TC TrustCenter
Certificate Policy Definitions for
EV Certificates

Version June 28th, 2010

1 Introduction

This document describes TC TrustCenter's Certificate Policy Definitions for issuing "Extended Validation" Certificates (EV Certificates). EV Certificates are issued only after a very thorough examination of the applicant's data and authorization. The criteria for the issuance of EV Certificates are published by the CA/Browser Forum and specified in the "Guidelines for the Issuance and Management of Extended Validation Certificates" (http://www.cabforum.org/EV_Certificate_Guidelines.pdf). The CA/Browser Forum is a voluntary organization of leading certification authorities (CAs) and Relying-Party Application Software Suppliers.

The term "Extended Validation" expresses that EV Certificates build on existing certificate formats (e.g. SSL), but provide an additional layer of protection in a strictly defined issuance process created to ensure that the certificate holder is who they claim to be.

The primary purpose of EV Certificates is to allow visitors of a web site to securely and reliably identify the web site visited and thus to increase the trust in a secure connection to the web site using an EV Certificate e.g. by highlighting the browser's address bar .

Especially phishing attempts with encrypted (and thereby on the first glance secure) websites are easier to discover if EV Certificates are used. Hence, the typical use of EV Certificates consists of securing web applications via HTTPS and thus providing enhanced security for users, e.g. for online banking.

Another type of EV Certificates is EV Code Signing Certificates. Code Signing Certificates are used to verify the identity of the Code Signing Certificate's holder as well as to verify the integrity of a piece of code. A Code Signing Certificate is not assigned to a dedicated piece of software or other code; an EV Code Signing Certificates identifies the certificate holder, who is then able to sign code with his/her name.

A user who downloads signed code from the internet is then able to securely identify the provider or producer of the code (using the certificate data) as well as to detect modifications to the code (modifications invalidate the signature). The trustworthiness of software distributors can be increased and the dissemination of malicious software can be reduced.

Moreover, the holder of a Code Signing Certificate can use this certificate to prove the origin and the legitimacy of code. This can be relevant for copyright affairs.

From a technical point of view there is no distinction between EV Certificates and other certificates. The differences consist in the issuing CA's practices for identification and authentication of the certificate holder.

This document, TC TrustCenter's Certificate Policy Definitions for EV Certificates, describes the practices and processes used by TC TrustCenter as a certification service provider when identifying applicants for EV Certificates and when issuing such certificates. TC TrustCenter strictly follows the guidelines specified in the "Guidelines for the Issuance and Management of Extended Validation Certificates".

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

Adjustment due to market necessities: Due to constantly changing market needs it is inevitable to adjust the services of a certification authority to the concrete needs of customers. The Certificate Policy Definitions are therefore adjusted regularly.

German edition prevails: Some documents and the website are available both in the German and the English edition. In cases of doubt, the German edition shall prevail.

Errors and omissions excepted: Errors on statements made in this document are expressly excepted, especially with regard to technical descriptions or procedures explained herein.

2 Important Notes

When issuing an EV Certificate TC TrustCenter confirms the following:

1. 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. Authorisation 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 data: 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 organization named in the EV Certificate has entered into a legally valid and enforceable Subscriber Agreement with TC TrustCenter that satisfies the requirements of this "Certificate Policy Definitions" and the "Guidelines for the Issuance and Management 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 ist business dealings, or
4. that it is „safe" to do business with the Subject named in the certificate.

Issuance of EV 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 certificate. A later modification of the Certificate Policy Definitions has no influence on already issued certificates.

No verification of creditworthiness: TC TrustCenter confirms the identity of a certificate applicant as described in this document according to the "Guidelines for the Issuance and Management of Extended Validation Certificates". This does not include verification of liquidity, creditworthiness or anything of that nature. A certificate provides a certain level of assur-

ance that the certificate belongs to the entity named therein (in the case of an EV SSL Certificate a webserver, in the case of an EV Code Signing Certificate a code developer) is who it claims to be. It gives no indication whatsoever about the trustworthiness of the entity itself.

No verification of harmlessness of software: TC TrustCenter issues, among others, special certificates for organizations and natural persons that can be used to sign programming code. It has to be taken into account that TC TrustCenter does not certify the programming code itself, its harmlessness, its algorithmical correctness, or its applicability. Certificates issued in this context are intended to enable the user to detect manipulations of the software distributed by the manufacturer. Next to this, the origin of the software can be deduced by such certificates.

No assurance of up-to-date certificate data: TC TrustCenter verifies the information contained in a certificate request only within the scope and 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. When renewing a certificate, the data contained therein will not be verified again. 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 certificates under different certificate policies, which describe the level of trust that may be placed in their authenticity. Any participant of the certification service must decide for himself whether a given certificate policy, which is represented by a certificate class as described in this document, meets the security needs for the application in question.

Participant's obligation to inform himself: 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, public key algorithms, and the authentication of SSL certificates.

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.

2.1 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.

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 Test for 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

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/EV_Certificate_Guidelines.pdf). 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 Obtaining EV Certificates

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

3.1.1 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 that 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.

3.1.2 Roles

The following roles in the applicant's organization are involved in the EV Certificate issuing process:

1. Certificate Requester

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

2. Certificate Approver

   The EV Certificate request must be approved by an authorized Certificate Approver. A Certificate Approver is a natural person who is either the Applicant, employed by the Applicant, or an authorized agent who has express authority to represent the Applicant to

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

3. Contract Signer

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

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

3.2 Validation of Certificate Data– Existence and Identity of Organizations

Prior to the issuance of an EV Certificate TC TrustCenter verifies correctness and accuracy of all certificate data according to TC TrustCenter's Certificate Policy Definitions for EV Certificates and in accordance with the „Guidelines for the Issuance and Management of Extended Validation Certificates".

This validation consists of

1) Verification of the Applicant's existence and identity
   a) Verification of legal existence and identity
   b) Verification of physical existence (business presence at a physical address)
   c) Verification of operational existence (business activity).;

2) If the application is for an EV SSL Certificate, verify the Applicant is a registered holder, or has exclusive control, of the Domain Name to be included in the EV Certificate;

3) Verify the Applicant's authorization for the EV Certificate, including;
   a. Verify the name, title, and authority of the Contract Signer, Certificate Approver, and Certificate Requester,
   b. Verify that a Contract Signer signed the Subscriber Agreement, and

c. Verify that a Certificate Approver has signed or otherwise approved the EV Certificate Request.

3.2.1 Verification of Applicant's Existence and Identity

3.2.1.1 Private Organizations Subjects

a) Legal Existence

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

b) Organization Name

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

c) Registration Number

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

d) Registered Agent

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

All information related to section 3.2.1.1, items a) to d) is obtained directly from the Incorporating or Registration Agency in the Applicant's Jurisdiction of Incorporation or Registration.

3.2.1.2 Government Enity Subjects

a) Legal Existence

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

b) Entity Name

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

c) Registration Number

In general, there is no register for Government entities. If such a register exists, TC TrustCenter obtains and verifies the register number. Otherwise, TC TrustCenter 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, TC TrustCenter enters appropriate language to indicate that the Subject is a Government Entity.

TC TrustCenter verifies all items listed above in items a) to c) either directly with, or obtained directly from, one of the following:

(i) a Qualified Government Information Source in the political subdivision in which such Government Entity operates;

(ii) a superior governing Government Entity in the same political subdivision as the Applicant (e.g. a Secretary of State may verify the legal existence of a specific State Department), or

(iii) from a judge that is an active member of the federal, state or local judiciary within that political subdivision, or

(iv) an attorney representing the Government Entity.

3.2.1.3 Other Organizations (Business Entity Subjects)

a) Legal Existence

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

b) Organisation Name

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

c) Registration Number

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

d) Principal Individual

Verify the identity of the identified Principal Individual according to Section 3.4.

All information related to items a) to d) in section 3.2.1.3 is obtained directly from the Incorporating or Registration Agency in the Applicant's Jurisdiction of Incorporation or Registration.

The Principal Individual's identification requires face-to-face validation and presentation of a valid government issued photo ID.

3.2.1.4 Non-commercial Organizations (International Organizations)

a) Legal Existence

Verify that the Applicant is a legally recognized International Organization Entity;

b) Entity Name

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

c) Registration Number

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

All items listed in section 3.2.1.4, a) to c) are verified either:

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

(ii) Directly with a signatory country's government, provided that TC TrustCenter is permitted to do business in that country. 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

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

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.

3.2.2 Verification of Applicant's Physical Existence

3.2.3 Address of Applicant's Place of Business

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

TC TrustCenter verifies that the address stated in the EV Certificate request matches the address obtained from the relevant Incorporating or Registration Agency.

If these addresses do not match, TC TrustCenter verifies the Place of Business through an on-site-visit.

Alternatively, TC TrustCenter may rely on a Verified Legal Opinion or a Verified Accountant Letter that indicates the address of the Applicant's or a Parent/Subsidiary Company's Place of Business and that business operations are conducted there.

A Verified Legal Opinion MUST be presented if the Place of Business is not in the country of incorporation or registration.

3.2.3.1 Telephone Number for Applicant's Place of Business

TC TrustCenter verifies that the telephone number provided by the Applicant is a main phone number for the Applicant's Place of Business.

TC TrustCenter confirms the telephone number by calling it and obtaining an affirmative response sufficient to enable a reasonable person to conclude that the Applicant is reachable by telephone at the number dialled.

In addition, the telephone number must be confirmed through:

– records provided by the applicable phone company or by a qualified independent telephone directory, or

– calling the telephone number during an on-site visit and direct verification that the call is answered from within the Applicant's Place of Business. The main telephone number must not be a mobile phone, or

– rely on a Verified Legal Opinion or a Verified Accountant Letter to the effect that the Applicant's telephone number, as provided, is a main phone number for the Applicant's Place of Business..

For Government Entity Applicants, TC TrustCenter may rely on the telephone number contained in the records of a Qualified Government Information Source in Applicant's Jurisdiction.

3.2.4 Verification of Applicant's Operational Existence

If the 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 (QIIS) or Qualified Tax Information System,(QTIS) TC TrustCenter verifies that the Applicant has the ability to engage in business by either

(i) Verifying that the 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 the Applicant has an active current Demand Deposit Account with the institution, or

(ii) Relying on a Verified Legal Opinion or a Verified Accountant Letter to the effect that the Applicant has an active current Demand Deposit Account with a Regulated Financial Institution.

3.3 Examination of the certificate data - Review of the domain name

To verify the Applicant's registration, or exclusive control, of the Domain Name(s) to be listed in the EV SSL 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. Domain registration information in the WHOIS database is public and shows the name, physical address, and administrative contact information for the organization;

   For Government Entity Applicants, TC TrustCenter may rely on the Domain Name listed for that entity in the records of the Qualified Government Information Source (QGIS) in the Applicant's Jurisdiction;
3. The Applicant
   a. Is the registered holder of the Domain Name, or
   b. has been granted the exclusive right to use the Domain Name by the registered holder of the Domain Name;
4. The Applicant is aware of its registration or exclusive control of the Domain Name.

3.4 Testing the certificate data - the existence and identity of persons

Persons who have to be identified for the issuance of an EV Certificate, e.g. an organization's Principal Individual, must be identified in a face-to-face meeting.

The face-to-face validation MUST be conducted before either an employee of the CA, a Latin Notary, a Notary (or equivalent in the Applicant's jurisdiction), a Lawyer, or Accountant (Third-Party Validator).

3.4.1 Verification of Existence and Identity of Principal Individuals

3.4.1.1 Documents Required for Identity Proofing

The person to be identified must present the following documentation (Vetting Documents):

1) A Personal Statement that includes the following information:
   a) Full name or names by which a person is, or has been, known (including all other names used);
   b) Residential Address at which he/she can be located;
   c) Date of birth; and
   d) An affirmation that all of the information contained in the Certificate Request is true and correct.
2) A current signed government-issued identification document that includes a photo of the Individual and is signed by the Individual such as
   a) A passport,
   b) A personal identification card.
   c) Documents which are accepted in other countries, e.g.
      i. A driver's license,
      ii. A military ID.
3) 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.
   – 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.
   – Other (non-financial) documents include:
     a) Recent original utility bills or certificates from a utility company confirming the arrangement to pay for the services at a fixed address (not a mobile/cellular telephone bill),

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

c) A certified copy of a birth certificate,

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

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

3.4.1.2 Activities Performed for Identity Proofing

The person performing the face-to-face validation

1) attest to the signing of the Personal Statement (section 3.4.1.1 No. 1)) and the identity of the signer,
2) identify the original vetting documents used to perform the identification(section 3.4.1.1 No. 2) and 3)), and
3) attest on a copy of the current signed government-issued photo identification document (section 3.4.1.1 No. 2)) that it is a full, true, and accurate reproduction of the original.

3.4.1.3 Cross-checking of Identity Proofing

If the identity proofing has not been performed by an employee of TC TrustCenter, TC TrustCenter reviews the documentation to determine that the information is consistent, matches the information in the application, and identifies the Individual.

The following documents must be submitted to TC TrustCenter for cross-checking:

1) the original signed and attested Personal Statement according to section 3.4.1.1 No. 1) ,
2) a list of the vetting documents used to perform identity proofing according to section 3.4.1.2 No. 2),
3) the attested copy of the current signed government-issued photo identification document according to section 3.4.1.2 No. 3).

3.4.1.4 Verification of Person Conducting Identity Proofing

TC TrustCenter independently verifies that the person who conducted the identity proofing is a legally-qualified Latin Notary or Notary (or legal equivalent in the Applicant's jurisdiction), lawyer, or accountant in the jurisdiction of the Individual's residency, and that he/she actually did perform the services stated in section 3.4.1.2 and did attest to the signature of the Individual.

3.4.2 Verification of Existence and Authorization for Persons

3.4.2.1 Verification of Name, Title, and Authority of Contract Signer and Certificate Approver

TC TrustCenter verifies name, title and authority of both the Contract Signer and the Certificate Approver. TC TrustCenter may use 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**.**

Whether Contract Signer and/or Certificate Approver are agents representing the applicant is confirmed by

- Contacting the Applicant's Human Resources Department by phone or mail (at the phone number or address for the Applicant's Place of Business, verified in accordance with these Guidelines) and obtaining confirmation that the Contract Signer and/or the Certificate Approver, as applicable, is an employee; or
- Obtaining an Independent confirmation from the 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 the applicant.

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

3.4.2.2 Authorization of Contract Signer and Certificate Approver

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

(i) Legal Opinion,

(ii) Accountant Letter,

(iii) Corporate Resolution or Independent Confirmation from Applicant,

(iv) Contract between TC TrustCenter and Applicant that designates the Certificate Approver with such EV Authority,

(v) Prior Equivalent Authority.

If TC TrustCenter and Applicant contemplate the submission of multiple future EV Certificate Requests, then the Applicant may expressly authorize one or more Certificate Approver(s) to exercise EV Authority with respect to each future EV Certificate Request submitted on behalf of the Applicant and properly authenticated as originating with, or otherwise being approved by, such Certificate Approver(s).

3.5 Reasons for EV Certificate Refusal

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.

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.

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 Character Set and Rules for Conversion

The X.509 compliant certificates contain in the designated fields as defined in RFC 3280 „Internet X.509 Public Key Infrastructure, Certificate and Certificate Revocation List (CRL) Profile 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 ID document or register extract. 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 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.

  Examples:

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 GmbH	Meier und Meier GmbH
Meier & Meier GmbH	Meier u. Meier GmbH
Meier & Meier GmbH	Meier + Meier GmbH