laboratory in the United States).

EV Timestamp Certificates MUST meet the minimum content requirements of this appendix and Section 6 and Appendix B of the EV Guidelines, except that the Domain Name SHALL be omitted.

Certificate extensions MUST be included as follows:

##### (a) keyUsage

This extension MUST be present and MUST be marked critical. The bit position for digitalSignature MUST be set. All other bit positions SHOULD NOT be set.

##### (b) extKeyUsage

This extension MUST be present and MUST be marked critical. The value id-kp-timeStamping MUST be present. Other values SHOULD NOT be present.

## Appendix J

### Code-signing: Requirements for Signing Authorities (Normative)

1. **Certificate.** The Signing Authority SHALL obtain an EV Code-Signing Certificate issued in accordance with these Guidelines and identifying the Subscriber (i.e. its customer) as the subject. The certificate MUST meet the minimum content requirements of Section 6 and Appendix B of the EV Guidelines, except that the Domain Name SHALL be omitted and the keyUsage extension SHALL be set as follows:

- (a) **keyUsage**

This extension MUST be present and MUST be marked critical. The bit position for digitalSignature MUST be set. All other bit positions SHOULD NOT be set.

The extended key usage certificate extension SHOULD be set as follows:

- (b) **extKeyUsage**

This extension MUST be present and MUST be marked critical. The value `id-kp-codeSigning` MUST be present. Other values SHOULD NOT be present.

2. **Signature request verification.** The verification requirements of Sections 13 through 17 and 19 through 25 of the EV Guidelines, as they apply to Certification Authorities and certificate requests, SHALL apply to Signing Authorities and signature requests. Section 18 of the EV Guidelines regarding validation of the Applicant's Domain Name SHALL NOT apply.
3. **Issuance.** The guidelines and policies of Section 4 of the EV Guidelines, as they apply to Certification Authorities and certificate requests, SHALL apply to Signing Authorities and signature requests. Specifically, the Signing Authority, its Issuing CA and Root CA, MUST follow the compliance requirements of 4(a), the EV Policies of 4(b), the Insurance requirements of 4(c) and the audit requirements of 4(d). Signing Authorities meeting the requirements of Section 4 MAY issue EV Signatures to Subscribers that meet the requirements of Section 5 of the EV Guidelines.
4. **Revocation.** If the Signing Authority becomes aware (by whatever means) that it has signed code that contains malicious software or a serious vulnerability, then it MUST immediately inform the Issuing CA.

If a Signing Authority's private key, or private key activation data, is compromised or believed to be compromised, the Signing Authority MUST contact the Issuing CA immediately and request that the certificate be revoked.

5. **Employee and Third Party Issues.** The Signing Authority SHALL operate under the Trustworthiness and Competence and Delegation of Functions to Registration Authorities and Subcontractors obligations, duties, and requirements of Sections 29 and 30 of the EV Guidelines.
6. **Data and Record Issues.** The Signing Authority SHALL operate under the Document and Auditing Trail, Document Retention, Reuse and Updating Information and Documentation, and Data Security requirements of Section 31-34 of the EV Guidelines. The Signing Authority SHALL abide by the Compliance guidelines and requirements of Section 35 of the EV Guidelines.
7. **Other Contractual Issues.** The Signing Authority, its Issuing CA and Root CA, MUST comply with the privacy terms as set forth in Section 36 of the EV Guidelines. Likewise, the Signing Authority MUST follow the guidelines regarding Limitations on Liability and Indemnification as set forth in Section 37 of the EV Guidelines.
8. **Subscriber agreement.**

Dealings between the Signing Authority and its customer MUST be governed by an agreement . The agreement MUST contain an obligation and warranty:

- (a) To use the EV Signature solely in compliance with the requirements set forth in this Appendix and the applicable EV Guidelines;
- (b) To use the EV Signature solely in compliance with all applicable laws;
- (c) To use the EV Signature solely for authorized company business;
- (d) To use the EV Signature solely in accordance with the Subscriber Agreement;
- (e) To not knowingly submit software for signature that contains Suspect Code;
- (f) To inform the Signing Authority if it is discovered (by whatever means) that code submitted to the Signing Authority for signature contains malware or a serious vulnerability.