



TC TrustCenter Zertifizierungsrichtlinien

Version vom 1. Oktober 1999

1	EINLEITUNG	2
2	WICHTIGE HINWEISE	3
3	ZERTIFIKATSKLASSEN	4
3.1	CLASS 0 ZERTIFIKATE (NUR FÜR TESTZWECKE).....	4
3.2	CLASS 1-ZERTIFIKATE	4
3.3	CLASS 2-ZERTIFIKATE	4
3.4	CLASS 3-ZERTIFIKATE	5
3.5	CLASS 4-ZERTIFIKATE	6
4	DIE PERSÖNLICHE IDENTITÄTSFESTSTELLUNG	7
4.1	DAS POST IDENT-VERFAHREN.....	7
4.2	TC TRUSTCENTER IDENT POINTS®	7
5	REGELN FÜR DIE NAMENSGEBUNG	9
5.1	X.509-ZERTIFIKATE	9
5.2	PGP-ZERTIFIKATE	10
5.3	BEISPIELE FÜR X.509 DISTINGUISHED NAMES	11
5.4	BEISPIELE FÜR PGP-BENUTZERKENNUNGEN.....	11
6	ÜBERPRÜFUNG DER ZERTIFIKATSDATEN	12
7	SPERREN VON ZERTIFIKATEN	14



1 Einleitung

Dieses Dokument beschreibt die Zertifizierungsrichtlinien von TC TrustCenter. Es wird die Einteilung in verschiedene Zertifikatsklassen sowie deren Bedeutung für Antragsteller bzw. Zertifikatsinhaber und jene erläutert, die anhand dieser Klassifikation eine Entscheidung darüber treffen möchten, 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 Anschluss an die Einteilung der Zertifikatsklassen werden Hinweise zur persönlichen Identitätsfeststellung gegeben, die für einige Zertifikatsklassen notwendig ist, um das Vertrauen in die Bindung zwischen Zertifikat und Zertifikatsinhaber zu stärken.

Danach werden Richtlinien zur Wahl eines (Zertifikat-) Namens gegeben, der häufig nur aus Name und E-Mail-Adresse des Inhabers besteht, aber auch Angaben zur Firma und deren Sitz oder aber zum Wohnsitz des Zertifikatsinhabers enthalten kann. Zur Veranschaulichung sind am Ende des Abschnitts Beispiele für geeignet gewählte Namen beigefügt.

Anschließend wird erläutert, wie TC TrustCenter die im Zertifikat enthaltenen Informationen überprüft. Nicht alle in einem Zertifikat enthaltenen Daten sind notwendigerweise verifiziert worden, und jede Relying Party 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.

Detaillierte Produktinformationen finden Sie in den Produktseiten auf unserer Web Site.

Allgemeine Informationen zu Verschlüsselung oder Public Key Verfahren entnehmen Sie bitte den Infoseiten auf unserer Web Site.

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

Kontaktinformationen:

TC TrustCenter AG
Sonninstrasse 24-28
20097 Hamburg
Deutschland

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



2 Wichtige Hinweise

TC TrustCenter ist keine gemäß Signaturgesetz § 4 genehmigte Zertifizierungsstelle. TC TrustCenter hat bereits einen Antrag auf Genehmigung bei der [Regulierungsbehörde für Telekommunikation und Post](#) gestellt.

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 angegebenen Inhalte abgeschätzt werden. 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 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 Zusicherung der Aktualität der Daten. TC TrustCenter überprüft die im Zertifikatsantrag angegebenen Daten nur bei der Zertifikatsausstellung. Eine Zusicherung der Aktualität dieser Daten wird von TC TrustCenter daher nicht gegeben. Auch bei der Verlängerung eines Zertifikats werden die Daten keiner erneuten Prüfung unterzogen; die maximale Anzahl der Verlängerungen ist auf zwei beschränkt.

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 Zertifizierungsservice muss selbst individuell entscheiden und verantworten, 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 Zertifizierungsservice Grundkenntnisse über Public Key Verfahren anzueignen. Informationen und Hilfestellung zu Fragen zu digitalen Signaturen, Zertifikaten und dem Zertifizierungsservice werden von TC TrustCenter auf der Web Site bereitgestellt.

Sorgfalts- und Mitwirkungspflicht des Zertifikatsinhabers. Der Zertifikatsinhaber muss zur Sicherheit der Verfahren beitragen. Dazu muss er die Sorgfalts- und Mitwirkungspflichten in den Allgemeinen Geschäftsbedingungen ([AGB](#)) beachten.

Anpassung an Marktbedürfnisse. Aufgrund der sich stetig ändernden Marktanforderungen ist es unerlässlich, dass die Dienste der Zertifizierungsstelle den konkreten Bedürfnissen der Kunden angepasst werden. Die AGB und die Zertifizierungsrichtlinien werden dementsprechend regelmäßig überarbeitet. Dabei kann es in Detailfragen zu kurzzeitigen Differenzen zwischen den verschiedenen Dokumenten kommen.

Deutsche Versionen sind maßgebend. Einige der Dokumente und Webseiten stehen sowohl in deutscher als auch in englischer Fassung zur Verfügung. In Zweifelsfällen ist für alle Dokumente die deutsche Version maßgebend.

Irrtum vorbehalten.



3 Zertifikatsklassen

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 angegebenen Inhalte abgeschätzt 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 Verwendung von Class 1-Zertifikaten genauso wie bei Class 2, 3- oder 4-Zertifikaten (bei identischer Schlüssellänge) in gleichem Maße gewährleistet. Die Zertifikatsklassen unterscheiden sich in der Verlässlichkeit der durch die Zertifizierung getroffenen Aussage, dass der Zertifikatsinhaber tatsächlich derjenige ist, dessen Name im Zertifikat genannt wird.

3.1 Class 0-Zertifikate (nur für Testzwecke)

Zu bestimmten Zwecken stellt TC TrustCenter für Geschäftskunden auf Nachfrage Demozertifikate aus. Diese haben standardmäßig eine verkürzte Gültigkeitsdauer und dürfen nur zu Testzwecken verwendet werden.

Die Angaben in Demozertifikaten werden von TC TrustCenter keinerlei Prüfung unterzogen!

3.2 Class 1-Zertifikate

Class 1-Zertifikate werden nur für Privatpersonen ausgestellt. Class 1-Zertifikate beinhalten immer eine E-Mail-Adresse. Class 1-Zertifikate bestätigen, dass die angegebene E-Mail-Adresse existiert, und der Besitzer des zugehörigen öffentlichen Schlüssels Zugriff auf diese E-Mail-Adresse hat.

Class 1-Zertifikate stellen damit einen nur sehr geringen Nachweis der Identität dar. Die Angaben des Antragstellers in einem Class 1-Zertifikatsantrag werden, abgesehen von einem einfachen Zugriffstest auf die E-Mail-Adresse, in keiner Weise überprüft. Jegliche Teilnehmerdaten sind, mit Ausnahme der E-Mail-Adresse, als nicht verifiziert anzusehen.

Class 1-Zertifikate sind hauptsächlich für Client-Authentisierung (gegenüber einem Web Server) oder persönliche E-Mail gedacht, um hierbei ein Mindestmaß an Sicherheit zu bieten. Class 1-Zertifikate sollten nicht für private oder kommerzielle Anwendungen verwendet werden, für die eine persönliche Überprüfung der Identität notwendig ist.

3.3 Class 2-Zertifikate

Class 2-Zertifikate werden sowohl für private als auch geschäftliche Nutzung ausgestellt. Das Angebot für Privatkunden gilt jedoch nicht in Deutschland, dort ist die persönliche Identitätsfeststellung über das Post Ident-Verfahren oder in einem Ident Point[®] ohne großen Aufwand möglich und deshalb vorzuziehen.

Vor der Beantragung von Class 2-Zertifikaten für Geschäftskunden sollte in telefonischer und schriftlicher Form eine Kontaktaufnahme mit TC TrustCenter erfolgen, um eventuelle Fragen zu klären und Informationen über den genauen Ablauf zu erhalten.

Mit der Ausstellung eines Class 2-Zertifikats für Geschäftskunden bestätigt TC TrustCenter, dass



1. das angegebene Unternehmen existiert. Dazu muss TC TrustCenter die Kopie eines aktuellen Handelsregisterauszugs (HRA) oder eines vergleichbaren Dokuments vorliegen. Werden mehrere Zertifikate beantragt, so ist die Kopie nur einmal beizubringen, sofern sich zwischenzeitlich keine wesentlichen Änderungen ergeben haben. TC TrustCenter behält sich vor, im Zweifelsfall eine neue Kopie anzufordern.
2. zeichnungsberechtigte Personen des Unternehmens den Inhalt des Zertifikats persönlich oder über von ihnen bestimmte Dritte bestätigt haben. Diese Bestätigung muss entweder handschriftlich unterschrieben oder mit einem TC TrustCenter Class 2, 3 oder 4 Zertifikat digital signiert sein.
3. die Zertifikatsdaten, abgesehen von persönlichen Informationen, zusätzlich soweit möglich von TC TrustCenter überprüft wurden (siehe dazu den Abschnitt „Überprüfung der Zertifikatsdaten“). Beispielsweise wird bei Server-Zertifikaten die Registrierung der angegebenen Domain auf die im Zertifikatsantrag genannte Organisation überprüft. Sofern E-Mail-Adressen angegeben sind, wird wie bei Class 1 der Zugriff auf diese E-Mail-Adresse geprüft; Class 2 umfasst also Class 1.

Privatkunden erhalten eine Antragsbestätigung, welche die Zertifikatsdaten enthält. Diese ist zu unterschreiben und zusammen mit einer Kopie des Ausweises (Personalausweis oder Reisepass) an TC TrustCenter zurückzusenden. Die Ausweiskopie bei Privatkunden tritt an die Stelle der Kopie des Handelsregisterauszugs bei Geschäftskunden, um ein vergleichbares Maß an Sicherheit bezüglich der Identität des Antragsteller zu erlangen.

Class 2-Zertifikate bieten ein Mindestmaß an Sicherheit für die Kommunikation im geschäftlichen Bereich. Eine persönliche Identitätsfeststellung ist jedoch nicht erforderlich. Für Electronic Commerce, Electronic Banking oder ähnliche, offen ausgelegte Anwendungen, die Finanztransaktionen oberhalb des Micropayment-Niveaus beinhalten, sollten unbedingt Class 3-Zertifikate verwendet werden, um ein höheres Maß an Vertrauen zu schaffen!

Class 2-Zertifikate sind hauptsächlich für gesicherte Kommunikation zwischen einander auch außerhalb des Internets bekannten Partnern gedacht, beispielsweise um Niederlassungen eines Unternehmens die sichere Übermittlung geschäftlicher Interna zu ermöglichen, oder für sichere E-Mail-Kommunikation im geschäftlichen Bereich.

Nicht in Deutschland lebende Privatkunden können durch Class 2-Zertifikate auf einfachem Wege ein Zertifikat beantragen, deren „Level of Trust“ höher ist als bei einfachen Class 1-Zertifikaten, die nur eine Prüfung der E-Mail-Adresse erfordern.

3.4 Class 3-Zertifikate

Class 3-Zertifikate werden sowohl für private als auch geschäftliche Nutzung ausgestellt. Class 3 umfasst für Privatpersonen den Zugriffstest, wie bei Class 1, auf eine im Zertifikat angegebene E-Mail-Adresse (sofern vorhanden), für Organisationen die bei Class 2 durchgeführten Prüfungen, wobei abweichend zu den dort genannten Anforderungen ein vom Amtsgericht beglaubigter Handelsregisterauszug (keine Kopie) vorliegen muss.

Class 3 beinhaltet darüber hinaus eine Identitätsprüfung derjenigen natürlichen Person, auf die sich das Class 3-Zertifikat bezieht. Bei geschäftlich genutzten Zertifikaten, die nicht auf eine natürliche Person ausgestellt sind – Beispiel: SSL-Zertifikate für Web Server –, ist dies eine im Handelsregisterauszug (oder vergleichbaren Dokumenten) genannte zeichnungsberechtigte (natürliche) Person, also üblicherweise ein Geschäftsführer oder Prokurist.

Mit der Ausstellung eines Class 3-Zertifikats bestätigt TC TrustCenter zusätzlich zu den für Class 1 bzw. 2 angegebenen Prüfungen, dass

1. diese Person anhand ihres Personalausweises oder Reisepasses identifiziert worden ist.



2. im Zertifikat enthaltene Angaben zur Person mit den Angaben im Ausweis übereinstimmen.

Class 3-Zertifikate stellen das notwendige Vertrauen für die Kommunikation sowohl im privaten als auch im geschäftlichen Bereich her. Geschäftliche Angaben im Zertifikat sind anhand schriftlicher Bestätigungen von verantwortlichen Personen und des Handelsregisterauszugs geprüft. Zu jedem Zertifikat gibt es eine verantwortliche Person, die persönlich anhand ihres Ausweises identifiziert worden ist.

Class 3-Zertifikate sind vor allem für Anwendungen im Electronic Commerce gedacht, beispielsweise für Internet Banking oder Online Shopping, wo eine persönliche Identitätsfeststellung notwendig ist oder bevorzugt wird.

TC TrustCenter stellt auch spezielle Zertifikate für Software-Entwickler aus (Microsoft Authenticode, Netscape Object Signing), und zwar sowohl für Firmen als auch für Einzelpersonen. Zu beachten ist, dass TC TrustCenter nicht das Programm selbst, dessen Unbedenklichkeit, programmtechnische Korrektheit oder sonstige Eignung für einen bestimmten Zweck zertifiziert, sondern dem Hersteller lediglich ein Mittel in die Hand gibt, um böswillige Modifikationen der von ihm vertriebenen Programme zu verhindern oder zumindest durch den Benutzer der Software erkennbar zu machen.

3.5 Class 4-Zertifikate

Class 4-Zertifikate werden nur für Privatpersonen ausgestellt. Class 4-Zertifikate umfassen dieselben Prüfungen wie entsprechende Class 3-Zertifikate. Die Identitätsfeststellung findet bei Class 4-Zertifikaten jedoch bei einer Meldebehörde statt, wobei die Ausweisdaten anhand des Melderegisters überprüft werden.

Class 4-Zertifikate stellen den höchsten Grad an Vertrauen für die Kommunikation im privaten Bereich her. Ein Vortäuschen einer falschen Identität mittels eines gefälschten Ausweises wird verhindert.



4 Die persönliche Identitätsfeststellung

Erfordert eine Zertifikatsklasse eine persönliche Identitätsfeststellung (Class 3 und 4), so kann diese entweder bei einer Postfiliale über das sogenannte Post Ident-Verfahren erfolgen, oder aber bei einem TC TrustCenter Ident Point[®]. TC TrustCenter ist selbst ein solcher Ident Point[®]; auch im Hause von TC TrustCenter in Hamburg kann also die Identitätsfeststellung durchgeführt werden. Für Class 4-Zertifikate erfolgt diese bei einer Meldebehörde, der eigentliche Ablauf ist aber der gleiche wie bei einem anderen TC TrustCenter Ident Point[®].

Vor der persönlichen Identitätsfeststellung muss stets der Zertifikatsantrag über das Online-Formular auf unseren Webseiten gestellt worden sein. Der Kunde erhält daraufhin an die im Zertifikatsantrag angegebene E-Mail-Adresse eine Nachricht, die eine für die Identitätsfeststellung benötigte Kontrollnummer enthält.

Beachten Sie vor der Erzeugung eines X.509- bzw. PGP-Schlüssels bitte den Abschnitt „Regeln für die Namensgebung“ hinsichtlich der einzutragenden Benutzerdaten.

4.1 Das Post Ident-Verfahren

Die Identitätsfeststellung über das Post Ident-Verfahren kann bei jeder Filiale der Deutschen Post vorgenommen werden.

In der Regel treffen ein bis zwei Werktage nach der Antragstellung über das Online-Formular die für die Identitätsfeststellung notwendigen Unterlagen beim Antragsteller ein. Dazu gehören neben dem Anschreiben detaillierte Erläuterungen zum weiteren Ablauf, ein Informationsblatt betreffend der Sorgfalts- und Mitwirkungspflichten des Zertifikatsinhabers, eine Antragsbestätigung, ein Coupon für das Post Ident-Verfahren sowie je ein blauer und weißer Umschlag.

Auf der Antragsbestätigung ist die per E-Mail erhaltene Kontrollnummer zu notieren sowie zu unterschreiben. Die unterschriebene Bestätigung wird zusammen mit einer vom Antragsteller anzufertigenden Ausweiskopie (beide Seiten) in den blauen Umschlag gesteckt, und dieser daraufhin verschlossen. Sodann begibt sich der Antragsteller mit den beiden Umschlägen und dem Coupon zu einer beliebigen Postfiliale und händigt sie dem Postmitarbeiter aus, der daraufhin die Identitätsfeststellung vornimmt und alle erforderlichen Unterlagen (inklusive des blauen Umschlags) im weißen Freiumschlag an TC TrustCenter weiterleitet.

Nach Eintreffen der Unterlagen bei TC TrustCenter werden diese geprüft und bei erfolgreicher Überprüfung wird das Zertifikat ausgestellt (üblicherweise innerhalb eines Werktages). Der Antragsteller wird per E-Mail von der Ausstellung des Zertifikats benachrichtigt und erhält darin Informationen zu dessen Installation und Benutzung.

4.2 TC TrustCenter Ident Points[®]

Die Identitätsfeststellung bei einem TC TrustCenter Ident Point[®] ist unkomplizierter und schneller als das Post Ident-Verfahren.

Während beim Post Ident-Verfahren die Unterlagen per Post zunächst an den Antragsteller und nach der Identitätsfeststellung in der Postfiliale an TC TrustCenter zurückgesendet werden müssen, erfolgt die Identitätsfeststellung im TC TrustCenter Ident Point[®] online, so dass das Zertifikat im Regelfall noch am selben Tag ausgestellt und dem Antragsteller zugesandt wird. Sobald der Antragsteller per E-Mail die Kontrollnummer erhalten hat, kann er sich, ausgerüstet mit dieser Kontrollnummer sowie der Antragsnummer und seinem Ausweis, zu ei-



nem TC TrustCenter Ident Point[®] begeben und die Identitätsfeststellung dort vornehmen lassen.

Im TC TrustCenter Ident Point[®] muss der Antragsteller die E-Mail-Kontrollnummer und die Antragsnummer nennen. Nach Eingabe der Ausweisdaten werden diese an TC TrustCenter gesendet, dort abgeglichen und das Zertifikat ausgestellt. Der Antragsteller muss eine Antragsbestätigung unterschreiben und eine Kopie seines Ausweises anfertigen lassen, die vom Ident Point[®] an TC TrustCenter zur Überprüfung weitergeleitet werden.

Sollte sich es herausstellen, dass Unstimmigkeiten im Zertifikatsantrag vorhanden sind, behält sich TC TrustCenter vor, das Zertifikat zu sperren. Im Falle der Sperrung des Zertifikats wird der Inhaber hiervon in Kenntnis gesetzt und erhält die Möglichkeit, einen neuen Antrag zu stellen und die fehlerhaften Angaben zu korrigieren.



5 Regeln für die Namensgebung

TC TrustCenter stellt Zertifikate sowohl nach dem PGP- als auch nach dem X.509-Standard aus. PGP-Zertifikate werden für die verschlüsselte Kommunikation per E-Mail oder das Verschlüsseln von Dateien verwendet. X.509-Zertifikate finden bei Web Browsern und Web Servern Anwendung, um eine gesicherte WWW-Verbindung oder eine Authentifikation des Benutzers gegenüber dem Server zu erreichen. X.509-Zertifikate können zudem für das in viele Browser oder populäre E-Mail-Produkte wie Microsoft Outlook '98 integrierte Verschlüsselungs- und Signaturverfahren S/MIME verwendet werden.

Dieser Abschnitt enthält eine Leitlinie für die Wahl einer geeigneten PGP-Benutzerkennung (PGP) bzw. das Ausfüllen der einzelnen Datenfelder des X.509-Zertifikatsantrags.

5.1 X.509-Zertifikate

X.509-Zertifikatsanträge enthalten die folgenden Datenfelder, die im Anschluss an nachstehende Tabelle näher erläutert und durch Beispiele veranschaulicht werden. Die dritte Spalte enthält die Bezeichnung der entsprechenden Eingabefelder auf unseren Online-Antragsseiten, die bei der Erzeugung des Zertifikatsantrags mit Hilfe eines Internet Browsers angezeigt werden.

Feld	Bedeutung	Bezeichnung im Online-Formular
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 Standardkürzel für das betreffende Land. Bei X.509-Zertifikatsanträgen, die mit dem Browser generiert werden, können Sie das Land auswählen, woraufhin automatisch das richtige Kürzel eingetragen wird. Bei Server-Zertifikatsanträgen hingegen, die mit der Server-Software (Microsoft Internet Information Server, Netscape Enterprise Server, Apache, ...) 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 bei X.509-Zertifikatsanträgen aus den USA gedacht. In Deutschland könnte man hier das Bundesland eintragen. Wir empfehlen Ihnen jedoch, dieses Datenfeld einfach leer zu lassen.

L (Locality): In dieses Feld können Sie den Firmensitz (geschäftlich genutzte Zertifikate) bzw. den Ort eintragen, in dem Sie laut Ausweis gemeldet sind (privat genutzte Zertifikate). Die Postleitzahl sollte hier nicht angegeben werden.

O (Organisation): Bei geschäftlich genutzten Zertifikaten können Sie hier Ihre Firma, Geschäfts- oder Organisationsbezeichnung eintragen. Wir empfehlen Ihnen, die Firma laut Handelsregistrauszug (sofern vorhanden) einzutragen, also beispielsweise „Computer Service AG“ statt „Computer Service“ oder „CS AG“.



Bei Code Signing-Zertifikatsanträgen von Einzelpersonen (freiberufliche Entwickler u. ä.) wird hier automatisch „Individual Software Publisher“ eingetragen.

OU (Organisational Unit): In dieses Feld können Sie die Abteilung eintragen, der das Zertifikat zugeordnet ist. Bei Code Signing-Zertifikatsanträgen wird hier automatisch „MS Authenticode“ oder „Netscape Object Signing“ eingetragen, je nach verwendetem Browser.

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, wobei ein Titel, der dem Vornamen voranzustellen ist, nur angegeben werden darf, wenn dieser im Ausweis eingetragen ist.

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.trustcenter.de`.

Ähnliches gilt für Organisationszertifikate, bei denen keine Person genannt werden soll. Als Eintrag in das CN-Feld empfiehlt es sich dann, die Firma zu verwenden.

Bei Code Signing Zertifikaten für Unternehmen 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 signierte Software überprüft.

Email: Dieses Feld muss, sofern 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, eine persönliche E-Mail-Adresse zu verwenden.

Die zuvor aufgeführten sieben Felder zusammen bilden den sogenannten Distinguished Name (DN). Ein bestimmter DN darf jeweils nur einer bestimmten Identität (dieser ggf. mehrfach für verschiedene Zertifikate) zugeordnet werden.

5.2 PGP-Zertifikate

PGP verwendet ab der Version 6.5 neben dem eigenen Zertifikatsformat auch X.509-Zertifikate für PGP-Schlüssel. TC TrustCenter unterstützt dies zum Zeitpunkt der Veröffentlichung dieser Richtlinien jedoch noch nicht, die nachstehende Darstellung beschränkt sich deshalb auf das PGP-eigene Zertifikatsformat. Bitte fragen Sie ggf. per E-Mail an info@trustcenter.de nach, wenn Sie X.509-Zertifikate mit PGP 6.5 oder höher verwenden möchten.

Das PGP-Zertifikatsformat sieht keinerlei Datenfelder vor. Ab Version 5.0 wird lediglich 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:

```
Hans Muster <hm@provider.de>
```

Für geschäftlich genutzte Zertifikate empfehlen wir Ihnen, 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 Feldbezeichner optional. In der Regel sollte auf die Angabe von OU, L und C verzichtet werden, also beispielsweise

Hans Muster, Muster GmbH <mm@muster-gmbh.de>

oder alternativ (ausführlicher aber unübersichtlicher)

Hans Muster, Muster GmbH, Marketing, Hamburg, DE <hm@muster-gmbh.de>

Es ist aber auch eine Benutzerkennung der Form

Muster GmbH Marketing <marketing@muster-gmbh.de>

möglich, falls ein Zertifikat einer Gruppe von Personen zugeordnet werden soll. Auch hier gibt es aber eine für die Verwaltung des zum Zertifikat gehörenden Signaturschlüssels verantwortliche Person, die TC TrustCenter bekannt sein muss.

5.3 Beispiele für X.509 Distinguished Names

	C	SP	L	O	OU	CN	EMAIL
Privat	DE		Hamburg			Hans Muster	hm@provider.de
Geschäftlich	DE		Kiel	Muster GmbH	Einkauf	Hans Muster	hm@muster.de
Organisation	DE	Schleswig Holstein	Kiel	Muster GmbH	Einkauf		einkauf@muster.de
Server	DE		Hamburg	Muster GmbH	Internet Services	www.muster.de	webmaster@muster.de
Code Signing	DE		Hamburg	Muster GmbH	MS Authenticode	Muster GmbH	info@muster.de
Code Signing Individual	DE		Hamburg	Individual Software Publisher	Netscape Object Signing	Hans Muster	hm@provider.de

5.4 Beispiele für PGP-Benutzerkennungen

Privat	Hans Muster, Musterstadt <hm@provider.de> Hans K. Muster <hm@provider.de>
Geschäftlich	Manfred Muster, Muster GmbH, Musterstadt <hm@muster-gmbh.de>
Organisation	Muster GmbH, Organisation Key <info@muster.de> Muster GmbH Bestellannahme, Musterstadt, DE <bestellung@muster.de>



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 privat	Keine Prüfung	Keine Prüfung	Keine Prüfung	Leer	Leer	Keine Prüfung	Zugriffstest
Class 2 privat	Ausweis	Keine Prüfung	Ausweis	Leer	Leer	Ausweis	Zugriffstest
Class 2 geschäftlich	HRA (Kopie)	Schriftliche Bestätigung	HRA (Kopie)	HRA (Kopie)	Schriftliche Bestätigung	Schriftliche Bestätigung, HRA (Kopie), Domain	Zugriffstest
Class 3 privat	Ident Point	Keine Prüfung	Ident Point	Leer	Leer	Ident Point	Zugriffstest
Class 3 geschäftlich	HRA (beglaubigt)	Schriftliche Bestätigung	HRA (beglaubigt)	HRA (beglaubigt)	Schriftliche Bestätigung	Ident Point + schriftl. Bestätigung, HRA (beglaubigt), Domain	Zugriffstest
Class 4 privat	Ident Point + Melderegister	Keine Prüfung	Ident Point + Melderegister	Leer	Leer	Ident Point + Melderegister	Zugriffstest

Keine Prüfung: TC TrustCenter überprüft dieses Datenfeld nicht. Dies trifft beispielsweise für das Feld SP (Bundesland) zu, dessen Angabe optional ist. Das Ausfüllen des Feldes SP wird für Zertifikatsanträge, die nicht aus den USA stammen, nicht empfohlen. Jegliche Daten in mit „Keine Prüfung“ markierten Feldern sind als nicht überprüft anzusehen!

Leer: Das Feld darf nicht ausgefüllt sein. Dies betrifft die Angabe von geschäftlichen Daten in den Feldern O und OU bei Zertifikatsanträgen von Privatpersonen.

Zugriffstest: Um die Existenz einer E-Mail-Adresse und die Erreichbarkeit des Zertifikatsinhabers unter derselben zu überprüfen, wird eine E-Mail an diese Adresse geschickt. Diese E-Mail enthält Daten, die zur vollständigen Identitätsfeststellung an uns zurückgesendet werden müssen.

HRA: Die Angaben in diesem Datenfeld werden anhand des Handelsregisterauszugs (oder vergleichbaren Dokumenten) geprüft. Dieser liegt entweder als Kopie oder als vom Amtsgericht beglaubigte Abschrift des Handelsregisters vor.

Schriftliche Bestätigung: Diese Daten müssen von einem Zeichnungsberechtigten unterschrieben und bestätigt werden. Dazu werden in der Antragsbestätigung Name und Abteilung der Mitarbeiter genannt, die ein Zertifikat erhalten sollen.

Ausweis: Die Überprüfung dieser Daten erfolgt durch Abgleich mit der Ausweiskopie, die TC TrustCenter zugesendet wird. Es findet jedoch keine persönliche Identitätsfeststellung statt.

Ident Point: Die Überprüfung dieser Daten erfolgt durch Abgleich mit der Ausweiskopie und dem unterschriebenen Antrag statt, die im Rahmen der Identitätsfeststellung TC TrustCenter zugesendet werden. Hinsichtlich der persönlichen Identitätsfeststellung beachten Sie bitte den Abschnitt „Die persönliche Identitätsfeststellung“.



Melderegister: Die Überprüfung dieser Daten erfolgt durch Abgleich mit dem Auszug des Melderegisters, der von der Meldebehörde, welche Identitätsfeststellung vornimmt, an TC TrustCenter geschickt wird.

Domain: Bei Server-Zertifikatsanträgen wird der Inhalt des Feldes CN, also der volle Domainname des Web Servers (beispielsweise `www.trustcenter.de`), durch Abfrage der Datenbank einer Internet-Registrierungsstelle dahingehend überprüft, ob die Domain (im Beispiel `trustcenter.de`) auf die im Feld O genannte Organisation registriert ist. Ist dies nicht der Fall, so muss TC TrustCenter eine Erlaubnis vom Inhaber der Domain für die Nutzung der Domain durch den Zertifikatsinhaber vorgelegt werden.



7 Sperren von Zertifikaten

Ein Zertifikat ist zu sperren, falls

1. der zugehörige private Schlüssel verloren oder kompromittiert wurde,
2. Angaben im Zertifikat ungültig sind (z. B. nach Wechsel der E-Mail-Adresse).

Ein Sperrung kann auf mehrere Arten veranlasst werden:

1. Wenn der Zertifikatsinhaber noch Zugriff auf seinen privaten Schlüssel hat, so kann er den [Sperrantrag](#) verwenden, der auf den Webseiten von TC TrustCenter zur Verfügung gestellt wird. Dazu muss er sich mit seinem Zertifikat authentisieren.
2. Hat der Zertifikatsinhaber seinen privaten Schlüssel verloren oder ist der Zugriff darauf aus irgendwelchen Gründen nicht mehr möglich, so kann er sich telefonisch bei TC TrustCenter melden und sich durch Nennung des bei der Antragstellung vergebenen Notfallpasswortes authentisieren.
3. Der Zertifikatsinhaber kann schriftlich bei TC TrustCenter die Sperrung seines Zertifikats beantragen. Zur Authentisierung wird die Unterschrift des Inhabers herangezogen.
4. Jeder Dritte, der Zertifikatsinhalte bestätigt hat, muss TC TrustCenter schriftlich darüber informieren, sobald die betreffenden Daten ungültig werden. Hat TC TrustCenter Kenntnis über ungültige Zertifikatsangaben erlangt, wird das betreffende Zertifikat umgehend gesperrt.

TC TrustCenter bestätigt die Ausführung der Sperrung per digital signierter E-Mail.