finanz informatik
technologie service

Richtlinie

Zertifikate im FI-TS Trustcenter

Dokumentenverantwortliche/r: Fehlauer, Katrin

Geltungsbereich: FI-TS gesamt
(alle MitarbeiterInnen, alle Standorte,
alle Organisationseinheiten)
Alle Nutzer von Zertifikaten des FI-TS Trustcenter

Dieses Dokument wird auf der Home-Page des FI-TS Trustcenter veröffentlicht.
Freigegeben ist ausschließlich die im Intranet bzw. Internet veröffentlichte Version.
Ausdrucke unterliegen keiner Aktualisierung!

Inhaltsverzeichnis

1 Ziel

Dieses Dokument beschreibt die technischen Standards des FI-TS Trustcenters für die Ausstellung von Zertifikaten. Dieses Dokument wird durch die Richtlinie „Zertifizierung im FI-TS Trustcenter“ ergänzt. Ziel beider Dokumente ist es, eine Einschätzung der Vertrauenswürdigkeit der durch das FI-TS Trustcenter ausgestellten Zertifikate zu ermöglichen.

Zertifikatsrichtlinie und Zertifizierungsrichtlinie sind Teil der Vertragsgrundlagen, die jeder Teilnehmer mit der Beantragung eines Zertifikats anerkennt.

Diese Richtlinie ist angelehnt an den “X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework”, veröffentlicht als RFC 3647 durch die IETF (Internet Engineering Task Force) und den RFC 3280 - “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile”.

Das Dokument orientiert sich außerdem an den Anforderungen der ISO 27002 Kapitel 12.3.2.

1.1 Identifikation des Dokumentes

Name: Zertifikate im FI-TS Trustcenter

OID: 1.3.6.1.4.1.23389.1.2.1.1.2

1.2 Abgrenzung

Zusätzlich zu den Richtlinien „Zertifikate im FI-TS Trustcenter“ und „Zertifizierung im FI-TS Trustcenter“ können vertragliche Vereinbarungen mit Kunden bestehen. FI-TS sichert zu, keine Vereinbarungen zu schließen, die der Intention dieser Dokumente zuwiderlaufen oder sie schwächen.

Im Falle etwaiger Abweichungen zwischen vertraglichen Vereinbarungen und diesem Dokument gelten die vertraglichen Vereinbarungen.

Es können in wenigen Fällen für Kunden des FI-TS Trustcenters bereitgestellte Managed PKI bestehen. Diese Managed PKI unterliegen *nicht* dieser Richtlinie, sondern der Kunde erstellt hierfür eigene Policies und betreibt seine Managed PKI eigenverantwortlich nach diesen Richtlinien.

Sofern der Betrieb solcher PKI an das FI-TS Trustcenter übertragen wird, kann diese Richtlinie Anwendung finden.

Das FI-TS Trustcenter erstellt keine qualifizierten Zertifikate im Sinne des deutschen Signaturgesetzes. Damit sind diese Zertifikate nicht zur Durchführung von Rechtsgeschäften geeignet.

Es besteht kein Rechtsanspruch auf die Ausstellung eines Zertifikates.

2 Schreibweise

Für dieses Dokument werden folgende Schreibweisen definiert:

[name]	Variabler Parameter, der in der Implementierung und Betriebsphase definiert wird. z.B. [fqdn] kann durch www.f-i-ts.de ersetzt werden.
[alt1| alt2]	Variabler Parameter, der einen definierten Alternativwert annehmen kann. z.B. [c=de|c=at] hat die gültigen Werte c=de oder c =at

3 Allgemeines

3.1 Anwendungsbereich

Das FI-TS Trustcenter wird von Finanz Informatik Technologie Service GmbH & Co. KG betrieben, im folgenden auch FI-TS genannt. Es werden Zertifikate für FI-TS, seine Kunden sowie Institutionen aus dem Banken- und Versicherungsumfeld ausgestellt.

3.2 Kontaktinformationen

Ansprechsprechpartner:
Finanz Informatik Technologie Service GmbH & Co. KG
FI-TS Trustcenter
Richard-Reitzner-Allee 8
D-85540 Haar
Telefon 089 94511 -0

4 Schlüsselprofile

Seitens des FI-TS Trustcenters werden Zertifikate für Schlüssel mit folgenden Eigenschaften ausgestellt.

- Algorithmus: RSA mit sha2 oder elliptische Kurve (NIST CURVE)
- Schlüssellänge:

CA-Schlüssel	RSA 4096 bit oder ECC 512 bit
Public Keys der Nutzer-Zertifikate	RSA 2048 oder 4096 bit NIST CURVE 256, 384 oder 521 bit

Hinweise:

Es bestehen noch einige wenige Signing-CAs mit einer Schlüssellänge geringer als RSA 4096 bit. Diese CAs werden ausschließlich zur Erstellung der CRLs verwendet. Neue Zertifikate werden damit nicht mehr ausgestellt.

Nutzer-Zertifikate mit einer Schlüssellänge geringer als RSA 2048 bit werden nicht mehr ausgestellt.

5 Zertifikatsprofile

Die Zertifikatsprofile sind an die IETF-Dokumente “Internet X.509 Public Key Infrastructure: Certificate and Certificate Revocation List (CRL) Profile”, veröffentlicht als RFC 3280, und an „Internet Attribute Certificate Profile for Authorization“, veröffentlicht als RFC 3281, angelehnt.

Die nachfolgenden Ausführungen geben einen Überblick. Details sind in der Arbeitsanleitung „Prüfung von Zertifikatsanträgen“ geregelt.

5.1 Basis-Zertifikatsfelder

Das FI-TS Trustcenter betreibt folgende PKIs:

5.1.1 Root F04 G1 und Root EBP G1

Standard: X.509 V3

Root bzw. Intermediate	Generation	CN	Aussteller	Schlüssel-länge	Signatur-Algorithmus	Gültigkeit
Root	1	Finanz Informatik Technologie Service F04 Root CA G1	self-signed	4096	sha256With-RSAEncryption	bis 02.03.2035
Class1	2	Finanz Informatik Technologie Service F04 Class1 CA G2	Finanz Informatik Technologie Service F04 Root CA G1	4096	sha256With-RSAEncryption	bis 28.02.2034
Class2	2	Finanz Informatik Technologie Service F04 Class2 CA G2	Finanz Informatik Technologie Service F04 Root CA G1	4096	sha256With-RSAEncryption	bis 01.03.2035
Class2	3	Finanz Informatik Technologie Service F04 Class2 CA G3	Finanz Informatik Technologie Service F04 Root CA G1	ECC512	sha256With-RSAEncryption	bis 01.01.2035
Class2 BayernLB	2	Finanz Informatik Technologie Service F04 Class2 BayernLB CA G2	Finanz Informatik Technologie Service F04 Root CA G1	4096	sha256With-RSAEncryption	bis 28.02.2034
Root	1	Finanz Informatik Technologie Service EBP Root CA G1	self-signed	ECC512	ecdsa-with-SHA512	bis 17.01.2047
Class1	1	Finanz Informatik Technologie Service EBP Class1 CA G1	Finanz Informatik Technologie Service EBP Root CA G1	ECC512	ecdsa-with-SHA512	bis 17.01.2047
Class2	1	Finanz Informatik Technologie Service EBP Class2 CA G1	Finanz Informatik Technologie Service EBP Root CA G1	ECC512	ecdsa-with-SHA512	bis 17.01.2047

5.1.2 Managed PKI

Neben diesen in Verantwortung des FI-TS Trustcenters betriebenen PKIs können für Kunden auf besonderen Wunsch eine Managed PKI eingerichtet und bereitgestellt sein.

Solche PKI sind nicht Gegenstand dieser Richtlinie (siehe hierzu Kap. 1.2 Abgrenzung).

5.1.3 Zertifikats-Subject

Das Subject-Feld enthält einen eindeutigen X.500 Distinguished Name (DN). Dieser DN ist aus folgenden Objektklassen aufgebaut:

CN =[Identifizierung des Endnutzers],
OU =[Organisationseinheit],
O =[Name des Unternehmens/Kunden],
C =[Countrycode]

Die einzelnen Felder sind in Abhängigkeit von Zertifikats-Typ und der Zertifikatsklasse wie folgt zu füllen:

Objektklasse C:

Diese Objektklasse muss grundsätzlich gesetzt sein. Für die Zertifikatsklasse 1 können Ausnahmen bestehen. Näheres regelt die Fachliche Richtlinie „Windows CAs“. Alle Zertifikate verwenden hier den zweistelligen ISO Countrycode für den Staat, in dem das Unternehmen bzw. der Kunde seinen Sitz hat.
Beispiel: Deutschland: C=DE

Objektklasse O:

Diese Objektklasse muss grundsätzlich gesetzt sein. Hier werden folgende Verwendungen unterschieden:

- CA- und Sub-CA-Zertifikate:
  Die Objektklasse muss für diese Zertifikate stets gesetzt sein und sie muss grundsätzlich auf O=Finanz Informatik Technologie Service GmbH & Co. KG gesetzt sein. Für die CAs der Secure Email-Gateways ist vertraglich vereinbart, die Objektklasse mit O=Finanz Informatik GmbH & Co. KG zu setzen. Andere Inhalte dieser Objektklasse sind für diese Zertifikate nicht zulässig.

- Endnutzer-Zertifikate (Zertifikate für end-entities):
  Die Objektklasse muss für diese Zertifikate grundsätzlich gesetzt sein. Für die Zertifikatsklasse 1 können Ausnahmen bestehen. Näheres regelt die Fachliche Richtlinie „Windows CAs“.
  Die Objektklasse sollte auf die Bezeichnung des Kunden/Mandanten gemäß seines Handelsregistereintrages gesetzt sein. Alternativ kann auch ein aussagefähiges und eindeutiges Kürzel pro Kunde/Mandant verwendet werden. Die Schreibweise dieses Kürzels gibt das FI-TS Trustcenter vor.
  Beispiel für FI-TS:
  O=Finanz Informatik Technologie Service GmbH & Co. KG bzw. O=FI-TS

Objektklasse OU:

Diese Objektklasse ist optional. Entsprechend den Anforderungen können die Werte mit dem FI-TS Trustcenter abgestimmt und festgelegt werden:

- Für CA- und Sub-CA Zertifikate: Soweit diese Objektklasse genutzt wird, kann hier ein eindeutiger Name der Organisationseinheit, die für die Sub-CA verantwortlich ist oder ein Hinweis auf den Einsatzzweck der CA enthalten sein.

- Für Endnutzer-Zertifikate: Hier können Hinweise auf Organisationseinheiten, Applikationen oder andere Werte enthalten sein.
  Beispiel: OU=Abteilung 76050 bzw. OU=76050

Objektklasse CN:

Diese Objektklasse muss stets gesetzt sein. Die Werte sind unabhängig von den Zertifikatsklassen.

- CA-Zertifikate:

Die Objektklasse muss für Class2 oder Class3-CAs auf CN= Finanz Informatik Technologie Service [Art der CA] gesetzt sein.
Beispiel: Finanz Informatik Technologie Service F04 Root CA G1

Bei Class1-CAs kann der der Unternehmensname im CN auch abgekürzt sein auf CN=FI-TS [Art der CA]
Beispiel: FI-TS F04 Class1 Win-Mail-Online CA G2

Für seit 2012 in Betrieb befindliche und künftig neu zu erstellende PKI werden neben den oben aufgeführten Inhalten des CN wesentliche Merkmale der CA zur besseren Unterscheidbarkeit im CN vermerkt:

- Hinweis auf die Schlüssellänge, z.B. F04 für RSA 4096 bit, F08 für 8192 bit.
- Klasse, z.B. Class2.
- Generation, z.B. G1, G2 usw. Eine neue Generation der gleichen Klasse mit gleicher Schlüssellänge wird z.B. dann angelegt, wenn ein neuer Signatur-Algorithmus einzuführen ist.

Beispiel: Finanz Informatik Technologie Service F04 Class2 CA G2

Alternativ kann der CN einen Namen enthalten, der dem jeweiligen Mandanten/Kunden eindeutig zuzuordnen ist. Dieser Name darf um weitere Informationen, wie zum Beispiel einen Verwendungszweck, erweitert werden.
Beispiel: „Secure E-Mail CA Sparkasse Rhein-Haardt“ oder auch „Finanz Informatik Technologie Service F04 Class2 BayernLB CA G2“.

- Natürliche Personen

  Im CN muss der Name der natürlichen Person oder ein äquivalentes, für den Anwendungsfall eindeutiges Kennzeichen hinterlegt sein (z.B. AD Anmeldename, E-Mail Adresse).

- Juristische Personen

  Im CN muss ein gültiger Name der juristischen Person oder ein äquivalentes eindeutiges Merkmal hinterlegt sein (z.B. Nummer des Handelsregistereintrags)

- Maschinennamen

  Im CN Feld muss der FQDN oder eine andere Form des Maschinennamens eingetragen sein. Dieser Name muss die Maschine in ihrem Kontext eindeutig identifizieren.

  Sollte der CN einen Domain-Namen betreffen, der öffentlich registriert ist, muss der Auftraggeber eine entsprechende Autorisierung gem. Richtlinie „Zertifizierung im FI-TS Trustcenter“ – dort Kapitel 8 – nachweisen.

- Maschinenadressen

  Im CN muss der FQDN oder eine andere Form des Maschinennamens eingetragen sein.

  Maschinenadressen werden in den dafür vorgesehenen Feld subjectAltIp eingetragen.

Das FI-TS Trustcenter kann mehrere Zertifikate mit dem gleichen CN für den gleichen Zertifikatsinhaber ausstellen.

Zusätzlich zum Zertifikats-Subject kann die Version 3 Erweiterung „subjectAltName“ zur Identifikation des Zertifikatsinhabers genutzt werden. Hierfür gelten sinnentsprechend dieselben Regeln. Da die Objektklasse CN nicht leer sein darf, wird der subjectAltName (s. Abschnitt 5.2.4) als nicht kritisch eingestuft.

Weitere Regelungen zur erlaubten Belegung der Felder sind in der Arbeitsanleitung „Prüfung von Zertifikatsanträgen“ festgelegt.

5.2 Zertifikatserweiterungen

Zertifikatserweiterungen (Extensions) legen zusätzliche Vorgaben zum Einsatzzweck von Zertifikaten fest. Es werden zwei Klassen von Erweiterungen unterschieden:

- kritisch: Die das Zertifikat nutzende Anwendung *muss* diese Erweiterung auswerten; wenn sie dies nicht kann, muss das Zertifikat als ungültig verworfen werden.
- unkritisch: Die das Zertifikat nutzende Anwendung *kann selbst entscheiden*, ob sie diese Erweiterung bei der Prüfung des Zertifikats nutzt.

5.2.1 Einsatzzweck des mit dem Zertifikat verbundenen Schlüsselmaterials (Key Usage)

OID: 2.5.29.15

Status: kritisch

Dieses Feld beschreibt den Verwendungszweck des zertifizierten öffentlichen und des damit verbundenen privaten Schlüssels.

Folgende Parameter werden grundsätzlich vom FI-TS Trustcenter verwendet:

Zertifikatstyp	Key Usage
CA und SUB-CA-Zertifikate	Signierung von Zertifikaten (certsign), Signierung von Zertifikatssperrlisten (crlsign)
Natürliche Personen	Verschlüsselung von Schlüsselmaterial (Key Encipherment) Digitale Signatur (Digital Signature)
Juristische Personen	Verschlüsselung von Schlüsselmaterial (Key Encipherment) Digitale Signatur (Digital Signature)
Maschinennamen und -adressen	Verschlüsselung von Schlüsselmaterial (Key Encipherment) Digitale Signatur (Digital Signature)

Aufgrund technischer Erfordernisse hinsichtlich des Einsatzzweckes eines Zertifikates können geänderte oder weitere Parameter Verwendung finden. Weitere Regelungen zu erlaubten Kombinationen von Key Usage und Extended Key Usage sind in der Arbeitsanleitung „Prüfung von Zertifikatsanträgen“ festgelegt.

5.2.2 Erweiterungen des Einsatzzweckes des mit dem Zertifikat verbundenen Schlüsselmaterials (Extended Key Usage)

Dieses Feld beschreibt den erweiterten Verwendungszweck des zertifizierten öffentlichen Schlüssels und des damit verbundenen privaten Schlüssels.

OID: 2.5.29.37

Status: nicht kritisch

Folgende Parameter werden vom FI-TS Trustcenter verwendet:

Zertifikatstyp	Extended Key Usage	OID
CA und SUB-CA-Zertifikate	nicht gesetzt	
Natürliche Personen	clientauth	1.3.6.1.5.5.7.3.2
Juristische Personen	codesigning	1.3.6.1.5.5.7.3.3
Maschinennamen und –adressen	serverauth und clientauth	1.3.6.1.5.5.7.3.1

Weitere Regelungen zur erlaubten Belegung der Felder sind in der Arbeitsanleitung „Prüfung von Zertifikatsanträgen“ festgelegt.

5.2.3 Zertifikatsrichtlinie

OID: 2.5.29.32
Status: Nicht kritisch
Folgende Parameter werden vom FI-TS Trustcenter verwendet:

Parameter	Wert
OID der Zertifizierungsrichtlinie	1.3.6.1.4.1.23389.1.2.1.1.1
URL an der die Zertifizierungsrichtlinie veröffentlicht wird	URL der Zertifizierungsrichtlinie
Name der Organisation die das Zertifikat ausstellt.	Finanz Informatik Technologie Service GmbH & Co. KG

5.2.4 subjectAltName

OID: 2.5.29.17
Status: Nicht kritisch
Folgende Parameter werden vom FI-TS Trustcenter verwendet:

	Natürliche Personen	Juristische Personen	Maschinennamen oder -adressen
Mailadresse[1] (rfc822Name)	✓	-	-
Vollständiger Domainname (DNSName)	-	-	✓
IP-Adresse (IPAddress)	-	-	✓

Beispiele für die einzelnen Werte:

	Beispiel
Mailadresse[2] (rfc822Name)	hans.mueller@f-i-ts.de
Vollständiger Domainname (DNSName)	webserver.f-i-ts.de
IP-Adresse (IPAddress)	192.168.1.2

5.3 CRL Verteilungspunkt

OID: 2.5.29.31
Status: nicht kritisch
Diese Erweiterung wird in allen Endnutzer -Zertifikaten verwendet und in CA-Zertifikaten, die ab 1.10.2018 ausgestellt wurden.
Die Bereitstellung der CRLs erfolgt per HTTP. Die URIs der CRL Verteilungspunkte werden pro CA festgelegt und sind in den Endnutzer-Zertifikaten enthalten.
Beispiel:

```
X509v3 CRL Distribution Points:
...
                    URI:http://pki.f-i-ts.de/crl/F04C2IZ2/CRL11.crl
```

Es ist möglich, segmentierte CRL oder Gesamt-CRL bereitzustellen.
Es ist außerdem möglich, CRL-Distribution Points zusätzlich per LDAP bereitzustellen.

[1] Mailadresse gemäß RFC 822

[2] Mailadresse gemäß RFC 822

5.4 Basic Constraints

OID: 2.5.29.19

Status: kritisch

Diese Erweiterung wird in allen CA-Zertifikaten (aber nicht Root-Zertifikaten) verwendet, die ab 1.10.2018 ausgestellt wurden.

Die Pfad-Länge ist so zu konfigurieren, dass auf Ebene der Issuing-CAs der Wert „0“ enthalten ist. Damit dürfen nach den internationalen Regelungen mit diesem CA-Zertifikat ausschließlich Endnutzer-Zertifikate ausgestellt werden.

Beispiel:

```
            X509v3 Basic Constraints: critical
                CA:TRUE,
pathlen:0
```

Bei Nutzerzertifikaten ist es möglich, aber nicht vorgeschrieben, Basic Constraints zu verwenden.

6 Zertifikatsrückrufliste (CRL)

Die durch das FI-TS Trustcenter erstellten CRLs werden per http bereitgestellt und im Internet veröffentlicht. Je nach zugrundeliegender Software werden die CRLs bevorzugt als performance-günstige segmentierte CRL oder aber als Gesamt-CRL erstellt.

- Segmentierte CRL:
  Hierbei wird nach einer festgelegten Anzahl ausgestellter Zertifikate eine neue CRL eröffnet und damit die CRL auf eine Maximalanzahl möglicher Einträge begrenzt. Für eine CA, die segmentierte CRLs erstellt, bestehen daher typischerweise mehrere CRLs.

  Sobald das Gültigkeitsende des am längsten laufendenden Zertifikates erreicht ist, wird die betr. CRL nicht mehr aktualisiert.
- Gesamt-CRL:
  Bei einer Gesamt-CRL werden *alle* gesperrten Zertifikate einer CA in genau einer gemeinsamen Liste geführt.

Darüber hinaus ist möglich, CRL per ldap bereitzustellen. Die URI der relevanten CRL ist in jedem Nutzerzertifikat vermerkt.

6.1 Format

Das FI-TS Trustcenter erstellt CRLs gemäß dem X509 Profil in der Version 3.

6.2 Grund eines Zertifikatsrückrufs

Folgende Gründe für einen Zertifikatswiderruf werden von dem FI-TS Trustcenter unterstützt:

Sperrgrund	**Sperrcode**
Sperrgrund nicht genauer spezifiziert	Unspecified
Kompromittierung eines privaten Teilnehmerschlüssels	keyCompromise
Kompromittierung eines privaten Schlüssels einer Zertifizierungsstelle	CACompromise
Änderung der Namensinformationen eines Zertifikates, ohne dass eine Kompromittierung des privaten Schlüssels vorliegt	affiliationChanged
Ablauf der Gültigkeit eines Zertifikates, ohne dass eine Kompromittierung des privaten Schlüssels vorliegt	superseded

Sperrgrund	Sperrcode
Zertifikat wird vor Ablauf seiner Gültigkeit nicht mehr benötigt, ohne dass eine Kompromittierung des privaten Schlüssels vorliegt	cessationOfOperation

7 Online Certificate Status Protocol (OCSP)

Online Certificate Status Protocol wird derzeit nicht allgemein angeboten.

8 Internes Kontrollsystem (IKS)

8.1 Kontrollziele aus dem „Sicheren IT-Betrieb“

Konzept-Nr	Bezeichnung	Kontrollziel
K106	Vertrauenswürdige Kanäle	Gewährleistung vertrauenswürdiger Kanäle zur Identifikation, Authentisierung und Nachrichtenübertragung
K108	Key-Management	Gewährleistung der sicheren Bereitstellung, Verteilung und Verwaltung von Schlüsseln

8.2 Zuordnung der Kontrollziele, -verfahren und -ergebnisse

Kontrollziel	Kontrollverfahren	Kontrollergebnis	Bemerkungen
Siehe oben	In dieser Richtlinie werden die Rahmenbedingungen für die Zertifizierung beschrieben. Der Ablauf der Zertifizierung und somit auch der Kontrollverfahren werden in der Richtlinie „Zertifizierung im FI-TS Trustcenter“ dokumentiert.		Die Richtlinie „Zertifizierung im FI-TS Trustcenter“ ist im Intranet unter IMS / Schriftliche Ordnung / Richtlinien veröffentlicht.

9 Anhang

9.1 Definitionen

Begriff	Definition
Freigabe-Ansprechpartner	Namentlich definierte Gruppen von Personen eines Kunden/Mandanten, die berechtigt sind, einen Zertifikatsrequest von Endteilnehmern dieses Kunden zu prüfen und freizugeben bzw. einen Rückruf eines Zertifikats zu initiieren. Diese Ansprechpartner werden beim Vertragsabschluss benannt und in der Vertragsdokumentation hinterlegt.
Kunde/Mandant	Ein Kunde/Mandant definiert zwei Gruppen: intern: Eine OE von FI-TS, die die Berechtigung hat, das FI-TS Trustcenter zu nutzen, der Antragsweg ist über ARS festgelegt. Extern: Ein Kunde von FI-TS, der einen Vertrag über die Trustcenter-Dienstleistung des FI-TS Trustcenters abgeschlossen hat.
Zertifikatsinhaber	Der Zertifikatsinhaber ist diejenige Person oder Organisation, für die dieses Zertifikat gemäß den Zertifikatsattributen ausgestellt wurde und die autorisierten Zugriff auf den zu einem Zertifikat gehörenden privaten Schlüssel besitzt. Organisationen werden durch einen namentlich dem FI-TS Trustcenter bekannten Vertreter vertreten.
Certification Revocation List	Hierbei handelt es sich um eine Auflistung von Zertifikaten, die innerhalb ihres Gültigkeitszeitraums für ungültig erklärt wurden, weil sie z. B. nicht mehr benötigt werden bzw. weil der private Schlüssel kompromittiert wurde.

9.2 Abkürzungen

API	Application Programming Interface
CA	Certification Authority: Zertifizierungsstelle
CP	Certification Policy: Zertifikatspolicy
CPS	Certification Practice Statement: Zertifizierungsrichtlinie
CRL	Certification Revocation List: Liste der widerrufenen Zertifikate
CRL-DP	Certification Revocation List Distribution Point
DN	Distinguished Name
http	Hyper Text Transfer Protocol
LDAP	Lightweight Directory Access Protocol
NTP	Network Time Protocol
OCSP	Online Certificate Status Protocol
OID	Objekt Identifikator
PKCS	Public Key Cryptographic Standards
PKI	Public Key Infrastructure
PKIX	Public Key Infrastruktur für X.509-Zertifikate
RA	Registration Authority: Registrierungsstelle
RSA	Rivest, Shamir, & Adleman Public Key Verschlüsselungsmethode
SCEP	Simple Certificate Enrollment Protocol
SHA1	Secure Hash Algorithm Version 1.0
SSL	Secure Socket Layer
TLS	Transport Layer Security
URI	Uniform Ressource Identifier
USB	Universal Serial Bus
VPN	Virtual Private Network
X.509	ISO Standard zum Format digitaler Zertifikate