

UNIZETO



**POWSZECHNE
CENTRUM CERTYFIKACJI**

Certification Practice Statement of CERTUM's Certification Services

Appendix 3: Guidelines for the issuance and management of Extended Validation SSL certificates

Version 3.0

Date: 5th of October, 2009

Status: valid

Unizeto Technologies S.A.
„CERTUM – Powszechne Centrum Certyfikacji”
21 Królowej Korony Polskiej, street
70-486 Szczecin
<http://www.certum.pl>

Contents

A. INTRODUCTION	1
1. Introduction.....	1
B. BASIC CONCEPT OF THE EV SSL CERTIFICATE.....	1
2. Purpose of EV SSL Certificates.....	1
(a) Primary Purposes.....	1
(b) Secondary Purposes	1
(c) Excluded Purposes	2
3. EV SSL Certificate Warranties and Representations.....	2
(a) By CERTUM.....	2
(b) By the Subscriber	3
C. COMMUNITY AND APPLICABILITY	3
4. Issuance of EV SSL Certificates.....	3
(a) Compliance	3
(b) EV SSL Policies	4
(c) Insurance	4
5. Obtaining EV SSL Certificates.....	4
(a) Private Organization Subjects	4
(b) Business Entities	5
D. EV SSL CERTIFICATE CONTENT AND PROFILE.....	6
6. EV SSL Certificate Content Requirements.....	6
7. EV Certificate Policy Identification Requirements	8
8. Maximum Validity Period	8
9. Other Technical Requirements for EV SSL Certificates.....	9
E. EV SSL CERTIFICATE REQUEST REQUIREMENTS	9
10. General Requirements.....	9
11. EV SSL Certificate Request Requirements.....	10
12. Subscriber Agreement Requirements.....	11
F. INFORMATION VERIFICATION REQUIREMENTS	12
13. General Overview	12
14. Verification of Applicant’s Legal Existence and Identity	13
15. Verification of Applicant’s Legal Existence and Identity – Assumed Name ...	15
16. Verification of Applicant’s Physical Existence	15
17. Verification of Applicant’s Operational Existence.....	17
18. Verification of Applicant’s Domain Name	17
19. Verification of Name, Title, and Authority of Contract Signer and Certificate Approver.....	19
20. Verification of Signature on Subscriber Agreement and EV SSL Certificate Requests	21
21. Verification of Approval of EV SSL Certificate Request	22
22. Verification of Certain Information Sources	23
23. Other Verification Requirements.....	27
24. Final Cross-Correlation and Due Diligence	28
25. Certificate Renewal Verification Requirements	28
G. CERTIFICATE STATUS CHECKING AND REVOCATION ISSUES	28

26. EV SSL Certificate Status Checking.....	28
27. EV SSL Certificate Revocation	29
28. EV SSL Certificate Problem Reporting and Response Capability	29
H. EMPLOYEE AND THIRD PARTY ISSUES	30
29. Trustworthiness and Competence.....	30
30. Delegation of Functions to Registration Authorities and Subcontractors	30
I. DATA AND RECORD ISSUES	31
31. Documentation and Audit Trail Requirements	31
32. Document Retention	32
33. Reuse and Updating Information and Documentation	32
34. Data Security	32
J. COMPLIANCE	32
35. Audit Requirements.....	32
K. OTHER CONTRACTUAL COMPLIANCE.....	35
36. Privacy/Confidentiality Issues	35
37. Limitations on EV SSL Certificate Liability.....	35
References	36
Glossary	37

A. INTRODUCTION

1. Introduction

These procedures for Extended Validation Certificates document supplemental procedures to CERTUM's currently published CPS procedures for issuing Extended Validation Certificates ("EV Certificates") in terms of the Guidelines for Extended Validation Certificates v 1.1 (hereinafter called EV Guidelines) published by the CAB forum at <http://www.cabforum.org/>. The Guidelines describe certain of the minimum requirements that a Certificate Authority (CA) must meet in order to issue Extended Validation Certificates ("EV SSL Certificates"). Organization information from Valid EV SSL Certificates may be displayed in a special manner by certain 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.

B. BASIC CONCEPT OF THE EV SSL CERTIFICATE

2. Purpose of EV SSL 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 SSL 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 SSL 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 SSL 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 SSL 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 SSL 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 SSL Certificate is not intended to provide any assurances, or otherwise represent or warrant:

- (1) That the Subject named in the EV SSL Certificate is actively engaged in doing business;
- (2) That the Subject named in the EV SSL Certificate complies with applicable laws;
- (3) That the Subject named in the EV SSL 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 SSL Certificate.

3. EV SSL Certificate Warranties and Representations

(a) By CERTUM

Beneficiaries of EV SSL Certificates may be:

- (1) The Subscriber entering into the Subscriber Agreement for the EV SSL Certificate;
- (2) The Subject named in the EV SSL Certificate;
- (3) 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;
- (4) All Relying Parties that actually rely on such EV SSL Certificate during the period when it is Valid.

When CERTUM issues an EV SSL Certificate, it represents and warrants to the EV SSL Certificate Beneficiaries, during the period when the EV SSL Certificate is valid, that the CA has followed the requirements of the Guidelines and its EV Policies in issuing the EV SSL Certificate and in verifying the accuracy of the information contained in the EV SSL Certificate (“EV SSL Certificate Warranty”). This EV SSL Certificate Warranties specifically includes, but are not limited to, the following:

- (1) **Legal Existence:** CERTUM has confirmed with the Incorporating or Registration Agency in the Subject’s Jurisdiction of Incorporation or Registration that, as of the date the EV SSL Certificate was issued, the Subject named in the EV SSL Certificate legally exists as a valid organization or entity in the Jurisdiction of Incorporation or Registration;
- (2) **Identity:** CERTUM has confirmed that, as of the date the EV SSL Certificate was issued, the legal name of the Subject named in the EV SSL 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;

- (3) Right to Use Domain Name: CERTUM has taken all steps reasonably necessary to verify that, as of the date the EV SSL Certificate was issued, the Subject named in the EV SSL Certificate has the exclusive right to use the domain name(s) listed in the EV SSL Certificate;
- (4) Authorization for EV SSL Certificate: CERTUM has taken all steps reasonably necessary to verify that the Subject named in the EV SSL Certificate has authorized the issuance of the EV SSL Certificate;
- (5) Accuracy of Information: CERTUM has taken all steps reasonably necessary to verify that all of the other information in the EV SSL Certificate is accurate, as of the date the EV SSL Certificate was issued;
- (6) Subscriber Agreement: The Subject named in the EV SSL Certificate has entered into a legally valid and enforceable Subscriber Agreement with CERTUM that satisfies the requirements of these Guidelines;
- (7) Status: CERTUM 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 SSL Certificate as Valid or revoked; and
- (8) Revocation: CERTUM will follow the requirements of the Guidelines and revoke the EV SSL Certificate upon the occurrence of any revocation event as specified in the Guidelines.

(b) By the Subscriber

CERTUM 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 SSL Certificate Beneficiaries.

C. COMMUNITY AND APPLICABILITY

4. Issuance of EV SSL Certificates

When issuing EV SSL Certificates, CERTUM satisfies the following requirements as required by the Guidelines:

(a) Compliance

CERTUM shall 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 the 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 SSL Certificates.

(b) EV SSL Policies

- (1) **Implementation.** The CERTUM CPS together with this Appendix to the CERTUM CPS:
 - (A) Implement the requirements of the 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 CERTUM entire root certificate hierarchy including all roots that its EV SSL Certificates depend on for proof of those EV SSL Certificates' authenticity.
- (2) **Disclosure.** CERTUM publicly discloses its EV Policies through this CPS that is available on a 24x7 basis from CERTUM online repository. CERTUM's CPS is structured according to RFC 3647 format.
- (3) **Commitment to Comply with Guidelines.** CERTUM 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 CERTUM 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 SSL Certificates. CERTUM MUST enforce compliance with such terms.

(c) Insurance

CERTUM maintains the following insurance related to their respective performance and obligations under the Guidelines as follows:

- (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 SSL 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.

5. Obtaining EV SSL Certificates

In terms of the Guidelines, EV SSL Certificates can only be issued to Private Organizations, overnment Entities, and Business Entities that satisfy the requirements specified below:

(a) Private Organization Subjects

CERTUM may issue EV SSL 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 CERTUM is prohibited from doing business or issuing a certificate by the laws of the CERTUM’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 CERTUM’s jurisdiction.

(b) Business Entities

CERTUM may issue EV SSL Certificates to Business Entities that 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 CERTUM is prohibited from doing business or issuing a certificate by the laws of the CERTUM’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 CERTUM’s jurisdiction.

D. EV SSL CERTIFICATE CONTENT AND PROFILE

6. EV SSL Certificate Content Requirements

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

(a) Subject Organization Information

Subject to the requirements of the Guidelines, the EV SSL Certificate 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

This field contains 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 CERTUM as provided herein. CERTUM MAY abbreviate the organization prefixes or suffixes in the Organization name, e.g., if the QGIS shows “*Company Name* Incorporated” CERTUM MAY include *Company Name*, Inc. CERTUM uses 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 5280, CERTUM will use only the full legal organization name in the certificate.

If the Organization name by itself exceeds 64 characters, CERTUM 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, CERTUM will **not** issue the EV SSL certificate.

(2) Domain name

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

Required/Optional: Required

This field contains 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 SSL certificates.

(3) Business Category

Certificate Field: subject:businessCategory (OID 2.5.4.15)

Required/Optional: Required

Contents This field contains 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 5280

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 5280

Country:

subject:jurisdictionOfIncorporationCountryName (OID 1.3.6.1.4.1.311.60.2.1.3)

ASN.1 - X520countryName as specified in RFC 5280

Required/Optional Required

These fields contains 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, CERTUM 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

For Private Organizations, this field contains 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 field will include the date of incorporation.

For Government Entities that do not have a Registration Number or readily verifiable date of creation, CERTUM 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

This field contains the address of the physical location of the Subject's Place of Business.

7. EV Certificate Policy Identification Requirements

(a) EV Subscriber Certificates

Each EV SSL Certificate issued by CERTUM will include CERTUM's EV OID in the certificate's certificatePolicies extension. CERTUM's EV OID used for this purpose is 1.2.616.1.113527.2.5.1.1

(b) EV Subordinate CA Certificates

Certificates issued to Subordinate CA (i.e. Certum Extended Validation CA) is controlled by the Root CA MAY and contain the special anyPolicy OID (2.5.29.32.0).

(c) Root CA Certificates

CERTUM's Root CA Certificate for EV SSL Certificates is the **Certum Trusted Network CA**. This Root CA Certificates SHOULD NOT contain the certificatePolicies or extendedKeyUsage extensions.

8. Maximum Validity Period

(a) For EV SSL Certificate

The validity period for an EV SSL Certificate is twenty seven (27) months.

(b) For Validated Data

The age of validated data used to support issuance of an EV SSL Certificate cannot exceed the following limits:

- Legal existence and identity – thirteen (13) months;
- Assumed name – thirteen (13) months;

- Address of Place of Business – thirteen months (13), but thereafter data MAY be refreshed by checking a Qualified Independent Information Source, even where a site visit was originally required;
- Telephone number for Place of Business – thirteen (13) months;
- Bank account verification – thirteen (13) months;
- Domain name – thirteen (13) months;
- Identity and authority of Certificate Approver – thirteen (13) months, unless a contract is in place between CERTUM 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 SSL Certificates

See Appendix 4 and Appendix 5 attached to CPS.

E. EV SSL CERTIFICATE REQUEST REQUIREMENTS

10. General Requirements

(a) Documentation Requirements

Prior to the issuance of an EV SSL Certificate, CERTUM obtains from Applicant the following documentation, in compliance with the requirements of the Guidelines:

- EV SSL Certificate Request
- Subscriber Agreement
- Such additional documentation required by CERTUM to satisfy its verification obligations under the Guidelines

(b) Role Requirements

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

- **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 SSL Certificate Request on behalf of Applicant.
- **Certificate Approver** – The EV SSL 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 SSL Certificate Requests submitted by other Certificate Requesters.

- **Contract Signer** – A Subscriber Agreement applicable to the requested EV SSL 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 SSL Certificate Request Requirements

(a) General

Prior to the issuance of an EV SSL Certificate, CERTUM obtains from Applicant (via a Certificate Requester authorized to act on Applicant's behalf) a properly completed and signed EV SSL Certificate Request in a form prescribed by the CA and that complies with the Guidelines.

(b) Request and Certification

The EV SSL Certificate Requests contains a request from, or on behalf of, Applicant for the issuance of an EV SSL certificate, or certificates, 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 SSL Certificate Request MAY include all factual information about Applicant to be included in the EV SSL Certificate, and such additional information as is necessary for CERTUM to obtain from Applicant in order to comply with the Guidelines and CERTUM's own policies. In cases where the EV SSL Certificate Request does not contain all necessary information about Applicant, CERTUM 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. CERTUM must obtain following information before issuing EV SSL certificate:

- **Organization Name:** Applicant's formal legal organization name to be included in the EV SSL 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);
- **Assumed Name (Optional):** Applicant's assumed name (e.g., d/b/a name) to be included in the EV SSL Certificate, as recorded in the jurisdiction of Applicant's Place of Business, if requested by Applicant;
- **Domain Name:** Applicant's domain name to be included in the EV SSL Certificate;
- **Jurisdiction of Incorporation or Registration:** Applicant's Jurisdiction of Incorporation or Registration to be included in the EV SSL Certificate, and consisting of:
 - (a) City or town (if any),
 - (b) State or province (if any), and

- (c) Country.
- **Incorporating or Registration Agency:** The name of Applicant's Incorporating or Registration Agency;
- **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 SSL Certificate.
- **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.
- **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 SSL Certificate Application on behalf of Applicant; and
- **Certificate Requester:** Name and contact information of the Certificate Requester submitting the EV SSL 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 SSL Certificate, CERTUM obtains 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, and MUST apply to the EV SSL Certificate to be issued pursuant to the EV SSL Certificate Request. A separate Subscriber Agreement MAY be used for each EV SSL Certificate Request, or a single Subscriber Agreement MAY be used to cover multiple future EV SSL Certificate Requests and resulting EV SSL Certificates, so long as each EV SSL Certificate that CERTUM 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 shall, 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:

- Accuracy of Information: An obligation and warranty to provide accurate and complete information at all times to CERTUM, both in the EV SSL Certificate Request and as otherwise requested by CERTUM in connection with the issuance of the EV SSL Certificate(s) to be supplied by CERTUM;
- 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 SSL

Certificate(s) (and any associated access information or device, e.g. password or token);

- Acceptance of EV SSL Certificate: An obligation and warranty that it will not install and use the EV SSL Certificate(s) until it has reviewed and verified the accuracy of the data in each EV SSL Certificate;
- Use of EV SSL Certificate: An obligation and warranty to install the EV SSL Certificate only on the server accessible at a domain name listed on the EV SSL Certificate, and to use the EV SSL Certificate solely in compliance with all applicable laws, solely for authorized company business, and solely in accordance with the Subscriber Agreement;
- Reporting and Revocation Upon Compromise: An obligation and warranty to promptly cease using an EV SSL Certificate and its associated Private Key, and promptly request CERTUM to revoke the EV SSL Certificate, in the event that: (a) any information in the EV SSL 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 SSL Certificate;
- Termination of Use of EV SSL Certificate: An obligation and warranty to promptly cease all use of the Private Key corresponding to the Public Key listed in an EV SSL Certificate upon expiration or revocation of that EV SSL Certificate.

F. INFORMATION VERIFICATION REQUIREMENTS

13. General Overview

This part of CERTUM's procedures for issuing EV SSL Certificates sets forth Verification Requirements required in the Guidelines and procedures used by CERTUM to satisfy the requirements.

- (a) **Verification Requirements – Overview** Before issuing an EV SSL Certificate, CERTUM ensures that all Subject organization information in the EV SSL Certificate conforms to the requirements of, and has been verified in accordance with, these Guidelines and matches the information confirmed and documented by CERTUM pursuant to its verification processes. **Such verification processes are intended to accomplish the following:**

- 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).
- Verify Applicant is a registered holder, or has exclusive control, of the domain name to be included in the EV Certificate;
- 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

(b) Verification Requirements

To verify Applicant's legal existence and identity, CERTUM does the following:

(1) Private Organizations

Legal Existence – Verifies 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.

Organization Name – Verifies 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 SSL Certificate Request.

Registration Number – Obtains 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, CERTUM obtains Applicant's date of Incorporation or Registration.

Registered Agent – Obtains 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

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

Entity Name – Verifies that Applicant's formal legal name matches Applicant's name in the EV SSL Certificate Request.

Registration Number – CERTUM obtains 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, CERTUM enters appropriate language to indicate that the Subject is a Government Entity

(3) Business Entities

Legal Existence – Verifies that Applicant is engaged in business under the name submitted by Applicant in the Application.

Organization Name – Verifies 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 SSL Certificate Request.

Registration Number – Obtains 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, CERTUM obtains Applicant's date of Registration.

Principal Individual – Verifies the identity of the identified Principal Individual.

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

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

Entity Name – Verifies that Applicant's formal legal name matches Applicant's name in the EV SSL Certificate Request.

Registration Number – CERTUM obtains 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, CERTUM enters appropriate language to indicate that the Subject is an International Organization Entity.

The International Organization Entity is verified either:

- With reference to the constituent document under which the International Organization was formed; or
- Directly with a signatory country's government in which CERTUM 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
- Directly against any current list of qualified entities that the CABForum may maintain at www.cabforum.org.
- In cases where the International Organization applying for the EV SSL certificate is an organ or agency - including a non-governmental organization (NGO) of a verified International Organization, then CERTUM 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

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 SSL 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, CERTUM verifies 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.

CERTUM 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. CERTUM 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

To verify Applicant's physical existence and business presence, CERTUM verifies 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, or 'care of' (C/O) address, such as an address for an agent of the Organization), and is 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 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 CERTUM confirms that Applicant's address as listed in the EV SSL 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, CERTUM confirms that the address provided by Applicant in the EV SSL 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 will:
 - (a) Verify that Applicant's business is located at the exact address stated in the EV SSL 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 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, CERTUM relies 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

To further verify Applicant's physical existence and business presence, as well as to assist in confirming other verification requirements, CERTUM verifies that the telephone number provided by Applicant is a main phone number for Applicant's Place of Business.

To verify Applicant's telephone number, CERTUM performs A and either B or C as listed below:

- (A) Confirms 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;
- (B) Confirms 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 Qualified Independent Information Source or Qualified Governmental Information Source, or in a Qualified Governmental Tax Information Source;
- (C) Relies 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.

17. Verification of Applicant's Operational Existence

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, CERTUM verifies that Applicant has the ability to engage in business.

To verify Applicant's operational existence, CERTUM performs one of the following:

- (A) Verifies Applicant has an active current Demand Deposit Account with a Regulated Financial Institution. CERTUM receives authenticated documentation directly from a Regulated Financial Institution verifying that Applicant has an active current Demand Deposit Account with the institution.
- (B) Relies 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

To verify Applicant's registration, or exclusive control, of the domain name(s) to be listed in the EV SSL Certificate, CERTUM verifies 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, CERTUM relies on the domain name listed for that entity in the records of the QGIS in Applicant's Jurisdiction to verify Domain Name.
- (3) Applicant is the registered holder of the domain name, or 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;
- (A) Acceptable methods by which CERTUM verifies that Applicant is the registered holder of the domain name include the following:
- (1) 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
 - (2) 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;
 - (3) In cases where domain registration information is private, and the domain registrar offers services to forward communication to the registered domain holder, CERTUM contacts Applicant through the domain registrar by e-mail or paper mail.
- (B) In cases where Applicant is not the registered holder of the domain name, CERTUM verifies Applicant's exclusive right to use the domain name(s). In addition, CERTUM verifies 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.

In cases where the registered domain holder cannot be contacted, CERTUM will:

- Relies 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
- Relies 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;

CERTUM may verify the Applicant is aware that it has exclusive control of the domain name obtaining a confirmation from the Contract Signer or Certificate Approver verifying that Applicant is aware that it has exclusive control of the domain name.

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

For both the Contract Signer and the Certificate Approver, CERTUM verifies the following:

- (1) **Name, Title and Agency** – CERTUM verifies the name and title of the Contract Signer and the Certificate Approver, as applicable. CERTUM also verifies that the Contract Signer and the Certificate Approver are agents representing Applicant.
 - (2) **Authorization of Contract Signer** – CERTUM verifies, 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** – CERTUM verifies, 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 SSL Certificate Request (“EV Authority”):
 - Submit, and, if applicable, authorize a Certificate Requester to submit, the EV SSL Certificate Request on behalf of Applicant; and
 - Provide, and, if applicable, authorize a Certificate Requester to provide, the information requested from Applicant by CERTUM for issuance of the EV SSL Certificate; and
 - Approve EV SSL Certificate Requests submitted by a Certificate Requester.
- (A) Acceptable methods of verification of the name, title, and agency status of the Contract Signer and the Certificate Approver include:
- (1) **Name and Title** – CERTUM verifies 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** – CERTUM verifies agency of the Contract Signer and the 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 the Guidelines) and obtaining confirmation that the Contract Signer and/or the Certificate Approver, as applicable, is an employee; or
 - Obtaining an Independent Confirmation From Applicant, or a Verified Legal Opinion, or a Verified Accountant Letter verifying that the Contract Signer and/or the Certificate Approver, as applicable, is either an employee or has otherwise been appointed as an agent of Applicant.

CERTUM MAY also verifies 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.

- (B) 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
 - (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
 - (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 CERTUM 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. 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. CERTUM records 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:
 - Agreement title
 - Date of Contract Signer's signature
 - Contract reference number
 - Filing location

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:

- Under contract to CERTUM, has served (or is serving) as an Enterprise RA for the Applicant
 - 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 CERTUM 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.
- (7) **Pre-Authorized Certificate Approver** – Where the CERTUM and Applicant contemplate the submission of multiple future EV SSL Certificate Requests, then, after CERTUM:
- Has verified the name and title of the Contract Signer and that he/she is an employee or agent of Applicant, and
 - Has verified the Signing Authority of such Contract Signer in accordance with one of the procedures in the preceding Subsection (B).

CERTUM 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 SSL 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 SSL 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 CERTUM 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 SSL Certificate Requests

Both the Subscriber Agreement and each non pre-approved EV Certificate Request MUST be signed. The Subscriber Agreement MUST be signed by an authorized Contract Signer. The EV SSL 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 applicable signatures MUST be a legally valid and enforceable seal or handwritten signature (for a paper Subscriber Agreement and/or EV SSL 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** – CERTUM authenticates the signature of the Contract Signer on the Subscriber Agreement and the signature of the Certificate Requester on each EV SSL 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 SSL 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 SSL Certificate Request by a Certificate Approver can substitute for authentication of the signature of the Certificate Requester on such EV SSL Certificate Request.

(b) 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 CERTUM 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 SSL Certificate Request

In cases where an EV SSL Certificate Request is submitted by a Certificate Requester, before CERTUM may issue the requested EV SSL Certificate, CERTUM verifies that an authorized Certificate Approver reviewed and approved the EV SSL Certificate Request. Acceptable methods of verifying the Certificate Approver's approval of an EV SSL 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 SSL Certificate Request;

- (2) Notifying the Certificate Approver that one or more new EV SSL 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 SSL Certificate Request.

22. Verification of Certain Information Sources

(a) Verified Legal Opinion

Before relying on any legal opinion, CERTUM verifies that such legal opinion meets the following requirements (“Verified Legal Opinion”):

- (A) **Status of Autor** – CERTUM verifies 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:
 - (1) 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
 - (2) 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** – CERTUM verifies 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** – To confirm the authenticity of the legal opinion, CERTUM makes 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, CERTUM uses 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 no further verification of authenticity is required.

(b) Verified Accountant Letter

Before relying on any accountant letter, CERTUM verifies that such accountant letter meets the following requirements (“Verified Accountant Letter”):

- (A) **Status of Autor** – CERTUM verifies 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** – CERTUM verifies 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** – To confirm the authenticity of the accountant’s opinion, CERTUM 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, CERTUM uses 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 no further verification of authenticity is required.

(c) Face-to-face Validation

Before relying on any face-to-face vetting documents, CERTUM verifies that the Third-Party Validator meets the following requirements:

- (A) **Qualification of Third-Party Validator** – CERTUM 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** – CERTUM verifies 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 CERTUM confirms the authenticity of the vetting documents received from the Third-Party Validator. CERTUM 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. CERTUM relies 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, 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 CERTUM 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 CERTUM 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) CERTUM initiates 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 CERTUM in accordance with the procedures; 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) CERTUM 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 CERTUM by telephone, by e-mail, or by paper mail, so long as CERTUM can reliably verify that it was provided by a Confirming Person in response to the Confirmation Request.

(e) Qualified Independent Information Sources (QIIS)

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.

(f) Qualified Government Information Source (QGIS)

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.

(g) Qualified Government Tax Information Source (QGTIS)

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

CERTUM seeks 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 the Guidelines.

CERTUM identifies 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 SSL 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 CERTUM that include previously revoked EV SSL Certificates and previously rejected EV SSL Certificate Requests due to suspected phishing or other fraudulent usage.

(b) Denied Lists and Other Legal Black Lists

CERTUM will not issue any EV SSL 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:

- (A) 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 CERTUM’s jurisdiction(s) of operation; and
- (B) has its Jurisdiction of Incorporation, Registration, or Place of Business in any country with which the laws of CERTUM’s jurisdiction prohibit doing business

CERTUM takes reasonable steps to verify with the following lists and regulations:

- (A) Denied Persons List
- (B) Denied Entities List
- (C) Treasury Department List of Specially Designated Nationals and Blocked Persons
- (D) Government export regulations

24. Final Cross-Correlation and Due Diligence

CERTUM requires that after all of the verification processes and procedures are completed, CERTUM has a person who is not responsible for the collection of information review all of the information and documentation assembled in support of the EV SSL Certificate application and look for discrepancies or other details requiring further explanation.

25. Certificate Renewal Verification Requirements

In conjunction with the EV Certificate Renewal process, CERTUM performs all authentication and verification tasks required by the Guidelines to ensure that the renewal request is properly authorized by Applicant and that the information in the EV SSL Certificate is still accurate and valid.

G. CERTIFICATE STATUS CHECKING AND REVOCATION ISSUES

26. EV SSL Certificate Status Checking

CERTUM maintains an online 24x7 Repository mechanism whereby Internet browsers can automatically check online the current status of all certificates.

- (1) For EV SSL Certificates:
 - (A) CRLs are updated and reissued at least every seven days, and the nextUpdate field value SHALL NOT be more ten days; or
 - (B) OCSP Since January 2010 **Certum Extended Validation CA** will provide revocation information via an Online Certificate Status Protocol (OCSP) service and update that service at least every four days. OCSP responses from this service will have a maximum expiration time of ten days.
- (2) For subordinate Certum Extended Validation CA:
 - (A) CRLs are updated and reissued at least every twelve months, and the nextUpdate field value SHALL NOT be more twelve months; or
 - (B) OCSP Since January 2010 the **Certum Trusted Network CA** will provide revocation information via an Online Certificate Status Protocol (OCSP) service and update that service at least every twelve months. OCSP responses from this service will have a maximum expiration time of twelve months..

CERTUM operates and maintains 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 SSL Certificates issued by CERTUM. CERTUM ensures all CRLs for an EV SSL Certificate chain can be downloaded in no more than three (3) seconds over an analog telephone line under normal network conditions.

Revocation entries on a CRL or OCSP are not removed until after the expiration date of the revoked EV SSL Certificate.

27. EV SSL Certificate Revocation

CERTUM revokes an EV SSL Certificate it has issued upon the occurrence of any of the following events:

- (1) The Subscriber requests revocation of its EV SSL Certificate;
- (2) The Subscriber indicates that the original EV SSL Certificate Request was not authorized and does not retroactively grant authorization;
- (3) CERTUM obtains reasonable evidence that the Subscriber's Private Key (corresponding to the Public Key in the EV SSL Certificate) has been compromised, or that the EV SSL Certificate has otherwise been misused;
- (4) CERTUM receives notice or otherwise becomes aware that a Subscriber has violated one or more of its material obligations under the Subscriber Agreement;
- (5) CERTUM 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 SSL Certificate, or that the Subscriber has failed to renew its domain name;
- (6) CERTUM receives notice or otherwise becomes aware of a material change in the information contained in the EV SSL Certificate;
- (7) A determination, in CERTUM's sole discretion, that the EV SSL Certificate was not issued in accordance with the terms and conditions of these Guidelines or the CERTUM's EV Policies;
- (8) CERTUM determines that any of the information appearing in the EV SSL Certificate is not accurate.
- (9) CERTUM ceases operations for any reason and has not arranged for another EV CA to provide revocation support for the EV SSL Certificate;
- (10) CERTUM's right to issue EV SSL Certificates under these Guidelines expires or is revoked or terminated, unless CERTUM makes arrangements to continue maintaining the CRL/OCSP Repository;
- (11) The Private Key of the CERTUM's Root Certificate used for issuing that EV SSL Certificate is suspected to have been compromised;
- (12) Such additional revocation events as CERTUM publishes in its EV Policies; or
- (13) CERTUM 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 CERTUM's jurisdiction of operation.

28. EV SSL Certificate Problem Reporting and Response Capability

CERTUM provides Subscribers, Relying Parties, Application Software Vendors, and other third parties an online form to report complaints or suspected Private Key compromise, EV SSL Certificate misuse, or other types of fraud, compromise, misuse, or inappropriate conduct related to EV SSL Certificates ("Certificate Problem Reports"), and a 24x7 capability to accept and acknowledge such Reports, at: www.certum.pl/repository

CERTUM will begin investigation of all Certificate Problem Reports within twenty-four business 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 SSL 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.

CERTUM also provides reasonable steps to 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 SSL Certificate that is the subject of such a complaint.

H. EMPLOYEE AND THIRD PARTY ISSUES

29. Trustworthiness and Competence

Prior to the commencement of employment of any person by CERTUM for engagement in the EV SSL Certificate process, whether as an employee, agent, or an independent contractor, of CERTUM, is subject to following procedures:

- (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

CERTUM requires all Validation Specialists to pass an internal examination on the EV SSL Certificate validation criteria outlined in these procedures.

30. Delegation of Functions to Registration Authorities and Subcontractors

CERTUM 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 CERTUM fulfills the requirement of Section 24. Affiliates and/or RAs must comply with the qualification requirements of Section 29 of the Guidelines.

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

- (i) An Enterprise RA cannot authorize CERTUM to issue an Enterprise EV SSL 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 SSL Certificate MUST be an organization verified by CERTUM in accordance with the Guidelines;

- (iii) CERTUM 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 the Guidelines MAY be performed by a single person representing the Enterprise RA.

In all cases, CERTUM contractually obligates each such Affiliate, RA, subcontractor, and Enterprise RA to comply with all applicable requirements in the Guidelines and to perform them as required of CERTUM itself. CERTUM shall enforce compliance with such terms.

I. DATA AND RECORD ISSUES

31. Documentation and Audit Trail Requirements

CERTUM records in detail every action taken to process an EV SSL Certificate Request and to issue an EV SSL Certificate, including all information generated or received in connection with an EV SSL 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 CERTUM's practices. The foregoing also applies to all Registration Authorities (RAs) and subcontractors as well.

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

- (i) CERTUM key lifecycle management events, including:
 - (a) Key generation, backup, storage, recovery, archival, and destruction; and
 - (b) Cryptographic device lifecycle management events.
- (ii) CERTUM and Subscriber EV SSL Certificate lifecycle management events, including:
 - (a) EV SSL 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 SSL Certificate Requests;
 - (e) Issuance of EV SSL Certificates; and
 - (f) Generation of EV SSL 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 CERTUM 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

Audit logs are made available to independent auditors upon request. Audit logs are retained for at least seven years.

CERTUM retains all documentation relating to all EV SSL Certificate Requests and verification thereof, and all EV SSL Certificates and revocation thereof, for at least seven years after any EV Certificate based on that documentation ceases to be valid. In connection therewith, CERTUM maintains current an internal database of all previously revoked EV SSL Certificates and previously rejected EV SSL Certificate Requests due to suspected phishing or other fraudulent usage or concerns. Such information is used to flag suspicious EV SSL Certificate Requests.

33. Reuse and Updating Information and Documentation

(a) Use of Documentation to Support Multiple EV SSL Certificates

CERTUM may issue multiple EV SSL Certificates listing the same Subject and based on a single EV SSL Certificate Request, subject to the aging and updating requirement in (b) below.

(b) Use of Pre-Existing Information or Documentation

- (1) Each EV SSL Certificate issued by CERTUM MUST be supported by a valid current EV SSL 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 SSL Certificate Request MUST NOT exceed the Maximum Validity Period for such information set forth in the Guidelines, 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 CERTUM 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, CERTUM repeats the verification processes required in the Guidelines.

34. Data Security

Section 5 and 6 of the CERTUM CPS describe CERTUM's Security Controls.

J. COMPLIANCE

35. Audit Requirements

(a) Pre-Issuance Readiness Audit

Before issuing EV SSL Certificates CERTUM successfully complete a point-in-time readiness assessment audit against the WebTrust for CA Program, and a point-in-time

readiness assessment audit against the WebTrust EV Program, or an equivalent audit procedures approved by the CA/Browser Forum.

(b) Regular Self Audits

During the period in which it issues EV SSL Certificates, CERTUM strictly control its service quality by performing ongoing self audits against a randomly selected sample of at least three percent of the EV SSL Certificates it has issued in the period beginning immediately after the last sample was taken.

(c) Annual Independent Audit

CERTUM undergoes 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 the Guidelines regardless of whether they are performed directly by CERTUM or delegated to an RA or subcontractor.

The audit report is made publicly available by CERTUM.

(d) Auditor Qualifications

All audits required under the 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 CERTUM's Qualified Auditor may 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 CERTUM, during its root key and certificate generation process:

- Documented its Root CA key generation and protection procedures in its Certificate Policy, and its Certification Practices Statement, (CP and CPS);
- 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;
- 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
- Performed, during the root key generation process, all the procedures required by its Root Key Generation Script.
- A video of the entire key generation ceremony may be recorded for auditing purposes.

K. OTHER CONTRACTUAL COMPLIANCE

36. Privacy/Confidentiality Issues

CERTUM will 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 SSL Certificate vetting process.

37. Limitations on EV SSL Certificate Liability

(a) CA Liability

- (1) **Subscribers and Relying Parties** – In cases where CERTUM has issued and managed the EV SSL Certificate in compliance with the Guidelines and its CPS, CERTUM shall not be liable to the EV SSL Certificate Subscribers or Relying Parties or any other third parties for any losses suffered as a result of use or reliance on such EV SSL Certificate. In cases where CERTUM has not issued or managed the EV SSL Certificate in complete compliance with the Guidelines and this CPS, CERTUM's liability to the Subscriber for legally recognized and provable claims for losses or damages suffered as a result of the use or reliance on such EV SSL Certificate shall be the greater of (a) the damages recoverable under the Netsure Protection plan or (b) \$2,000. CERTUM's liability to Relying Parties or any other third parties for legally recognized and provable claims for losses or damages suffered as a result of the use or reliance on such EV SSL Certificate shall not exceed \$2,000.
- (2) **Indemnification of Application Software Vendors** – Notwithstanding any limitations on its liability to Subscribers and Relying Parties, CERTUM understands and acknowledges that the Application Software Vendors who have a root certificate distribution agreement in place with CERTUM do not assume any obligation or potential liability of CERTUM under the Guidelines or that otherwise might exist because of the issuance or maintenance of EV SSL Certificates or reliance thereon by Relying Parties or others. Thus, CERTUM 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 SSL Certificate issued by CERTUM, 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 SSL Certificate issued by CERTUM where such claim, damage, or loss was directly caused by such Application Software Vendor's software displaying as not trustworthy an EV SSL Certificate that is still valid, or displaying as trustworthy: (1) an EV SSL Certificate that has expired, or (2) an EV SSL Certificate that has been revoked (but only in cases where the revocation status is currently available from CERTUM online, and the browser software either failed to check such status or ignored an indication of revoked status).

References

1. CA/BROWSER FORUM Guidelines for the issuance and Management of Extended Validation Certificates, Version 1.1, 10 April 2008
2. VeriSign CPS – VeriSign Certification Practice Statement, ver.3.8, June 01, 2008, <http://www.verisign.com>

Glossary

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

Guidelines for the Issuance and Management of Extended Validation Certificates v 1.1 – Document published at <http://www.cabforum.org>. The Guidelines describe certain of the minimum requirements that a Certificate Authority (CA) must meet in order to issue EV Certificates.

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

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.

Request - A request from an Applicant (or authorized agent of the Applicant) to a CA for the issuance of a Certificate.

Subscriber Agreement – An agreement between the CA and the Subject named or to be named in an EV SSL Certificate that specifies the rights and responsibilities of the parties, and that complies with the requirements of these Guidelines.

Applicant – The Private Organization, Business Entity, or Government Entity that applies for (or seeks renewal of) an EV SSL Certificate naming it as the Subject.

Certificate Requester - [defined in Section 10]

Certificate Approver - [defined in Section 10]

Contract Signer - [defined in Section 10]

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.

Operational Existence – business activity

Independent Confirmation From Applicant - [defined in Section 19]

Confirming Person - [defined in Section 22(d)]

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 SSL Certificates.

Subscriber – The organization identified as the Subject in the Subject:organizationName field of an EV SSL Certificate issued pursuant to these Guidelines, as qualified by the Jurisdiction of Incorporation information in the EV SSL Certificate.

Qualified Government Information Source (QGIS) - [defined in Section 22(f)]

Qualified Government Tax Information Source (QGTIS) - [defined in Section 22(g)]

Qualified Independent Information Source (QIIS) - [defined in Section 22(e)]

Certain Information Sources – The following sources of information about a subscriber are considered to be certain:

- Verified Legal Opinion
- Verified Accountant Letter
- Face-to-face Validation
- Independent Confirmation From Applicant
- Qualified Independent Information Sources (QIIS)
- Qualified Government Information Source (QGIS)
- Qualified Government Tax Information Source (QGTIS)

High Risk Applicants - [defined in Section 23(a)]