



TRUSTCENTER
Now part of Symantec

TC TrustCenter Certificate Policy Definitions for EV Certificates

Version of February 28th, 2012

1	INTRODUCTION.....	3
2	IMPORTANT NOTES.....	4
2.1	REMARKS ABOUT CODE SIGNING CERTIFICATES.....	4
2.2	EV CERTIFICATE PROBLEM REPORTING.....	6
2.3	TESTPAGES FOR APPLICATION SOFTWARE VENDORS	7
3	EV CERTIFICATES	7
3.1	ROLE REQUIREMENTS	8
3.1.1	<i>Verification of Roles.....</i>	8
3.2	OBTAINING EV CERTIFICATES	10
3.2.1	<i>Documents.....</i>	10
3.3	VERIFICATION OF INDIVIDUALS.....	12
3.3.1	<i>Face-to-face validation:.....</i>	12
3.3.2	<i>Cross-checking of Information:.....</i>	13
3.3.3	<i>Verification of Third-party validator:</i>	13
3.4	VERIFICATION OF SIGNATURE ON SUBSCRIBER AGREEMENT AND EV CERTIFICATE REQUESTS	13
3.5	VERIFICATION OF APPROVAL OF EV CERTIFICATE REQUEST	15
3.6	VERIFICATION OF ORGANIZATIONS	15
3.6.1	<i>Verification of Applicant's Legal Existence and Identity.....</i>	15
3.6.2	<i>Verification of the Applicant's Physical Existence.....</i>	18
3.6.3	<i>Verification of the Applicant's Operational Existence.....</i>	20
3.7	VERIFICATION OF DOMAIN NAME	20
3.7.1	<i>Verification Requirements.....</i>	21
3.7.2	<i>Method of Verification</i>	21
3.8	VERIFICATION OF INFORMATION SOURCES	22
3.8.1	<i>Verified Legal Opinion.....</i>	22
3.8.2	<i>Verified Accountant Letter</i>	23
3.8.3	<i>Face-to-face Validation by Third Party Validator.....</i>	24
3.8.4	<i>Independent Confirmation From Applicant</i>	24
3.8.5	<i>Qualified Independent Information Sources (QIIS)</i>	26
3.8.6	<i>Qualified Government Information Source (QGIS)</i>	26
3.8.7	<i>Qualified Government Tax Information Source (QGTIS)</i>	26
3.9	OTHER VERIFICATION REQUIREMENTS	27
3.9.1	<i>High Risk Status</i>	27
3.9.2	<i>Denied Lists and Other Legal Black Lists</i>	27
3.10	CERTIFICATE RENEWAL VERIFICATION REQUIREMENTS	28
4	REVOCATION OF EV CERTIFICATES.....	28
4.1	REVOCATION OF EV CODE SIGNING CERTIFICATES SIGNING MALICIOUS CODE.....	29
5	NAMING CONVENTIONS	29
5.1	CHARACTER SET AND RULES FOR CONVERSION	29
5.1.1	<i>Conversion of Characters</i>	30
6	EV CERTIFICATE CONTENT	30

1 Introduction

Extended Validation Certificates (EV Certificates) are a special type of [X.509](#) certificates which require more extensive investigation of the requesting entity by the [Certificate Authority](#) before being issued.

This document describes the requirements on the verification of data for the issuance of Extended Validation Certificates and the measures taken by TC TrustCenter in order to comply with 'Guidelines for the Issuance and Management of Extended Validation Certificates' (EV Guidelines).

These EV Guidelines have been established by the CA/Browser Forum. They present criteria for issuing, maintaining, and revoking digital certificates for use in Internet website commerce. Certificates issued in compliance with the EV Guidelines provide a high level of trust.

The legal, commercial, and technical principles and practices that TC TrustCenter employs in providing certification services as well as the conditions of issuance, revocation and renewal of certificates are laid down in TC TrustCenter's Certification Practice Statement (CPS).

Contact information:

TC TrustCenter GmbH
Sonninstrasse 24-28
20097 Hamburg
Germany

WWW: <http://www.trustcenter.de>
E-Mail: info@trustcenter.de
Phone: +49 (0)40 80 80 26-0
Fax: +49 (0)40 80 80 26-126

Copyright notice: This document is protected by intellectual property rights. No information or images, fully or partially, in any form or by any means, may be reproduced, copied, duplicated, published or used in electronic systems or translations without the prior written consent of TC TrustCenter. This represents a crime, excluding printing and duplicating for one's own use.

All information in this document is compiled with great care. Neither TC TrustCenter nor the author are liable for any damages or disservice, that are in connection with the use of this document.

„TC TrustCenter“ and the TC TrustCenter logo are registered trademarks of the TC TrustCenter GmbH.

All brands, product names and trademarks used in this document, but not listed above, are trademarks or service marks of the respective owners.

Copyright © 2010 TC TrustCenter GmbH, Sonninstrasse 24 – 28, 20097 Hamburg, Germany. All rights reserved.

2 Important notes

When issuing an Extended Validation certificate TC TrustCenter assures:

1. Legal Existence
TC TrustCenter has confirmed with the Incorporating or Registration Agency in the Subject's Jurisdiction of Incorporation or Registration that, as of the date the EV Certificate was issued, the Subject named in the EV Certificate legally exists as a valid organization or entity in the Jurisdiction of Incorporation or Registration;
2. Identity
TC TrustCenter has confirmed that, as of the date the EV Certificate was issued, the legal name of the Subject named in the EV Certificate matches the name on the official government records of the Incorporating or Registration Agency in the Subject's Jurisdiction of Incorporation or Registration, and if an assumed name is also included, that the assumed name is properly registered by the Subject in the jurisdiction of its Place of Business;
3. Right to Use Domain Name
TC TrustCenter has taken all steps reasonably necessary to verify that, as of the date the EV Certificate was issued, the Subject named in the EV Certificate has the exclusive right to use the domain name(s) listed in the EV Certificate;
4. Authorization for EV Certificate
TC TrustCenter has taken all steps reasonably necessary to verify that the Subject named in the EV Certificate has authorized the issuance of the EV Certificate;
5. Accuracy of Information
TC TrustCenter has taken all steps reasonably necessary to verify that all of the other information in the EV Certificate is accurate, as of the date the EV Certificate was issued;
6. Subscriber Agreement
The Subject named in the EV Certificate has entered into a legally valid and enforceable Subscriber Agreement with TC TrustCenter that satisfies the requirements of the Guidelines for the Issuance of Extended Validation Certificates.

EV Certificates confirm the identity of the certificate owner; they do not provide information about the certificate holder's behaviour. By issuing an EV Certificate TC TrustCenter does not warrant

1. that the Subject named in the certificate is actively engaged in doing business,
2. that the Subject named in the certificate complies with applicable laws,
3. that the Subject named in the 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 certificate.

2.1 Remarks about Code Signing Certificates

Life-Cycle

Code may be signed at any point in the development or distribution process, either by a software publisher or a user organization. Signed code may be verified at any time, including during: download, unpacking, installation, reinstallation, or execution, or during a forensic investigation.

Subscribers may obtain an EV Code Signing Certificate with a validity period not exceeding 39 (thirty-nine) months. In the absence of time stamping, their code signatures will no longer be valid once their certificate has expired.

Timestamp Authorities and Signing Authorities may obtain an EV Timestamp Certificate or EV Code Signing Certificate (respectively) with a validity period not exceeding 123 (one hundred and twenty three) months.

Ordinarily, a code signature created by a Subscriber may be considered valid for a period of up to 39 months.

However, a code signature may be treated as valid for a period of up to 123 months by means of one of the following methods: the “Timestamp” method or the “Signing Authority” method.

- a) **Timestamp Method:** In this method, the Subscriber signs the code, appends its EV Code Signing Certificate (whose expiration time is less than 39 months in the future) and submits it to an EV Timestamp Authority to be time-stamped. The resulting package can be considered valid up to the expiration time of the timestamp certificate (which may be up to 123 months in the future).
- b) **Signing Authority Method:** In this method, the Subscriber submits the code, or a digest of the code, to an EV Signing Authority for signature. The resulting signature is valid up to the expiration time of the Signing Authority certificate (which may be up to 123 months in the future).

Private-Key Protection

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

- a) Use of an HSM, verified by means of a manufacturer’s certificate;
- b) Contractual terms in the subscriber agreement requiring the Subscriber to protect the private key to a standard equivalent to FIPS 140-2 and with compliance being confirmed by means of an audit.

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

Code Signing Certificate Content

EV Code Signing Certificates in principle contain the same data objects as EV SSL Certificates. However, they do **not** contain a domain name.

The keyUsage extensions of a Code Signing Certificate must be set as follows:

keyUsage

This extension **MUST** be present and **MUST** be marked critical.

The bit position for *digitalSignature* **MUST** be set.

All other bit positions **SHOULD NOT** be set.

extKeyUsage

This extension **MUST** be present and **MUST** be marked critical.

The value id-kp-codeSigning **MUST** be present.

Other values **SHOULD NOT** be present.

Issuance of certificates according to the current Certificate Policy Definitions: All EV Certificates issued by TC TrustCenter are issued based on the “Certificate Policy Definitions for EV Certificates” being valid at the time of the issuance of the EV Certificate. A later modification of the “CPD for EV Certificates” has no influence on already issued EV Certificates.

No verification of creditworthiness: An EV Certificate confirms the identity of a certificate applicant as described in this document. This does not include verification of liquidity, creditworthiness or anything of that nature. A certificate provides a certain level of assurance that the certificate belongs to the entity named therein. It gives no indication whatsoever about the trustworthiness of the entity itself.

No assurance of up-to-date certificate data: Information contained in an EV Certificate is verified only during registration at the time of issuance of a certificate. TC TrustCenter accordingly does not provide any assurance that this data is up-to-date **after** registration. Every certificate holder is obliged to revoke its certificate if data contained therein is not accurate any more.

The end user must determine whether a given certificate is adequate: TC TrustCenter issues EV Certificates in compliance with its “CPD for EV Certificates”, TC TrustCenter’s CPS, and in compliance with the EV Guidelines published by the CA/Browser Forum (<http://www.cabforum.org/>). Any participant of the certification service must decide for itself whether these policies and guidelines meet the security needs for the application in question.

Participant’s obligation to inform itself: It is essential for any end user participating in TC TrustCenter’s certification services to acquire sufficient knowledge about the use of digital signatures, certificates, and public key algorithms.

Subscriber’s duties to take good care and to cooperate: The subscriber has to contribute to the security of certificates and digital signatures. Therefore, it is essential to follow the guidelines as set out in this document.

TC TrustCenter reserves its right to revoke certificates: If cryptographic algorithms or associated parameters become unsafe due to technical progress or new developments in cryptology, TC TrustCenter reserves its right to revoke certificates that are based on such algorithms and parameters. Certificates may also be revoked if the certificate holder provided false information, if certificates are misused or are used for criminal purposes, or if TC TrustCenter has obtained knowledge that data in the certificate do no longer comply with the facts.

2.2 EV Certificate Problem Reporting

TC TrustCenter provides web pages, available 24x7, for Subscribers, Relying Parties, Application Software Vendors, and other third parties. Via these web pages problem reports consisting e.g. of complaints of suspected private key compromise, EV Certificate misuse, or other types of fraud, compromise, misuse, or inappropriate conduct related to EV Certificates can be submitted to TC TrustCenter.

TC TrustCenter will begin investigation of all Certificate Problem Reports within 24 hours and decide whether revocation or other appropriate action is warranted based on at least the following criteria:

- (i) The nature of the alleged problem;
- (ii) The number of Certificate Problem Reports received about a particular EV Certificate or Web site;
- (iii) The identity of the complainants (for example, a complaint from a law enforcement official that a Web site is engaged in illegal activities carries more weight than a complaint from a consumer alleging that they didn’t receive the goods they ordered); and

- (iv) Relevant legislation.

TC TrustCenter maintains a continuous 24x7 ability to internally respond to high-priority Certificate Problem Reports, and, where appropriate, forwards such complaints to law enforcement and/or revokes an EV Certificate that is the subject of such a complaint.

2.3 Testpages for Application Software Vendors

TC TrustCenter provides test web pages that allow Application Software Vendors to test their software. For each EV related Root there is a web page with a valid, a revoked, and an expired EV Certificate.

Root	Status	URL
Universal III	valid	testserver.universal-III.trustcenter.de
Universal III	revoked	testserver-revoked.universal-III.trustcenter.de
Universal III	expired	testserver-expired.universal-III.trustcenter.de
Universal I	valid	testserver.universal-I.trustcenter.de
Universal I	revoked	testserver-revoked.universal-I.trustcenter.de
Universal I	expired	testserver-expired.universal-I.trustcenter.de

3 EV Certificates

Each certificate is only as trustworthy as the procedures followed for its issuance. Such procedures are typically defined in guidelines.

The guidelines for the issuance of EV Certificates have been defined by the CA/Browser Forum, in order to achieve an internationally uniform quality of EV Certificates. These guidelines have been published by the CA/Browser Forum in the document „Guidelines for the Issuance and Management of Extended Validation Certificates“ (available at <http://www.cabforum.org/>). The CA/Browser Forum is a voluntary organization of leading certification authorities (CAs) and Relying-Party Application Software Suppliers.

All EV Certificates issued by TC TrustCenter are compliant to this document (TC TrustCenter Certificate Policy Definitions for EV Certificates) and the „Guidelines for the Issuance and Management of Extended Validation Certificates“.

Because the „Guidelines for the Issuance and Management of Extended Validation Certificates“ are intended for international use, some of the steps for verification of the Subscriber's identity and authorization are specified in an abstract manner. These steps must be defined by the issuing CA according to local conditions and local feasibility and without violating the minimal requirements specified in the „Guidelines for the Issuance and Management of Extended Validation Certificates“.

This document, TC TrustCenter's Certificate Policy Definitions for EV Certificates, describes the procedures implemented by TC TrustCenter for the verification of data related to the issuance of EV Certificates and the procedures verifying the Subscriber's identity and authorization to apply for an EV Certificate.

In the case of deviations of this document or TC TrustCenter's CPS from the „Guidelines for the Issuance and Management of Extended Validation Certificates“ the stipulations in the

“Guidelines” shall prevail. This applies e.g. to the retention period for archive; records related to EV Certificates are archived for 7 years.

3.1 Role Requirements

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

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

(2) **Certificate Approver** – The EV Certificate Request must be approved by an authorized Certificate Approver. A Certificate Approver is a natural person who is either Applicant, employed by Applicant, or an authorized agent who has express authority to represent Applicant to

- (i) act as a Certificate Requester and to authorize other employees or third parties to act as a Certificate Requester, and
- (ii) to approve EV Certificate Requests submitted by other Certificate Requesters.

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

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

3.1.1 Verification of Roles

TC TrustCenter verifies name, title, and authority of Contract Signer and Certificate Approver before accepting any EV Certificate request.

3.1.1.1 Name, Title, and Agency

(1) Name and Title

In order to provide reasonable assurance that a person claiming to act in the role Contract Signer or Certificate Approver is in fact the named person designated to act in such role Contract Signer and the Certificate Approver must present the copy of an official ID document to TC Trustcenter.

(2) Agency

TC TrustCenter verifies the agency of the Contract Signer and the Certificate Approver by:

- (A) Contacting Applicant's Human Resources Department by phone or mail (at the phone number or address for Applicant's Place of Business, verified in accordance with these EV-CPD) and obtaining confirmation that the Contract Signer and/or the Certificate Approver, as applicable, is an employee; or
- (B) Obtaining an Independent Confirmation From Applicant, or a Verified Legal Opinion (as described in Section 3.8.1), or a Verified Accountant Letter (as described in Section 3.8.2) verifying that the Contract Signer and/or the Certificate Approver, as applicable,

cable, is either an employee or has otherwise been appointed as an agent of Applicant.

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

3.1.1.2 Authorization

Verification of the Signing Authority of the Contract Signer and the EV Authority of the Certificate Approver, as applicable, are performed through one of the following methods:

(1) **Legal Opinion or 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 Legal Opinion (as described in Section 3.8.1) or by reliance on a Verified Accountant Letter (as described in Section 3.8.2);

(2) **Contract between CA and Applicant**

The EV Authority of the Certificate Approver may be verified by reliance on a contract between TC TrustCenter 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.

(3) **Prior Equivalent Authority**

The signing authority of the Contract Signer, and/or the EV authority of the Certificate Approver, may be verified by relying on a demonstration of Prior Equivalent Authority.

(A) TC TrustCenter assumes a Prior Equivalent Authority of a Contract Signer for confirmation or verification of the signing authority of the Contract Signer only if the Contract Signer has executed a binding contract between TC TrustCenter 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.

(B) TC TrustCenter assumes Prior Equivalent Authority of a Certificate Approver for confirmation or verification of the EV authority of the Certificate Approver only if the Certificate Approver has performed one or more of the following:

- (1) Under contract to TC TrustCenter, has served (or is serving) as an Enterprise RA for the Applicant or
- (2) has participated in the approval of one or more certificates issued by TC TrustCenter, which are currently in use by the Applicant. In this case TC TrustCenter 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.

3.1.1.3 Pre-Authorized Certificate Approver

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

- (1) Has verified the name and title of the Contract Signer and that he/she is an employee or agent of Applicant, and
- (2) Has verified the Signing Authority of such Contract Signer in accordance with one of the procedures in the preceding Subsection 3.1.1.

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

3.2 Obtaining EV Certificates

TC TrustCenter issues EV Certificates to Private Organizations, Government Entities, and other Business Entities.

3.2.1 Documents

Before issuing an EV Certificate the following documents must be presented to TC TrustCenter in compliance with the „Guidelines for the Issuance and Management of Extended Validation Certificates“:

- EV Certificate application
- Subscriber Agreement
- Documents verifying correctness, authenticity, and authorization for application pursuant to these Certificate Policy Definitions and the „Guidelines for the Issuance and Management of Extended Validation Certificates“.

It must be verified

- the Subscriber’s legal existence and identity,
- the Subscriber’s physical existence,
- the Subscriber’s operational existence, and
- the authorization of all persons involved in the application.

Documents presented for validating certificate data must not be older than 13 months. The verification of other data, e.g. telephone numbers, domain names, or the existence of bank accounts, must not be longer than 13 months ago.

a) Private Organization Subjects

TC TrustCenter may issue EV Certificates to Private Organizations that satisfy the requirements below:

- (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;
- (1) Doing business with the Private Organization must be permitted according to TC TrustCenter’s Export-Guidelines. TC TrustCenter’s Export-Guidelines regulate which countries and which organizations are admissible for doing business with, and which countries and organizations must be excluded from doing business with, e.g. due to government denial list or prohibited list (e.g., trade embargo) under the laws of the TC TrustCenter’s jurisdiction.

b) Government Entity Subjects

TC TrustCenter may issue EV Certificates to Government Entities that satisfy the requirements below:

- (1) The legal existence of the Government Entity must be confirmed by a superior government entity or by a supervising government entity.
- (2) Doing business with the Government Entity must be permitted according to TC TrustCenter’s Export-Guidelines. TC TrustCenter’s Export-Guidelines regulate which countries and which organizations are admissible for doing business with, and which countries and organizations must be excluded from doing business with, e.g. due to government denial list or prohibited list (e.g., trade embargo) under the laws of the TC TrustCenter’s jurisdiction.

c) Other Business Entities

Under the term “Other Business Entities” all organizations are subsumed which are neither considered as Private Organizations nor as Government Entities. Examples are partnerships and sole proprietorships.

TC TrustCenter may issue EV Certificates to other Business Entities that satisfy the requirements below:

- (1) The Business Entity must be a legally recognized entity. The formation of the Business Entity must have 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, TC TrustCenter verifies that
 - (i) the Business Entity’s has registered its use of the assumed name with the appropriate government agency for such filings and that
 - (ii) such filing continues to be valid;

- (6) Doing business with the Business Entity must be permitted according to TC TrustCenter's Export-Guidelines. TC TrustCenter's Export-Guidelines regulate which countries and which organizations are admissible for doing business with, and which countries and organizations must be excluded from doing business with, e.g. due to government denial list or prohibited list (e.g., trade embargo) under the laws of the TC TrustCenter's jurisdiction.

d) Non-commercial Organizations (International Organizations)

TC TrustCenter may issue EV Certificates to Non-commercial Entities that do not qualify as entities defined in a), b), or c) above and that satisfy the requirements below:

- (1) The Applicant is an International Organization Entity, created under a charter, treaty, convention or equivalent instrument that was signed by, or on behalf of, more than one country's government.
- (2) The International Organization Entity must not be headquartered in any country where TC TrustCenter is prohibited from doing business;
- (3) Doing business with the Non-commercial Entity must be permitted according to TC TrustCenter's Export-Guidelines. TC TrustCenter's Export-Guidelines regulate which countries and which organizations are admissible for doing business with, and which countries and organizations must be excluded from doing business with, e.g. due to government denial list or prohibited list (e.g., trade embargo) under the laws of the TC TrustCenter's jurisdiction.

Subsidiary organizations or agencies of qualified International Organizations may also qualify for EV Certificates.

3.3 Verification of Individuals

TC TrustCenter validates Individuals associated with Business Entities in a face-to-face setting. TC TrustCenter may rely upon a face-to-face validation of the Principal Individual performed by the Registration Agency, provided that TC TrustCenter has evaluated the validation procedure and concluded that it satisfies the requirements of the EV Guidelines for face-to-face validation procedures.

3.3.1 Face-to-face validation:

The face-to-face validation must be conducted before either an employee of TC TrustCenter, a Latin Notary, a Notary (or equivalent in Applicant's jurisdiction), a Lawyer, or Accountant ("Third-Party Validator"). The Individual has to present the following documentation ("Vetting Documents") directly to the Third- Party Validator:

- (i) A Personal Statement that includes the following information:
 - (1) Full name or names by which a person is, or has been, known (including all other names used);
 - (2) Residential Address at which he/she can be located;
 - (3) Date of birth;
 - (4) An affirmation that all of the information contained in the Certificate Request is true and correct.
- (ii) A current signed government-issued identification document that includes a photo of the Individual and is signed by the Individual such as:
 - (1) A passport;
 - (2) A drivers license;

- (3) A personal identification card;
- (4) A concealed weapons permit;
- (5) A military ID.

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

(1) Acceptable financial institution documents include:

- a. A major credit card, provided that it contains an expiration date and it has not expired.
- b. A debit card from a regulated financial institution, provided that it contains an expiration date and it has not expired.
- c. A mortgage statement from a recognizable lender that is less than six months old.
- d. A bank statement from a regulated financial institution that is less than six months old.

(2) Acceptable non-financial documents include:

- a. Recent original utility bills or certificates from a utility company confirming the arrangement to pay for the services at a fixed address (not a mobile/cellular telephone bill).
- b. A copy of a statement for a payment of a lease provided the statement is dated within the past six months.
- c. A certified copy of a birth certificate.
- d. A local authority tax bill for the current year.
- e. A certified copy of a court order, such as a divorce certificate, annulment papers, or adoption papers.

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

- 1. Attest to the signing of the Personal Statement and the identity of the signer; and
- 2. Identify the original Vetting Documents used to perform the identification. In addition, the Third-Party Validator must attest on a copy of the current signed government-issued photo identification document that it is a full, true, and accurate reproduction of the original.

3.3.2 Cross-checking of Information:

TC TrustCenter must obtain the original signed and attested Personal Statement together with the attested copy of the current signed government-issued photo identification document. TC TrustCenter reviews the documentation to determine that the information is consistent, matches the information in the application and identifies the Individual.

3.3.3 Verification of Third-party validator:

TC TrustCenter independently verifies that the Third-Party Validator is a legally-qualified Latin Notary or Notary (or legal equivalent in Applicant's jurisdiction), Lawyer, or Accountant in the jurisdiction of the Individual's residency, and that the Third-Party Validator actually did perform the services and did attest to the signature of the Individual.

3.4 Verification of Signature on Subscriber Agreement and EV Certificate Requests

Both the Subscriber Agreement and each EV Certificate Request must be signed. The Subscriber Agreement must be signed by an authorized Contract Signer. The EV Certificate Request must be signed by the Certificate Requester submitting the document.

If the Certificate requester is not also an authorized Certificate Approver, then an authorized Certificate Approver must independently approve the EV Certificate Request.

In all cases, the signature must be a legally valid and enforceable seal or handwritten signature (for a paper Subscriber Agreement and/or EV Certificate Request), or a legally valid and enforceable electronic signature (for an electronic Subscriber Agreement and/or EV Certificate Request), that binds Applicant to the terms of each respective document.

(a) Verification Requirements

(1) Signature

TC TrustCenter authenticates the signature of the Contract Signer on the Subscriber Agreement and the signature of the Certificate Requester on each EV Certificate Request in a manner that makes it reasonably certain that the person named as the signer in the applicable document is, in fact, the person who signed the document on behalf of Applicant.

(2) Approval Alternative

In cases where an EV Certificate Request is signed and submitted by a Certificate Requester who does not also function as a Certificate Approver, approval and adoption of the EV Certificate Request by a Certificate Approver in accordance with the requirements of Section 3.5 can substitute for authentication of the signature of the Certificate Requester on such EV Certificate Request.

(b) Acceptable Methods of Signature Verification

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

- (1) A phone call to Applicant's or Agent's phone number, as verified in accordance with these EV-CPD, 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 EV-CPD, 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 TC TrustCenter independently verifies that such notary is a legally qualified notary in the jurisdiction of the Certificate Requester or Contract Signer;

3.5 Verification of Approval of EV Certificate Request

If an EV Certificate Request is submitted by a Certificate Requester, TC TrustCenter verifies that an authorized Certificate Approver reviewed and approved the EV Certificate Request.

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

- (1) Contacting the Certificate Approver by phone or mail at a verified phone number or address for Applicant and obtaining oral or written confirmation that the Certificate Approver has reviewed and approved the EV Certificate Request;
- (2) Notifying the Certificate Approver that one or more new EV Certificate Requests are available for review and approval at a designated access-controlled and secure website, followed by a login by, and an indication of approval from, the Certificate Approver in the manner required by the website; or
- (3) Verifying the signature of the Certificate Requester on the EV Certificate Request in accordance with Section 3.4 of these EV-CPD.

3.6 Verification of Organizations

Before issuing an EV Certificate, TC TrustCenter must ensure that all Subject organization information in the EV Certificate conforms to the requirements of, and has been verified in accordance with, this EV-CPD and matches the information confirmed and documented by TC TrustCenter pursuant to its verification processes. Such verification processes accomplish the following:

- (1) Verify Applicant's existence and identity, including;
 - (a) Verify Applicant's legal existence and identity (as more fully set forth in Section 3.6.1 below),
 - (b) Verify Applicant's physical existence (business presence at a physical address), and
 - (c) Verify Applicant's operational existence (business activity).
- (2) Verify Applicant is a registered holder, or has exclusive control, of the domain name to be included in the EV Certificate;
- (3) Verify Applicant's authorization for the EV Certificate, including;
 - (a) Verify the name, title, and authority of the Contract Signer, Certificate Approver, and Certificate Requester;
 - (b) Verify that Contract Signer signed the Subscriber Agreement; and
 - (c) Verify that a Certificate Approver has signed or otherwise approved the EV Certificate Request

3.6.1 Verification of Applicant's Legal Existence and Identity

3.6.1.1 Private Organizations

a. Legal Existence

Verify that Applicant is a legally recognized entity, in existence and validly formed (e.g., incorporated) with the Incorporating or Registration Agency in Applicant's Jurisdiction of Incorporation or Registration, and not designated on the

records of the Incorporating or Registration Agency by labels such as “inactive”, “invalid”, “not current”, or the equivalent.

b. Organization Name

Verify that Applicant’s formal legal name as recorded with the Incorporating or Registration Agency in Applicant’s Jurisdiction of Incorporation or Registration matches Applicant’s name in the EV Certificate Request.

c. Registration Number

Obtain the specific Registration Number assigned to Applicant by the Incorporating or Registration Agency in Applicant’s Jurisdiction of Incorporation or Registration. Where the Incorporating or Registration Agency does not assign a Registration Number, TC TrustCenter shall obtain Applicant’s date of Incorporation or Registration.

d. Registered Agent

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

3.6.1.1.1 Method of Verification

TC TrustCenter verifies all items listed in subsection 3.6.1.1 above with data obtained directly from the Incorporating or Registration Agency in Applicant’s Jurisdiction of Incorporation or Registration. Such verification may be through use of a Qualified Government Information Source operated by, or on behalf of, the Incorporating or Registration Agency, or by direct contact with the Incorporating or Registration Agency in person or via mail, e-mail, web address, or telephone, using an address or phone number obtained from a Qualified Independent Information Source.

3.6.1.2 Government Entities

a. Legal Existence

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

b. Entity Name

Verify that Applicant’s formal legal name matches Applicant’s name in the EV Certificate Request.

c. Registration Number

Obtain Applicant’s date of incorporation, registration, or formation, or the identifier for the legislative act that created the Government Entity. In circumstances where this information is not available, TC TrustCenter enters appropriate language to indicate that the Subject is a Government Entity.

3.6.1.2.1 Method of Verification

TC TrustCenter verifies all items listed in subsection 3.6.1.2 above directly with data from one of the following:

- 1) a QGIS in the political subdivision in which such Government Entity operates;

- 2) a superior governing Government Entity in the same political subdivision as Applicant (e.g. a Secretary of State may verify the legal existence of a specific State Department), or
- 3) from a judge that is an active member of the federal, state or local judiciary within that political subdivision, or
- 4) an attorney representing the Government Entity.

Any communication from a judge will be verified in the same manner as is used for verifying factual assertions that are asserted by an Attorney as set forth in Section 3.8.1 (a) below.

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

3.6.1.3 Business Entities

a. Legal Existence

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

b. Organization Name

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

c. Registration Number

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

d. Principal Individual

Verify the identity of the identified Principal Individual.

3.6.1.3.1 Method of Verification

TC TrustCenter verifies all items listed in subsection 3.6.1.3 above directly with data from the Registration Agency in Applicant's Jurisdiction of Registration. Such verification may be through use of a Qualified Government Information Source, a Qualified Governmental Tax Information Source, or by direct contact with the Registration Agency in person or via mail, e-mail, web address, or telephone, using an address or phone number obtained from a Qualified Independent Information Source. In addition, TC TrustCenter validates a Principal Individual associated with the Business Entity pursuant to the requirements in subsection 0 above.

3.6.1.4 Non-Commercial Entities (International Organization Entities)

a. Legal Existence

Verify that Applicant is a legally recognized International Organization Entity.

b. Entity Name

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

c. Registration Number

Obtain Applicant's date of formation, or the identifier for the legislative act that created the International Organization Entity. In circumstances where this information is not available, TC TrustCenter enters appropriate language to indicate that the Subject is an International Organization Entity.

3.6.1.4.1 Method of Verification

TC TrustCenter verifies all items listed in subsection 3.6.1.4 either:

- (a) With reference to the constituent document under which the International Organization was formed; or
- (b) Directly with a signatory country's government in which TC TrustCenter is permitted to do business. Such verification may be obtained from an appropriate government agency or from the laws of that country, or by verifying that the country's government has a mission to represent it at the International Organization; or
- (c) Directly against any current list of qualified entities that the CAB Forum may maintain at www.cabforum.org.
- (d) In cases where the International Organization applying for the EV certificate is an organ or agency - including a non-governmental organization (NGO) of a verified International Organization, then TC TrustCenter may verify the International Organization applicant directly with the verified umbrella International Organization of which the applicant is an organ or agency.

3.6.2 Verification of the Applicant's Physical Existence**3.6.2.1 Address of Applicant's Place of Business****3.6.2.1.1 Verification Requirements**

To verify Applicant's physical existence and business presence, TC TrustCenter 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), and is the address of Applicant's Place of Business.

3.6.2.1.2 Methods of Verification

To verify the address of Applicant's Place of Business:

- (A) For Applicants whose Place of Business is in the same country as Applicant's Jurisdiction of Incorporation or Registration:
 - (1) For Applicants 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, TC TrustCenter confirms that Applicant's address as listed in the EV Certificate Request is a valid business address for Applicant or a Parent/Subsidiary Company by reference to such Qualified Independent Information Sources or a Qualified Governmental Tax Information Source, and relies 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, TC TrustCenter confirms that the address provided by Applicant in the EV Certificate Request is in fact Applicant's or a Parent/Subsidiary Company's business address, by obtaining documentation of a site visit to the business address. TC TrustCenter uses only reliable individuals or firms to perform such a site visit.

The documentation of the site visit must:

- (a) Verify that Applicant's business is located at the exact address stated in the EV Certificate Request (e.g., via permanent signage, employee confirmation, etc.);
 - (b) Identify the type of facility (e.g., office in a commercial building, private residence, storefront, etc.) and whether it appears to be a permanent business location;
 - (c) Indicate whether there is a permanent sign (that cannot be moved) that identifies Applicant;
 - (d) Indicate whether there is evidence that Applicant is conducting ongoing business activities at the site (e.g., that it is not just a mail drop, P.O. box, etc.); and
 - (e) Include one or more photos of
 - (i) the exterior of the site (showing signage indicating Applicant's name, if present, and showing the street address if possible), and
 - (ii) the interior reception area or workspace
- (3) For all Applicants, TC TrustCenter may alternatively rely on a Verified Legal Opinion or a Verified Accountant Letter that indicates the address of Applicant's or a Parent/Subsidiary Company's Place of Business and that business operations are conducted there.
- (4) For Government Entity Applicants, TC TrustCenter may rely on the address contained in the records of the QGIS in Applicant's Jurisdiction.

- (B) For Applicants whose Place of Business is not in the same country as Applicant's Jurisdiction of Incorporation or Registration, the Applicant must submit to TC TrustCenter a Verified Legal Opinion that indicates the address of Applicant's Place of Business and that business operations are conducted there.

3.6.2.2 Telephone Number for Applicant's Place of Business

3.6.2.2.1 Verification Requirements

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

3.6.2.2.2 Methods of Verification

To verify Applicant's telephone number, TC TrustCenter performs A and one of B, C, or D as listed below:

- (A) Confirm Applicant's telephone number by calling it and obtaining an affirmative response sufficient to enable a reasonable person to conclude that Applicant is reachable by telephone at the number dialed; and
- (B) Confirm that the telephone number provided by Applicant is listed as Applicant's or Parent/Subsidiary Company's telephone number for the verified address of its Place of Business in records provided by the applicable phone company, or, alternatively, in either at least one (1) Qualified Independent Information Source or a Qualified Governmental Tax Information Source; *or*
- (C) During a site visit, the person who is conducting the site visit **MUST** confirm Applicant's or Parent/Subsidiary Company's main telephone number by calling it and obtaining an affirmative response sufficient to enable a reasonable person to conclude that Applicant is reachable by telephone at the number dialed. TC TrustCenter will also confirm that Applicant's main telephone number is not a mobile phone; *or*
- (D) Rely on a Verified Legal Opinion or a Verified Accountant Letter to the effect that Applicant's telephone number, as provided, is a main phone number for Applicant's Place of Business.
- (E) For Government Entity Applicants, TC TrustCenter **MAY** rely on the telephone number contained in the records of the QGIS in Applicant's Jurisdiction.

3.6.3 Verification of the Applicant's Operational Existence

3.6.3.1 Verification Requirements

If Applicant has been in existence for less than three years, as indicated by the records of the Incorporating Agency or Registration Agency, and is not listed in either the current version of one Qualified Independent Information Source or a Qualified Governmental Tax Information Source, TC TrustCenter verifies that Applicant has the ability to engage in business.

3.6.3.2 Methods of Verification

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

- (1) Verify that Applicant has an active current Demand Deposit Account with a Regulated Financial Institution. TC TrustCenter must receive authenticated documentation directly from a Regulated Financial Institution verifying that Applicant has an active current Demand Deposit Account with the institution.
- (2) Rely on a Verified Legal Opinion or a Verified Accountant Letter to the effect that Applicant has an active current Demand Deposit Account with a Regulated Financial Institution.

3.7 Verification of Domain Name

TC TrustCenter verifies that the Applicant is a registered holder of the domain name to be included in the EV Certificate, or has exclusive control of the domain name.

3.7.1 Verification Requirements

To verify Applicant's registration, or exclusive control, of the domain name(s) to be listed in the EV Certificate, TC TrustCenter 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) Applicant is either the registered holder of the domain name, or Applicant has been granted the exclusive right to use the domain name by the registered holder of the domain name;
- (3) Applicant is aware of its registration or exclusive control of the domain name;

3.7.2 Method of Verification

TC TrustCenter performs a WHOIS inquiry on the internet for the domain name supplied by Applicant.

- (1) If the Applicant is the registered holder of the domain name, the WHOIS response will indicate this fact.
- (2) In cases where Applicant is not the registered holder of the domain name, TC TrustCenter verifies Applicant's exclusive right to use the domain name(s) as follows:
 - (a) In cases where the registered domain holder can be contacted using information obtained from WHOIS, or through the domain registrar, TC TrustCenter must obtain positive confirmation from the registered domain holder by paper mail, e-mail, telephone, or facsimile that Applicant has been granted the exclusive right to use the requested Fully Qualified Domain Name (FQDN).

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

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

In addition, TC TrustCenter verifies Applicant's exclusive right to use the domain name using one of the following methods:

- (1) The Applicant must present 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) The Applicant must present a representation from the Contract Signer, or the Certificate Approver, if expressly so authorized in a mutually-agreed-upon contract.

- (b) In cases where the registered domain holder cannot be contacted, the Applicant must present:
 - (1) A Verified Legal Opinion to the effect that Applicant has the exclusive right to use the specified domain name in identifying itself on the Internet, and
 - (2) A representation from the Contract Signer, or the Certificate Approver, if expressly so authorized in a mutually-agreed-upon contract, coupled with a practical demonstration by Applicant establishing that it controls the domain name by making an agreed-upon change in information found online on a web page identified by a uniform resource identifier containing Applicant's FQDN;
- (3) In order to verify that the Applicant is aware that it has exclusive control of the domain name, the Applicant must present:
 - (a) A Verified Legal Opinion to the effect that Applicant is aware that it has exclusive control of the domain name; or
 - (b) A confirmation from the Contract Signer or Certificate Approver verifying that Applicant is aware that it has exclusive control of the domain name.
- (4) Mixed Character Set Domain Names
EV Certificates may include domain names containing mixed character sets only in compliance with the rules set forth by the domain registrar.

If a domain name with mixed character set is in compliance with the domain registrar's rules, TC TrustCenter visually compares this domain name with known high risk domains. If a similarity is found then TC TrustCenter flags the EV Certificate Request as High Risk and performs appropriate additional authentication and verification to be certain beyond reasonable doubt that the Applicant and the target in question are the same organization.

If a domain name with mixed character set is in conflict with the domain registrar's rules, TC TrustCenter rejects the application and informs the Applicant about this fact and the reason for the rejection.

3.8 Verification of Information Sources

3.8.1 Verified Legal Opinion

A Verified Legal Opinion must meet the following requirements:

- (a) The author of a Verified Legal Opinion must be an independent Legal Practitioner retained by and representing Applicant (or an in-house legal practitioner employed by Applicant) (Legal Practitioner) who is either:
 - i. A lawyer (or solicitor, barrister, advocate, or equivalent) licensed to practice law in the country of Applicant's Jurisdiction of Incorporation or Registration or any jurisdiction where Applicant maintains an office or physical facility; or
 - ii. A notary that is a member of the International Union of Latin Notaries, and is licensed to practice in the country of Applicant's Jurisdiction of Incorporation or Registration or any jurisdiction where Applicant maintains an office or physical facility (and that such jurisdiction recognizes the role of the Latin Notary).

TC TrustCenter verifies this professional status by directly contacting the authority responsible for registering or licensing such Legal Practitioner(s) in the applicable jurisdiction.

- (b) The text of the legal opinion must make it clear that the Legal Practitioner is acting on behalf of Applicant and that the conclusions of the legal opinion are based on the Legal Practitioner's stated familiarity with the relevant facts and the exercise of the practitioner's professional judgment and expertise. The legal opinion MAY also include disclaimers and other limitations customary in the Legal Practitioner's jurisdiction, provided that the scope of the disclaimed responsibility is not so great as to eliminate any substantial risk (financial, professional, and/or reputational) to the Legal Practitioner, should the legal opinion prove to be erroneous.
- (c) TC TrustCenter confirms the authenticity of the legal opinion by making a telephone call or sending 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 Practitioners, and obtaining 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, TC TrustCenter may use the number listed for the Legal Practitioner in records provided by the applicable phone company, a QGIS, or a QIIS.

If the legal opinion is digitally signed and this signature confirms the authenticity of the document and the identity of the signer, as verified by TC TrustCenter in Section 3.8.1(a), no further verification of authenticity is required.

3.8.2 Verified Accountant Letter

A Verified Accountant Letter must meet the following requirements:

- (a) The author of a Verified Legal Opinion must be 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.

TC TrustCenter verifies this professional status by directly contacting the authority responsible for registering or licensing such Accounting Practitioner(s) in the applicable jurisdiction.

- (b) The text of the accountant letter must make it clear that the Accounting Practitioner is acting on behalf of Applicant and that the information in the accountant letter is based on the Accounting Practitioner's stated familiarity with the relevant facts and the exercise of the practitioner's professional judgment and expertise. The accountant letter may also include disclaimers and other limitations customary in the Accounting Practitioner's jurisdiction, provided that the scope of the disclaimed responsibility is not so great as to eliminate any substantial risk (financial, professional, and/or reputational) to the Accounting Practitioner, should the accountant letter prove to be erroneous.
- (c) TC TrustCenter confirms the authenticity of the accountant's opinion by making a telephone call or sending 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 Account-

ing Practitioner listed with the authority responsible for registering or licensing such Accounting Practitioners, and obtaining 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, TC TrustCenter may use the number listed for the Accountant in records provided by the applicable phone company, a QGIS, or a QIIS.

If the accountant letter is digitally signed and this signature confirms the authenticity of the document and the identity of the signer, as verified by TC TrustCenter in Section 3.8.2(a), no further verification of authenticity is required.

3.8.3 Face-to-face Validation by Third Party Validator

Face-to-face vetting documents submitted to TC TrustCenter by a Third Party Validator are accepted by TC TrustCenter only if the following requirements are met:

- (a) TC TrustCenter has independently verified that the Third-Party Validator is a legally-qualified Latin Notary or Notary (or legal equivalent in Applicant's jurisdiction), Lawyer, or Accountant by directly contacting the authority responsible for registering or licensing such Third-Party Validators in the applicable jurisdiction
- (b) In order to verify the document chain of custody the Third-Party Validator must submit a statement to TC TrustCenter which attests that they obtained the Vetting Documents submitted to TC TrustCenter during a face-to-face meeting with the individual being validated.
- (c) If the Third-Party Validator is not a Latin Notary, then TC Trustcenter confirms the authenticity of the vetting documents received from the Third-Party Validator by making a telephone call to the Third-Party Validator and obtaining confirmation from them or their assistant that they performed the face-to-face validation.

TC TrustCenter may rely upon self-reported information obtained from the Third-Party Validator for the sole purpose of performing this verification process.

If an attestation is digitally signed and this signature confirms the authenticity of the document(s) and the identity of the signer, as verified by TC TrustCenter in Section 3.8.3, no further verification of authenticity is required.

3.8.4 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 TC TrustCenter 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 TC TrustCenter in a manner that authenticates and verifies the source of the confirmation; and
- (iii) Binding on Applicant.

TC TrustCenter accepts an Independent Confirmation from Applicant provided that it has been obtained via the following procedure:

- (a) TC TrustCenter sends a Confirmation Request via an appropriate out-of-band communication requesting verification or confirmation of the particular fact at issue as follows:

TC TrustCenter directs the Confirmation Request 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) TC TrustCenter directs the Confirmation Request to the Confirming Person in a manner reasonably likely to reach such person using one of the following ways:
- (i) By paper mail addressed to the Confirming Person at:
 - (a) The address of Applicant's Place of Business as verified by TC TrustCenter in accordance with these EV-CPD; 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 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 Ac-

countant Letter. The cover page must be clearly addressed to the Confirming Person.

- (c) The response to the Confirmation Request may be provided to the TC TrustCenter by telephone, by email, or by paper mail, so long as TC TrustCenter can reliably verify that it was provided by a Confirming Person in response to the Confirmation Request.

3.8.5 Qualified Independent Information Sources (QIIS)

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

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.

In order to enforce independence of information services, TC TrustCenter does not use its own databases as QIIS, i.e. databases do NOT qualify as a QIIS if TC TrustCenter or its owners or affiliated companies maintain a controlling interest, or if any Registration Authorities or subcontractors to whom TC TrustCenter has outsourced any portion of the vetting process (or their owners or affiliated companies) maintain any ownership or beneficial interest.

3.8.6 Qualified Government Information Source (QGIS)

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

3.8.7 Qualified Government Tax Information Source (QGTIS)

A Qualified Governmental Tax Information System is a QGIS that specifically contains tax information relating to Private Organizations, Business Entities or Individuals (e.g. the I.R.S. in the United States).

3.9 Other Verification Requirements

3.9.1 High Risk Status

TC TrustCenter MUST seek to identify Applicants likely to be at a high risk of being targeted for fraudulent attacks (“High Risk Applicants”), and conduct such additional verification activity and take such additional precautions as are reasonably necessary to ensure that such Applicants are properly verified under these Guidelines.

TC TrustCenter identifies High Risk Applicants by checking appropriate lists of organization names that are most commonly targeted in phishing and other fraudulent schemes and automatically flags EV Certificate Requests from Applicants named on these lists for further scrutiny before issuing a certificate.

Examples of such lists are:

- Lists of phishing targets published by the Anti-Phishing Work Group (APWG); and
- Internal databases maintained by TC TrustCenter that include previously revoked EV Certificates and previously rejected EV Certificate Requests due to suspected phishing or other fraudulent usage.

If an Applicant is flagged as a High Risk Applicant, TC TrustCenter performs reasonably appropriate additional authentication and verification to be certain beyond reasonable doubt that Applicant and the target in question are the same organization.

3.9.2 Denied Lists and Other Legal Black Lists

TC TrustCenter does not issue EV Certificates if Applicant, the Contract Signer, or the Certificate Approver is identified on any government denied list, list of prohibited persons, or other list that prohibits doing business with such organization or person under U.S laws or German laws.

TC TrustCenter verifies whether the Applicant or one of the persons involved in the application process (Contract Signer, Certificate Approver, Certificate Requester) are identified on a list of denied persons and organizations. This list is based on a UN Resolution against international terrorism in combination with Council Regulation (EC) No 881/2002 and No 2580/2001 of the Council of the European Union. The list prohibits doing business or otherwise providing resources to persons named on the list.

In contrast with national sanctions these regulations are „tied“ to persons – the embargo “follows” the persons, regardless of their current residence.

In addition TC TrustCenter verifies whether the applying organization is located in a country where TC TrustCenter’s Export Guidelines prohibit doing business.

TC TrustCenter also uses the following lists published by the Bureau of Industry and Security of the U.S. Department of Commerce:

- BIS Denied Persons List - <http://www.bis.doc.gov/dpl/thedeniallist.asp> und
- BIS Denied Entities List - <http://www.bis.doc.gov/Entities/Default.htm>.

If either the Applicant, the Contract Signer, or Certificate Approver or if the Applicant’s Jurisdiction of Incorporation or Registration or Place of Business is on any such list, TC TrustCenter rejects the EV Certificate Request and does not issue an EV Certificate.

3.10 Certificate Renewal Verification Requirements

An EV Certificate can be renewed only if TC TrustCenter has performed all authentication and verification tasks required by this EV-CPD to ensure that the renewal request is properly authorized by Applicant and that the information in the EV Certificate is still accurate and valid.

4 Revocation of EV Certificates

TC TrustCenter maintains a 24x7 Revocation Service where the revocation of an EV Certificate can be requested at any time.

TC TrustCenter revokes an EV Certificate it has issued if one (or more) of the following applies:

- 1) The Subscriber requests revocation of its EV Certificate;
- 2) The Subscriber indicates that the original EV Certificate Request was not authorized and does not retroactively grant authorization;
- 3) TC TrustCenter obtains reasonable evidence that the Subscriber's Private Key (corresponding to the Public Key in the EV Certificate) has been compromised or is suspected of compromise (e.g. Debian known weak keys), or that the EV Certificate has otherwise been misused;
- 4) TC TrustCenter receives notice or otherwise becomes aware that a Subscriber has violated one or more of its material obligations under the Subscriber Agreement;
- 5) TC TrustCenter receives notice or otherwise becomes aware that a court or arbitrator has revoked a Subscriber's right to use the Domain Name listed in the EV Certificate, or that the Subscriber has failed to renew its rights to the Domain Name;
- 6) TC TrustCenter receives notice or otherwise becomes aware of a material change in the information contained in the EV Certificate;
- 7) A determination, in the TC TrustCenter's sole discretion, reveals that the EV Certificate was not issued in accordance with the terms and conditions of these Guidelines or the „Guidelines for the Issuance and Management of Extended Validation Certificates“ of the CA/Browser Forum;
- 8) TC TrustCenter determines that any of the information appearing in the EV Certificate is not accurate;
- 9) TC TrustCenter ceases operations for any reason and has not arranged for another EV CA to provide revocation support for the EV Certificate;
- 10) TC TrustCenter's right to issue EV Certificates under these Guidelines expires or is revoked or terminated, unless the CA makes arrangements to continue maintaining the CRL/OCSP Repository.
- 11) The Private Key of TC TrustCenter's Root Certificate used for issuing that EV Certificate is suspected to have been compromised;
- 12) TC TrustCenter 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 TC TrustCenter's jurisdiction of operation;
- 13) Cryptographic algorithms or parameters become insecure due to technological progress or new developments in cryptology and if the certificates are based on those algorithms and parameters, such that EV Certificates could be forged.

- 14) Additional reasons for revocation apply, which have been published in these CPS for EV Certificates.

4.1 Revocation of EV Code Signing Certificates Signing Malicious Code

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

If TC TrustCenter becomes aware (by whatever means) that a Signing Authority using an EV Code Signing Certificate issued by TC TrustCenter has signed code that contains malicious software or a serious vulnerability, then TC TrustCenter immediately informs the Signing Authority and begins an investigation. If this investigation reveals that malicious code has been signed, then TC TrustCenter revokes the affected EV Code Signing Certificate.

5 Naming conventions

TC TrustCenter issues EV Certificates in accordance with the X.509 standard. X.509 certificates are, among other things, used by Web servers and Web browsers to ensure secure Internet communication or to enable an authentication of the web server. X.509 certificates can also be utilized for code-signing.

This section provides guidelines on entering the appropriate information in the data fields that make up the certificates.

5.1 Character Set and Rules for Conversion

The X.509 compliant EV Certificates contain in the designated fields the Distinguished Names of the issuer and of the certificate holder. The following character set is supported:

Upper-case characters	A .. Z
Lower-case characters	a .. z
Digits	0 .. 9
Apostrophe	'
Left parenthesis	(
Right parenthesis)
Plus	+
Comma	,

Hyphen	-
Dot	.
Slash	/
Colon	:
Equal	=
Question mark	?
Space	

This character set contains a limited number of characters. However, TC TrustCenter's certification policies require data in certificates to be spelled exactly as they are spelled in the relevant ID document or document proving the existence of an organization. Consequently, there must exist rules for the conversion of "non-presentable" characters.

TC TrustCenter recommends adherence to the following conversion rules. Otherwise the proper functioning of the certificates in connection with other components can not be assured. For example it can not be excluded that some components in a PKI, e.g. older browsers, are not capable of interpreting umlauts correctly.

5.1.1 Conversion of Characters

- Umlauts (Ä, Ö, Ü, ä, ö, ü) are replaced by the respective non-diacritical strings (Ae, Oe, Ue, ae, oe, ue), thereby respecting capitalization and use of lower-case characters.

Examples:

Original	Converted
Müller	Mueller
Überstorf	Ueberstorf

- Characters and symbols not being part of the supported character set must be assigned to corresponding characters.

Beispiele:

Original	Converted
René	Rene
François	Francois

- Special characters not contained in the supported character set should either be spelled out or be replaced by corresponding equivalent characters.

Examples:

Original	Converted
Meier & Meier Ltd.	Meier and Meier Ltd.
Meier & Meier Ltd.	Meier a. Meier Ltd.
Meier & Meier Ltd.	Meier + Meier Ltd.

6 EV Certificate Content

EV Certificates must include the following information about the Subject Organization:

(1) Organization name:

Certificate Field: subject:organizationName

Required/Optional: Required

Contents: 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 TC TrustCenter as provided herein. TC TrustCenter may abbreviate the organization prefixes or suffixes in the Organization name, e.g., if the QGIS shows "<Company Name> Incorporated" TC TrustCenter may include "<Company Name>, Inc." TC TrustCenter will always use common abbreviations that are generally accepted in the Jurisdiction of Incorporation or Registration.

In addition, an assumed name, "trading as," or "doing-business-as" 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, trading as, or doing-business-as name exceeds 64 characters, as defined by RFC 3280, TC TrustCenter will use only the full legal Organization name in the certificate.

If the Organization name by itself exceeds 64 characters, TC TrustCenter abbreviates 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, provided that a Relying Party will not be misled into thinking they are dealing with a different Organization. In cases where this is not possible, TC TrustCenter will not issue the EV certificate.

(2) Domain name:

Certificate Field: subject:commonName or SubjectAlternativeName:dNSName

Required/Optional: Required

Contents: This field contains one or more host domain name(s) owned or controlled by the Subject and to be associated with Subject's publicly accessible server. Such server may be owned and operated by the Subject or another entity (e.g., a hosting service). Wildcard certificates are not allowed for EV certificates.

(3) Business Category:

Certificate Field: subject:businessCategory (OID 2.5.4.15)

Required/Optional: Required

Contents: This field contains information about the qualification of the Applicant for an EV certificate. It contains one of the following strings in UTF-8 English:

- 'Private Organization' if Applicant is a Private Organization,
- 'Government Entity' if Applicant is a Government Entity,
- 'Business Entity' if Applicant is a Business Entity, or
- 'Non-Commercial Entity' if Applicant is a Non Commercial Entity

(4) Jurisdiction of Incorporation or Registration:

Certificate Fields:

Locality (if required):

subject:jurisdictionOfIncorporationLocalityName

State or province (if required):

subject:jurisdictionOfIncorporationStateOrProvinceName

Country:

subject:jurisdictionOfIncorporationCountryName

Required/Optional: Required

Contents: These fields contain information only to the level of the Incorporating Agency or Registration Authority – e.g., the Jurisdiction of Incorporation for an Incorporating Agency or Jurisdiction of Registration for a Registering Authority at the country level would include country information but would not include state or province or city or town information; the Jurisdiction of Incorporation for an Incorporating Agency or Jurisdiction of Registration for a Registering Authority at the state or province level would include both country and state or province information, but would not include city or town information; and so forth.

Country information is specified using the applicable ISO country code. State or province information, and city or town information (where applicable) for the Subject's Jurisdiction of Incorporation or Registration is specified using the full name of the applicable jurisdiction.

(5) Registration Number:

Certificate Field: Subject:serialNumber

Required/Optional: Required

Contents: For Private Organizations, this field contains the unique registration number assigned to the Subject by the Incorporating or Registration Agency in its Jurisdiction of Incorporation or by the Registration Agency in its Jurisdiction of Registration, as appropriate.

For other Business Entities, this field contains the registration number that was received by the Business Entity upon government registration.

If the Jurisdiction of Incorporation or Registration or the Incorporating or Registration Agency does not provide a Registration Number, then this field contains the date of Incorporation or Registration instead of a registration number.

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

City or town subject:localityName

State or province (if any) subject:stateOrProvinceName

Country subject:countryName

Postal code (optional) subject:postalCode

Required/Optional: City, state, and country – Required;

Street and postal code – Optional

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