



TC TrustCenter-Zertifizierungsrichtlinien

Fassung vom 12. Juni 2002

1	EINLEITUNG	2
2	WICHTIGE HINWEISE	4
3	ÄNDERUNGEN ZUR VERSION VOM 1. OKTOBER 1999	5
4	ZERTIFIKATSKLASSEN	6
4.1	CLASS 0-ZERTIFIKATE	6
4.2	CLASS 1-ZERTIFIKATE	6
4.3	CLASS 2-ZERTIFIKATE	6
4.3.1	<i>Überprüfung der Angaben über natürliche Personen</i>	6
4.3.2	<i>Überprüfung der Angaben über Organisationen</i>	7
4.3.3	<i>Überprüfung der Angaben über die Beziehung der natürlichen Person zur Organisation</i>	7
4.4	CLASS 3-ZERTIFIKATE	7
4.4.1	<i>Überprüfung der Angaben über natürliche Personen</i>	7
4.4.2	<i>Überprüfung der Angaben über Organisationen</i>	8
4.4.3	<i>Überprüfung der Angaben über die Beziehung der natürlichen Person zur Organisation</i>	8
5	REGELN FÜR DIE NAMENSGEBUNG	8
5.1	X.509-ZERTIFIKATE.....	9
5.2	WTLS-ZERTIFIKATE.....	10
5.3	PGP-ZERTIFIKATE	11
6	ÜBERPRÜFUNG DER ZERTIFIKATSDATEN	12
7	SPERREN VON ZERTIFIKATEN	13

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.

Jedes Zertifikat ist nur so vertrauenswürdig wie die Verfahren, nach denen es ausgestellt wird. Je höher die Zertifikatsklasse, desto umfangreichere Identifikationsprüfungen liegen der Ausstellung zu Grunde. Die Zertifikate selbst enthalten als Information für diejenigen, die sich auf dieses Zertifikat 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 verschiedene 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 Server-Zertifikaten, die keiner natürlichen Person zugeordnet sind – 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 (Ziffer 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 (Ziffer 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 (Ziffer 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 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 (Ziffer 7).

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

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

TC TrustCenter Zertifizierungsrichtlinien

Fassung vom 12. Juni 2002

Kontaktinformationen:

TC TrustCenter AG
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.

Urheberrechts-Notiz: Dieses Dokument ist urheberrechtlich geschützt. Die Verwendung der Texte und Abbildungen, 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 ist 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 AG.

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

Copyright © 2002 TC TrustCenter AG, Sonninstraße 24 - 28, 20097 Hamburg/Germany. Alle Rechte vorbehalten.

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 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 und der Identitätsfeststellung 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 der angegebenen Identität 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, bzw. TC TrustCenter von der Veränderung der im Zertifikat enthaltenen Daten Kenntnis erlangt.

3 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.

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 Klasse eines Zertifikats beschreibt die grundsätzliche Art der Überprüfung der Inhalte des Zertifikats und der Identitätsfeststellung des Zertifikatsinhabers. Je höher die Zertifikatsklasse, desto umfangreichere Identifikationsprüfungen liegen der Ausstellung zu Grunde.

Die Zertifikate selbst enthalten als Information für diejenigen, die sich auf dieses Zertifikat verlassen wollen (Relying Party), die 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, kann in diesen Zertifizierungsrichtlinien nachgelesen werden.

Die Sicherheit der Verschlüsselung und damit der Schutz der elektronischen Kommunikation gegen unbefugte Kenntnisnahme ist von der verwendeten Schlüssellänge 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.

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 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 Zugriffstest 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 die Organisation die Korrektheit der E-Mail-Adresse bestätigen.

- Namensangaben zu einer natürlichen Person werden verifiziert durch
 - a) Zusicherung Dritter über die Richtigkeit und Vollständigkeit der Daten
oder durch
 - b) Bestätigung der Angaben durch Vorlage der Kopie eines amtlichen Lichtbildausweises mit Unterschriftszug und durch handschriftliche Unterschrift bzw. digitale Signatur.

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 nachweist (aktuelle Auszug aus einem zuständigen amtlichen Register, in dem die Organisation geführt wird bzw. vergleichbare Dokumente). Die Überprüfung kann auch anhand von Datenbanken vertrauenswürdiger Dritter erfolgen.
- 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.

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

- Die Zugehörigkeit der im Zertifikat genannten Person 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. Das bei einer digitalen Signatur verwendete Zertifikat muss ein TC TrustCenter Class 2-Zertifikat (mit Überprüfung der Angaben gemäß 4.3.1 b)), ein TC TrustCenter Class 3-Zertifikat oder ein signaturgesetzkonformes Zertifikat sein.

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. Werden im Zertifikat Angaben über eine Organisation gemacht, kann auch die Organisation die Korrektheit der E-Mail-Adresse bestätigen.
- Wenn eine natürliche Person im Class 3-Zertifikat genannt ist, ist das persönliche Erscheinen dieser Person und die Vorlage eines 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.

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 tatsächlich existiert. Die vorgelegten Dokumente müssen aktuell (nicht älter als drei Monate) und, wenn möglich, beglaubigt sein. Wie bei Class 2-Zertifikaten kann diese Überprüfung auch anhand von Datenbanken vertrauenswürdiger Dritter erfolgen.
- Weitere Zertifikatsdaten werden soweit möglich überprüft. So wird z.B. bei Server-Zertifikaten die Registrierung der angegebenen Domain auf die im Zertifikatsantrag genannte Organisation überprüft.

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

- Die Zugehörigkeit der Person 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. Das bei einer digitalen Signatur verwendete Zertifikat muss ein TC TrustCenter Class 3-Zertifikat oder ein signaturgesetzkonformes Zertifikat sein.

5 Regeln für die Namensgebung

TC TrustCenter stellt Zertifikate nach dem X.509-, dem WTLS und dem PGP-Standard aus. X.509-Zertifikate finden u. a. bei Web Browsern und Web Servern 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. WTLS-Zertifikate dienen zur sicheren mobilen Datenübertragung zwischen WAP-Servern und WAP-Clients (z. B. Handys). PGP-Zertifikate werden u. a. für die verschlüsselte Kommunikation per E-Mail oder das Verschlüsseln und Signieren von Dateien verwendet.

Dieser Abschnitt enthält eine Leitlinie für das Ausfüllen der einzelnen Datenfelder des X.509-Zertifikatsantrags, die Bildung eines Zertifikatsnamen für WTLS-Zertifikate und die Wahl einer geeigneten PGP-Benutzerkennung.

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 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 zweibuchstabile Länderkürzel nach ISO 3166-1. Personen ohne Organisationszugehörigkeit geben hier das Land des Wohnsitzes an, Organisationen das Land des Firmensitzes. Bei Server-Zertifikatsanträgen, die mit einer Server-Software erzeugt werden müssen, ist auf die richtige Eingabe des Kürzels zu achten, also beispielsweise „DE“ für Deutschland, „AT“ für Österreich oder „CH“ für die Schweiz.

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 AG“ statt „TC TrustCenter“ oder „TCTC AG“.

OU (Organisational Unit): In dieses Feld kann die Abteilung eingetragen werden, der das Zertifikat zugeordnet ist. Bei Code Signing-Zertifikatsanträgen wird hier automatisch die zur Signaturerstellung verwendete Software eingetragen.

CN (Common Name): Dieses Datenfeld enthält üblicherweise den Namen der Person, der das Zertifikat zugeordnet ist. Bei im Browser generierten Zertifikaten setzt sich dieser aus den separat erfragten Eingaben für Vor- und Nachname zusammen. Die Namen und Namensbestandteile sind so anzugeben, 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 sind dem Vornamen voranzustellen.

Eine Ausnahme bilden Server-Zertifikate: Damit diese mit den gängigen Browsern funktionieren, muss in das Feld CN der vollständige Domainname des Servers eingetragen werden, also beispielsweise `www.stonehillbaker.com`

TC TrustCenter Zertifizierungsrichtlinien

Fassung vom 12. Juni 2002

Bei TC CodeSigning-Zertifikaten wird automatisch der Inhalt des Feldes O (Organisation) in das Feld CN kopiert, da üblicherweise der Inhalt des Feldes CN angezeigt wird, wenn ein Benutzer signierten Programmcode überprüft.

Email: Dieses Feld muss, wenn ausgefüllt, eine gültige E-Mail-Adresse enthalten. Bei Server-Zertifikaten lässt sich dieses Feld oftmals nicht eingeben, da ein Server 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@firma.de` oder `info@firma.de` anzugeben. Es ist nicht ratsam, in einem solchen Fall eine persönliche E-Mail-Adresse zu verwenden.

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.

Beispiele für X.509 Distinguished Names

	C	SP	L	O	OU	CN	EMAIL
Natürliche Person	DE		Hamburg			Dr. John Freeman	john.freeman@stonehillbaker.com
Organisation	DE		Hamburg	Stonehillbaker Deutschland GmbH	Einkauf	Dr. John Freeman	john.freeman@stonehillbaker.com
Server	DE		Hamburg	Stonehillbaker Deutschland GmbH	Internet Services	www.stonehillbaker.com	webmaster@stonehillbaker.com
CodeSigning	DE		Hamburg	Stonehillbaker Deutschland GmbH	Microsoft Authenticode	Stonehillbaker Deutschland GmbH	info@stonehillbaker.com

5.2 WTLS-Zertifikate

WTLS-Zertifikate kennen keine Datenfelder wie bei X.509-Zertifikaten, aus denen sich der Zertifikatsname (X.509-Terminologie: Distinguished Name, siehe dazu den Abschnitt „X.509-Zertifikate“) zusammensetzt. Stattdessen ist der Zertifikatsname eine im Prinzip frei wählbare Zeichenkette.

Ungeachtet dessen empfiehlt es sich, diese Zeichenkette wie einen X.509-DN zu bilden, dabei jedoch wegen des geringeren Speicher- und Anzeigeplatzes der WAP-Endgeräte nur die notwendigsten Informationen aufzunehmen.

Beispiele für WTLS-Zertifikatsnamen

```
/C=DE/O=Stonehillbaker Deutschland GmbH/CN=wap.stonehillbaker.com
```

```
/C=DE/O=Stonehillbaker Deutschland GmbH  
/CN=wap.stonehillbaker.com/Email=info@stonehillbaker.com
```

5.3 PGP-Zertifikate

Das PGP-Zertifikatsformat sieht im Gegensatz zu X.509 keine Datenfelder vor. Ab Version 5.0 wird die Eingabe der E-Mail-Adresse separat erfragt, die, eingeschlossen in spitze Klammern (ab PGP 5.0 werden diese Klammern automatisch eingefügt), auf den Namen des Schlüsselinhabers folgt. Eine PGP-Benutzerkennung hat also z. B. die folgende Form, welche für privat genutzte Zertifikate zu empfehlen ist:

Dr. John Freeman <john.freeman@stonehillbaker.com>

Für geschäftlich genutzte Zertifikate ist es sinnvoll, eine Benutzerkennung zu wählen, welche die gleichen Daten enthält wie ein entsprechendes X.509-Zertifikat. Unter Benutzung der Datenfeldbezeichnungen des X.509-Standards hat diese folgende Form:

CN, O, OU, L, C <Email>

Dabei sind im Prinzip alle genannten Feldbezeichnungen optional. In der Regel sollte auf die Angabe von OU, L und C verzichtet werden, also beispielsweise

Dr. John Freman, Stonehillbaker Deutschland GmbH
<john.freeman@stonehillbaker.com>

oder alternativ (ausführlicher, aber unübersichtlicher)

Dr. John Freeman, Stonehillbaker Deutschland GmbH, Marketing, Hamburg, DE
<john.freeman@stonehillbaker.com>

Die direkte Beantragung von Zertifikaten aus der PGP-Software heraus wird von TC TrustCenter derzeit nicht unterstützt.

Beispiele für PGP-Benutzerkennungen

Person	Dr. John Freeman, Hamburg Dr. John Freeman <john.freeman@stonehillbaker.com>
Organisation	Dr. John Freeman, Stonehillbaker Deutschland GmbH, Hamburg <john.freemann@stonehillbaker.com>

6 Überprüfung der Zertifikatsdaten

TC TrustCenter überprüft X.509-Zertifikatsanträge gemäß der folgenden Tabelle (PGP analog). 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
Class 2 Organisation	RegA oder ADB	Keine Prüfung	RegA oder ADB	RegA oder ADB	Schriftl. Bestätigung	Schriftl. Bestätigung	Zugriffstest oder schriftl. Bestätigung
Class 2 Natürliche Person mit Organisation	RegA oder ADB	Keine Prüfung	RegA oder ADB	RegA oder ADB	Schriftl. Bestätigung	Schriftl. Bestätigung	Zugriffstest oder schriftl. Bestätigung
Class 3 Organisation	Beglaubigter RegA oder WDB	Keine Prüfung	Beglaubigter RegA oder WDB	Beglaubigter RegA oder WDB	Schriftl. Bestätigung	Ident, ggf. Domain	Zugriffstest oder schriftl. Bestätigung
Class 3 Natürliche Person mit Organisation	Beglaubigter RegA oder WDB	Keine Prüfung	Beglaubigter RegA oder WDB	Beglaubigter RegA oder WDB	Schriftl. Bestätigung	Ident	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 dem 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 auskunftsgibende Stellen in Frage. Bei privatwirtschaftlich organisierten Unternehmen ist dies üblicherweise das Handelsregister (Commercial Register). Für öffentlich-rechtliche Organisationen (wie Behörden, Ministerien, Anstalten des öffentlichen Rechts) werden in der Regel keine Register geführt. Hier ist von der dienstsiegelführenden Stelle oder von der zuständigen Aufsichtsbehörde 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: Diese Daten müssen von einem Verantwortlichen unterschrieben und bestätigt werden. Dazu werden in der Antragsbestätigung Name und Abteilung der Mitarbeiter, gegebenenfalls auch die E-Mail-Adresse oder der Domainname, 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.

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 Server-Zertifikatsanträgen wird der Inhalt des Feldes CN, also der vollständige Domainname des Web Servers (beispielsweise `www.stonehillbaker.com`), durch Abfrage der Datenbank einer Internet-Registrierungsstelle dahingehend überprüft, ob die Domain (im Beispiel `stonehillbaker.com`) auf die im Feld O genannte Organisation registriert ist. Ist dies nicht der Fall, so holt der Antragsteller eine Erlaubnis vom Inhaber der Domain für die Nutzung der Domain durch den Zertifikatsinhaber ein.

7 Sperren von Zertifikaten

Ein Zertifikat ist (schriftlich, telefonisch oder über das Internet-Angebot von TC TrustCenter) zu sperren, falls

1. der zugehörige private Schlüssel verloren wurde,
2. der Verdacht besteht, dass unberechtigte Personen Zugriff auf den privaten Schlüssel haben oder ihn manipulieren können,
3. Angaben im Zertifikat ungültig sind (z. B. nach Wechsel der E-Mail-Adresse).

* * *