



TC TrustCenter Zertifizierungsrichtlinien

Version vom 1. März 1999

1	EINLEITUNG	2
2	WICHTIGE HINWEISE	3
3	ZERTIFIKATKLASSEN	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	5
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 ZERTIFIKATDATEN	12
7	SPERREN VON ZERTIFIKATEN	13



1 Einleitung

Dieses Dokument beschreibt die Zertifizierungsrichtlinien von TC TrustCenter. Es wird die Einteilung in verschiedene Zertifikatklassen sowie deren Bedeutung für Antragsteller bzw. Zertifikatinhaber 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“ (Zertifikatinhaber) und „Relying Party“ (sich auf die Vertrauenswürdigkeit eines Zertifikats verlassende Partei) genannt, werden in der Folge als „Teilnehmer“ bezeichnet.

Im Anschluß an die Einteilung der Zertifikatklassen werden Hinweise zur persönlichen Identitätsfeststellung gegeben, die für einige Zertifikatklassen notwendig ist, um das Vertrauen in die Bindung zwischen Zertifikat und Zertifikatinhaber zu erhöhen.

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 Zertifikatinhabers enthalten kann. Beispiele für geeignet gewählte Namen finden sich im Anschluß an die Darlegung der Richtlinien.

Abschließend 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 Zertifikatklasse auf welche Weise gecheckt werden.

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 for Security in Data Networks GmbH
Am Werder 1
21073 Hamburg
Deutschland

WWW:<http://www.trustcenter.de>
E-Mail: info@trustcenter.de
Telefon: +49 40 76629-3301
Telefax: +49 40 76629-577



2 Wichtige Hinweise

TC TrustCenter ist keine gemäß SigG §4 genehmigte Zertifizierungsstelle. TC TrustCenter hat bereits einen Antrag auf Genehmigung bei der [RegTP](#) gestellt.

Je höher die Zertifikatklasse, 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 Zertifikates 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 Zertifikatinhaber tatsächlich derjenige ist, der er vorgibt zu sein. Sie geben keinerlei Hinweise auf die Vertrauenswürdigkeit des Zertifikatinhabers selbst.

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 Zertifikatklasse 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 Zertifikatinhabers. Der Zertifikatinhaber muß zur Sicherheit der Verfahren beitragen. Dazu muß er die Sorgfalts- und Mitwirkungspflichten in den [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. Dieses Dokument, 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 Zertifikatklassen

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 Zertifikates 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 Zertifikatklasse. 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 Zertifikatklassen unterscheiden sich in der Verlässlichkeit der durch die Zertifizierung getroffenen Aussage, daß der Zertifikatinhaber 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 Testzertifikate aus. Diese haben standardmäßig eine verkürzte Gültigkeitsdauer und dürfen nur zu Testzwecken verwendet werden.

Die Angaben in Testzertifikaten 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 Teilnehmers in einem Class 1 Zertifikat werden über einen einfachen Zugriffstest auf die E-Mail-Adresse hinaus, abgesehen von der Eindeutigkeit und Gültigkeit des Zertifikatnamens unter den von TC TrustCenter ausgestellten Zertifikaten (siehe dazu den Abschnitt „Regeln für die Namensgebung“), in keiner Weise überprüft. Jegliche Teilnehmerdaten sind, abgesehen von der E-Mail-Adresse, als nicht überprüft 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 nur an Organisationen und für die geschäftliche Nutzung ausgestellt. Class 2 Zertifikate bestätigen, daß

1. das angegebene Unternehmen existiert. Dazu muß TC TrustCenter ein aktueller Handelsregisterauszug oder ein vergleichbares Dokument vorliegen. Vor Ausstellung von Class 2 Zertifikaten muß eine persönliche Kontaktaufnahme mit TC TrustCenter in telefonischer und schriftlicher Form erfolgen.
2. zeichnungsberechtigte Personen des Unternehmens den Inhalt des Zertifikates persönlich oder über von ihnen bestimmte Dritte bestätigt haben. Diese Bestätigung muß ent-



weder handschriftlich unterschrieben oder digital signiert mit einem TC TrustCenter Zertifikat Class 2, 3 oder 4 erfolgen.

3. die Zertifikatdaten, abgesehen von persönlichen Informationen, zusätzlich soweit möglich von TC TrustCenter überprüft wurden (siehe dazu den Abschnitt „Überprüfung der Zertifikatdaten“). Beispielsweise wird bei Serverzertifikaten die Registrierung der angegebenen Domain auf die im Zertifikatantrag 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.

Class 2 Zertifikate stellen das notwendige Vertrauen für die Kommunikation im geschäftlichen Bereich her. Die im geschäftlichen Bereich wichtigsten Informationen sind anhand schriftlicher Bestätigungen von verantwortlichen Personen und des Handelsregisterauszugs geprüft. Eine persönliche Identitätsfeststellung ist jedoch nicht erforderlich.

Class 2 Zertifikate sind hauptsächlich für gesicherte Übertragungen vom und zum Web Server gedacht, beispielsweise um den eigenen Kunden die sichere Übermittlung persönlicher Informationen zu ermöglichen, sowie für sichere E-Mail-Kommunikation im geschäftlichen Bereich.

3.4 Class 3 Zertifikate

Class 3 Zertifikate werden sowohl für private als auch geschäftliche Nutzung ausgestellt. Class 3 Zertifikate umfassen für Privatpersonen den Zugriffstest wie bei Class 1 auf eine im Zertifikat angegebene E-Mail-Adresse, für Organisationen die bei Class 2 durchgeführten Prüfungen. Zusätzlich wird die Identität derjenigen natürlichen Person geprüft, auf die sich das Class 3 Zertifikat bezieht.

Class 3 Zertifikate bestätigen zusätzlich zu den in 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 Softwareentwickler aus (MS Authenticode, Netscape Object Signing), und zwar sowohl für Firmen als auch für Einzelpersonen.

3.5 Class 4 Zertifikate

Class 1 Zertifikate werden nur für Privatpersonen ausgestellt. Class 4 Zertifikate umfassen dieselben Prüfungen wie Class 3 Zertifikate. Die Identitätsfeststellung findet bei Class 4 Zertifikaten jedoch bei einer Meldebehörde statt, wobei die Ausweisdaten anhand des Melderegisters überprüft werden.

TC TrustCenter Zertifizierungsrichtlinien

Version vom 1. März 1999



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 Zertifikatklasse 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 der anderen TC TrustCenter Ident Points.

Vor der persönlichen Identitätsfeststellung muß stets der Zertifikatantrag über das Online-Formular auf unseren Webseiten gestellt worden sein. Der Kunde erhält daraufhin an die im Zertifikatantrag 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 ist für die meisten Benutzer sicherlich der einfachste Weg, da sie bei jeder Filiale der Deutschen Post vorgenommen werden kann und somit selten ein weiter Weg nötig ist.

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 Zertifikatinhabers, 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 Personalausweiskopie (beide Seiten) in den blauen Umschlag gesteckt, und dieser daraufhin verschlossen. Sodann begibt sich der Antragsteller mit den beiden Umschlägen und dem Coupon zur nächstgelegenen Postfiliale und händigt sie dem Postbeamten 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 das Zertifikat erzeugt (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 TC TrustCenter Ident Points ist unkomplizierter und schneller als das Post Ident Verfahren, allerdings gibt es erheblich mehr Postfilialen als TC Ident Points.

Während beim Post Ident Verfahren die Unterlagen per Post zunächst an den Antragsteller und nach der Identitätsfeststellung im Postamt 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, ausgerü-

TC TrustCenter Zertifizierungsrichtlinien

Version vom 1. März 1999



stet mit dieser Kontrollnummer sowie der Antragsnummer und seinem Personalausweis, zum von ihm gewählten TC TrustCenter Ident Point begeben und die Identitätsfeststellung dort vornehmen lassen.

Im TC TrustCenter Ident Point muß der Antragsteller E-Mail-Kontrollnummer und Antragsnummer nennen. Nach Eingabe der Personalausweisdaten 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 Zertifikatantrag vorhanden sind, behält sich TC TrustCenter vor, daß Zertifikat zu revozieren. 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 die in viele Browser oder populäre E-Mail-Produkte wie MS Outlook '98 integrierte E-Mail-Verschlüsselung (S/MIME) verwendet werden.

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

5.1 X.509-Zertifikate

X.509-Zertifikatrequests 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 Requests mit Hilfe eines Internet Browsers angezeigt werden.

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

C (Country): Dieses Feld enthält stets das zweibuchstabile ISO-Kürzel für das betreffende Land. Bei Zertifikatrequests, die mit dem Browser generiert werden, können Sie das Land auswählen, worauf automatisch das richtige Kürzel eingetragen wird. Bei Server-Zertifikatanträgen hingegen, die mit der Server-Software (MS 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 die Eintragung des Bundesstaates bei Zertifikatrequests aus den USA gedacht. In Deutschland könnte man hier das Bundesland eintragen. Wir empfehlen Ihnen jedoch, dieses Datenfeld einfach freizulassen.

L (Locality): In dieses Feld können Sie den Firmensitz (geschäftlich genutzte Zertifikate) bzw. den Ort eintragen, in dem Sie laut Personalausweis gemeldet sind (privat genutzte Zertifikate).

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 Zertifikatrequests 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 Zertifikatrequests 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 CN 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 ist bei Benutzerzertifikaten Pflichtfeld und muß 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 E-Mail-Adresse wie `webmaster@firma.de` oder `info@firma.de` anzugeben.

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-Zertifikate sehen 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 wie ein entsprechendes X.509-Zertifikat enthält. Unter Benutzung der Datenfeldbezeichnungen des X.509-Standards hat diese folgende Form:

```
CN, O, [OU, L, C] <Email>
```

Dabei sind alle in eckigen Klammern genannten Feldbezeichner optional und sollten in der Regel weggelassen 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>

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 Zertifikatdaten

TC TrustCenter überprüft X.509-Zertifikatrequests 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 geschäftlich	HRA	Schriftliche Bestätigung	HRA	HRA	Schriftliche Bestätigung	Schriftliche Bestätigung, HRA, InterNIC	Zugriffstest
Class 3 privat	Ausweis	Keine Prüfung	Ausweis	Leer	Leer	Ausweis	Zugriffstest
Class 3 geschäftlich	HRA	Schriftliche Bestätigung	HRA	HRA	Schriftliche Bestätigung	Ausweis + schriftl. Bestätigung, HRA, InterNIC	Zugriffstest
Class 4 privat	Ausweis + Melderegister	Keine Prüfung	Ausweis + Melderegister	Leer	Leer	Ausweis + Melderegister	Zugriffstest

Keine Prüfung: TC TrustCenter überprüft dieses Datenfeld nicht. Dies trifft beispielsweise meistens für das Feld SP (Bundesland) zu, dessen Angabe optional ist. Das Ausfüllen des Feldes SP wird von uns für Zertifikatanträge, 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 Zertifikatrequests von Privatpersonen.

Zugriffstest: Um die Existenz einer E-Mail-Adresse und die Erreichbarkeit des Zertifikatinhabers 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.

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

Ausweis: Die Überprüfung dieser Daten erfolgt durch Abgleich mit der Personalausweiskopie, die im Rahmen der Identitätsfeststellung TC TrustCenter zugesendet oder selbst erzeugt wird. 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 an TC TrustCenter geschickt wird.

InterNIC: Bei Server-Zertifikatrequests wird der Inhalt des Feldes CN, also der volle Domainname des Web Servers (beispielsweise `www.trustcenter.de`), durch Abfrage der Datenbank des InterNIC oder entsprechender Dienste dahingehend überprüft, ob die Domain (im Beispiel `trustcenter.de`) auf die im Feld O genannte Organisation registriert ist.



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 Zertifikatinhaber 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 Zertifikatinhaber 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 Zertifikatinhaber kann schriftlich bei TC TrustCenter die Sperrung seines Zertifikates beantragen. Zur Authentisierung wird die Unterschrift des Inhabers herangezogen.
4. Jeder Dritte, der Zertifikat Inhalte bestätigt hat, muß TC TrustCenter schriftlich darüber informieren, sobald die betreffenden Daten ungültig werden. Sobald TC TrustCenter Kenntnis über ungültige Zertifikatangaben erlangt, wird das betreffende Zertifikat umgehend gesperrt.

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