finanz informatik
technologie service

Richtlinie

Zertifikate im FI-TS Trustcenter

Dokumentenverantwortliche/r: Birnbaum, Lutz

Vertraulichkeitsklasse: Offen

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 Trsutcenter“ 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 Trustcenter 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.

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, die in der Implementierung und Betriebsphase definiert, 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

Vom FI-TS-Trustcenter werden Zertifikate für Schlüssel mit folgenden Eigenschaften ausgestellt.

- Algorithmus: Public/Private Key: RSA mit sha2
- Schlüssellänge:

CA-Schlüssel	1024 bit oder 4096 bit
Public Keys der Nutzer-Zertifikate	>= 2048 bit

Hinweise:

Es bestehen noch Root- und Signing-CAs mit einer Schlüssellänge geringer als 4096 bit und auch solche, die Nutzerzertifikate noch mit dem Signauralgorithmus sha1 signieren. Diese CAs werden nur noch zur Erstellung der CRLs verwendet. Neue Zertifikate werden damit nicht mehr ausgestellt.

Nutzer-Zertifikate mit einer Schlüssellänge geringer als 2048 bit werden nicht mehr ausgestellt. Es sind jedoch noch Nutzer-Zertifikate mit einer geringeren Schlüssellänge in Umlauf.

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.

5.1 Basis-Zertifikatsfelder

Das FI-TS Trustcenter betreibt folgende PKIs:

5.1.1 Root F01 G1

Standard: X.509 V3

Root bzw. Intermediate	Generation	CN	Aussteller	Schlüssellänge	Signatur-Algorithmus	Gültigkeit
Root	1	Finanz Informatik Technologie Service Root CA	self-signed	1024	sha1With-RSAEncryption	bis 01.03.2035
Class2	1	Finanz Informatik Technologie Service Class 2 CA	Finanz Informatik Technologie Service Root CA	1024	sha1With-RSAEncryption	bis 01.03.2035
Class2 BayernLB	1	Finanz Informatik Technologie Service Class 2 BLB CA	Finanz Informatik Technologie Service Root CA	2048	sha1With-RSAEncryption	bis 01.09.2030

5.1.2 Root F04 G1

Standard: X.509 V3

Root bzw. Intermediate	Generation	CN	Aussteller	Schlüssellänge	Signatur-Algorithmus	Gültigkeit
Root	1	Finanz Informatik Technologie Service F04 Root CA G1	self-signed	4096	sha256With-RSAEncryption	bis 02.03.2035
Class1	1	Finanz Informatik Technologie Service F04 Class1 CA G1	Finanz Informatik Technologie Service F04 Root CA G1	4096	sha1With-RSAEncryption	bis 01.03.2035
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	1	Finanz Informatik Technologie Service F04 Class2 CA G1	Finanz Informatik Technologie Service F04 Root CA G1	4096	sha1With-RSAEncryption	bis 01.03.2035
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	1	Finanz Informatik	Finanz Informatik	4096	sha1With-	bis

Root bzw. Intermediate	Generation	CN	Aussteller	Schlüssellänge	Signatur-Algorithmus	Gültigkeit
BayernLB		Technologie Service F04 Class2 BayernLB CA G1	Technologie Service F04 Root CA G1		RSAEncryption	01.03.2035
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

5.1.3 Managed PKI

Neben diesen in Verantwortung des FI-TS Trustcenter betriebenen PKIs wurde für einen Kunden auf besonderen Wunsch eine Managed PKI eingerichtet und bereitgestellt. Für den Betrieb dieser Managed PKI ist der betr. Kunde in eigener Regie zuständig und verantwortlich. Diese PKI ist nicht Gegenstand dieser Richtlinie.

5.1.4 Betreff (Subject)

Das Betreff-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 gesetzt sein. 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 gesetzt sein. Hier werden folgende Verwendungen unterschieden:

- CA- und Sub-CA-Zertifikate: Die Objektklasse muss auf O=Finanz Informatik Technologie Service GmbH & Co. KG gesetzt sein.
- Endnutzer-Zertifikate: Die Objektklasse sollte ein Kundenkürzel beinhalten, das eindeutig pro Kunde/Mandant des FI-TS Trustcenters definiert ist. Alternativ kann auch die Bezeichnung des Kunden/Mandant gemäß seines Handelsregister-eintrages verwendet werden.
  Beispiel für FI-TS:
  O=FI-TS bzw. O= Finanz Informatik Technologie Service GmbH & Co. KG

Objektklasse OU:

Diese Oblektklasse 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 Endnutzerzertifikate: Hier können Hinweise auf Organisationseinheiten, Applikationen oder andere Werte enthalten sein..
  Beispiel: OU=Abteilung 76050: bzw. OU=76050

Objektklasse CN:

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

- CA-Zertifikate:

  Die Objektklasse muss auf CN= Finanz Informatik Technologie Service [Art der CA] gesetzt sein.
  Beispiel: Finanz Informatik Technologie Service F04 Root CA G1.

  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 4096 bit, F08 für 8192 bit.
  - Klasse, z.B. Class2.
  - Generation, z.B. G1, G2. 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“.

- Server-Zertifikate:

Class 1	Class 2	übrige
Frei wählbar	• Full Qualified Domain Name (FQDN) des zugehörigen Endsystems (z.B. CN=webserver.f-i-ts.de) oder • IP-Adresse des zugehörigen Endsystems (z.B. CN=192.168.1.2) oder • Eigener Name des Systems oder der Anwendung (z.B. CN=MQ-Series-MT01)	wie Class 2

- Client-Zertifikate für Geräte:

Class 1	Class 2	übrige
Frei wählbar	Der CN muß das Gerät bzw. in seinem Kontext eindeutig identifizieren, z.B.: ▪ Full Qualified Domain Name (FQDN) des zugehörigen Endsystems (z.B. CN=clientxyz.f-i-ts.de) ▪ Eigener, eindeutiger Name des Gerätes (z.B. CN=abc00004711) ▪ MAC-Adresse des Gerätes (z.B. 00-80-41-ae-fd-7e oder 00:80:41:ae:fd:7e)	wie Class 2

- Client-Zertifikate für Personen:

Class 1	Class 2	übrige

Class 1	Class 2	übrige
Frei wählbar	Der CN muß die Person eindeutig identifizieren, z.B.: • Emailadresse in Form eines RFC 822 Namens z.B. (CN=hans.mueller@f-i-ts.de) • eindeutige Benutzerkennung des Zertifikatsinhabers gemäß seiner Personaldaten. • Vorname und Name Bei Namensgleichheit wird eine fortlaufende Nummer zur eindeutigen Identifizierung eingesetzt, z.B. Hans Mueller, Hans Mueller2	wie Class 2

Sollte der CN einen Domain-Namen betreffen, der nicht für FI-TS oder den auftraggebenden Kunden registriert ist, muß der Auftraggeber eine entsprechende Autorisierung (Domänenautorisierung) nachweisen. Ein entsprechender Vordruck wird auf der Web-Site des FI-TS Trustcenter zum Download angeboten.

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

Zusätzlich zum Betreff kann die Version 3 Erweiterung „subjectAltName“ zur Identifikation des Zertifikatsinhabers genutzt werden. Hierfür gelten sinnentsprechend dieselben Regeln. Da der Betreff nicht leer sein darf, wird der subjectAltName (s. Abschnitt 5.2.3) als nicht kritisch eingestuft.

5.2 Zertifikatserweiterungen

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

- kritisch: Anwendung muss diese Erweiterung auswerten; wenn sie dies nicht kann, muss das Zertifikat als ungültig verworfen werden.
- unkritisch: 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 verbundenen privaten Schlüssels.

Folgende Parameter werden grundsätzlich vom FI-TS-Trustcenter verwendet:

Zertifikatstyp	Key Usage
CA und SUB-CA-Zertifikate	Signierung von Zertifikaten (keyCertSign), Signierung von Zertifikatssperrlisten (keyCertSign)
Server-Zertifikate	Schlüsselaushandlung (keyAgreement) Verschlüsselung von Schlüsselmaterial (keyEncipherment) Digitale Signatur (keySign)
Client-Zertifikate	Schlüsselaushandlung (keyAgreement) Verschlüsselung von Schlüsselmaterial (keyEncipherment) Digitale Signatur (keySign)

Aufgrund technischer Erfordernisse hinsichtlich des Einsatzzweckes eines Zertifikates, können geänderte oder weitere Parameter Verwendung finden.

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	
Server-Zertifikate	Server Auth und Client Auth	1.3.6.1.5.5.7.3.1
Client-Zertifikate	Client Auth	1.3.6.1.5.5.7.3.2

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:

	Server-Zertifikat	Client-Zertifikat für Geräte	Client-Zertifikat für Personen
Mailadresse[1] (rfc822Name)	-	-	➨
Vollständiger Domainname (dNSName)	➨	➨	-
URI (uniformResourceIdentifier)	➨	➨	-
IP-Adresse (IPAddress)	➨	➨	-

Beispiele für die einzelnen Werte:

	Beispiel
Mailadresse[2] (rfc822Name)	hans.mueller@f-i-ts.de

[1] Mailadresse gemäß RFC 822

[2] Mailadresse gemäß RFC 822

Vollständiger Domainname (dNSName)	webserver.f-i-ts.de
URI (uniformResourceIdentifier)	http://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 nur in Endnutzer-Zertifikaten verwendet.

Die Bereitstellung der CRLs erfolgt ausschließlich per HTTP. Die URIs CRL Verteilungspunkte werden pro CA festgelegt und sind in den Endnutzer-Zeritifikaten enthalten.

Beispiel:

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

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 eine Maximalanzahl möglicher Einträge festgelegt. Für eine CA, die segmentierte CRLs erstellt, bestehen typischerweise mehrere CRLs.
- Gesamt-CRL:
  Bei einer Gesamt-CRL werden *alle* gesperrten Zertifikate einer CA in genau einer gemeinsamen Liste geführt.

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 2.

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

7 Online Certificate Status Protocol (OCSP)

Das FI-TS Trustcenter unterstützt grundsätzlich Online Certificate Status Protocol. OCSP wird derzeit allerdings nicht allgemein angeboten, denn dieser Dienst wird ggf. kundenspezifisch bereitgestellt. Die Verwendung ist im jeweiligen Vertragsverhältnis explizit zu vereinbaren. Die genauen technischen Parameter werden ebenfalls individuell festgelegt.

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 Appendix

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 Kunden/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 Zertifikate gehörenden privaten Schlüssel besitzt. Organisationen werden durch einen namentlich dem FI-TS Trustcenter bekannten Vertreter vertreten.
Certication Revocation List	Hierbei handelt es sich um Zertifikate, 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: Zertifikatpolicy
CPS	Certification Practice Statement: Zertifizierungsrichtlinie
CRL	Certication Revocation List: Liste der widerrufenen Zertifikate
CRL-DP	Certication 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 Protokoll
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 Enrolment 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