



TC TrustCenter

Zertifizierungsrichtlinien für EV-Zertifikate

Fassung vom 10. September 2009

1	EINLEITUNG	3
2	WICHTIGE HINWEISE.....	5
2.1	HINWEISE FÜR CODE SIGNING ZERTIFIKATE	6
2.2	MELDUNG VON PROBLEMEN	7
2.3	TESTSEITEN FÜR SOFTWAREHERSTELLER.....	8
3	EV-ZERTIFIKATE	9
3.1	VORAUSSETZUNGEN FÜR DIE AUSSTELLUNG VON EV-ZERTIFIKATEN	9
3.1.1	<i>Dokumente</i>	9
3.1.2	<i>Rollen</i>	11
3.2	PRÜFUNG DER ZERTIFIKATSDATEN – EXISTENZ UND IDENTITÄT VON ORGANISATIONEN	12
3.2.1	<i>Verifikation der Existenz und Identität der antragstellenden Organisation.....</i>	<i>12</i>
3.2.2	<i>Überprüfung der physischen Existenz einer Organisation.....</i>	<i>14</i>
3.2.3	<i>Überprüfung der Geschäftstätigkeit einer Organisation.....</i>	<i>15</i>
3.3	PRÜFUNG DER ZERTIFIKATSDATEN – ÜBERPRÜFUNG DES DOMAIN-NAMENS	15
3.4	PRÜFUNG DER ZERTIFIKATSDATEN – EXISTENZ UND IDENTITÄT VON PERSONEN	15
3.4.1	<i>Überprüfung der Existenz und Identität von Handlungsbevollmächtigten.....</i>	<i>15</i>
3.4.2	<i>Überprüfung der Existenz und Autorisierung von Personen.....</i>	<i>17</i>
3.5	GRÜNDE, DIE DER AUSSTELLUNG EINES EV-ZERTIFIKATES ENTGEGENSTEHEN	17
4	REVOZIERUNG VON EV-ZERTIFIKATEN.....	19
5	ZEICHENSATZ UND KONVERSIONSREGELN	21
5.1	KONVERSION VON ZEICHEN	21

1 Einleitung

Dieses Dokument beschreibt die Zertifizierungsrichtlinien von TC TrustCenter für die Ausstellung von „Extended Validation“ Zertifikaten (EV-Zertifikaten). EV-Zertifikate sind Zertifikate, deren Ausstellung an eine strenge Überprüfung der Antragsteller gebunden ist. Die Vergabekriterien für die Ausstellung von EV-Zertifikaten werden dabei in den vom CA/Browser Forum herausgegebenen „Guidelines for the Issuance and Management of Extended Validation Certificates“ (http://www.cabforum.org/EV_Certificate_Guidelines.pdf) spezifiziert. Das CA/Browser Forum ist ein freiwilliger Zusammenschluss von Browser-Herstellern und Zertifizierungsstellen (Certification Authorities, CAs).

Der Begriff „Extended Validation“ soll bei diesen Zertifikaten zum Ausdruck bringen, dass bei der Ausstellung von EV-Zertifikaten gegenüber „normalen SSL-Zertifikaten“ eine erweiterte, gründlichere Prüfung des Zertifikatsinhabers erfolgt, wodurch eine zuverlässigere Bindung des Zertifikatsinhabers an das Zertifikat erfolgt.

Das vorrangige Ziel bei der Verwendung von EV-Zertifikaten ist es, den Besuchern einer Webseite eine sichere und zuverlässige Authentifizierung des besuchten Webservers zu ermöglichen und das Vertrauen der Benutzer in die sichere Verbindung zu einer gewünschten Webseite durch die bei der Nutzung eines EV-Zertifikats grün hinterlegte Adresszeile des Browsers zu stärken.

Insbesondere Phishing-Versuche mit verschlüsselten, und damit auf den ersten Blick sicheren, Webseiten werden durch den Einsatz von EV-Zertifikaten für den Benutzer leichter erkennbar. Typischerweise werden EV-Zertifikate also genutzt, um Webanwendungen per HTTPS zu sichern und den Anwendern (vor dem Hintergrund von Phishing-Angriffen) eine zusätzliche Sicherheit zu geben, z.B. beim online Banking.

Eine weitere Anwendung finden EV-Zertifikate als EV Code Signing Zertifikate. Code Signing Zertifikate werden benutzt, um sowohl die Identität des Inhabers eines solchen Code Signing Zertifikates als auch die Integrität des Code zu verifizieren. Ein Code Signing Zertifikat wird nicht einem bestimmten Stück Software oder anderem Code zugeordnet, es identifiziert vielmehr den Inhaber des Zertifikates, der dann damit Code mit seinem Namen signieren kann.

Ein Nutzer, der sich z.B. aus dem Internet Code herunterlädt, hat somit die Möglichkeit, sowohl den Anbieter oder Produzenten des Codes anhand der Zertifikatsdaten sicher zu identifizieren, als auch eventuelle Modifikationen an dem Code zu erkennen. Auf diese Weise kann die Vertrauenswürdigkeit von Software-Plattformen erhöht und die Verbreitung von Schadsoftware eingeschränkt werden.

Der Inhaber eines Code Signing Zertifikats kann dieses Zertifikat verwenden, um Ursprung und Legitimität des von ihm erzeugten Codes nachzuweisen, was z.B. auch bei Urheberrechts-Fragen relevant sein kann.

Technisch unterscheidet sich ein EV-Zertifikat nicht von einem normalen Zertifikat. Der Unterschied besteht lediglich darin, dass die CA als Herausgeber des EV-Zertifikats den Inhaber des Zertifikats besonders genau überprüft hat.

Diese Zertifizierungsrichtlinien für EV-Zertifikate beschreiben das Verfahren, nach welchem TC TrustCenter die Identifizierung von Antragstellern auf die Ausstellung eines EV-Zertifikats durchführt. TC TrustCenter hält sich dabei strikt an die Vorgaben, die in den „Guidelines for the Issuance and Management of Extended Validation Certificates“ gemacht werden.

Kontaktinformationen:

TC TrustCenter GmbH
Sonninstraße 24 - 28
20097 Hamburg
Germany

Internet: <http://www.trustcenter.de>
E-Mail: info@trustcenter.de
Telefon: +49 (0)40 80 80 26-0
Telefax: +49 (0)40 80 80 26-1 26

Anpassung an übergeordnete Richtlinien: Sollten sich die Anforderungen an die Ausstellung von EV-Zertifikaten ändern, z.B. durch eine Aktualisierung der „Guidelines for the Issuance and Management of Extended Validation Certificates“, so werden diese Zertifizierungsrichtlinien für EV-Zertifikate entsprechend überarbeitet.

Deutsche Fassungen sind maßgebend: Einige der Dokumente und Web-Seiten von TC TrustCenter stehen sowohl in deutscher als auch in englischer Fassung zur Verfügung. In Zweifelsfällen ist für alle Dokumente die deutsche Fassung maßgebend.

Irrtum vorbehalten: TC TrustCenter behält sich Irrtümer über in diesem Dokument enthaltene Aussagen, insbesondere über technische Erklärungen oder hierin beschriebene Verfahren, vor.

Urheberrechts-Notiz: Dieses Dokument ist urheberrechtlich geschützt. Die Verwendung der Texte, auch auszugsweise, ist ohne die schriftliche Zustimmung von TC TrustCenter unzulässig und strafbar. Das gilt insbesondere für Vervielfältigungen, Verbreitungen, Übersetzungen oder die Verwendung in elektronischen Systemen. Ausgenommen hiervon sind das Kopieren und der Ausdruck zum eigenen Gebrauch.

Alle Informationen in diesem Dokument wurden mit größter Sorgfalt erstellt. TC TrustCenter kann nicht für Schäden haftbar gemacht werden, die in Zusammenhang mit der Verwendung dieses Dokumentes stehen.

„TC TrustCenter“, das TC TrustCenter Logo, „IdentPoint“, „TC PKI“, „TC fit“, „TC QuickStart“ und „TC Qsign“ sind eingetragene Marken der TC TrustCenter GmbH.

Alle in diesem Dokument verwendeten, aber hier nicht genannten Marken- oder Produktnamen sind Marken oder Warenzeichen der entsprechenden Inhaber.

Copyright © 2009 TC TrustCenter GmbH, Sonninstraße 24 - 28, 20097 Hamburg/Germany. Alle Rechte vorbehalten.

2 Wichtige Hinweise

TC TrustCenter macht durch die Ausstellung eines EV-Zertifikats die folgenden Zusicherungen:

1. Existenz: TC Trustcenter hat die Existenz der Organisation, für die das EV-Zertifikat ausgestellt worden ist, zum Zeitpunkt der Ausstellung über das zuständige Register oder eine äquivalente Quelle verifiziert.
2. Identität: TC TrustCenter hat verifiziert, dass der im EV-Zertifikat genannte Name der Organisation mit den offiziellen behördlichen Einträgen im zuständigen Register oder einer äquivalenten Quelle übereinstimmt.
3. Nutzungsrecht des Domain-Namens: TC TrustCenter hat verifiziert, dass die im EV-Zertifikat genannte Organisation zum Zeitpunkt der Ausstellung des Zertifikats das exklusive Recht zur Nutzung des Domain-Namens innehatte.
4. Autorisierung: TC TrustCenter hat verifiziert, dass die im EV-Zertifikat genannte Organisation die Ausstellung des EV-Zertifikats autorisiert hat.
5. Korrektheit: TC TrustCenter hat, soweit dies möglich und vertretbar ist, alle weiteren Angaben im EV-Zertifikat auf ihre Korrektheit und Genauigkeit überprüft.
6. Subscriber Agreement: Die im EV-Zertifikat genannte Organisation hat ein rechtsgültige und durchsetzbare Erklärung unterzeichnet, die den Anforderungen an ein Subscriber Agreement gemäß diesen Zertifizierungsrichtlinien und den „Guidelines for the Issuance and Management of Extended Validation Certificates“ entspricht.

EV-Zertifikate machen ausschließlich eine Aussage über die Identität des Zertifikatsinhabers, aber nicht über das Verhalten des Zertifikatsinhabers. TC TrustCenter sichert durch die Ausstellung eines EV-Zertifikats also keinesfalls zu,

1. dass die im EV-Zertifikat genannte Person oder Organisation tatsächlich aktiv Geschäfte tätigt,
2. dass die im EV-Zertifikat genannte Person oder Organisation sich an die Gesetze hält,
3. dass die im EV-Zertifikat genannte Person oder Organisation vertrauenswürdig, ehrlich oder seriös ist,
4. dass es „sicher“ ist, mit der im EV-Zertifikat genannten Person oder Organisation in eine Geschäftsbeziehung einzutreten.

Ausstellung der Zertifikate nach den jeweils gültigen Zertifizierungsrichtlinien: Alle von TC TrustCenter ausgestellten Zertifikate werden nach den jeweils zum Zeitpunkt der Ausstellung der Zertifikate gültigen Zertifizierungsrichtlinien für den jeweiligen Zertifikatstyp erstellt. Eine spätere Änderung der Zertifizierungsrichtlinien hat keinen Einfluss auf bereits ausgestellte Zertifikate.

Keine Prüfung von Kreditwürdigkeit: TC TrustCenter prüft die Korrektheit der in Zertifikaten angegebenen Identität auf die in diesem Dokument beschriebene Weise gemäß den Vorschriften für die Ausstellung von EV-Zertifikaten. Es werden keinerlei Prüfungen über Liquidität, Kreditwürdigkeit oder dergleichen durchgeführt. Zertifikate schaffen Vertrauen darin, dass der Zertifikatsinhaber, im Fall von EV-SSL-Zertifikaten ein Webserver, im Fall von EV Code Signing Zertifikaten ein Code-Entwickler, tatsächlich derjenige ist, der er vorgibt zu

sein. EV-Zertifikate geben keinerlei Hinweise auf die Vertrauenswürdigkeit des Zertifikatsinhabers selbst.

Keine Prüfung der Unbedenklichkeit von Software: TC TrustCenter stellt Code Signing Zertifikate für Organisationen und natürliche Personen zum Signieren von Programmcode aus. Zu beachten ist, dass TC TrustCenter nicht den signierten Programmcode selbst, dessen Unbedenklichkeit, programmtechnische Korrektheit oder sonstige Eignung für einen bestimmten Zweck zertifiziert. Die in diesem Kontext ausgegebenen Zertifikate geben dem Hersteller aber ein Mittel in die Hand, um Manipulationen der von ihm vertriebenen Programme für den Benutzer der Software erkennbar zu machen. Weiterhin wird durch derartige Zertifikate die Herkunft der Software überprüfbar.

Keine Zusicherung der Aktualität der Daten: TC TrustCenter überprüft die im Zertifikatsantrag angegebenen Daten nur im Rahmen und zum Zeitpunkt der Registrierung zur Ausstellung eines Zertifikats. Eine Zusicherung der Aktualität dieser Daten nach der Registrierung wird von TC TrustCenter daher nicht gegeben. Jeder Zertifikatsinhaber ist verpflichtet, sein Zertifikat sperren zu lassen, wenn darin enthaltene Daten nicht mehr aktuell sind.

Die Entscheidung über die Angemessenheit für eine Anwendung liegt beim Teilnehmer: Jeder Teilnehmer an den angebotenen Zertifizierungsdiensten muss selbst entscheiden, ob eine bestimmtes Zertifikat den Anforderungen seiner speziellen Anwendung genügt.

Informationspflicht des Teilnehmers: Es wird ausdrücklich darauf hingewiesen, dass es unerlässlich ist, sich vor der Antragstellung oder Teilnahme am Zertifizierungsdienst Grundkenntnisse über Public Key-Verfahren, Signaturen und die Verifikation von Signaturen sowie Überprüfung der Authentizität von SSL-Zertifikaten anzueignen.

TC TrustCenter behält sich vor, Zertifikate zu sperren: Sollten kryptographische Algorithmen oder zugehörige Parameter durch technologische Fortschritte oder neue Entwicklungen in der Kryptologie unsicher werden, behält TC TrustCenter sich vor, Zertifikate, die mit diesen Algorithmen und Parametern erzeugt wurden, zu sperren. Zertifikate können auch dann gesperrt werden, wenn der Zertifikatsinhaber falsche Angaben gemacht hat, die Zertifikate missbräuchlich oder zu strafbaren Handlungen eingesetzt werden oder TC TrustCenter von der Veränderung der im Zertifikat enthaltenen Daten Kenntnis erlangt.

2.1 Hinweise für Code Signing Zertifikate

Lebens-Zyklus

Code kann in jedem Stadium des Software Entwicklungs- oder Verteilungsprozesses entweder durch einen Software-Hersteller oder eine Nutzer-Organisation signiert werden.

Signierter Code kann immer verifiziert werden, also insbesondere während Download, Entpacken, Installation, Ausführung oder während einer forensischen Untersuchung.

EV Code-Signing Certificate haben eine Gültigkeit von nicht mehr als 39 Monaten. Ohne einen angebrachten Zeitstempel verlieren die Signaturen ihre Gültigkeit sobald das signierende Zertifikat abläuft.

Zeitstempeldienste-Anbieter und Anbieter von Signierdiensten können EV Zeitstempel-Zertifikate bzw. EV Code Signing Zertifikate mit einer Gültigkeit von maximal 123 Monaten erhalten.

Normalerweise wird eine Code-Signatur für einen Zeitraum von bis zu 39 Monaten als gültig betrachtet, dieser Zeitraum kann allerdings durch eine der beiden folgenden Methoden auf bis zu 123 Monate ausgedehnt werden:

- a) **Zeitstempel-Methode**
Bei dieser Methode signiert der Anwender seinen Code unter Verwendung seines Code Signing Zertifikats (dessen Ablaufdatum weniger als 39 Monate in der Zukunft liegt) und sendet den signierten Code an einen EV-Zeitstempeldienst um ihn dort zeitstempeln zu lassen. Mit angebrachtem Zeitstempel kann der nun signierte und zeitgestempelte Code bis zum Ungültigwerden des Zeitstempel-Zertifikats angesehen werden, also bis zu 123 Monate.
- b) **Signierdienste-Anbieter-Methode**
Bei dieser Methode übermittelt der Anwender seinen Code (oder den Hashwert seines Codes) an einen Signierdienste-Anbieter. Dieser signiert den Code (bzw Hashwert) unter Verwendung seines EV Code Signing Zertifikats. Diese Signatur ist bis zum Ablauf des Signierdienste-Zertifikats, also bis zu 123 Monate, gültig.

Schutz des geheimen Schlüssels

Die geheimen Schlüssel von Code Signing Zertifikaten müssen durch ein Kryptographie-Modul (Hardware Security Module, HSM) geschützt werden, das mindestens den Anforderungen des Standards FIPS 140-2 Level 2 (oder äquivalent) entspricht.

Der Nachweis, dass ein Kryptographie-Modul diesen Anforderungen entspricht, kann erfolgen durch:

- a) Verwendung eines HSM, das über eine entsprechende Zertifizierung verfügt;
- b) Vertragliche Regelungen, in denen sich der Zertifikatsinhaber verpflichtet, seinen geheimen Schlüssel gemäß einem zu FIPS 140-2 äquivalenten Standard zu schützen, in Verbindung mit einem Audit, das die Einhaltung dieser Sicherheitsmaßnahmen bestätigt

Inhalt von Code Signing Zertifikaten

EV Code Signing Zertifikate enthalten im Prinzip die gleichen Felder wie EV SSL Zertifikate, allerdings **keinen** Domain Namen.

Die keyUsage Extensions eines Code Signing Zertifikats müssen wie folgt besetzt sein:

keyUsage

Diese Extension MUSS vorhanden sein und sie MUSS als kritisch markiert sein.

Das Bit für digitalSignature MUSS gesetzt sein, alle anderen Bits sollen nicht gesetzt sein.

extKeyUsage

Diese Extension MUSS vorhanden sein und sie MUSS als kritisch markiert sein.

Der Wert id-kp-codeSigning MUSS belegt sein. Andere Werte sollen nicht vorhanden sein.

2.2 Meldung von Problemen

TC TrustCenter stellt eine jederzeit verfügbare Webseite für Inhaber von EV-Zertifikaten, Relying Parties, Softwarehersteller und andere Dritte zur Verfügung, über die Problemmeldungen an TC TrustCenter übermittelt werden können. Solche Problemmeldungen können

z.B. Beschwerden, vermutete Schlüsselkompromittierungen, Missbrauch von EV-Zertifikaten, Betrug und andere Meldungen über unerwünschte Nutzung von EV-Zertifikaten sein.

TC TrustCenter beginnt innerhalb von 24 Stunden nach Eingang einer solchen Meldung mit der Untersuchung der Problemmeldung und entscheidet in der Folge über eine angemessene Reaktion, also ob eine Sperrung oder eine andere Reaktion seitens TC TrustCenter angebracht ist. Bei einer solchen Entscheidung werden unter anderem die folgenden Kriterien in Betracht gezogen:

- (i) die Art des Problems,
- (ii) die Anzahl der Problemmeldungen, die für ein EV-Zertifikat oder eine Website bereits vorliegen
- (iii) die Identität des Meldenden, so hat z.B. die Meldung eines behördlichen Gesetzesvertreters dass eine Website in illegale Aktivitäten verwickelt ist, mehr Gewicht als die Meldung eines Verbrauchers, der z.B. seine gekauften Waren nicht erhalten hat
- (iv) die Gesetzeslage.

Bei allen Problemmeldungen, denen eine hohe Priorität zugeordnet wird, erfolgt eine Reaktion durch TC TrustCenter innerhalb von 24 Stunden. Dies kann z.B. eine Sperrung des betroffenen EV-Zertifikates sein oder eine Meldung an die zuständigen Behörden.

2.3 Testseiten für Softwarehersteller

Für Softwarehersteller stellt TC TrustCenter Testseiten zur Verfügung, auf denen die Funktion von Software im Zusammenhang mit EV-Zertifikaten getestet werden kann.

Dazu steht für jede verwendete Root jeweils eine Webseite mit einem gültigen, einem gesperrten und einem abgelaufenen Zertifikat zur Verfügung.

Root	Status	URL
Universal III	Gültig	testserver.universal-III.trustcenter.de
Universal III	Revoziert	testserver-revoked.universal-III.trustcenter.de
Universal III	Abgelaufen	testserver-expired.universal-III.trustcenter.de
Universal I	Gültig	testserver.universal-I.trustcenter.de
Universal I	Revoziert	testserver-revoked.universal-I.trustcenter.de
Universal I	Abgelaufen	testserver-expired.universal-I.trustcenter.de

3 EV-Zertifikate

Die Vertrauenswürdigkeit von Zertifikaten hängt von den Verfahren ab, nach denen sie ausgestellt werden. Diese Verfahren werden in Richtlinien definiert.

Die Richtlinien für die Ausstellung von EV-Zertifikaten werden vom CA/Browser Forum definiert, um eine international einheitliche Qualität der EV-Zertifikate zu erreichen. Diese Richtlinien werden vom CA/Browser Forum in dem Dokument „Guidelines for the Issuance and Management of Extended Validation Certificates“ veröffentlicht und sind unter http://www.cabforum.org/EV_Certificate_Guidelines.pdf öffentlich verfügbar. Das CA/Browser Forum ist ein freiwilliger Zusammenschluss von Browser-Herstellern und CAs.

Alle von TC TrustCenter ausgestellten EV-Zertifikate werden gemäß diesen Zertifizierungsrichtlinien für EV-Zertifikate und den „Guidelines for the Issuance and Management of Extended Validation Certificates“ ausgestellt.

Da die „Guidelines for the Issuance and Management of Extended Validation Certificates“ international Anwendung finden sollen, sind zwangsläufig einige für die Überprüfung der Identität und Autorisierung von Antragstellern notwendige Prüfschritte und Verfahren in den Guidelines allgemein formuliert. Diese Prüfschritte müssen von jeder CA entsprechend den lokalen Gegebenheiten und Möglichkeiten umgesetzt werden, ohne die in den Guidelines spezifizierten Mindestanforderungen zu verletzen.

Dieses Dokument, die TC TrustCenter Zertifizierungsrichtlinien für EV-Zertifikate, beschreibt die von TC TrustCenter vorgenommene Art der Überprüfung der Inhalte von EV-Zertifikaten und die Verfahren zur Feststellung der Identität und Autorisierung von Antragstellern für EV-Zertifikate.

Bei eventuellen Abweichungen zwischen diesen Zertifizierungsrichtlinien und den „Guidelines for the Issuance and Management of Extended Validation Certificates“ haben die Regelungen aus den „Guidelines for the Issuance and Management of Extended Validation Certificates“ Vorrang. Dies betrifft z.B. die Archivierungsfristen für Registrierungsdaten, die bei EV-Zertifikaten 7 Jahre beträgt.

3.1 Voraussetzungen für die Ausstellung von EV-Zertifikaten

TC TrustCenter stellt EV-Zertifikate für privatwirtschaftliche Organisationen, Behörden und andere Organisationen aus.

3.1.1 Dokumente

Vor der Ausstellung eines EV-Zertifikats müssen TC TrustCenter die folgenden Dokumente in Übereinstimmung mit den „Guidelines for the Issuance and Management of Extended Validation Certificates“ vorgelegt werden:

- Antrag auf Ausstellung eines EV-Zertifikats
- Subscriber Agreement
- Dokumente, um die Korrektheit, Authentizität und Autorisierung des Antrags gemäß diesen Zertifizierungsrichtlinien und den „Guidelines for the Issuance and Management of Extended Validation Certificates“ zu verifizieren.

Grundsätzlich zu verifizieren ist

- die juristische Existenz und Identität der Organisation, die ein EV-Zertifikat beantragt,
- die physische Existenz der Organisation, die ein EV-Zertifikat beantragt und
- die operationelle Existenz der Organisation, die ein EV-Zertifikat beantragt

- die Autorisierung der am Antragsprozess beteiligten Personen.

Dokumente, die zur Validierung von Angaben im Laufe des Antragsprozesses vorgelegt werden, dürfen nicht älter als 13 Monate sein.

Auch die Überprüfung weiterer Angaben, wie z.B. Telefonnummern, Domainnamen oder die Existenz von Bankkonten darf nicht länger als 13 Monate zurückliegen.

a) Privatwirtschaftliche Organisationen

- (1) Bei einer privatwirtschaftlichen Organisation muss es sich um eine juristische Person handeln, die in einem amtlichen Register geführt wird, für die es amtliche Dokumente der Gründung gibt oder die durch eine Behörde zugelassen worden ist.
- (2) Eine privatwirtschaftliche Organisation muss über einen Handlungsbevollmächtigten und über einen physisch verifizierbaren Firmensitz verfügen,.
- (3) Eine privatwirtschaftliche Organisation darf nicht in den amtlichen Registern als inaktiv, ungültig, gelöscht oder nicht aktuell geführt sein.
- (4) Der Handel mit einer privatwirtschaftlichen Organisation muss gemäß TC TrustCenters Export-Richtlinien zulässig sein. TC TrustCenters Export-Richtlinien regeln, mit welchen Staaten und mit welchen Organisationen TC TrustCenter Handel treiben darf und welche Staaten und Organisationen aufgrund staatlicher Verbotslisten (z.B. Handelsembargo) vom Handel ausgeschlossen sind.

b) Behörden

- (1) Die Existenz einer Behörde muss durch eine übergeordnete oder aufsichtführende Behörde nachgewiesen werden.
- (2) Der Handel mit einer Behörde muss gemäß TC TrustCenters Export-Richtlinien zulässig sein. TC TrustCenters Export-Richtlinien regeln, mit welchen Staaten und mit welchen Organisationen TC TrustCenter Handel treiben darf und welche Staaten und Organisationen aufgrund staatlicher Verbotslisten (z.B. Handelsembargo) vom Handel ausgeschlossen sind.

c) Andere Organisationen

Unter dem Begriff "andere Organisationen" werden Organisationen zusammengefasst, die weder als privatwirtschaftliche Organisation noch als Behörde bezeichnet werden können. Beispiele sind Partnerschaften, Sozietäten und Einzelunternehmen.

- (1) Die Organisation muss juristisch anerkannt sein. Die Gründung der Organisation muss bei der zuständigen Stelle aktenkundig sein (z.B. durch eine vorgelegte Satzung, Zulassung, etc.), so dass die Existenz der Organisation durch die zuständige Stelle verifiziert werden kann.
- (2) Die Organisation muss nachweislich physisch existieren und geschäftlich agieren.
- (3) Mindestens eine handlungsbevollmächtigte Person der Organisation muss identifiziert und überprüft werden.
- (4) Die identifizierte handlungsbevollmächtigte Person muss die in den Subscriber Agreements gemachten Zusicherungen bestätigen.
- (5) Handelt die Organisation unter einem angenommenen Namen, dann muss die legale Nutzung des Namens überprüfbar sein.
- (6) Der Handel mit einer Organisation muss gemäß TC TrustCenters Export-Richtlinien zulässig sein. TC TrustCenters Export-Richtlinien regeln, mit welchen Staaten und mit welchen Organisationen TC TrustCenter Handel treiben darf und welche Staaten und Organisationen aufgrund staatlicher Verbotslisten (z.B. Handelsembargo) vom Handel ausgeschlossen sind.

d) Nicht-kommerzielle Organisationen (Internationale Organisationen)

TC TrustCenter kann EV-Zertifikate für nicht-kommerzielle Organisationen ausstellen, die mit den obigen Bereichen nicht erfasst sind, aber folgende Anforderungen erfüllen:

- (i) Der Antragsteller ist eine internationale Organisation, die aufgrund einer Satzung, eines Vertrages, einer Übereinkunft oder vergleichbarer Erklärungen, die von mehreren Staaten unterschrieben wurden, gegründet wurde.
- (ii) Die internationale Organisation darf ihren Hauptsitz nicht in einem Staat haben, mit dem TC TrustCenter keinen Handel treiben darf.
- (iii) Der Handel mit einer internationalen Organisation muss gemäß TC TrustCenters Export-Richtlinien zulässig sein. TC TrustCenters Export-Richtlinien regeln, mit welchen Staaten und mit welchen Organisationen TC TrustCenter Handel treiben darf und welche Staaten und Organisationen aufgrund staatlicher Verbotslisten (z.B. Handelsembargo) vom Handel ausgeschlossen sind.

Für Tochterorganisationen oder Agenturen von zulässigen internationalen Organisationen können ebenfalls EV-Zertifikate ausgestellt werden.

3.1.2 Rollen

Die folgenden Rollen sind bei der antragstellenden Organisation für die Ausstellung eines EV-Zertifikats beteiligt:

1. **Zertifikats-Beantrager (Certificate Requester)**
Der Antrag auf Ausstellung eines EV-Zertifikats muss durch einen autorisierten Zertifikats-Beantrager an TC TrustCenter übermittelt werden. Ein Zertifikats-Beantrager ist eine natürliche Person, bei der es sich um einen Angestellten der antragstellenden Organisation, einen Vertretungsberechtigten der Organisation oder einen Dritten handeln kann, der EV-Anträge im Namen der Organisation stellen darf (z.B. ein ISP oder Hosting-Unternehmen).
2. **Zertifikats-Bestätiger (Certificate Approver)**
Der Antrag auf ein EV-Zertifikat muss durch einen Zertifikats-Bestätiger genehmigt werden. Ein Zertifikats-Bestätiger ist eine natürliche Person, bei der es sich um einen Angestellten der antragstellenden Organisation oder einen Bevollmächtigten der Organisation handelt, der berechtigt ist
 - i. als Zertifikats-Beantrager zu handeln und andere Personen als Zertifikats-Beantrager einzusetzen und
 - ii. Anträge auf Ausstellung von EV-Zertifikaten zu genehmigen, die von anderen Zertifikats-Beantragern gestellt wurden.
3. **Vertragsunterzeichner (Contract Signer)**
Das zu einem EV-Zertifikat gehörende Subscriber Agreement muss von einem dazu berechtigten Vertragsunterzeichner unterzeichnet werden. Ein Vertragsunterzeichner ist eine natürliche Person, bei der es sich um einen Angestellten der antragstellenden Organisation oder einen Bevollmächtigten der Organisation handelt, der berechtigt ist, im Namen der Organisation Subscriber Agreements zu unterzeichnen.

Die antragstellende Organisation kann eine einzelne Person bevollmächtigen, eine, zwei oder alle drei Rollen einzunehmen, vorausgesetzt, dass Zertifikats-Bestätiger und Vertragsunterzeichner Angestellte der Organisation sind.

Ebenfalls zulässig ist es, eine Rolle mit mehreren Personen zu besetzen.

3.2 Prüfung der Zertifikatsdaten – Existenz und Identität von Organisationen

Vor der Ausstellung eines EV-Zertifikats überprüft TC TrustCenter die Korrektheit aller Angaben im Zertifikat gemäß den hier vorliegenden Zertifizierungsrichtlinien für EV-Zertifikate und gemäß den „Guidelines for the Issuance and Management of Extended Validation Certificates“.

Durch diese Prüfungen erfolgt:

- 1) Verifikation der Existenz und Identität der antragstellenden Organisation, inklusive
 - a) Verifikation der juristischen Existenz und Identität
 - b) Verifikation der physischen Existenz (Geschäftstätigkeit gekoppelt an physische Adresse)
 - c) Verifikation der operationalen Existenz (tatsächliche Geschäftstätigkeit)
- 2) Bei SSL-Zertifikaten Verifikation der Domainregistrierung des Domain-Namens oder der exklusiven Kontrolle über den Domain-Namen, der im EV-Zertifikat enthalten sein soll.
- 3) Verifikation der Autorisierung des Antragstellers für das EV-Zertifikat, beinhaltend:
 - a. Verifikation von Name, Titel und Autorisierung von Vertragsunterzeichner, Zertifikats-Bestätiger und Zertifikats-Beantrager
 - b. Verifikation, dass der Vertragsunterzeichner das Subscriber Agreement unterschrieben hat
 - c. Verifikation, dass der Zertifikats-Bestätiger den Zertifikats-Request signiert oder anderweitig genehmigt hat.

3.2.1 Verifikation der Existenz und Identität der antragstellenden Organisation

3.2.1.1 Privatwirtschaftliche Organisationen

- a) Juristische Existenz
Verifikation, dass es sich bei der Organisation um eine ordnungsgemäße und registrierte Kapitalgesellschaft oder Aktiengesellschaft handelt, die nicht als inaktiv, ungültig, gelöscht oder nicht aktuell gekennzeichnet ist.
- b) Name der Organisation
Verifikation, dass der Name der Organisation mit dem Eintrag im zuständigen Register und mit dem in das EV-Zertifikat aufzunehmenden Namen übereinstimmt.
- c) Registernummer
Überprüfung der Registernummer unter der die Organisation im zuständigen Register geführt wird. Wenn das Register keine Nummern vergibt, dann wird das Datum der Gründung der Organisation oder das Datum der Registrierung verwendet.
- d) Handlungsbevollmächtigter
Überprüfung der Identität eines Handlungsbevollmächtigten der Organisation oder der Adresse der offiziellen Geschäftsanschrift.

Die Angaben zur Verifikation der Punkte a) bis d) werden direkt von dem zuständigen behördlichen Register bezogen.

3.2.1.2 Behörden

- a) Juristische Existenz
Verifikation, dass es sich bei der Organisation um eine juristisch anerkannte Behörde handelt
- b) Name der Organisation
Verifikation, dass der Name der Organisation mit dem in das EV-Zertifikat aufzunehmenden Namen übereinstimmt.
- c) Registernummer
Behörden werden üblicherweise nicht in einem Register geführt. Falls ein solches Register existiert, erfolgt eine Überprüfung der Registernummer unter der die Behörde im zuständigen Register geführt wird, anderenfalls Überprüfung des Datums der Gründung der Behörde, das Datum der Registrierung der Behörde oder des Gesetzes-Paragrafen, der die Existenz der Behörde bestimmt.

Die Angaben zur Verifikation der Punkte a) bis c) kann erfolgen durch:

- (i) ein behördliches Informationssystem, welches speziell für derartige Auskünfte eingerichtet wurde,
- (ii) eine dem Antragsteller übergeordnete Behörde,
- (iii) einen aktiven Richter, in dessen Zuständigkeitsbereich die antragstellende Behörde fällt,
- (iv) einen Bevollmächtigten, der die Behörde repräsentiert.

3.2.1.3 Andere Organisationen

- a) Juristische Existenz
Verifikation, dass die Organisation unter dem im EV-Zertifikats-Antrag angegebenen Namen agiert.
- b) Name der Organisation
Verifikation, dass der Name der Organisation mit dem Eintrag im zuständigen Register und mit dem in das EV-Zertifikat aufzunehmenden Namen übereinstimmt.
- c) Registernummer
Überprüfung der Registernummer unter der die Organisation im zuständigen Register geführt wird. Wenn das Register keine Nummern vergibt, dann wird das Datum der Gründung der Organisation verwendet.
- d) Handlungsbevollmächtigter
Überprüfung der Identität eines Handlungsbevollmächtigten der Organisation gemäß Abschnitt 3.4.

Die Angaben zur Verifikation der Punkte a) bis d) werden direkt von dem zuständigen Register bezogen.

Zur Überprüfung der Identität des Handlungsbevollmächtigten ist dessen persönliches Erscheinen und die Vorlage eines gültigen amtlichen Lichtbildausweises erforderlich.

3.2.1.4 Nicht-kommerzielle Organisationen (Internationale Organisationen)

- a) Juristische Existenz
Verifikation, dass es sich bei der Organisation um eine juristisch anerkannte Internationale Organisation handelt.
- b) Name der Organisation
Verifikation, dass der Name der Organisation mit dem in das EV-Zertifikat aufzunehmenden Namen übereinstimmt.
- c) Registernummer
Verifikation des Datums der Gründung der Organisation oder die Bezeichnung des Gesetzes, welchem die Gründung der Organisation zugrunde liegt.

Die Angaben zur Verifikation der Punkte a) bis c) können verifiziert werden durch:

- (i) eine Referenz auf das konstituierende Dokument, mit dem die Organisation gegründet wurde.,
- (ii) direkte Bestätigung durch eine Regierungsbehörde des Staates, in dem die internationale Organisation ansässig ist,
- (iii) eine vom CAB Forum geführte Liste, in der internationale Organisationen aufgelistet sind.

Die Existenz und Identität eines Organs oder einer Teilorganisation einer internationalen Organisation kann durch die übergeordnete Organisation bestätigt werden.

3.2.2 Überprüfung der physischen Existenz einer Organisation

3.2.2.1 Geschäftsadresse

TC TrustCenter verifiziert, dass sich an der im Antrag angegebenen Geschäftsadresse tatsächlich Geschäftsräume der im Antrag genannten Organisation befinden.

Dazu überprüft TC Trustcenter, ob die im Antrag genannte Geschäftsadresse mit der im zuständigen (Handels-)Register (oder äquivalenten Informationsquelle, z.B. bei Behörden) genannten Adresse identisch ist.

Sollten die Adressen nicht übereinstimmen, wird die Existenz von Geschäftsräumen der antragstellenden Organisation an der im Antrag genannten Adresse durch einen Vor-Ort-Besuch verifiziert.

Alternativ kann die antragstellende Organisation eine anwaltliche Stellungnahme vorlegen, die bestätigt, dass sich die Geschäftsräume an der angegebenen Adresse befinden und die Geschäftstätigkeit auch von dort geführt wird.

Eine anwaltliche Stellungnahme muss immer vorgelegt werden, wenn sich die Geschäftsräume nicht in dem Land befinden, in dem die Organisation registriert ist oder gegründet wurde.

3.2.2.2 Telefonnummer

TC TrustCenter verifiziert die Telefonnummer, unter der die antragstellende Organisation in ihren Geschäftsräumen erreichbar ist.

Zu diesem Zweck ruft TC TrustCenter die angegebene Telefonnummer an und lässt sich telefonisch bestätigen, mit der richtigen Organisation verbunden zu sein.

Zusätzlich wird die Korrektheit der Telefonnummer bestätigt durch:

- Vergleich der angegebenen Telefonnummer mit den Angaben in einem öffentlichen Telefonverzeichnis der zuständigen Telefongesellschaft bzw. einer anderen geeigneten Informationsquelle oder
- Anruf bei der angegebenen Telefonnummer während eines Vor-Ort-Besuchs in den Geschäftsräumen und direkte Überprüfung, ob der Anruf tatsächlich in den Geschäftsräumen über eine Festnetzleitung (kein Mobiltelefon) entgegengenommen wird oder
- Vorlage einer anwaltlichen Stellungnahme.

Bei Behörden kann die Korrektheit der angegebenen Telefonnummer auch dadurch nachgewiesen werden, dass diese Telefonnummer in einem geeigneten öffentlichen behördlichen Informationssystem als die Telefonnummer der fraglichen Behörde geführt wird.

3.2.3 Überprüfung der Geschäftstätigkeit einer Organisation

Wenn die Organisation nicht seit mindestens 3 Jahren existiert und auch nicht in öffentlichen behördlichen Informationssystemen aufgelistet wird, muss eine Bestätigung eines anerkannten Finanzinstituts vorgelegt werden, die besagt, dass für die Organisation dort ein aktives Geschäftskonto besteht.

Alternativ kann eine anwaltliche Stellungnahme vorgelegt werden, die die Existenz eines aktiven Geschäftskontos bestätigt.

3.3 Prüfung der Zertifikatsdaten – Überprüfung des Domain-Namens

Um zu verifizieren, dass der Antragsteller den Domain-Namen, der im EV-SSL-Zertifikat angegeben werden soll, registriert hat oder die exklusive Kontrolle über den Domain-Namen hat, überprüft TC Trustcenter die folgenden Punkte:

1. Der Domain-Name muss bei einer von der Internet Corporation for Assigned Names and Numbers (ICANN) anerkannten Registrierungsstelle oder in einem von der Internet Assigned Numbers Authority (IANA) geführten Register registriert sein.
2. Die Registrierungs-Informationen in den WHOIS Datenbanken sollen öffentlich sein und Name, Adresse und administrativen Kontakt der Organisation enthalten.

Bei Behörden kann die Korrektheit des Domain-Namens auch dadurch nachgewiesen werden, dass dieser Domain-Name in einem geeigneten öffentlichen behördlichen Informationssystem als Domain-Name der betroffenen Behörde geführt wird.

3. Der Antragsteller muss
 - a. der registrierte Eigentümer des Domain-Namens sein oder
 - b. von dem registrierten Eigentümer des Domain-Namens das exklusive Nutzungsrecht für den Domain-Namen übertragen bekommen haben.
4. Dem Antragsteller muss bewusst sein, dass er den Domain-Namen registriert hat oder über das Nutzungsrecht verfügt.

3.4 Prüfung der Zertifikatsdaten – Existenz und Identität von Personen

Personen, die für die Ausstellung eines EV-Zertifikats identifiziert werden sollen, z.B. Handlungsbevollmächtigte für Organisationen, müssen zur Identitätsfeststellung persönlich erscheinen.

Berechtigt zur Identitätsfeststellung sind Mitarbeiter von TC TrustCenter, Notare und Rechtsanwälte.

3.4.1 Überprüfung der Existenz und Identität von Handlungsbevollmächtigten

3.4.1.1 Dokumente zur Identitätsfeststellung

Zur Identitätsfeststellung sind die folgenden Dokumente vorzulegen:

- 1) Persönliche Erklärung mit den folgenden Angaben:
 - a) Vollständiger Name
 - b) Wohnort
 - c) Geburtsdatum
 - d) Erklärung, dass alle Angaben in dem EV-Zertifikats-Request wahr und korrekt sind.

- 2) Gültiges, behördlich ausgestelltes Ausweisdokument mit Lichtbild und Unterschrift, wie
 - a) Reisepass
 - b) Personalausweis
 - c) In anderen Ländern anerkannte Ausweisdokumente, wie z.B.
 - i. Führerschein
 - ii. Militärausweis
- 3) Mindestens zwei weitere Dokumente, die den Namen der zu identifizierenden Person enthalten und so deren Identität bestätigen, eines davon von einem Finanzinstitut.
 - Dokumente von Finanzinstituten, die anerkannt werden beinhalten z.B.
 - a) Gültige Kreditkarte eines allgemein anerkannten Finanzinstituts mit Ablaufdatum
 - b) Gültige Bank- oder Scheckkarte eines anerkannten Finanzinstituts mit Ablaufdatum
 - c) Hypothekenauskunft, nicht älter als sechs Monate, von einem anerkannten Darlehensgeber
 - d) Bankauskunft, nicht älter als sechs Monate, von einem anerkannten Finanzinstitut
 - Andere Dokumente, die anerkannt werden beinhalten z.B.
 - a) Aktuelle Rechnung eines Versorgungsbetriebs mit Adressangabe (keine Rechnung für Mobiltelefon)
 - b) Aktuelle Bestätigung über Miet- oder Pachtzahlungen (nicht älter als sechs Monate)
 - c) Beglaubigte Geburtsurkunde
 - d) Steuerbescheinigung für das laufende Jahr
 - e) Beglaubigte Kopie eines Gerichtsbeschlusses (z.B. Scheidungsurkunde, Adoptionspapiere,...)

3.4.1.2 Tätigkeiten während der Identitätsfeststellung

Die Person, die die Identitätsfeststellung durchführt, muss:

- 1) Die Identität der zu identifizierenden Person sowie die eigenhändige Unterschrift der identifizierten Person unter der Erklärung aus Abschnitt 3.4.1.1 Nr. 1) bestätigen
- 2) Die zur Identitätsfeststellung vorgelegten Dokumente aus Abschnitt 3.4.1.1 Nr. 2) und 3) benennen
- 3) Auf einer Kopie des Ausweisdokuments aus Abschnitt 3.4.1.1 Nr. 2) bescheinigen, dass es sich bei der Kopie um eine vollständige, wirklichkeitsgetreue und fehlerfreie Widergabe des Originaldokuments handelt.

3.4.1.3 Überprüfung der Identitätsfeststellung

Wenn die Identitätsfeststellung nicht durch einen Mitarbeiter von TC TrustCenter durchgeführt worden ist, müssen TC Trustcenter zur Kontrolle die während der Identitätsfeststellung erstellten Dokumente vorgelegt werden:

- 1) Das Original der in Abschnitt 3.4.1.1 Nr. 1) abgegebenen Erklärung des Antragstellers inklusiver der Bestätigung aus Abschnitt 3.4.1.2 Nr. 1) zu dieser Erklärung.
- 2) Die Auflistung der zur Identitätsfeststellung vorgelegten Dokumente gemäß Abschnitt 3.4.1.2 Nr. 2)
- 3) Die beglaubigte Kopie des Ausweisdokuments gemäß Abschnitt 3.4.1.2 Nr. 3)

3.4.1.4 Überprüfung der Person, die die Identifizierung durchgeführt hat

TC TrustCenter überprüft, dass es sich bei der Person, die die Identitätsfeststellung durchgeführt hat, um einen am Wohnort der identifizierten Person zugelassenen Notar oder Rechtsanwalt handelt. Weiterhin überprüft TC TrustCenter, ob der Notar oder Rechtsanwalt die in Abschnitt 3.4.1.2 aufgeführten Tätigkeiten tatsächlich durchgeführt hat und die entsprechenden Bestätigungen abgegeben bzw. Beglaubigungen ausgestellt hat.

3.4.2 Überprüfung der Existenz und Autorisierung von Personen

3.4.2.1 Name, Titel und Tätigkeit von Vertragsunterzeichner und Zertifikats-Bestätiger

TC TrustCenter verifiziert Name, Titel und Tätigkeit des Vertragsunterzeichners und des Zertifikats-Bestätigers. TC TrustCenter kann dazu jede angemessene Methode verwenden, die sicherstellt, dass es sich bei der Person, die behauptet die jeweilige Rolle zu besetzen, auch tatsächlich um die um die benannte Person handelt.

Ob es sich bei dem Vertragsunterzeichner und/oder Zertifikats-Bestätiger um Mitarbeiter der Organisation handelt, lässt sich TC TrustCenter

- telefonisch oder per Post durch die Personalabteilung der Organisation oder
- eine anwaltliche Stellungnahme bestätigen.

Der Status des Zertifikats-Bestätigers als Mitarbeiter der Organisation kann alternativ durch den Vertragsunterzeichner bestätigt werden, vorausgesetzt, der Status des Vertragsunterzeichners konnte erfolgreich durch TC TrustCenter verifiziert werden.

3.4.2.2 Autorisierung von Vertragsunterzeichner und Zertifikats-Bestätiger

Die Zeichnungsberechtigung des Vertragsunterzeichners bzw. die Berechtigung des Zertifikats-Bestätigers, EV-Zertifikate zu beantragen, kann auf verschiedene Weise nachgewiesen werden:

- (i) Anwaltliche Stellungnahme
- (ii) Stellungnahme eines zugelassenen Wirtschaftsprüfers
- (iii) Erklärung der antragstellenden Organisation
- (iv) Vertrag zwischen TC TrustCenter und der Organisation, in dem die berechtigten Personen namentlich benannt sind
- (v) Vorherige vergleichbare Berechtigung.

Falls eine Organisation im Laufe der Zeit mehrere EV-Zertifikate benötigt, kann sie für in der Zukunft liegende Anträge einen oder mehrere Zertifikats-Bestätiger zur Beantragung von EV-Zertifikaten berechtigen.

3.5 Gründe, die der Ausstellung eines EV-Zertifikates entgegenstehen

TC TrustCenter prüft während des Antragsprozesses für EV-Zertifikate, ob sich die antragstellende Organisation oder einer der am Antragsprozess beteiligten Mitarbeiter der Organisation auf einer Sanktionsliste mit verbotenen Personen oder Organisationen befindet. Diese Liste beruht auf UN-Resolutionen zum Kampf gegen den internationalen Terrorismus einher-

gehend mit den Verordnungen EU 881/2002 und EU 2580/2001 der europäischen Union, die es untersagen, den gelisteten Personen Ressourcen zur Verfügung zu stellen.

Im Gegensatz zu länderabhängigen Sanktionen sind diese Regelungen an die Person gebunden - das Embargo „folgt“ also den Personen, unabhängig von deren Aufenthaltsort.

Weiterhin prüft TC TrustCenter, ob sich die antragstellende Organisation in einem Land befindet, mit dem TC TrustCenter gemäß seiner Exportrichtlinien keinen Handel treiben darf.

Ebenfalls verwendet werden die folgenden Listen des Bureau of Industry and Security des 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>

Ergibt eine der Prüfungen, dass die Ausstellung eines EV-Zertifikates den gesetzlichen Regelungen zufolge untersagt ist, so lehnt TC TrustCenter den Antrag auf Ausstellung eines EV-Zertifikats ab und stellt kein Zertifikat aus.

4 Revozierung von EV-Zertifikaten

TC TrustCenter betreibt einen ständig verfügbaren Revozierungsdienst, über den die Revozierung von EV-Zertifikaten jederzeit beantragt werden kann.

TC TrustCenter sperrt ein von TC Trustcenter ausgestelltes EV-Zertifikat beim Eintreten eines der folgenden Ereignisse:

- 1) Die Organisation, der das EV-Zertifikat gehört, verlangt die Revozierung.
- 2) Die Organisation, der das EV-Zertifikat gehört, erklärt, dass das EV-Zertifikat nicht ordnungsgemäß autorisiert wurde und eine nachträgliche Autorisierung nicht erwünscht ist.
- 3) TC TrustCenter erhält davon Kenntnis, dass der zu einem EV-Zertifikat passende geheime Schlüssel kompromittiert wurde oder anderweitig missbräuchlich genutzt wird.
- 4) TC TrustCenter erhält davon Kenntnis, dass der Eigentümer des EV-Zertifikats wesentliche Verpflichtungen des Subscriber Agreements nicht eingehalten hat.
- 5) TC TrustCenter erhält davon Kenntnis, dass ein Gericht oder Schlichter dem Eigentümer des EV-Zertifikats das Nutzungsrecht des Domain-Namens entzogen hat oder das Nutzungsrecht durch den Eigentümer des Zertifikats nicht verlängert wurde.
- 6) TC TrustCenter erhält davon Kenntnis, dass wesentliche Inhalte des EV-Zertifikats nicht mehr den Tatsachen entsprechen.
- 7) TC TrustCenter stellt fest, dass ein EV-Zertifikat nicht gemäß diesen Zertifizierungsrichtlinien oder gemäß den „Guidelines for the Issuance and Management of Extended Validation Certificates“ des CA/Browser Forums ausgestellt worden ist.
- 8) TC TrustCenter stellt fest, dass Angaben im EV-Zertifikat ungenau oder fehlerhaft sind.
- 9) TC TrustCenter stellt den Zertifizierungsbetrieb ein und keine andere EV-CA übernimmt den Revozierungsdienst für EV-Zertifikate.
- 10) TC TrustCenters Berechtigung zur Ausstellung von EV-Zertifikaten erlischt oder wird widerrufen und der Betrieb des Systems zur Statusprüfung von EV-Zertifikaten wird nicht fortgesetzt.
- 11) Der geheime CA-Schlüssel, der zum Ausstellen eines EV-Zertifikats verwendet wurde, ist kompromittiert.
- 12) TC TrustCenter erhält Kenntnis, dass der Eigentümer eines EV-Zertifikats auf eine für TC TrustCenter rechtverbindliche Liste der Personen oder Organisationen gesetzt worden ist, mit denen TC TrustCenter keinen Handel treiben darf, oder das Land, in dem die Organisation ansässig ist, wurde auf eine solche Liste gesetzt.
- 13) Kryptographische Algorithmen und/oder zugehörige Parameter sind durch technologische Fortschritte oder neue Entwicklungen in der Kryptologie unsicher geworden, so dass EV-Zertifikate gefälscht werden können.
- 14) Weitere Revozierungsgründe, die TC TrustCenter in seinen Zertifizierungsrichtlinien veröffentlicht.

Sperrung von Zertifikaten die Schadcode signieren

Als Schadcode wird solcher Code verstanden, der schädliche Funktionen enthält und Schwachstellen ausnutzt. Unter diesen Begriff fallen z-B. Spyware, Malware und andere Programme, die sich ohne Einverständnis des Nutzers installieren und/oder sich ihrer Entfernung widersetzen. Weiterhin fällt unter diesen Begriff Code, der auf eine Weise ausge-

nutzt werden kann, die vom Hersteller nicht beabsichtigt worden ist und die Vertrauenswürdigkeit der zugrundeliegenden (Betriebssystem-) Plattform untergräbt.

Erhält TC TrustCenter nachvollziehbare und plausible Hinweise, dass ein mit einem EV Code Signing Zertifikat signiertes Code Objekt Schadcode enthält, so wird TC Trustcenter die Korrektheit dieser Hinweise prüfen. Ergibt die Prüfung, das Ergebnis, dass es sich tatsächlich um Schadcode handelt, so wird TC TrustCenter das entsprechende EV Code Signing Zertifikat sperren.

5 Zeichensatz und Konversionsregeln

Die X.509 konformen Zertifikate enthalten in den dafür vorgesehenen Feldern den Distinguished Name des Herausgebers und des Zertifikatsinhabers. Es wird der folgende Zeichensatz unterstützt:

Grossbuchstaben	A .. Z
Kleinbuchstaben	a .. z
Zahlen	0 .. 9
Apostroph	'
Klammer auf	(
Klammer zu)
Plus	+
Komma	,

Bindestrich	-
Punkt	.
Schrägstrich	/
Doppelpunkt	:
Gleichzeichen	=
Fragezeichen	?
Leerzeichen	

Da dieser Zeichensatz beschränkt ist, die Zertifizierungsrichtlinien der TC TrustCenter GmbH jedoch die Schreibweise entsprechend Ausweisdokument bzw. Handelsregisterauszug vorschreiben, gibt es Konversionsregeln für ‚nicht darstellbare‘ Zeichen.

TC TrustCenter empfiehlt, die im Folgenden dargestellten Konversionsregeln einzuhalten, weil anderenfalls die ordnungsgemäße Funktion der Zertifikate im Zusammenhang mit weiteren Komponenten nicht sichergestellt ist. So kann es z.B. nicht ausgeschlossen werden, dass einige der in einer PKI eingesetzten Komponenten, wie etwa ältere Browser, Umlaute fehlerhaft interpretieren.

5.1 Konversion von Zeichen

- Umlaute (Ä, Ö, Ü, ä, ö, ü) sollten durch die jeweiligen nicht-diakritischen Zeichenfolgen (Ae, Oe, Ue, ae, oe, ue) unter Berücksichtigung der Gross-/Kleinschreibung ersetzt werden.

Beispiele:

Original	Konvertiert
Müller	Mueller
Überstorf	Ueberstorf

- Buchstaben und Zeichen, die gemäß den zu prüfenden Unterlagen nicht im unterstützten Zeichensatz enthalten sind, sollten den ihnen am besten entsprechenden Zeichen zugeordnet werden.

Beispiele:

Original	Konvertiert
René	Rene
François	Francois

- Sonderzeichen, die gemäß den zu prüfenden Unterlagen nicht im unterstützten Zeichensatz enthalten sind, und für die es dort keine direkte Entsprechung gibt, sollten ausgeschrieben oder sinngemäß abgekürzt oder ersetzt werden.

Beispiele:

Original	Konvertiert
Meier & Meier GmbH	Meier und Meier GmbH
Meier & Meier GmbH	Meier u. Meier GmbH
Meier & Meier GmbH	Meier + Meier GmbH