TC TrustCenter-Zertifizierungsrichtlinien

Fassung vom 22. Januar 2010

Inhaltsverzeichnis

1 Einleitung

Dieses Dokument beschreibt die Zertifizierungsrichtlinien von TC TrustCenter. Der Sinn dieses Dokumentes ist es, eine Einschätzung der Vertrauenswürdigkeit der durch TC TrustCenter ausgestellten Zertifikate zu ermöglichen.

Ein Zertifikat ist eine elektronische Bescheinigung, mit der ein öffentlicher kryptographischer Schlüssel einer Person oder Organisation zugeordnet wird und mit der die Identität der Person oder Organisation bestätigt wird. Ein Zertifikat stellt also eine Verbindung zwischen einer Person oder Organisation und einem kryptographischen Schlüssel her.

Jedes Zertifikat ist nur so vertrauenswürdig wie die Verfahren, nach denen es ausgestellt wird. TC TrustCenter teilt dazu Zertifikate in „Zertifikatsklassen“ ein. Je höher die Zertifikatsklasse, desto umfangreichere Identifikationsprüfungen liegen der Ausstellung eines Zertifikates zu Grunde. Die Zertifikate selbst enthalten als Information für diejenigen, die sich auf diese Zertifikate verlassen wollen, die Angabe über die Klasse des Zertifikats. Welche Prüfungen hinter einer Zertifikatsklasse stehen, kann diesen Zertifizierungsrichtlinien entnommen werden.

Die Zertifizierungsrichtlinien beschreiben das Verfahren, nach welchem TC TrustCenter als Zertifizierungsdiensteanbieter (Certification-Authority) die Identifizierung von Zertifikatsinhabern durchführt. Das Dokument erläutert sowohl für Antragsteller bzw. Zertifikatsinhaber sowie für Dritte die Einteilung der Zertifikate in die verschiedenen Zertifikatsklassen. Dadurch wird ermöglicht, anhand dieser Klassifikation eine Entscheidung darüber zu treffen, ob das von einem Inhaber präsentierte Zertifikat den Anforderungen der eingesetzten Anwendung genügt. Beide Parteien, häufig auch „Subscriber“ (Zertifikatsinhaber) und „Relying Party“(sich auf die Vertrauenswürdigkeit eines Zertifikats verlassende Partei) genannt, werden mit dem Begriff „Teilnehmer“ zusammengefasst.

Im Rahmen der Einteilung in die Zertifikatsklassen wird zwischen natürlichen Personen und Organisationen unterschieden. Zertifikate für Personen, die keine Angabe zu einer Organisation machen, enthalten demgemäß auch keine Angaben zu Organisationen, denen der Zertifikatsinhaber angehört. Im Gegensatz dazu enthalten Organisationszertifikate Angaben zu einer Organisation. Sie können entweder nur der Organisation – z. B. bei Zertifikaten für Web-Server, in denen keine natürliche Person genannt wird – oder aber einem Mitglied einer Organisation zugeordnet sein, also beispielsweise dem Mitarbeiter eines Unternehmens. Die Informationen zur Organisation müssen bei Organisationszertifikaten in allen Fällen in das Zertifikat aufgenommen werden.

Zusammen mit der Einteilung der Zertifikatsklassen (Abschnitt 4) werden Hinweise zur persönlichen Identitätsfeststellung gegeben. Die persönliche Identitätsfeststellung ist für einige Zertifikatsklassen notwendig, um das Vertrauen in die Bindung zwischen Zertifikat und Zertifikatsinhaber zu stärken.

Danach werden Richtlinien zur Wahl eines (Zertifikat-) Namens erläutert (Abschnitt 5). Dieser besteht häufig nur aus Name und E-Mail-Adresse des Inhabers, kann aber auch Angaben zur Organisation und deren Sitz oder aber zum Wohnsitz des Zertifikatsinhabers enthalten. Zur Veranschaulichung sind im Abschnitt 5 Beispiele für geeignete Namen beigefügt.

Anschließend wird erläutert, wie TC TrustCenter die im Zertifikat enthaltenen Informationen überprüft (Abschnitt 6). Nicht alle in einem Zertifikat enthaltenen Daten werden notwendigerweise überprüft. Jede Person, die sich auf ein Zertifikat von TC TrustCenter verlassen will, kann anhand einer Tabelle (siehe Seite 19) nachvollziehen, welche Angaben bei welcher Zertifikatsklasse auf welche Weise geprüft werden.

Schließlich wird dargestellt, aus welchem Anlass und auf welche Weise ein Zertifikat zu sperren ist (Abschnitt 7).

Informationen zu Produkten und Dienstleistungen können unserem Internet-Angebot entnommen werden.

Beachten Sie bitte unbedingt den nachstehenden Abschnitt „Wichtige Hinweise“!

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 Marktbedürfnisse: Aufgrund der sich stetig ändernden Marktanforderungen ist es unvermeidbar, dass die Dienste der Zertifizierungsstelle den konkreten Bedürfnissen der Kunden angepasst werden. Die Zertifizierungsrichtlinien werden dementsprechend regelmäßig überarbeitet.

Deutsche Fassungen sind maßgebend: Einige der Dokumente und Web-Seiten 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.

2 Wichtige Hinweise

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.

Je höher die Zertifikatsklasse, desto höher die Vertrauenswürdigkeit: Alle von TC TrustCenter angebotenen Zertifikate werden in eine „Level of Trust"-Klasse eingeordnet, welche die grundsätzliche Art der Überprüfung der Inhalte der Zertifikate und der Identitätsfeststellung der Zertifikatsinhaber beschreibt. Anhand der Klasse eines vorgelegten Zertifikats kann auf einfache Weise die Vertrauenswürdigkeit der im Zertifikat angegebenen Inhalte abgeschätzt werden: Je höher die Zertifikatsklasse, desto höher die Vertrauenswürdigkeit. Die Sicherheit der Verschlüsselung und damit der Vertraulichkeit ist hiervon nicht betroffen.

Keine Prüfung von Kreditwürdigkeit: TC TrustCenter prüft die Korrektheit der in Zertifikaten angegebenen Identität auf die in diesem Dokument beschriebene Weise. Es werden keinerlei Prüfungen über Liquidität, Kreditwürdigkeit oder dergleichen durchgeführt. Zertifikate schaffen Vertrauen darin, dass der Zertifikatsinhaber tatsächlich derjenige ist, der er vorgibt zu sein. Sie geben keinerlei Hinweise auf die Vertrauenswürdigkeit des Zertifikatsinhabers selbst.

Keine Prüfung der Unbedenklichkeit von Software: TC TrustCenter stellt u. a. spezielle 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. Auch bei der Verlängerung eines Zertifikats werden die Daten keiner erneuten Prüfung unterzogen. 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: TC TrustCenter bietet Zertifikate verschiedener Klassen an, die den Grad an Vertrauenswürdigkeit in die Zertifikate beschreiben. Jeder Teilnehmer des Zertifizierungsdienstes muss selbst entscheiden, ob eine bestimmte Zertifikatsklasse 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 anzueignen.

Sorgfalts- und Mitwirkungspflicht des Zertifikatsinhabers: Der Zertifikatsinhaber muss zur Sicherheit der Verfahren beitragen. Dazu sind die in diesen Richtlinien enthaltenen Sorgfalts- und Mitwirkungspflichten zu beachten.

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.

3 Versionsänderungen

3.1 Änderungen zur Version vom 1. Oktober 1999

- TC TrustCenter stellt auch Zertifikate für WAP-Gateways (WTLS) aus.
- Die Anforderungen von Class 3 für Organisationen sind im Vergleich zu der vorherigen Version kundenfreundlicher gestaltet worden: Die persönliche Identitätsfeststellung eines im beglaubigten Handelsregisterauszug aufgeführten (oder anhand vergleichbarer Dokumente legitimierten) Vertretungsberechtigten der Organisation ist nicht mehr erforderlich. Statt dessen kann ein Vertretungsberechtigter der Organisation schriftlich eine Person benennen (PKI-Administrator), die für die Verwaltung der organisationsbezogenen Zertifikate zuständig ist. Diese Person muss dann persönlich identifiziert werden.
- Die Identitätsfeststellung des Zertifikatsinhabers ist für Class 3-Zertifikate stets erforderlich und kann entweder in einem TC TrustCenter IdentPoint®, über das Post Ident®-Verfahren oder im autorisierten IdentPoint® nach den Richtlinien zur Identitätsfeststellung von TC TrustCenter vorgenommen werden.
- Zusätzlich zur Überprüfung der Daten anhand eines (beglaubigten) Auszuges aus einem zuständigen amtlichen Register ist die Möglichkeit geschaffen worden, die Verifizierung über vertrauenswürdige und allgemein als Referenz von TC TrustCenter akzeptierte Adress- oder Wirtschafts-Datenbanken Dritter vorzunehmen.
- Im Rahmen der Reorganisation der Zertifikats-Klassenstruktur sind die Class 4-Zertifikate entfallen. Die vor Inkrafttreten dieser Zertifizierungsrichtlinien ausgestellten Class 4-Zertifikate entsprechen den zum Zeitpunkt ihrer Ausstellung gültigen Zertifizierungsrichtlinien.

3.2 Änderungen zur Version vom 12. Juni 2002

- Für Class 2 Zertifikate werden jetzt auch Fax-Kopien anerkannt.

  Bei der Zusendung von Unterlagen, insbesondere international, entstehen häufig unerwünscht lange Brieflaufzeiten.

  Um Kunden die Möglichkeit zu bieten, Class 2 Zertifikate zeitnah zu erwerben, werden Dokumente, die als Fax zugestellt werden, von TC TrustCenter anerkannt.

  Das bedeutet, dass an allen Stellen in diesen Zertifizierungsrichtlinien, an denen die Vorlage der Kopie eines Dokumentes gefordert wird, ein Fax zulässig ist.

- Registerauszüge werden in 3 Altersklassen eingeteilt.

  Registerauszüge, die nicht älter als 9 Monate sind, werden ohne weiteres als aktuell anerkannt. Bei Registerauszügen, die zwischen 9 Monaten und 36 Monaten alt sind, muss zusätzlich eine Bestätigung eines Zeichnungsberechtigten vorgelegt werden, die beinhaltet, dass Name und Rechtsform der Organisation immer noch mit den Daten des vorge-

legten Auszugs übereinstimmen. Registerauszüge, die älter als 36 Monate sind, werden nicht akzeptiert.

- TC TrustCenter stellt jetzt auch Team-Zertifikate und Funktionszertifikate aus.

  Ein Team-Zertifikat kann von einer Gruppe von Personen genutzt werden (z.B. einer Abteilung), es wird aber trotzdem formal einer Person zugeordnet, die für die Gruppe von Personen verantwortlich zeichnet (z.B. Abteilungsleiter).

  Funktionszertifikate sind Zertifikate, die für einen ausgewählten Zweck (z.B. Signatur von Rechnungen) üblicherweise einem Rechner oder einer Applikation fest zugeordnet werden. Der Rechner oder die Applikation können das Zertifikat dann nutzen, um automatisch eine Vielzahl von Signaturen zu erstellen.

- Die Ausstellung von PGP-Zertifikaten außerhalb geschlossener Benutzergruppen wurde eingestellt.

3.3 Änderungen zur Version vom 15. Juli 2004

- TC TrustCenter stellt jetzt auch Wildcard-Zertifikate aus. Wildcard-Zertifikate enthalten anstelle eines Servernamens das Zeichen „*“, welches als Platzhalter für mehrere verschiedene Servernamen dient. Ein Wildcard-Zertifikat schützt somit gleich mehrere Websites. Für Organisationen, die eine einzelne Domain besitzen, innerhalb dieser Domain aber mehrere Server betreiben, ist ein Wildcard-Zertifikat eine effiziente Lösung, weil zum Schutz mehrerer Server nur ein Zertifikat verwaltet werden muss.
- TC TrustCenter behält sich das Recht vor, Zertifikate zu sperren, die missbräuchlich und/oder zu strafbaren Zwecken verwendet werden.

3.4 Änderungen zur Version vom 23. Oktober 2006

- TC TrustCenter stellt jetzt auch Publisher IDs aus. Eine Publisher ID ist ein Zertifikat, welches von Softwareentwicklern verwendet wird, um sich auf einem Portal (z.B. eines Hardware- oder Betriebssystemherstellers) zu authentifizieren oder um entwickelten Code zu signieren. Bei Publisher IDs wird im Common Name Feld des Zertifikates der Organisationsname oder der individuelle Name des Software-Entwicklers angegeben.
- Die bisherigen CodeSigning-Zertifikate werden in dem Produkt Publisher ID mit erfasst.
- Die Ausstellung von WTLS Zertifikaten wurde eingestellt.

4 Zertifikatsklassen

Die Vertrauenswürdigkeit von Zertifikaten hängt von den Verfahren ab, nach denen sie ausgestellt werden. Diese Verfahren werden in Richtlinien definiert. Alle von TC TrustCenter angebotenen Zertifikate werden in eine „Level of Trust"-Klasse eingeordnet, die die grundsätzliche Art der Überprüfung der Inhalte des Zertifikats und der Identitätsfeststellung des Zertifikatsinhabers festlegt. Je höher die Zertifikatsklasse, desto umfangreichere Identitätsprüfungen liegen der Ausstellung eines Zertifikates zu Grunde.

Die Sicherheit der Verschlüsselung und damit der Schutz der elektronischen Kommunikation gegen unbefugte Kenntnisnahme ist von den verwendeten kryptographischen Verfahren und Schlüssellängen abhängig und nicht von der Zertifikatsklasse. Er ist bei der Verwendung von Class 1-Zertifikaten in gleichem Maße wie bei Class 2- oder Class 3-Zertifikaten (bei identischer Schlüssellänge) gewährleistet.

Die Zertifikate selbst enthalten als Information für diejenigen, die sich auf dieses Zertifikat verlassen wollen (Relying Party), eine Angabe über die Klasse des Zertifikats. Anhand der Klasse eines vorgelegten Zertifikats kann so auf einfache Weise die Vertrauenswürdigkeit der darin angegebenen Inhalte abgeschätzt werden. Welche Prüfungen hinter einer Zertifikatsklasse stehen, wird in diesen Zertifizierungsrichtlinien dargestellt.

Die in den folgenden Abschnitten aufgeführten Erklärungen zu den vorgenommenen Überprüfungen beziehen sich auf die Daten, die in den Zertifikaten enthalten sind.

Zusätzlich zu diesen Prüfungen, welche die Angaben im Zertifikat selbst betreffen, werden bei Zertifikaten, die für Organisationen ausgestellt werden, weitere Prüfungen vorgenommen. Diese Prüfungen dienen in erster Linie dem Nachweis, dass der Zertifikats-Antragsteller tatsächlich über eine Berechtigung zur Beantragung von Zertifikaten verfügt.

Dieser Nachweis (Antragsbestätigung) kann durch eine dazu berechtigte Person der Organisation schriftlich, per E-Mail oder per Fax erfolgen. Alternativ kann TC TrustCenter die Berechtigung zur Zertifikats-Beantragung durch eine telefonische Überprüfung verifizieren.

4.1 Class 0-Zertifikate

TC TrustCenter stellt auf Antrag Zertifikate für Test- und Demonstrationszwecke aus, die standardmäßig eine verkürzte Gültigkeitsdauer haben.

Die Angaben in Class 0-Zertifikaten werden von TC TrustCenter keinerlei Prüfung unterzogen!

4.2 Class 1-Zertifikate

Class 1-Zertifikate beinhalten immer eine E-Mail-Adresse. Class 1-Zertifikate bestätigen, dass die im Zertifikat angegebene E-Mail-Adresse zum Zeitpunkt der Antragstellung existiert hat, und der Besitzer des zugehörigen privaten Schlüssels Zugriff auf diese E-Mail-Adresse hatte.

Class 1 Zertifikate stellen damit einen nur sehr geringen Nachweis der Identität des Zertifikatinhabers dar. Die Angaben des Teilnehmers in einem Class 1-Zertifikat werden über einen einfachen Zugrifftest auf die E-Mail-Adresse hinaus in keiner Weise überprüft.

4.3 Class 2-Zertifikate

4.3.1 Überprüfung der Angaben über natürliche Personen

Angaben in Class 2-Zertifikaten über natürlichen Personen, wenn solche enthalten sind, werden wie folgt geprüft:

- Wenn im Zertifikat eine E-Mail-Adresse angegeben ist, wird deren Korrektheit durch einen Zugriffstest überprüft. Alternativ kann auch ein Verantwortlicher der im O-Feld angegebenen Organisation (falls vorhanden) die Korrektheit der E-Mail-Adresse von Organisationsmitgliedern bestätigen.
- Namensangaben zu einer natürlichen Person werden verifiziert durch

  a) Zusicherung durch von TC TrustCenter zugelassene Dritte über die Richtigkeit und Vollständigkeit der Daten

  oder durch

  b) Bestätigung der Angaben durch Vorlage der Kopie eines amtlichen Lichtbildausweises mit Unterschriftszug.

4.3.2 Überprüfung der Angaben über Organisationen

Angaben in Class 2-Zertifikaten über Organisationen werden wie folgt geprüft:

- Name und Sitz der Organisation werden überprüft. Diese Überprüfung kann durch Vorlage einer Kopie eines Dokumentes erfolgen, welches die Existenz der Organisation zum Zeitpunkt der Antragstellung nachweist (Auszug aus einem zuständigen amtlichen Register, in dem die Organisation geführt wird bzw. vergleichbare Dokumente).

  Registerauszüge, die nicht älter als 9 Monate sind, werden als aktuell anerkannt.

  Bei Registerauszügen, die zwischen 9 Monaten und 36 Monaten alt sind, muss zusätzlich zu einer Kopie des Auszugs eine Bestätigung vorgelegt werden, die eine Aussage darüber beinhaltet, dass Name und Rechtsform der Organisation immer noch mit den Daten des vorgelegten bzw. vorliegenden Auszugs übereinstimmen. Die erneute Zusendung der Kopie eines Registerauszugs kann entfallen, wenn diese TC TrustCenter bereits vorliegt.

  Die Bestätigung muss auf dem Geschäftspapier der Organisation erfolgen und von einem Zeichnungsberechtigten handschriftlich unterschrieben werden. Eine Zusendung der Bestätigung kann auch per Fax oder E-Mail erfolgen. Eine E-Mail muss mit einem Zertifikat signiert werden, das mindestens den Anforderungen an ein TC Class 2 Zertifikat genügt. Registerauszüge, die älter als 36 Monate sind, werden nicht akzeptiert.

  Behörden werden üblicherweise nicht in einem Register geführt. Die Existenz und die richtige Bezeichnung von Behörden muss deshalb durch eine zuständige (z.B. übergeordnete oder aufsichtführende) Behörde auf offiziellem Briefpapier, versehen mit dem behördlichen Dienstsiegel oder Dienststempel und unterzeichnet von einer berechtigten Amtsperson, nachgewiesen werden.

  Alle Überprüfungen können auch anhand von Datenbanken vertrauenswürdiger Anbieter erfolgen.

  Wenn ein Antragsteller mehrere Zertifikate benötigt, diese aber nicht zum selben Zeitpunkt ausgestellt bekommen möchte, kann TC TrustCenter zum Zeitpunkt der Registrierung oder später Vorab-Überprüfungen von Zertifikatsdaten vornehmen. Der eigentliche Antrag für ein Zertifikat geht dann erst später ein, die Prüfergebnisse liegen aber schon

vor. Zum Zeitpunkt der Ausstellung des Zertifikates darf die zugehörige Vorab-Überprüfung nicht länger als 13 Monate zurückliegen.

- Die Korrektheit einer E-Mail-Adresse (wenn im Zertifikatsantrag angegeben) kann bei Organisationen und Organisationsmitgliedern durch einen Verantwortlichen der angegebenen Organisation bestätigt werden, so dass ein Zugriffstest in diesem Fall optional ist.
- Weitere Zertifikatsdaten werden soweit möglich überprüft. So wird z.B. bei Geräte-Zertifikaten die Registrierung der angegebenen Domain auf die im Zertifikatsantrag genannte Organisation überprüft, falls es sich um eine registrierungsfähige Domain handelt.

  Unter dem Begriff „Gerät“ werden dabei sowohl reale Objekte verstanden, die physikalisch als Hardware existieren (z.B. Server-Rechner, Mail-Gateways, Drucker, Smartphones etc.) als auch logische Objekte, die nicht physikalisch existieren (z.B. virtuelle Maschinen).
- Handelt es sich nicht um eine registrierungsfähige Domain, muss durch eine dazu berechtigte Person bestätigt werden, dass ein Gerät mit dem fraglichen Namen im internen Rechnernetz existiert und ein Zertifikat für dieses Gerät ausgestellt werden soll.

  Damit die Zuordnung von Zertifikaten zu Geräten eindeutig bleibt, behält TC TrustCenter sich vor, Anträge mit bereits von anderen Organisationen verwendeten internen Domainnamen abzulehnen.

  Zertifikate, die von einer Organisation nur intern genutzt werden, und deren Domainname nicht registrierungsfähig ist, z.B. domain.local oder domain.internal, müssen im Domainnamen eine Angabe enthalten, mit der das Zertifikat einer Organisation eindeutig zugeordnet werden kann.

  Ein Zertifikat für client-1.intranet.example erlaubt keine geeignete Zuordnung zu einer Organisation und ist aus diesem Grund nicht zulässig. Ein Zertifikat für client-1.stonehillbaker-intranet.local oder für client-1.shb-intranet.example erlaubt dagegen eine Zuordnung zu einer Organisation und ist daher zulässig.

  TC TrustCenter trägt dafür Sorge, dass Zertifikate mit identischen internen Namen nicht an unterschiedliche Organisationen ausgestellt werden. Hat also die Organisation Stonehillbaker ein Zertifikat für die (interne) Domain shb-intranet.example erhalten, so kann keine andere Organisation Zertifikate mit diesem Domainnamen bekommen.

- Eine Vorab-Prüfung der Domain-Registrierung ist möglich. Wenn das Zertifikat ausgestellt wird, darf die zugehörige Vorab-Überprüfung nicht länger als 13 Monate zurückliegen.
- Ein Team-Zertifikat kann von einer Gruppe von Personen genutzt werden (z.B. einer Abteilung), es wird aber trotzdem formal einer Person zugeordnet, die für die Gruppe von Personen verantwortlich zeichnet (z.B. Abteilungsleiter). Diese Person ist verantwortlich für den ordnungsgemäßen Einsatz des Zertifikats und wird gemäß den Richtlinien für Class 2 Zertifikate identifiziert.
- Funktionszertifikate sind Zertifikate, die für einen ausgewählten Zweck (z.B. Automatische Mail Signatur) üblicherweise einem Rechner oder einer Applikation fest zugeordnet werden. Der Rechner oder die Applikation können das Zertifikat dann nutzen, um automatisch eine Vielzahl von Signaturen zu erstellen. Die Funktionsbezeichnungen müssen von TC TrustCenter vor der Verwendung freigegeben werden. Formal wird dieses Zertifikat einer Person zugeordnet, die gegenüber TC TrustCenter als verantwortlich für den ordnungsgemäßen Einsatz des Zertifikats zeichnet. Diese für das Zertifikat verantwortliche Person wird dann gemäß den Richtlinien für Class 2 Zertifikate identifiziert.

4.3.3 Überprüfung der Angaben über die Beziehung der natürlichen Person zur Organisation

- Die Zugehörigkeit der Person, für die das Zertifikat beantragt wird, zu der angegebenen Organisation, gegebenenfalls auch zu einer Abteilung der Organisation, muss durch ein dazu berechtigtes Mitglied der Organisation bestätigt werden. Diese Bestätigung muss entweder handschriftlich unterschrieben und mit einem Firmenstempel versehen sein (bei Behörden mit einem Dienstsiegel) oder digital signiert sein. Die Zusendung der Bestätigung kann per Fax oder E-Mail erfolgen. Eine E-Mail muss mit einem TC Class 2 (mit Überprüfung der Angaben gemäß 4.3.1 b)), TC Class 3, einem spezielles Zertifikat für PKI-Administratoren oder einem qualifizierten Zertifikat gemäß Signaturgesetz digital signiert werden.

  Alternativ dazu kann die Zugehörigkeit der im Zertifikat genannten Person zu der angegebenen Organisation durch eine telefonische Überprüfung verifiziert werden.

4.4 Class 3-Zertifikate

4.4.1 Überprüfung der Angaben über natürliche Personen

Die Überprüfung der Angaben über natürliche Personen umfasst die folgenden Punkte:

- Wenn im Zertifikat eine E-Mail-Adresse angegeben ist, wird deren Korrektheit durch einen Zugriffstest überprüft. Alternativ kann auch ein Verantwortlicher der im O-Feld angegebenen Organisation (falls vorhanden) die Korrektheit der E-Mail-Adresse von Organisationsmitgliedern bestätigen.
- Wenn eine natürliche Person im Class 3-Zertifikat genannt ist, ist das persönliche Erscheinen dieser Person und die Vorlage eines gültigen amtlichen Lichtbildausweises erforderlich. Die Überprüfung der Identität des Zertifikatsinhabers kann entweder bei einer Postfiliale über das Post Ident®-Verfahren, bei einem TC TrustCenter-IdentPoint® (einem autorisierten IdentPoint® der Organisation) oder bei einem anderen zur Identitätsfeststellung autorisierten Repräsentanten von TC TrustCenter erfolgen.
- Für die Identitätsfeststellung werden nur amtliche Ausweisdokumente akzeptiert, die ein Lichtbild und den Unterschriftszug des Ausweisinhabers aufweisen. In der Bundesrepublik Deutschland zählen dazu neben dem Personalausweis und dem Reisepass auch solche Ausweisdokumente, die den Anforderungen des § 1 Abs. 2 Gesetz über Personalausweise bzw. den Anforderungen des § 4 Abs. 1 Passgesetz entsprechen.

  International werden solche Ausweisdokumente anerkannt, die

  - in dem jeweiligen Staat von einer Behörde ausgestellt worden sind und
  - im internationalen Rechtsverkehr als Ausweisdokumente anerkannt werden.

4.4.2 Überprüfung der Angaben über Organisationen

Bei einem Zertifikat für eine Organisation erfolgt eine Überprüfung der folgenden Punkte:

- Name und Sitz der Organisation. Für Class 3-Zertifikate ist je nach Organisation die Vorlage eines Auszugs aus dem zuständigen amtlichen Register bzw. eines vergleichbaren Dokumentes erforderlich. Wichtig ist, dass aus dem Dokument hervorgeht, dass die Organisation gegenwärtig tatsächlich existiert. Die vorgelegten Dokumente sollen aktuell und beglaubigt sein oder im Original vorliegen. Sollte weder die Vorlage eines Originals noch einer beglaubigten Kopie möglich sein, werden durch das Security Management von TC TrustCenter andere Prüfungen vorgenommen.

  Registerauszüge, die nicht älter als 9 Monate sind, werden als aktuell anerkannt.

Bei Registerauszügen, die zwischen 9 Monaten und 36 Monaten alt sind, muss zusätzlich zu dem Auszug eine Bestätigung eines Zeichnungsberechtigten vorgelegt werden, die eine Aussage darüber beinhaltet, dass Name und Rechtsform der Organisation immer noch mit den Daten des vorgelegten bzw. vorliegenden Auszugs übereinstimmen. Die erneute Zusendung eines Registerauszugs kann entfallen, wenn dieser TC TrustCenter bereits vorliegt.

Die Bestätigung muss auf dem Geschäftspapier der Organisation erfolgen und von einem Zeichnungsberechtigten handschriftlich unterschrieben werden. Eine Zusendung der Bestätigung kann auch per Fax oder E-Mail erfolgen. Eine E-Mail muss mit einem TC Class 2, TC Class 3, einem spezielles Zertifikat für PKI-Administratoren oder einem qualifizierten Zertifikat gemäß Signaturgesetz digital signiert werden.

Registerauszüge, die älter als 36 Monate sind, werden nicht akzeptiert.

Der Nachweis der Existenz von Behörden erfolgt wie bei Class 2 Zertifikaten.

- Weitere Zertifikatsdaten werden soweit möglich überprüft. So wird z.B. bei Geräte-Zertifikaten die Registrierung der angegebenen Domain auf die im Zertifikatsantrag genannte Organisation überprüft, falls es sich um eine registrierungsfähige Domain handelt.
- Handelt es sich nicht um eine registrierungsfähige Domain, muss durch eine dazu berechtigte Person bestätigt werden, dass ein Gerät mit dem fraglichen Namen im internen Rechnernetz existiert und ein Zertifikat für dieses Gerät ausgestellt werden soll.

  Damit die Zuordnung von Zertifikaten zu Geräten eindeutig bleibt, behält TC TrustCenter sich vor, Anträge mit bereits von anderen Organisationen verwendeten internen Domainnamen abzulehnen.

  Zertifikate, die von einer Organisation nur intern genutzt werden, und deren Domainname nicht registrierungsfähig ist, z.B. domain.local oder domain.internal, müssen im Domainnamen eine Angabe enthalten, mit der das Zertifikat einer Organisation eindeutig zugeordnet werden kann.

  Ein Zertifikat für client-1.intranet.example erlaubt keine geeignet Zuordnung zu einer Organisation und ist aus diesem Grund nicht zulässig. Ein Zertifikat für client-1.stonehillbaker-intranet.local oder für client-1.shb-intranet.example erlaubt dagegen eine Zuordnung zu einer Organisation und ist daher zulässig.

  TC TrustCenter trägt dafür Sorge, dass Zertifikate mit identischen internen Namen nicht an unterschiedliche Organisationen ausgestellt werden. Hat also die Organisation Stonehillbaker ein Zertifikat für die (interne) Domain shb-intranet.example erhalten, so kann keine andere Organisation Zertifikate mit diesem Domainnamen bekommen.
- Eine Vorab-Prüfung der Domain-Registrierung ist möglich. Wenn das Zertifikat ausgestellt wird, darf die zugehörige Vorab-Überprüfung nicht länger als 13 Monate zurückliegen.
- Eine automatische Überprüfung der Existenz einer Abteilung in einer Organisation (die z.B. im OU-Feld von Zertifikaten angegeben werden kann) ist in der Regel nicht möglich.
- Ein Team-Zertifikat kann von einer Gruppe von Personen genutzt werden (z.B. einer Abteilung), es wird aber trotzdem formal einer Person zugeordnet, die für die Gruppe von Personen verantwortlich zeichnet (z.B. Abteilungsleiter). Diese Person ist verantwortlich für den ordnungsgemäßen Einsatz des Zertifikats und wird gemäß den Richtlinien für Class 3 Zertifikate identifiziert.
- Funktionszertifikate sind Zertifikate, die für einen ausgewählten Zweck (z.B. Automatische Mail Signatur) üblicherweise einem Rechner oder einer Applikation fest zugeordnet werden. Der Rechner oder die Applikation können das Zertifikat dann nutzen, um automatisch eine Vielzahl von Signaturen zu erstellen. Formal wird dieses Zertifikat einer

Person zugeordnet, die gegenüber TC TrustCenter als verantwortlich für den ordnungsgemäßen Einsatz des Zertifikats zeichnet. Diese für das Zertifikat verantwortliche Person wird dann gemäß den Richtlinien für Class 3 Zertifikate identifiziert.

4.4.3 Überprüfung der Angaben über die Beziehung der natürlichen Person zur Organisation

- Die Zugehörigkeit der Person, für die das Zertifikat beantragt wird, zu der angegebenen Organisation, gegebenenfalls auch zu einer Abteilung der Organisation, muss durch ein dazu berechtigtes Mitglied der Organisation bestätigt werden. Diese Bestätigung muss entweder handschriftlich unterschrieben und mit einem Firmenstempel versehen sein (bei Behörden mit einem Dienstsiegel oder Dienststempel) oder digital signiert sein. Das bei einer digitalen Signatur verwendete Zertifikat muss mindestens den Anforderungen an ein TC TrustCenter Class 3-Zertifikat entsprechen.

5 Regeln für die Namensgebung

TC TrustCenter stellt Zertifikate nach dem X.509-Standard aus. X.509-Zertifikate finden u. a. bei Web Browsern, Web-Servern und Client-Rechnern Anwendung, um eine gesicherte Internet-Verbindung oder eine Authentifikation des Benutzers gegenüber dem Server zu erreichen, sowie zur Etablierung eines privaten Netzes über öffentliche Datenverbindungen (VPN). X.509-Zertifikate können zudem auch für das in viele Browser oder populäre E-Mail-Produkte integrierte Verschlüsselungs- und Signaturverfahren S/MIME verwendet werden.

Dieser Abschnitt enthält eine Leitlinie für das Ausfüllen der einzelnen Datenfelder des X.509-Zertifikatsantrags.

In speziellen Projekten und nach Absprache mit TC TrustCenter kann von den im Folgenden angegebenen Inhalten der einzelnen Felder eines Zertifikates abgewichen werden.

5.1 Zeichensatz und Konversionsregeln

Die X.509 konformen Zertifikate enthalten gemäß RFC 3280 „Internet X.509 Public Key Infrastructure, Certificate and Certificate Revocation List (CRL) Profile" in den dafür vorgesehenen Feldern den Distinguished Name des Herausgebers und des Zertifikatsinhabers, wobei mindestens der folgende Zeichensatz unterstützt wird:

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.

Darüber hinaus unterstützt TC TrustCenter fast alle Latin-1 Zeichen (ISO 859-1), insbesondere Umlaute sowie französische und skandinavische Zeichen, sowie japanische und chinesische Schriftzeichen.

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.

5.1.1 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

5.2 X.509-Zertifikate

X.509-Zertifikate enthalten üblicherweise die folgenden Datenfelder, die im Anschluss an nachstehende Tabelle näher erläutert und durch Beispiele veranschaulicht werden.

Feld	Bedeutung	
C	Country	Land
SP	State / Province	Bundesland
L	Locality	Ort
O	Organization	Organisation
OU	Organizational Unit	Abteilung
CN	Common Name	Vorname + Nachname
Email	Email	E-Mail

C (Country): Dieses Feld enthält stets das zweibuchstabige Länderkürzel nach ISO 3166-1. Personen ohne Organisationszugehörigkeit geben hier das Land des Wohnsitzes an, Organisationen das Land des Firmensitzes.

SP (State/Province): Dieses Feld ist für das Eintragen des Bundesstaates/Bundeslandes gedacht. In Deutschland könnte man hier das Bundesland eintragen. Wir empfehlen Ihnen, dieses Datenfeld leer zu lassen.

L (Locality): In dieses Feld kann der Sitz einer Organisation bzw. der Ort eingetragen werden, in dem der Zertifikatsinhaber laut amtlichem Ausweisdokument (oder amtlicher Meldebestätigung) gemeldet ist, wenn in dem Zertifikat im Feld O keine Organisation genannt wird. Die Postleitzahl ist nicht anzugeben.

O (Organisation): In dieses Feld kann der Name der Organisation eingetragen werden, wie er sich aus den zur Prüfung als Beleg eingereichten Unterlagen oder Datenbanken Dritter ergibt. Üblicherweise ist dies der Name unter dem die Organisation nach Außen auftritt und wie sie auf ihrem Briefkopf bezeichnet wird. Es empfiehlt sich, die Organisation mit ihrem vollen Namen und unter Nennung der Rechtsform einzutragen, also beispielsweise „TC TrustCenter GmbH“ statt „TC TrustCenter“ oder „TCTC AG“.

OU (Organisational Unit): In dieses Feld kann die Abteilung eintragen werden, der das Zertifikat zugeordnet ist. Ein Zertifikat kann mehr als ein OU-Feld enthalten.

CN (Common Name): Dieses Datenfeld enthält üblicherweise den Namen der Person, der das Zertifikat zugeordnet ist. Die Namen und Namensbestandteile werden so angeben, wie im amtlichen Ausweisdokument aufgeführt. Namensbestandteile wie auch Titel und Doktorgrad können nur aufgenommen werden, wenn sie im amtlichen Ausweisdokument aufgeführt sind oder durch vergleichbare Dokumente separat nachgewiesen werden. Doktorgrade oder vergleichbare Namensbestandteile werden dem Vornamen vorangestellt.

CN = <Name einer Person>

In diesem Fall handelt es sich um ein Zertifikat, das genau der im CN-Feld genannten Person zugeordnet ist. Da es mehrere Personen mit demselben Namen geben kann, behält TC TrustCenter sich vor, dem Namen im CN-Feld gegebenenfalls eine laufende Nummer hinzuzufügen, um Mehrdeutigkeiten auszuschließen.

Bei Einzelpersonen, die als Softwareentwickler handeln, kann in weiteren Zertifikatsfeldern ein entsprechender Hinweis (z.B. „Individual Software Publisher“) aufgenommen werden, um das Zertifikat als „Publisher ID“ zu kennzeichnen.

Darüber hinaus können anstelle des Namens der Person, der ein Zertifikat zugeordnet ist, auch andere Angaben im CN-Datenfeld auftreten. Selbst wenn in diesen Fällen nicht der Name einer natürlichen Person im CN-Feld des Zertifikates erscheint, wird ein solches Zertifikat trotzdem einer Person zugeordnet, die gegenüber TC TrustCenter als verantwortlich für den ordnungsgemäßen Einsatz des Zertifikats zeichnet. Diese für das Zertifikat verantwortliche Person wird dann gemäß den Richtlinien der entsprechenden Zertifikatsklasse identifiziert.

Typische Beispiele für Zertifikate, bei denen nicht der Name einer Person im CN-Feld eingetragen wird sind:

CN = <vollständiger Hostname oder vollständige IP-Adresse>

In diesem Fall handelt es sich um ein (SSL) Zertifikat für ein Gerät, üblicherweise ein Web-Server oder ein Client.-Rechner, z.B. www.stonehillbaker.com oder client-1.intranet.example.

CN = *.<Domainname>

In diesem Fall handelt es sich um ein Wildcard-Zertifikat. Wildcard-Zertifikate sind eine Sonderform von Geräte-Zertifikaten, die insbesondere bei Web-Servern zur Anwendung kommen. Anstelle des Namens eines Servers wird das Symbol „*“ eingetragen (z.B. *.stonehillbaker.com). Befinden sich innerhalb einer Domain mehrere verschiede-

ne Server mit unterschiedlichen Hostnamen, können diese Server alle dasselbe Zertifikat benutzen. *.stonehillbaker.com ließe sich z.B. also verwenden für www.stonehillbaker.com, mail.stonehillbaker.com, server.stonehillbaker.com. Ansonsten werden Wildcard-Zertifikate genau wie Zertifikate für Web-Server behandelt.

CN = <Funktionsbezeichnung>

Ist im CN-Feld eine Funktion (z.B. „Automatische Mail Signatur“) eingetragen, wird das Zertifikat für einen ausgewählten Zweck eingesetzt. Wenn dieser Zweck oder die Funktion nicht bereits durch die Wahl des Eintrags im CN-Feld beschrieben ist (z.B. „Automatische Mail Signatur“ beschreibt eindeutig den Zweck), stellt TC TrustCenter in einem gesonderten Dokument auf Anfrage den Zweck und die Funktion des Zertifikates dar. Auf diese Weise kann sich die Relying Party über den Verwendungszweck des Zertifikates informieren.

Damit TC TrustCenter in der Lage ist, Auskunft über den Zweck und die Funktion eines Funktionszertifikates zu geben, und weil Funktionsbezeichnungen aussagekräftig sein sollen, müssen die Funktionsbezeichnungen von TC TrustCenter vor der Verwendung freigegeben werden.

CN = <Inhalt des OU-Feldes> Team-Certificate

In diesem Fall handelt es sich um ein Team-Zertifikat, das von einer Gruppe von Personen oder einer Abteilung (z.B. Poststelle) genutzt werden kann. Um welche Gruppe oder Abteilung einer Organisation es sich dabei handelt, wird dem OU-Feld entnommen.

CN = <Name einer Organisation>

Beinhaltet das CN-Feld einen Organisationsnamen, handelt es sich üblicherweise um eine „Publisher ID“, also um ein Zertifikat, das von Softwareentwicklern verwendet wird, um sich auf einem Portal (z.B. eines Hardware- oder Betriebssystemherstellers) zu authentifizieren. Der Eintrag im CN-Feld ist mit dem Namen der Organisation im O-Feld identisch.

CN = <Beleibige Zeichenfolge> :PN

Ist im CN-Feld nur eine Zahl oder andere Zeichenfolge (gefolgt von dem Zusatz „:PN“) angegeben, handelt es sich um ein Pseudonym-Zertifikat, bei dem der Klarname des Zertifikatsinhabers nicht im Zertifikat enthalten ist. TC TrustCenter behält sich vor, irreführende, ungesetzliche oder aus anderen Gründen unerwünschte Pseudonyme abzulehnen bzw. die entsprechenden Zertifikate zu sperren.

Email: Dieses Feld muss, wenn ausgefüllt, eine gültige E-Mail-Adresse enthalten. Bei Zertifikaten für Web-Server oder andere Geräte lässt sich dieses Feld oftmals nicht eingeben, da ein Server oder anderes Gerät üblicherweise keine E-Mail-Adresse hat. Wenn die Server-Software eine Eingabe gestattet, so kann es sinnvoll sein, hier eine allgemeine E-Mail-Adresse wie `webmaster@stonehillbaker.de` oder `info@stonehillbaker.de` anzugeben. Es ist nicht ratsam, in einem solchen Fall eine persönliche E-Mail-Adresse zu verwenden.

Im Gegensatz dazu sollte bei Zertifikaten, die für natürliche Personen ausgestellt werden, auch die E-Mail-Adresse dieser natürlichen Person angegeben werden; auf allgemeine E-Mail-Adressen wie z.B. info@firma.de sollte bei individuellen Personenzertifikaten verzichtet werden.

Extensions: Häufig ist es wünschenswert, dass ein Objekt unter mehreren Namen bekannt oder erreichbar ist. In Zertifikaten wird dies typischerweise durch Zertifikats-Erweiterungen (Extensions) abgebildet. Wenn in den Zertifikats-Extensions wie z.B. im SubjectAlternativeName alternative Angaben, etwa zu DNS-Namen oder Email-Adressen, gemacht werden,

dann sind auch diese Angaben von TC TrustCenter gemäß den in den Kapiteln 4 und 6 beschriebenen Verfahren auf ihre Korrektheit geprüft.

Beispiele für X.509 Distinguished Names

Die zuvor aufgeführten sieben Felder zusammen bilden den sogenannten Distinguished Name (DN). Zur Konstruktion dieses DN folgendes Beispiel:

```
/C=DE/L=Hamburg/O=Stonehillbaker Deutschland
GmbH/CN=www.stonehillbaker.com/Email=webmaster@stonehillbaker.com
```

Ein bestimmter DN darf jeweils nur einer bestimmten Identität (dieser ggf. mehrfach für verschiedene Zertifikate) zugeordnet werden.

	C	SP	L	O	OU	CN
Natürliche Person	DE		Hamburg			Dr. John Freeman
Natürliche Person (gewerblich)	DE		Hamburg	Dr. John Freeman		Dr. John Freeman
Organisation	DE		Hamburg	Stonehillbaker Deutschland GmbH	Einkauf	Dr. John Freeman
Server	DE		Hamburg	Stonehillbaker Deutschland GmbH	Internet Services	www.stonehillbaker.com
Wildcard Server	DE		Hamburg	Stonehillbaker Deutschland GmbH	Internet Services	*.stonehillbaker.com
Publisher-ID	DE		Hamburg	Stonehillbaker Deutschland GmbH	Development	Stonehillbaker Deutschland GmbH
Funktion	DE		Hamburg	Stonehillbaker Deutschland GmbH	Vertrieb	Signatur von Rechnungen
Team-Zertifikat	DE		Hamburg	Stonehillbaker Deutschland GmbH	Poststelle	Poststelle Team-Certificate

6 Überprüfung der Zertifikatsdaten

TC TrustCenter überprüft X.509-Zertifikatsanträge gemäß der folgenden Tabelle. Die verwendeten Einträge sind im Anschluss erläutert.

Klasse	C	SP	L	O	OU	CN	Email
Class 0	Keine Prüfung	Keine Prüfung	Keine Prüfung	Keine Prüfung	Keine Prüfung	Keine Prüfung	Keine Prüfung
Class 1	Keine Prüfung	Keine Prüfung	Keine Prüfung	Leer	Leer	Keine Prüfung	Zugriffstest oder schrift. Bestätigung
Class 2 Organisation	RegA oder ADB oder WDB	Keine Prüfung	RegA oder ADB oder WDB	RegA oder ADB oder WDB	Schriftl. Bestätigung	Schriftl. Bestätigung, ggf. Domain	Zugriffstest oder schriftl. Bestätigung
Class 2 Publisher ID	RegA oder ADB oder WDB	Keine Prüfung	RegA oder ADB oder WDB	RegA oder ADB oder WDB	Schriftl. Bestätigung	RegA oder ADB oder WDB	Zugriffstest oder schriftl. Bestätigung
Class 2 Natürliche Person mit Organisation	RegA oder ADB oder WDB	Keine Prüfung	RegA oder ADB oder WDB	RegA oder ADB oder WDB	Schriftl. Bestätigung	Schriftl. Bestätigung oder telefon. Bestätigung	Zugriffstest oder schriftl. Bestätigung
Class 2 Funktion oder Team	RegA oder ADB oder WDB	Keine Prüfung	RegA oder ADB oder WDB	RegA oder ADB oder WDB	Schriftl. Bestätigung	Schriftl. Bestätigung	Zugriffstest oder schriftl. Bestätigung
Class 3 Organisation	RegA oder WDB	Keine Prüfung	RegA oder WDB	RegA oder WDB	Schriftl. Bestätigung	Ident, ggf. Domain	Zugriffstest oder schriftl. Bestätigung
Class3 Publisher ID	RegA oder WDB	Keine Prüfung	RegA oder WDB	RegA oder WDB	Schriftl. Bestätigung	RegA oder WDB	Zugriffstest oder schriftl. Bestätigung
Class 3 Natürliche Person mit Organisation	RegA oder WDB	Keine Prüfung	RegA oder WDB	RegA oder WDB	Schriftl. Bestätigung	Ident	Zugriffstest oder schriftl. Bestätigung
Class 3 Funktion oder Team	RegA oder WDB	Keine Prüfung	RegA oder WDB	RegA oder WDB	Schriftl. Bestätigung	Schriftl. Bestätigung mit Ident des Verantwortlichen	Zugriffstest oder schriftl. Bestätigung

Keine Prüfung: TC TrustCenter überprüft dieses Datenfeld nicht.

Leer: Das Feld darf nicht ausgefüllt sein.

Zugriffstest: Wenn das Zertifikat eine E-Mail-Adresse enthält, wird diese Adresse überprüft. Class 1-Zertifikate enthalten immer eine E-Mail-Adresse. Um die Existenz einer E-Mail-Adresse und die Erreichbarkeit des Zertifikatsinhabers unter derselben zu überprüfen, wird eine E-Mail an diese Adresse geschickt (Ausnahme: bei Class 2- und 3-Zertifikaten für Organisationen kann auf die Versendung dieser E-Mail verzichtet werden, sofern die Korrektheit der E-Mail-Adresse durch einen Verantwortlichen bestätigt wird, siehe oben). Diese E-Mail enthält Daten, die zur vollständigen Identitätsfeststellung des Antragstellers an TC TrustCenter zurückgesendet werden müssen.

RegA: Die Angaben in diesem Datenfeld werden anhand eines Auszuges aus einem zuständigen Register oder vergleichbarer Dokumente geprüft. Wichtig ist, dass aus dem Dokument hervorgeht, dass die Organisation tatsächlich existiert. Je nach Rechtsform und Land kommen hier unterschiedliche Auskunft gebende Stellen in Frage. Bei privatwirtschaftlich organisierten Unternehmen ist dies üblicherweise das Handelsregister (Commercial Regis-

ter). Für öffentlich-rechtliche Organisationen (wie Behörden, Ministerien, Anstalten des öffentlichen Rechts) werden in der Regel keine Register geführt. Hier ist von der Dienstsiegel führenden Stelle, von der zuständigen Aufsichtsbehörde oder einer anderen übergeordneten Behörde die Existenz der Organisation zu bestätigen.

ADB: Die Angaben in diesem Feld werden anhand von Adressdatenbanken Dritter geprüft (z. B. Kreditkarten-Unternehmen, Post). Angaben, die auf eigenen Anfragen der zu zertifizierenden Person beruhen, werden nicht akzeptiert.

WDB: Die Angaben in diesem Feld werden anhand von Wirtschaftsdatenbanken Dritter geprüft. Die Beglaubigung der Angaben ist hier nicht gefordert. Die WDB werden von TC TrustCenter direkt oder im Auftrag von TC TrustCenter angefragt. Angaben, die auf eigenen Anfragen der zu zertifizierenden Organisation beruhen, werden nicht akzeptiert.

Schriftliche Bestätigung: Die Korrektheit dieser Daten muss von einem Verantwortlichen durch eigenhändige Unterschrift oder elektronische Signatur bestätigt werden. Dazu werden in der Antragsbestätigung Name und Abteilung der Mitarbeiter, gegebenenfalls auch die E-Mail-Adresse oder der Domainname oder die Funktionsbezeichnung, genannt, die ein Zertifikat erhalten sollen. Diese Bestätigung muss nicht individuell für jedes Zertifikat vorliegen, sondern kann in allgemeiner Form auch für eine größere Anzahl von Zertifikaten gelten. Beispiel: Zertifikate für die Mitarbeiter einer Firma oder einer Abteilung einer Firma.

Telefonische Bestätigung: Die Korrektheit dieser Daten muss von einem Verantwortlichen der Organisation telefonisch bestätigt werden. Dazu nimmt TC TrustCenter oder eine von TC TrustCenter dazu bevollmächtigte Instanz telefonisch Kontakt zu der Organisation auf und erkundigt sich dort, ob die im Zertifikat genannte Person in der Organisation bekannt ist und ein Zertifikat beantragen darf.

Ident: Die Überprüfung dieser Daten erfolgt durch Abgleich mit dem vorgelegten amtlichen Ausweisdokument und dem unterschriebenen Antrag, der TC TrustCenter im Rahmen der Identitätsfeststellung zugesendet wird.

Domain: Bei Zertifikaten für Web-Server oder Clients wird der Inhalt des Feldes CN, also der vollständige Hostname (Fully Qualified Domain Name, FQDN) des Web Servers (beispielsweise `www.stonehillbaker.com`) bzw. bei Wildcard-Zertifikaten mangels Hostname nur der Domainname oder die IP-Adresse, durch Abfrage der Datenbank einer Internet-Registrierungsstelle dahingehend überprüft, ob die Domain (im Beispiel `stonehillbaker.com`) bzw. die IP-Adresse auf die im Feld O genannte Organisation registriert ist. Ist dies nicht der Fall, so muss der Antragsteller eine Erlaubnis vom Inhaber der Domain für die Nutzung der Domain bzw. des IP-Adresse durch den Zertifikatsinhaber einholen.

Zertifikate, die nur intern genutzt werden, und deren Domainname nicht registrierungsfähig ist, z.B. `domain.local` oder `domain.internal`, müssen im Domainnamen eine Angabe enthalten, mit der das Zertifikat einer Organisation eindeutig zugeordnet werden kann.
TC TrustCenter trägt dafür Sorge, dass Zertifikate mit identischen internen Namen nicht an unterschiedliche Organisationen ausgestellt werden. Hat also die Organisation Stonehillbaker ein Zertifikat für einen (internen) Server `server1.shb-intranet.example` erhalten, so ist für alle anderen die Ausstellung eines Zertifikates in der Domain `shb-intranet.example` ausgeschlossen.

7 Sperren von Zertifikaten

7.1 Sperrwege

Eine Sperrung ist für bestimmte Produkte auf der Web-Site von TC TrustCenter http://www.trustcenter.de/sperren <http://www.trustcenter.de/sperren> unter Verwendung des zu sperrenden Zertifikates möglich. Einzig eine solche Sperrung wird automatisiert durchgeführt.

Alle Sperranträge, die auf einem der folgenden Wege bei TC TrustCenter eingehen, werden individuell bearbeitet, so dass keine automatisierte Sperrung erfolgt.

Ein Sperrantrag kann per signierter E-Mail an certificate@trustcenter.de <mailto:certificate@trustcenter.de> gestellt werden.

Weiter kann ein Sperrantrag auch schriftlich an TC TrustCenter, Kennwort: Sperrung, Sonninstraße 24-28, 20097 Hamburg gerichtet werden.

Ebenfalls möglich ist es, einen Sperrantrag per Telefonanruf unter +49 (0) 40 / 80 80 26-1 13 zu stellen, wobei als Nachweis der Berechtigung des Anrufers die Nennung des korrekten Sperrpasswortes zwingend erforderlich ist.

Die angegebenen Adressen und Rufnummern sind ausschließlich für Sperrungen reserviert. Es wird keinerlei Hilfe oder Beratung geleistet. TC TrustCenter bestätigt die erfolgte Sperrung eines Zertifikates durch eine signierte E-Mail.

7.2 Sperrgründe

Bei den Sperrgründen ist zu unterscheiden zwischen den Rechten und den Pflichten zur Sperrung. Sperrpflichten sind unbedingt zu erfüllen im Gegensatz zu Sperrrechten, über dessen Ausübung der Sperrberechtigte selbst entscheiden kann. Sperrberechtigt können grundsätzlich drei verschiedene Personen, bzw. Organisationen sein: der Zertifikatsinhaber selbst, TC TrustCenter als verantwortliche Zertifizierungsstelle und Dritte. Alle drei Parteien haben eigene Sperrrechte und –pflichten.

a) Sperrpflichten des Zertifikatsinhabers

- Ein Zertifikatsinhaber ist verpflichtet, sein Zertifikat zu sperren, falls Angaben im Zertifikat ungültig sind (z. B. nach Wechsel der E-Mail-Adresse) oder Daten, die in seinem Zertifikat enthalten sind, nicht mehr den Tatsachen entsprechen beziehungsweise nicht mehr mit den Daten zum Zeitpunkt der Zertifizierung übereinstimmen.
- Ein Zertifikatsinhaber ist verpflichtet, sein Zertifikat zu sperren, falls der Datenträger mit dem privaten Schlüssel nicht mehr benötigt wird.
- Ein Zertifikatsinhaber ist verpflichtet, sein Zertifikat zu sperren, falls der zum Zertifikat gehörige private Schlüssel verloren wurde.
- Ein Zertifikatsinhaber ist verpflichtet, sein Zertifikat zu sperren, falls der Verdacht besteht, dass unberechtigte Personen Zugriff auf den privaten Schlüssel haben oder ihn manipulieren können.
- Ein Zertifikatsinhaber ist verpflichtet, sein Zertifikat zu sperren, falls der Verdacht besteht, dass sein privater Schlüssel kompromittiert wurde, beziehungsweise dass dieser durch Unbefugte genutzt wird.

- Ein Zertifikatsinhaber ist verpflichtet, sein Zertifikat zu sperren, falls Identifikationsdaten preisgegeben wurden oder ein solcher Verdacht besteht und die Identifikationsdaten nicht geändert wurden.

b) Sperrrechte des Zertifikatsinhabers

- Ein Zertifikatsinhaber ist jederzeit ohne Angabe von Gründen berechtigt, sein Zertifikat zu sperren

c) Sperrpflichten von TC TrustCenter

- TC TrustCenter ist verpflichtet, ein Zertifikat zu sperren, falls ein berechtigter Sperrantrag eines Zertifikatsinhabers oder eines Dritten vorliegt.
- TC TrustCenter ist verpflichtet, ein Zertifikat zu sperren, falls TC TrustCenter Kenntnis über einen verpflichtenden Sperrgrund des Zertifikatsinhabers erlangt.
- TC TrustCenter ist verpflichtet, ein Zertifikat zu sperren, falls dem Zertifikatsinhaber nachgewiesen werden kann, dass er gegen Bestimmungen aus dem zugrundeliegenden Vertrag oder gegen Bestimmungen des Certification Practice Statement (CPS) verstoßen hat. Dies betrifft auch die missbräuchlich Nutzung von Zertifikaten oder die Nutzung zu strafbaren Zwecken
- TC TrustCenter ist verpflichtet, ein Zertifikat zu sperren, falls die im Zertifikat genannte Person verstorben bzw. die im Zertifikat genannte Organisation umbenannt oder aufgelöst wurde.
- TC TrustCenter ist verpflichtet, ein Zertifikat zu sperren, falls der Kunde den Vertrag beendet.
- TC TrustCenter ist verpflichtet, ein Zertifikat zu sperren, falls TC TrustCenter davon überzeugt ist, dass die Sperrung notwendig ist, um die Vertrauenswürdigkeit der Zertifizierungsstelle zu schützen.
- TC TrustCenter ist verpflichtet, ein Zertifikat zu sperren, falls TC TrustCenter den Betrieb einstellt und es keine Übergabe an einen Nachfolger gibt oder der Betrieb anderweitig fortgeführt wird.

d) Sperrrechte von TC TrustCenter

- TC TrustCenter ist berechtigt, ein Zertifikat zu sperren, falls kryptographische Algorithmen oder zugehörige Parameter durch technologische Fortschritte oder neue Entwicklungen in der Kryptologie unsicher werden, wenn das Zertifikat mit diesen Algorithmen und Parametern erzeugt wurde.
- TC TrustCenter ist berechtigt, ein Zertifikat zu sperren, falls der Zertifikatsinhaber seinen vertraglichen Verpflichtungen nicht nachkommt, insbesondere das Zertifikat nicht bezahlt.
- TC TrustCenter ist berechtigt, ein Zertifikat zu sperren, falls Angaben im Zertifikat enthalten sind, die nicht den Richtlinien der ausstellenden CA entsprechen.
- TC TrustCenter ist berechtigt, ein Zertifikat zu sperren, falls es Hinweise auf eine Verletzung der Vertrauenswürdigkeit oder der Sicherheitsfunktionen des Zertifikates gibt, wie sie sich aus einer Missachtung der Sorgfalts- und Mitwirkungspflichten aus den jeweiligen allgemeinen Geschäftsbedingungen ergeben.

e) Sperrpflichten von Dritten

- Dritte sind verpflichtet, ein Zertifikat zu sperren, falls sie Kenntnis darüber erlangen, dass ein verpflichtender Sperrgrund für den Zertifikatsinhaber oder TC TrustCenter vorliegt.
- Dritte sind verpflichtet, ein Zertifikat zu sperren, falls bei Zertifikaten, die für die Organisation des Dritten ausgestellt wurden, die Person, auf die das Zertifikat ausgestellt wurde, aus der Organisation ausgeschieden ist.

f) Sperrrechte von Dritten

- Dritte sind berechtigt, ein Zertifikat zu sperren, falls sie Angaben zu einem Zertifikat bestätigt haben und diese Angaben nicht mehr den Tatsachen entsprechen.
- Dritte sind berechtigt, ein Zertifikat zu sperren, falls sie im Zertifikat genannt werden und die gemeinsame Nennung von Zertifikatsinhaber und Dritten im Zertifikat nicht länger erwünscht ist.

* * *