finanz informatik
technologie service

Richtlinie

Zertifizierung im FI-TS Trustcenter

Dokumentenverantwortliche/r: Fehlauer, Katrin

Vertraulichkeitsklasse: Intern

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!

© Finanz Informatik Technologie Service

Inhaltsverzeichnis

1 Ziel 6
1.1 Identifikation des Dokumentes 6
1.2 Abgrenzung 6
2 Schreibweise 6
3 Allgemeines 7
3.1 Anwendungsbereich 7
3.2 Kontaktinformationen 7
4 Einführung 8
4.1 PKI Teilnehmer 8
4.1.1 Certification Authority (CA) 8
4.1.2 Registration Authority (RA) 8
4.1.3 Zertifikatsinhaber 9
4.1.4 Auftraggeber 9
4.1.5 Zertifikatsnutzer 9
4.1.6 Weitere Teilnehmer 9
4.2 Nutzungszweck der Zertifikate 10
4.2.1 Zulässige Nutzungszwecke 10
4.2.2 Unzulässige Nutzungszwecke 10
4.3 Richtlinienverwaltung 10
4.3.1 Zuständige Organisation 10
4.3.2 Freigabeverantwortliche für Dokumente zum FI-TS Trustcenter 10
4.3.3 Veröffentlichungen des Trustcenters 10
4.4 Prozesse zur Freigabe der Zertifizierungsrichtlinie 11
5 Generelle Vorschriften 12
5.1 Verpflichtung der FI-TS Trustcenter CA 12
5.2 Verpflichtung der FI-TS Trustcenter RAs 12
5.3 Verpflichtungen des Freigabe-Ansprechpartners 12
5.4 Verpflichtungen des Zertifikatsinhabers 12
5.5 Verpflichtungen des Zertifikatsnutzers 13
6 Zertifikatsklassen 14
7 Typen von Zertifikaten 14
7.1 CA-Zertifikate 14
7.2 Server-Zertifikate 15
7.3 Client-Zertifikate für Geräte 15
7.4 Client-Zertifikate für Personen 15
7.5 Sonstige Zertifikate 15
8 Identifizierung und Authentisierung 16
8.1 Allgemeines 16
8.2 Namenskonventionen 16
8.2.1 Allgemeines 16
8.2.2 Wiedererkennung, Authentisierung und die Rolle von Schutzmarken 16
8.3 Methoden zur Überprüfung des Besitzes der privaten Schlüssel 16
8.4 Authentisierung von juristischen Personen (Organisationen oder Personen) 16
8.5 Authentisierung von natürlichen Personen 17

© Finanz Informatik Technologie Service
Dokumentenvorlage: Version 2.0 vom Juli 2015

8.6 Schlüsselerneuerung und Verlängerung von Zertifikaten 17
8.7 Änderung von Zertifikaten 17
8.8 Class 1-Zertifikate 18
8.8.1 Registrierung und Validierung 18
8.8.2 Erneuerung 20
8.8.3 Rückruf eines Zertifikats 20
8.9 Class 2-Zertifikate 21
8.9.1 Registrierung 21
8.9.2 Erneuerung 21
8.9.3 Rückruf eines Zertifikats 21
8.10 Class 3-Zertifikate 22
8.10.1 Registrierung 22
8.10.2 Erneuerung 22
8.10.3 Rückruf eines Zertifikats 22
8.11 Ausstellung weiterer Sub-CAs 24
8.11.1 Antragstellung 24
8.11.2 Technische Anforderungen 24
8.11.3 Anforderungen an die Richtlinie 24
9 Betriebliche Anforderungen für den Lebenszyklus eines Zertifikats 26
9.1 Berechtigung für Beantragung eines Zertifikats 26
9.2 Kriterien für Interoperation mit anderen CAs 26
9.3 Zeiträume für Bearbeitung von Anträgen 26
9.4 Ende der Subskription 26
9.5 Schlüsselhinterlegung und Schlüsselwiederherstellung 26
9.5.1 Schlüsselhinterlegungs- und Wiederherstellungspolicy und Prozeduren 26
9.5.2 Session-Schlüssel Kapselungs- und Wiederherstellungspolicy und Prozeduren 26
10 Sicherheitsmaßnahmen für die Bereiche Infrastruktur, Management, und Betrieb 27
10.1 Physikalische Sicherheitsmaßnahmen 27
10.1.1 Lage und Sicherungsmaßnahmen der Gebäude 27
10.1.2 Zutritt 27
10.1.3 Stromversorgung und Klimaanlage 27
10.1.4 Gefährdungspotential durch Wasser 27
10.1.5 Feuerschutzmaßnahmen 27
10.1.6 Lagerung von Backupmedien 27
10.2 Betriebliche Sicherheitsmaßnahmen 27
10.2.1 Rollenkonzept des FI-TS Trustcenters 27
10.2.2 Identifizierung und Authentisierung für die Rollen 27
10.3 Personelle Sicherheitsmaßnahmen 27
10.3.1 Anforderungen an die Qualifizierung 27
10.3.2 Qualifizierungsmaßnahmen 28
10.3.3 Anforderungen an externe Dienstleister 28
10.4 Audit Logging Prozeduren 28
10.4.1 Klassen von Events, die aufgezeichnet werden 28
10.4.2 Aufbewahrungsfrist der Audit Log-Daten 28
10.4.3 Schutz der Audit Log-Daten 28
10.4.4 Sicherung der Audit Log-Daten 28
10.4.5 System, das die Audit-Daten sammelt (extern oder intern) 29

© Finanz Informatik Technologie Service
Dokumentenvorlage: Version 2.0 vom Juli 2015

10.4.6 Information über Verursacher von Audit-Daten 29
10.4.7 Vulnerability Assessments 29
10.5 Datenarchivierung 29
10.5.1 Klassen von Daten, die archiviert werden 29
10.5.2 Aufbewahrungsfrist für archivierte Daten 29
10.5.3 Schutz der archivierten Daten 29
10.5.4 Sicherung der archivierten Daten 29
10.5.5 Zeitstempel für archivierte Daten 29
10.5.6 Lokation des Archives (intern oder extern) 29
10.5.7 Abläufe um Daten aus dem Archiv zu erhalten und diese zu verifizieren 30
10.6 Kompromittierung und Desaster-Recovery 30
10.6.1 Abläufe im Fall der Kompromittierung oder eines Sicherheitsvorfalls im Bereich des FI-TS Trustcenters 30
10.6.2 Abläufe im Fall von defekter Hardware, Software oder Daten 31
10.6.3 Möglichkeiten des Weiterbetriebs nach einer Krise 31
10.7 Beendigung des CA- oder RA-Dienstes 31
11 Technische Sicherheitsmaßnahmen 32
11.1 Schlüsselerzeugung und Installation 32
11.1.1 Schlüsselerzeugung 32
11.1.2 Übergabe des öffentlichen Schlüssels an den Aussteller von Zertifikaten 32
11.1.3 Veröffentlichung von CA-Zertifikaten für Zertifikatsnutzer 32
11.1.4 Schlüssellängen 32
11.1.5 Parameter für die Generierung von öffentlichen Schlüsseln und Qualitätsprüfung 32
11.1.6 Verwendungszweck der Schlüssel 32
11.2 Sicherheitsmaßnahmen zum Schutz des privaten Schlüssels und kryptographische Methoden 32
11.2.1 Standards und Schutzmaßnahmen der genutzten kryptographischen Methoden 32
11.2.2 Hinterlegung des privaten Schlüssels 32
11.2.3 Sicherung des privaten Schlüssels 33
11.2.4 Archivierung des privaten Schlüssels 33
11.2.5 Übermittlung des privaten Schlüssels in oder aus einem Verschlüsselungsmodul 33
11.2.6 Speicherung von privaten Schlüsseln in Verschlüsselungsmodulen 33
11.2.7 Aktivierungs- und Deaktivierungsmethode für den privaten Schlüssel 33
11.2.8 Löschen des privaten Schlüssels 33
11.3 Weitere Aspekte des Managements von Schlüsselpaaren 33
11.3.1 Archivierung des öffentlichen Schlüssels 33
11.3.2 Gültigkeitszeitraum für Zertifikate und Nutzungszeitraum für ein Schlüsselpaar 33
11.4 Maßnahmen zur Computersicherheit 33
11.4.1 Spezifische technische Anforderungen an die Computersicherheit 33
11.4.2 Bemessung der Computersicherheit 33
11.5 Zeitstempel 33
12 Audits 34
12.1 Häufigkeit der Audits 34
12.2 Identität/Qualifikation des Auditors 34

© Finanz Informatik Technologie Service
Dokumentenvorlage: Version 2.0 vom Juli 2015

12.3 Umfang des Audits 34
12.4 Maßnahmen nach Feststellung von Mängeln 34
12.5 Veröffentlichung der Ergebnisse des Audits 34
13 Sonstige Bestimmungen 35
13.1 Datenschutz 35
13.1.1 Vertrauliche Informationen 35
13.1.2 Nicht vertrauliche Informationen 35
13.1.3 Informationen zur Sperrung von Zertifikaten 35
13.1.4 Aushändigung von Informationen nach gerichtlicher Anforderung 35
13.1.5 Herausgabe bzw. Löschung von Informationen nach Aufforderung durch den Eigentümer der Information 36
13.1.6 Weitere Umstände für die Weitergabe von vertraulichen Informationen 36
13.2 Regelung der Urheberrechte und der Eigentumsrechte 36
13.3 Individuelle Vereinbarungen und Kommunikation zwischen den beteiligten Parteien 36
13.4 Zugrundeliegende gesetzliche Bestimmungen 36
14 Internes Kontrollsystem (IKS) 37
14.1 Kontrollziele aus dem „Sicheren IT-Betrieb“ 37
14.2 Zuordnung der Kontrollziele, -verfahren und -ergebnisse 37
15 Anhang 38
15.1 Definitionen 38
15.2 Abkürzungen 38

© Finanz Informatik Technologie Service
Dokumentenvorlage: Version 2.0 vom Juli 2015

1 Ziel

Dieses Dokument beschreibt die regulatorischen Richtlinien des FI-TS Trustcenters für die Ausstellung von Zertifikaten. Das Dokument wird durch die Richtlinie „Zertifikate 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 Auftraggeber mit der Beantragung eines Zertifikats anerkennt.

Diese Richtlinie ist angelehnt an das “X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework”, veröffentlicht als RFC 3647 durch die IETF (Internet Engineering Task Force).

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

1.1 Identifikation des Dokumentes

Name: Zertifizierung im FI-TS Trustcenter

OID: 1.3.6.1.4.1.23389.1.2.1.1.1

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 die ausgestellten 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

© Finanz Informatik Technologie Service
Dokumentenvorlage: Version 2.0 vom Juli 2015

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

© Finanz Informatik Technologie Service
Dokumentenvorlage: Version 2.0 vom Juli 2015

4 Einführung

Ein Zertifikat ist eine elektronische Bescheinigung, mit der ein öffentlicher kryptographischer Schlüssel einer Person oder Organisation zugeordnet wird und mit der die Identität dieser Person oder Organisation bestätigt wird. Ein Zertifikat stellt also eine Verbindung zwischen einer Person oder Organisation und einem kryptographischen Schlüssel her.

Jedes Zertifikat ist nur so vertrauenswürdig wie die Verfahren, wonach es ausgestellt wird.

Das FI-TS Trustcenter ordnet Zertifikate daher in „Zertifikatsklassen“ ein. Je höher die Zertifikatsklasse ist, desto umfangreichere Identifikationsprüfungen werden bei der Ausstellung eines Zertifikates durchgeführt. Dadurch kann anhand der Klassifikation eine Entscheidung darüber getroffen werden, ob das von einem Inhaber präsentierte Zertifikat den Anforderungen für den spezifischen Anwendungszweck genügt oder nicht.

Zertifikate werden für Organisationen, Personen, oder Geräte ausgestellt:

- *Zertifikate für Personen* sind immer einer natürlichen Person zugeordnet. Darüber hinaus müssen immer Angaben zu der Organisation enthalten sein, zu der die Person gehört.
- *Zertifikate für Organisationen* (jur. Personen) müssen in allen Fällen die Angaben des Unternehmens oder der Institution enthalten.
- *Zertifikate für Geräte* (z.B. Serverzertifikate oder Zertifikate für Applikationen) können entweder nur der Organisation – z. B. bei Server- Zertifikaten, die keiner natürlichen Person zugeordnet sind – oder aber einem Mitglied einer Organisation zugeordnet sein, also beispielsweise einem Mitarbeiter eines Unternehmens.

4.1 PKI Teilnehmer

4.1.1 Certification Authority (CA)

Alle Root-CAs des FI-TS Trustcenters stellen eine eigene Wurzelinstanz dar, d.h. jeder Root-CA Schlüssel ist jeweils selbstsigniert.

Untergeordnete CA-Zertifikate (Sub-CAs) werden von der betreffenden Root-CA zertifiziert. Die Sub-CAs zertifizieren die öffentlichen Schlüssel der Zertifikatsinhaber bzw. Auftraggeber (Nutzer-Zertifikate, Zertifikate für end-entities). Die ausgestellten Zertifikate werden – neben weiteren Informationen – in dem CA-System aufbewahrt.

Die Root- und Sub-CAs unterzeichnen Rückruflisten (CRLs) mit ihrem privaten Schlüssel.

Jede Sub-CA ist eindeutig einer Klasse zugeordnet und stellt Nutzer-Zertifikate (Zertifikate für end-entities) in der ihr zugewiesenen Klasse aus.

Es ist möglich, dass zu einer Klasse mehrere CAs mit unterschiedlichen Intentionen oder mit technischen Unterschieden bestehen, z.B. mit unterschiedlichen Signatur-Algorithmen oder unterschiedlicher Länge des CA-Schlüssels oder für unterschiedliche Einsatzszenarien. So bestehen z.B. neben der „Finanz Informatik Technologie Service F04 *Class1* CA G2“ weitere Class1 CAs für unterschiedliche Anwendungsbereiche. Die CAs einer Klasse unterliegen jeweils den gleichen organisatorischen Regelungen – mögliche *technische* Unterschiede sind für die Anwendung dieser Richtlinie nicht maßgeblich.

Zertifikate des FI-TS Trustcenters dürfen nur von Personen ausgestellt werden, wenn ihnen die dafür notwendigen Rollen zugewiesen wurden.

4.1.2 Registration Authority (RA)

Das FI-TS Trustcenter führt eine Antragsprüfung und Identifizierung auf Basis der für die einzelnen Zertifikatsklassen in dieser Richtlinie definierten Verfahren durch.

Es ist für definierte Teilbereiche des FI-TS Trustcenters möglich, die Identifizierung späterer Zertifikatsinhaber bzw. von Auftraggebern auf definierte Organisationseinheiten oder auch Ansprechpartner bei den Kunden von FI-TS zu verlagern, die nach positiver Prüfung die Freigabe für die Erzeugung von Zertifikaten oder für deren Rückruf erteilen.

© Finanz Informatik Technologie Service
Dokumentenvorlage: Version 2.0 vom Juli 2015

Für jede so gebildete RA gelten verbindlich die Richtlinien des FI-TS Trustcenters. Zusätzlich können für eine RA Richtlinien des Kunden selbst zur Anwendung kommen. Diese dürfen allerdings nicht im Widerspruch zu den Richtlinien des FI-TS Trustcenters stehen oder sie schwächen. Diese Richtlinien des Kunden sind zu dokumentieren und dem Trustcenter auf Anfrage zur Verfügung zu stellen.

Die Akkreditierung einer RA erfolgt durch:

1. Benennung der Mitarbeiter, die eine Rolle innerhalb der jeweiligen RA übernehmen, z.B. als Freigabe-Ansprechpartner oder Schlüsselverwalter. Die Benennung der Mitarbeiter ist zusammen mit der Vertragsdokumentation zu hinterlegen.
2. Einweisung aller RA-Mitarbeiter in die Dokumente und Abläufe einer RA durch das FI-TS Trustcenter.
3. Etablierung eines vertrauenswürdigen Kommunikationskanals zwischen RA-Mitarbeitern und dem FI-TS Trustcenter. Hierfür ist das Workflow-System von FI-TS vorgesehen.

4.1.3 Zertifikatsinhaber

Der Zertifikatsinhaber ist diejenige Person oder Organisation, für die ein Zertifikat ausgestellt wurde und die autorisierten Zugriff auf den zu einem Zertifikat gehörenden privaten Schlüssel besitzt.

Grundlegende Voraussetzung für die Ausstellung eines Zertifikats ist, dass sich das Objekt, dem das Zertifikat zugeordnet ist, eindeutig identifizieren lässt.

Das FI-TS Trustcenter stellt Zertifikate für FI-TS selbst, seine Kunden und Institutionen aus dem Umfeld der Kunden aus.

Zertifikate werden für Organisationen, Personen oder Geräte ausgestellt.

Organisationen werden durch einen namentlich dem FI-TS Trustcenter bekannten Repräsentant vertreten.

Alle Auftraggeber von Zertifikaten des FI-TS Trustcenters sind zur Beachtung der Nutzungsrichtlinien verpflichtet, siehe insbes. Kap. 5 Generelle Vorschriften.

4.1.4 Auftraggeber

Der Auftraggeber stellt über das FI-TS Workflow-System einen Antrag zur Ausstellung eines Zertifikates. Der Auftraggeber kann mit dem Zertifikatsinhaber identisch sein. Es ist jedoch auch möglich, dass Dritte, z.B. FI-TS Administratoren, Zertifikate für den späteren Inhaber beauftragen.

Der Auftraggeber muss das erhaltene Zertifikat und ggf. weitere Informationen an den Zertifikatsinhaber übergeben.

4.1.5 Zertifikatsnutzer

Der Zertifikatsnutzer ist diejenige Person oder Organisation, die anhand eines Zertifikats die Authentizität eines Kommunikationspartners feststellen und überprüfen kann.

4.1.6 Weitere Teilnehmer

Die Rollen des Freigabe-Ansprechpartners und des Schlüssel- und Zertifikatsverwalters werden üblicherweise im Rahmen einer RA (siehe Kap. 4.1.2 Registration Authority (RA)) etabliert.

4.1.6.1 Freigabe-Ansprechpartner

Freigabe-Ansprechpartner sind eine Gruppe von namentlich benannten Personen, die entsprechend den getroffenen vertraglichen Vereinbarungen berechtigt sind, einen Zertifikatsrequest von Auftraggebern eines Kunden zu prüfen und freizugeben bzw. einen Rückruf eines Zertifikats zu initiieren.

Eine erfolgte Freigabe umfasst sowohl die technisch-fachlichen als auch die kaufmännischen Aspekte.

© Finanz Informatik Technologie Service
Dokumentenvorlage: Version 2.0 vom Juli 2015

4.1.6.2 Schlüssel- und Zertifikatsverwalter

Nach Abstimmung mit dem FI-TS Trustcenter kann ein Zertifikatsinhaber die Schlüssel- und Zertifikatsverwaltung an Dritte delegieren. In diesem Fall ist auch der Dritte an die Zertifizierungs- und Zertifikatsrichtlinie gebunden. Der Zertifikatsinhaber ist für die Einhaltung der Zertifizierungs- und Zertifikatsrichtlinie durch den Dritten verantwortlich.

4.2 Nutzungszweck der Zertifikate

Es werden zwei grundsätzliche Gruppen von Zertifikatstypen unterschieden:

- CA-Zertifikate (Root-Zertifikate, Zertifikate von Sub-CAs, Issuing- oder Intermediate-CAs)
- Nutzer-Zertifikate (Zertifikate für end-entities)

4.2.1 Zulässige Nutzungszwecke

1. Root-CA Zertifikate: Root-Zertifikate dürfen ausschließlich zur Signierung untergeordneter CA-Zertifikate verwendet werden. Endnutzer-Zertifikate dürfen damit *nicht* signiert werden.
2. Sub-CA Zertifikate: Die Zertifikate untergeordneter CAs ("Sub-CA" oder Issuing-CA) werden zur Signierung von Nutzer-Zertifikaten verwendet. Damit ist die 2-stufige Aufbauform der PKI des FI-TS Trustcenter grundsätzlich festgelegt.
   Sofern besondere technische oder organisatorische Erfordernisse vorliegen, darf eine 3-stufige Aufbauform gewählt werden (z.B. für sog. Policy-CAs, Intermediate-CAs).
3. Nutzer-Zertifikate (Zertifikate für end-entities): Diese Zertifikate dürfen ausschließlich für den Zweck verwendet werden, der in der jeweiligen Zertifikatsklasse definiert ist und der durch die Attribute "Key Usage" bzw. „Extended Key Usage“ im Zertifikat hinterlegt ist. Andere Anwendungen sind untersagt und widersprechen auch den geltenden Normen.

4.2.2 Unzulässige Nutzungszwecke

Die Zertifikate dürfen nur für Zwecke genutzt werden, die in den Attributen „Key Usage“ oder „Extended Key Usage“ im Zertifikat vorgesehen sind.

Zertifikate ohne Eintrag in den Attributen „Key Usage“ oder „Extended Key Usage“ dürfen nicht ausgestellt und nicht verwendet werden.

4.3 Richtlinienverwaltung

4.3.1 Zuständige Organisation

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

4.3.2 Freigabeverantwortliche für Dokumente zum FI-TS Trustcenter

Folgende Abteilungen von FI-TS sind für die Freigabe der Dokumente des FI-TS Trustcenters verantwortlich:

- Geschäftsführung von Finanz Informatik Technologie Service GmbH & Co. KG
- Security Management
- Abteilung Sicherheitslösungen

4.3.3 Veröffentlichungen des Trustcenters

Kunden haben durch Veröffentlichung im Internet Zugriff auf folgende Dokumente:

- Zertifikatsrichtlinie
- Zertifizierungsrichtlinie

© Finanz Informatik Technologie Service
Dokumentenvorlage: Version 2.0 vom Juli 2015

- Root-Zertifikate inkl. Fingerabdruck
- Sub-CA-Zertifikate inkl. Fingerabdruck
- Certificate Revocation Lists (CRL)

Der Zugang zu weiteren Informationsquellen wird den Kunden ggf. nach Vertragsabschluss gewährt.

4.3.3.1 Zugriffskontrolle

Den Zertifikatsinhabern und ggf. der Öffentlichkeit wird lesender Zugriff auf die o.g. Informationen gewährt. Schreibenden Zugriff haben nur autorisierte Mitarbeiter des FI-TS Trustcenters. Die Systeme sind gegen unautorisierte Schreibzugriffe besonders geschützt.

4.4 Prozesse zur Freigabe der Zertifizierungsrichtlinie

Die Freigabe und Änderungen der Zertifizierungs- und Zertifikatsrichtlinie erfolgen im Rahmen der Verfahren und Prozesse des Sicherheitsmanagements und des Dokumentenmanagements von FI-TS.

© Finanz Informatik Technologie Service
Dokumentenvorlage: Version 2.0 vom Juli 2015

5 Generelle Vorschriften

Dieser Abschnitt beschreibt sowohl die Verpflichtungen der Betreiber des FI-TS Trustcenter als auch der Zertifikatsinhaber. Durch diese Vorschriften soll ein hohes Sicherheitsniveau und damit ein hohes Maß an Vertrauen zwischen den beteiligten Parteien erreicht werden.

5.1 Verpflichtung der FI-TS Trustcenter CA

Die CA als Instanz des FI-TS Trustcenters verpflichtet sich, nach den Vorgaben dieser Zertifizierungsrichtlinie sowie der Zertifikatsrichtlinie zu arbeiten. Dafür vertraut sie ausschließlich den Registrierungsstellen (RA) und lehnt unautorisierte Anträge ab. Die CA verpflichtet sich, Revokationsanträge unter Beachtung der dafür vertraglich vereinbarten Fristen zu bearbeiten und eine entsprechende CRL bereitzustellen.

Dem Schutz des privaten Schlüssels der Root- und der CA-Zertifikate kommt absolute Priorität zu.

Das Trustcenter verpflichtet sich, seine Funktionen durch qualifiziertes Personal abzudecken, wie in den internen Richtlinien von FI-TS beschrieben.

5.2 Verpflichtung der FI-TS Trustcenter RAs

Die RAs des FI-TS Trustcenters verpflichten sich, nach den Vorgaben dieser Zertifizierungsrichtlinie sowie der Zertifikatsrichtlinie zu arbeiten und die Identität der späteren Zertifikatsinhaber gemäß den Anforderungen zuverlässig zu prüfen.

Die RAs sind verpflichtet, für jedes angeforderte Zertifikat die Identität des Zertifikat-Subjects zu validieren.

Die RAs sind verpflichtet, jeden Auftrag zur Erstellung von Zertifikaten, der an die CA weitergeleitet wird, zu dokumentieren. Für automatisierte Verfahren geschieht die Dokumentation mit Hilfe entsprechender Log-Einträge.

Kommt eine RA außerhalb von FI-TS den hier aufgeführten Verpflichtungen nicht nach, haftet FI-TS nicht für die dadurch entstehenden Schäden.

CRLs werden regelmäßig aktualisiert. Nach Rückruf eines Zertifikats erfolgt eine Veröffentlichung der aktualisierten Sperrliste innerhalb der Frist, die für die jeweilige Zertifikatsklasse festgelegt ist.

5.3 Verpflichtungen des Freigabe-Ansprechpartners

Der Freigabe-Ansprechpartner ist verpflichtet, die ihm gemäß den Vereinbarungen zugeordneten Aufgaben ordnungsgemäß durchzuführen und zu dokumentieren.

Kommt ein Freigabe-Ansprechpartner den festgelegten Verpflichtungen nicht nach, haftet FI-TS nicht für die dadurch entstehenden Schäden.

5.4 Verpflichtungen des Zertifikatsinhabers

Ein Zertifikatsinhaber, der ein Zertifikat des FI-TS Trustcenters beantragt hat bzw. erhält, verpflichtet sich, diese Zertifizierungsrichtlinie sowie die Zertifikatsrichtlinie zu lesen und zu akzeptieren.

Er verpflichtet sich, sein Zertifikat gemäß der im Zertifikat und in der Zertifikatsrichtlinie angegebenen Verwendungszwecke (Key Usage und Extended Key Usage) und mit angemessener Vorsicht einzusetzen.

Der Zertifikatsinhaber muss sein Schlüsselpaar mit einem vertrauenswürdigen Verfahren generieren. Dieses Verfahren muss dem geforderten Sicherheitsniveau des Einsatzzweckes der Schlüssel entsprechen. Die entsprechenden Verfahren und Mindestschlüssellängen sind in der Richtlinie „Zertifikate im FI-TS Trustcenter“ definiert.

Er muss seinen privaten Schlüssel schützen und darf ihn keinesfalls zusammen mit ggf. zugehörigen PINs bzw. Passphrases aufbewahren. Bei jedem Einsatz eines zu einem gültigen

© Finanz Informatik Technologie Service
Dokumentenvorlage: Version 2.0 vom Juli 2015

Zertifikat gehörenden privaten Schlüssels wird angenommen, dass der Einsatz durch den Zertifikatsinhaber durchgeführt wurde.

Die ggf. übermittelte PIN eines Hardware-Tokens muss der Zertifikatsinhaber unverzüglich und vor der erstmaligen Verwendung seines privaten Schlüssels ändern.

Wird ein Schlüsselpaar zur Ver- und Entschlüsselung von Daten genutzt, muss der Zertifikatsinhaber für eine angemessene Sicherung des Schlüsselpaares sorgen – ggf. auch über die Gültigkeitsdauer des Zertifikates hinaus (z.B. wenn Schlüsselmaterial zur Ver- oder Entschlüsselung genutzt wurde).

Eine Weitergabe des privaten Schlüssels, des PINs o.ä. ist nicht gestattet. Kommt der private Schlüssel abhanden oder besteht die Möglichkeit, dass ein Dritter Kenntnis vom privaten Schlüssel erlangt hat, so ist dies dem FI-TS Trustcenter unverzüglich mitzuteilen, so dass eine zeitnahe Sperrung des Zertifikats erfolgen kann. Besteht die Möglichkeit, dass ein Dritter Kenntnis des PIN oder einer Passphrase erlangt hat, so sind PIN oder Passphrase unverzüglich zu ändern.

Sobald wesentliche Daten verändert sind, die mit der Beauftragung eines Zertifikates in Zusammenhang stehen, ist der Zertifikatsinhaber verpflichtet, ein neues Zertifikat ausstellen und das ursprüngliche sperren zu lassen. Dies betrifft sowohl Daten,

- die im Zertifikat selbst enthalten sind als auch solche, die
- zur Überwachung benötigt werden (z.B. geänderter Ansprechpartner).

Es handelt sich hierbei im Wesentlichen um die Angaben, die auch bei Beauftragung eines Zertifikates anzugeben sind.

5.5 Verpflichtungen des Zertifikatsnutzers

Nutzer ist derjenige, der das Zertifikat prüft oder zur Verschlüsselung nutzt. Ihm obliegen keine Pflichten im Sinne dieser Richtlinie.

© Finanz Informatik Technologie Service
Dokumentenvorlage: Version 2.0 vom Juli 2015

6 Zertifikatsklassen

Das FI-TS Trustcenter unterstützt drei verschiedene Zertifikatsklassen mit unterschiedlichen Vertrauenswürdigkeitsstufen. Dem Zertifikatsnutzer wird empfohlen, nur einer Sub-CA und damit der Klasse zu vertrauen, die seinen Sicherheitsanforderungen genügt.

Es ist möglich, dass mehrere CAs des FI-TS Trustcenters für die gleiche Klasse bestehen. Jede CA ist genau einer Klasse zugeordnet.

- Class 1 Zertifikate

  Class 1 Zertifikate bieten das geringste Niveau an Vertrauenswürdigkeit. Näheres zu Class 1 Zertifikaten siehe unter Kap. 8.8.
- Class 2 Zertifikate

  Class 2 Zertifikate bieten ein mittleres Niveau an Vertrauenswürdigkeit. Näheres zu Class 2 Zertifikaten siehe unter Kap. 0.
- Class 3 Zertifikate

  Class 3 Zertifikate bieten das höchste Niveau an Vertrauenswürdigkeit. Näheres zu Class 3 Zertifikaten siehe unter Kap. 8.10.

7 Typen von Zertifikaten

Alle durch das FI-TS Trustcenter erstellten Zertifikate sind X.509v3 (Version 3) Zertifikate.

Die maximale Laufzeit von Zertifikaten beträgt 3 Jahre, sofern im Folgenden keine anderen Konkretisierungen vorgenommen wurden. Die Laufzeit darf außerdem die des betr. CA-Zertifikats nicht überschreiten.

Die Erneuerung eines laufenden, nicht gesperrten Zertifikates soll mit einem ausreichenden zeitlichen Vorlauf, maximal aber 3 Monaten erfolgen.

Soweit keine anderweitigen vertraglichen Regelungen bestehen, sind in Kap 9.3 Zeiträume für Bearbeitung von Anträgen bei der zuständigen RA festgelegt.

Die Zertifikate werden u.a. anhand ihrer vorgesehenen Verwendungszwecke (Key Usage bzw. Extended Key Usage) unterschieden. Kombinationen mehrerer Key Usages und Extended Key Usages sind grundsätzlich zulässig. *Welche* Kombinationen im Einzelnen zulässig sind, regelt die Arbeitsanleitung „Prüfung von Zertifikatsanträgen“.

Es besteht kein Rechtsanspruch auf die Ausstellung von Zertifikaten.

Vom FI-TS Trustcenter werden die aufgeführten Zertifikatstypen unterstützt:

7.1 CA-Zertifikate

CA-Zertifikate dienen der Ausstellung von weiteren Zertifikaten und der Signierung der jeweiligen Sperrlisten (CRL). Es werden dabei drei Typen unterschieden:

- Root-Zertifikate: Diese Zertifikate sind selbstsigniert. Sie dienen ausschließlich zur Ausstellung von Issuing- bzw. Intermediate CA-Zertifikaten.
- CA-Zertifikate für Issuing-CAs: Diese Zertifikate sind von Root-Zertifikaten des FI-TS Trustcenter unterzeichnet. Sie dienen grundsätzlich der Ausstellung von Nutzer-Zertifikaten.
- CA-Zertifikate für Intermediate-CAs: Grundsätzlich besteht eine 2-stufige CA-Struktur (Root-CA und Issuing-CAs). Für besondere technische oder organisatorische Anforderungen können CA-Zertifikate z.B. für Policy-CAs ausgestellt werden. In diesen Fällen werden mit den CA-Zertifikaten ausschließlich weitere CA-Zertifikate für Issuing-CAs ausgestellt.

CA-Zertifikate sind von folgenden Merkmalen bestimmt:

1. Regulatorische Anforderungen
   - Zugehörigkeit zu genau einer Zertifikatsklasse
2. Technische Anforderungen

© Finanz Informatik Technologie Service
Dokumentenvorlage: Version 2.0 vom Juli 2015

- Schlüssellänge
- Algorithmus des Schlüsselpaares
- Signaturalgorithmus
- „Scope“ einer CA z.B. aufgrund von Netzwerkeinschränkungen bei Nutzung bestimmter Deployment-Funktionen (z.B. Windows Auto-Enrollment).

Diese Aufzählung ist nicht abschließend. Ändern sich diesbezügliche Anforderungen, kann die Ausstellung eines neuen CA-Zertifikates erforderlich werden.

Die Laufzeit von CA-Zertifikaten beträgt i.d.R. mindestens 10 Jahre, maximal aber bis zum Laufzeitende des betr. Root-Zertifikates.

Sofern der Widerruf eines CA-Zertifikates aufgrund eines kompromittierten CA-Schlüssels erforderlich werden sollte, erfolgt dies im Rahmen des FI-TS Krisenprozesses.

CA-Zertifikate werden ausschließlich manuell ausgegeben.

7.2 Server-Zertifikate

Server-Zertifikate sind Geräte-Zertifikate und dienen der eindeutigen Identifizierung von Servern oder Applikationen beim Aufbau von verschlüsselten Verbindungen mittels TLS.

Server-Zertifikate werden manuell, halbautomatisch oder automatisiert ausgegeben.

7.3 Client-Zertifikate für Geräte

Diese Client-Zertifikate sind ebenfalls Geräte-Zertifikate und dienen der eindeutigen Authentisierung von Client-Rechnern (z.B. PCs, Notebooks), Telefonen, Druckern und anderen Geräten gegenüber Servern, z.B. im Rahmen von 802.1x.

Client-Zertifikate werden manuell, halbautomatisch oder automatisiert ausgegeben.

7.4 Client-Zertifikate für Personen

Diese Client-Zertifikate sind Personen-Zertifikate und dienen der eindeutigen Authentisierung von Nutzern (natürlichen Personen) gegenüber Servern oder Applikationen. Dies sind unterschiedliche Komponenten und Anwendungen wie RAS, Zugang zu Servern oder Zugang zu bestimmten Netzbereichen (Authentisierung).

Client-Zertifikate für natürliche Personen können in Verbindung mit entsprechenden Key Usages darüber hinaus zur Verschlüsselung oder Signatur von Dokumenten oder Emails genutzt werden. Hierfür wird geeignete Infrastruktur benötigt, die das FI-TS Trustcenter jedoch nicht bereitstellt.

Client-Zertifikate werden manuell, halbautomatisch oder automatisiert ausgegeben. Die manuelle oder halbautomatische Ausgabe ist hierbei die Regel.

7.5 Sonstige Zertifikate

Über die vorgenannten Typen hinaus können weitere Zertifikate, z.B. Zertifikate für Organisationen zum Zwecke des Code-Signings ausgestellt werden.

© Finanz Informatik Technologie Service
Dokumentenvorlage: Version 2.0 vom Juli 2015

8 Identifizierung und Authentisierung

In diesem Abschnitt werden die Prozeduren zur Feststellung der Identität des späteren Zertifikatsinhabers beschrieben, der ein Zertifikat beantragt. Diese Verfahren unterscheiden sich für die verschiedenen Zertifikatsklassen.

Ergänzend und konkretisierend dazu gelten die Ausführungen der Arbeitsanleitung „Prüfung von Zertifikatsanträgen“.

8.1 Allgemeines

Für die Identifizierung und Authentisierung von Mitarbeitern der CA am FI-TS Trustcenter ist eine starke Authentisierung vorzusehen.

Auf der Seite des Kunden/Mandanten werden im Rahmen einer RA sogenannte Freigabe-Ansprechpartner definiert (siehe Kap. 4.1.2 Registration Authority (RA)). Deren Aufgabe ist es, die Zertifikatsanforderungen bzw. die Zertifikatswiderrufe zu prüfen. Ist die Zertifikatsanforderung bzw. der Zertifikatswiderruf zulässig und gültig, leitet der Freigabe-Ansprechpartner des Kunden/Mandanten den Zertifikatsrequest bzw. den Zertifikatswiderruf an das FI-TS Trustcenter weiter.

Für die Kommunikation zwischen der zentralen CA und auch der zentralen RA von FI-TS mit RA auf Kundenseite sind sichere Kanäle vorzusehen. Als sicherer Kanal werden das Workflow-System von FI-TS und verschlüsselte Emails betrachtet.

Der grundlegende Workflow ist wie folgt vorgesehen:

Der Auftraggeber bzw. künftige Zertifikatsinhaber erstellt einen Auftrag zur Zertifikatserstellung oder den -widerruf. Diese Zertifikatsanforderung oder Zertifikatsrückruf wird vom Freigabe-Ansprechpartner überprüft und ggf. genehmigt. Nach der Genehmigung wird der Auftrag automatisch an das Trustcenter weitergeleitet. Dieses nimmt die Validierung des Auftrages vor, stellt das Zertifikat aus bzw. widerruft es.

Grundsätzlich ist zur Beauftragung oder dem Widerruf von Zertifikaten ein separater Auftrag pro Zertifikat zu erstellen. Für festgelegte Fälle kann der Freigabe-Ansprechpartner mehrere Zertifikatsrequests oder die Zertifikatswiderrufe in einem Auftrag zusammenfassen und diesen genehmigt weiterleiten.

Bei automatisierten Ausstellungsverfahren müssen besondere Voraussetzungen erfüllt sein, wie sie in der Fachlichen Richtlinie „Windows CAs“ festgelegt sind.

8.2 Namenskonventionen

8.2.1 Allgemeines

Es gelten die Vorgaben der Richtlinie „Zertifikate im FI-TS Trustcenter“. Ergänzend gilt die Arbeitsanleitung „Prüfung von Zertifikatsanträgen“.

8.2.2 Wiedererkennung, Authentisierung und die Rolle von Schutzmarken

Das FI-TS Trustcenter überprüft die Inhalte von Zertifikaten nicht auf geschützte Namen. Der Auftraggeber bzw. künftige Zertifikatsinhaber ist verpflichtet, diese Überprüfung selbst vorzunehmen.

8.3 Methoden zur Überprüfung des Besitzes der privaten Schlüssel

Die RA kann vom Zertifikatsinhaber bzw. Auftraggeber einen Nachweis über den Besitz des privaten Schlüssels anfordern.

Bei Bedarf wird die RA ein Verfahren vorgeben, wie der Nachweis erfolgen soll.

8.4 Authentisierung von juristischen Personen (Organisationen oder Personen)

Immer wenn ein Auftraggeber ein Zertifikat anfordert, das als Bestandteil den Namen einer juristischen Person enthält (z.B. im O-Feld oder im CN), muss im Vorfeld auf der Basis eines

© Finanz Informatik Technologie Service
Dokumentenvorlage: Version 2.0 vom Juli 2015

Vertrages mit dieser juristischen Person die Berechtigung des FI-TS Trustcenters für die Ausstellung der Zertifikate geregelt werden.

8.5 Authentisierung von natürlichen Personen

Zertifikate für natürliche Personen, die nicht Angehörige einer juristischen Person (s. 8.4) sind, werden vom FI-TS Trustcenter nicht ausgestellt.

8.6 Schlüsselerneuerung und Verlängerung von Zertifikaten

Bei Ablauf eines Zertifikates ist es grundsätzlich dem Zertifikatsinhaber überlassen, ob er ein neues Schlüsselpaar erzeugen will oder nicht. Das FI-TS Trustcenter empfiehlt jedoch immer die Erzeugung eines neuen privaten Schlüssels.

Die Abläufe bei Erstregistrierung und wiederholter Ausstellung (Verlängerung) – gleichgültig ob mit wiederverwendetem oder neu generiertem Schlüssel – sind identisch.

8.7 Änderung von Zertifikaten

Die Änderung von Zertifikatsinhalten ist nicht möglich. Wird ein Zertifikat mit geändertem Inhalt benötigt, so muss immer eine neue Registrierung durchgeführt werden. Das ursprüngliche Zertifikat wird zurückgezogen.

In Absprache mit dem Freigabeverantwortlichen des Kunden kann zur Erleichterung der Migration auch eine Übergangszeit vereinbart werden, während der beide Zertifikate gültig sind. Dieser Zeitraum sollte nicht länger als zehn Arbeitstage andauern.

© Finanz Informatik Technologie Service
Dokumentenvorlage: Version 2.0 vom Juli 2015

8.8 Class 1-Zertifikate

Die Ausstellung dieser Zertifikate kann in Form von Registration Authorities an andere Organisationen außerhalb von FI-TS übertragen werden.

Diese Klasse ist insbes. zur Nutzung durch automatisierte Dienste wie z.B. SCEP oder andere Auto-Enrollment-Funktionen bestimmt. Alle Prüfungsschritte beschränken sich daher auf solche Aspekte, die automatisiert durchführbar sind.

Aufgrund der automatisierten Ausstellungsvorgänge sind Class1-Zertifikate insbes. für Maschinenzertifikate (Server- und Client-Zertifikate) vorgesehen, wie sie z.B. in Windows-Domains benötigt werden.

8.8.1 Registrierung und Validierung

Für die Zertifizierung eines öffentlichen Schlüssels als Class 1-Zertifikat sind folgende Kriterien notwendig:

1. Der Common Name (CN) muss den Konventionen der jeweils gültigen Zertifikatsrichtlinie entsprechen und den anfordernden Kunden/Mandanten zuordenbar sein.
   Sofern es sich bei dem zu validierenden CN um eine öffentlich registrierte Domain handelt, sind in Anlehnung an die Beschlüsse des CA/Browser-Forums (cab-Forum) folgende Verfahren zulässig. Es wird auf Ballot 224 (https://cabforum.org/wp-content/uploads/CA-Browser-Forum-BR-1.6.0.pdf) Bezug genommen:
   a. Email-Bestätigung durch den Domain-Kontakt (Methode 3.2.2.4.2)
      Dieses Verfahren kann nur für solche registrierten Domains Anwendung finden, für die FI-TS auch die Domain-Verwaltung durchführt, weil die Validierungs-Mail an den admin-c verschickt wird. Der admin-c muss dem FI-TS Trustcenter also bekannt sein.
      Die E-Mail enthält einen Random-Value, den der Domain-Kontakt an das FI-TS Trustcenter zurücksenden muss.
   b. “Constructed” Email an den Domain-Kontakt (Methode 3.2.2.4.4)
      Unter Nutzung von 'admin', 'administrator', 'webmaster', 'hostmaster', oder 'postmaster' als lokalem Bestandteil der Mail-Adresse und dem zu autorisierendem Domain-Name wird eine Mail verschickt. Der Kunde/Mandant kann aus diesen 5 Möglichkeiten den lokalen Bestandteil wählen.
      Die E-Mail enthält einen Random-Value, den der Kunde/Mandant an das FI-TS Trustcenter zurücksenden muss.
   c. Vereinbarte Änderung an der zu validierenden Web-Site (Methode 3.2.2.4.6)
      Dieses Verfahren kann nur für solche Domains angewandt werden, auf die das FI-TS Trustcenter per http oder https Zugriff hat.
   d. DNS Change (Methode 3.2.2.4.7)
      Hierbei muss ein Random-Value in den CAA-Record (Certification Authority Authorization) oder den TXT-Record des DNS-Eintrags eingetragen werden.
   e. Antragsteller als Domain-Kontakt (Methode 3.2.2.4.12)
      Bei dieser Methode kommt es darauf an, dass die ausstellende CA gleichzeitig der Registrar des Domain-Namens ist (oder ein Partner des Registrars).
      Diese Methode kann für alle Domains verwendet werden, für die FI-TS aufgrund entsprechender who-is Abfrage als Registrar eingetragen ist.

   Anmerkungen:
   - Das FI-TS Trustcenter gibt die anzuwendende Validierungsmethode vor und stimmt sie mit dem Kunden/Mandanten ab.
   - Jede Validierung muss binnen 30 Kalendertagen abgeschlossen sein.
   - Eine erfolgte Validierung behält eine Gültigkeit von 39 Monaten.

© Finanz Informatik Technologie Service
Dokumentenvorlage: Version 2.0 vom Juli 2015

- Eine Validierung für öffentlich registrierte Domains kann für die gesamte Domain oder Sub-Domains erfolgen.
- Weitere Validierungsmethoden, die das CA/Browser-Forum vorsieht, werden durch das FI-TS Trustcenter nicht unterstützt.
- Zertifikate auf IP-Adressen werden ausschließlich im Zusammenhang mit CN auf non-FQDN (Maschinenname) ausgestellt.

Für Zertifikate, deren CN nicht auf öffentlich registrierte Domains lautet, sind detaillierte Validierungsmaßnahmen in der Arbeitsanleitung „Prüfung von Zertifikatsanträgen“ festgelegt.

2. Im Falle von Subject Alternative Names (SAN) müssen alle betroffenen Domains, IP-Adressen oder Mail-Adressen dem gleichen Eigentümer gehören.
3. Das Organisations-Feld (O) muss mit einem Wert belegt sein, der mit der Domain des gewählten CN korrespondiert. Es darf insbesondere kein Widerspruch zu einer bestehenden Domain-Registrierung entstehen.
   Erlaubte Werte sind jeweils der juristische Name zur Bezeichnung der Organisation oder eine definierte Kurzform.
   Das Organisations-Feld darf leer sein, wenn die ausstellende CA ausschließlich für voll automatisierte Ausstellungs- und Deployment-Verfahren bestimmt ist und gleichzeitig der Bezug zum Kunden durch den Scope des Deployments eindeutig ist.
4. Das Country-Feld (C) muss zum Hauptsitz oder einer Niederlassung der Organisation passen.
   Das Country-Feld darf unter den gleichen Bedingungen wie das Organisations-Feld leer sein.
5. Alle übrigen Felder sind optional und werden nicht geprüft.
6. Die Beauftragungen für Zertifikate müssen gemäß dem für den jeweiligen Kunden/Mandanten definierten Antragsverfahren durchgeführt werden.
   Soweit vertraglich nichts anderes vereinbart ist und es sich nicht um voll automatisierte Ausstellungsvorgänge handelt, erfolgt die Beantragung über das Workflow-System von FI-TS:
   a. Alle Genehmigungen, die im Workflow-System für einen Zertifikatsantrag vorgesehen sind, müssen vorliegen, insbesondere die Prüfung des Freigabe-Ansprechpartners.
   b. Grundsätzlich erfolgt die Zertifikatsausstellung per Request. Liegt ein Request vor, muss er im Workflowsystem übermittelt werden. Nur in technisch bedingten Ausnahmefällen, z.B. wenn der Request erst im Rahmen eines Changes erstellt werden kann, ist eine nachträgliche Übermittlung per Email erlaubt. Dabei muss auf den Auftrag Bezug genommen werden.
   c. Es ist möglich, das Schlüsselmaterial zentral durch das FI-TS Trustcenter generieren zu lassen. In diesem Fall müssen die entsprechenden Angaben im Workflowsystem übermittelt werden.

   Die Überprüfung der Parameter erfolgt in der Regel durch den Freigabe-Ansprechpartner.

   Das FI-TS Trustcenter ist grundsätzlich befugt, zweckdienliche Änderungen vor der Signatur vorzunehmen.

   Sind alle Kriterien erfüllt, wird das Zertifikat erstellt und entsprechend dem Auftrag bereitgestellt.

   Sind eine oder mehrere Kriterien nicht erfüllt, wird der Auftrag abgelehnt und der Auftraggeber informiert. Die Information des Auftraggebers kann sowohl durch das FI-TS Trustcenter als auch den Freigabe-Ansprechpartner erfolgen. Für eine erneute, korrigierte Beantragung muss der komplette Antragsprozess erneut durchlaufen werden.

© Finanz Informatik Technologie Service
Dokumentenvorlage: Version 2.0 vom Juli 2015

Die Dokumentation des Ablaufs erfolgt durch die in 0 beschriebenen Verfahren.

Der entsprechende Freigabe-Ansprechpartner wird über die Ausstellung des Zertifikats informiert.

7. Alternativ zur vorstehend beschriebenen manuellen Beauftragung und Prüfung können Zertifikate auch voll automatisiert auf Grundlage dafür vorgesehener Protokolle ausgestellt werden. Es gelten dann folgende Kriterien:
    a. Zur Ausstellung der Zertifikate müssen eindeutige Kriterien (use-cases) festgelegt sein, insbes. hinsichtlich der möglichen CN und der Belegung des O-Feldes.
    b. Die use-cases müssen dokumentiert sein.
    c. Die use-cases müssen technisch so implementiert sein, dass die Ausstellung nicht vorgesehener Zertifikate abgewiesen wird.
    d. Die Validierungsschritte zur Ausstellung der Zertifikate sind sinnentsprechend zur manuellen Validierung einmalig durchzuführen.

   Es ist zu beachten, dass für Zertifikate, die aufgrund vollautomatischer Verfahren ausgestellt werden, keine Warnungen zum Zertifikatsablauf erstellt werden.

   Näheres regelt die Arbeitsanleitung „Prüfung von Zertifikatsanträgen“.

8.8.2 Erneuerung

Die Rezertifizierung bzw. Erneuerung eines existierenden Zertifikats muss explizit beauftragt werden. Eine automatische Rezertifizierung findet nicht statt, sofern nicht voll automatisierte Verfahren ein automatisches Renewal vorsehen. Ein solches Renewal muss durch diese etablierten Verfahren sichergestellt werden, nicht durch das FI-TS Trustcenter.

Die Rezertifizierung wird nach dem gleichen Verfahren wie die Erstregistrierung durchgeführt.

Sofern eine CA für voll automatisierte Ausstellungs- und Deployment-Verfahren vorgesehen ist, erfolgt vor dem Zertifikatsablauf keine Warnung.

Andernfalls erfolgt ca. 6 bis 8 Wochen vor dem Ablauf eines Class 1-Zertifikates eine Information über das Ticketsystem von FI-TS an den Auftraggeber.

8.8.3 Rückruf eines Zertifikats

Sofern für die Organisation eines Zertifikatsinhabers eine RA definiert ist, erfolgt der Rückruf eines Zertifikates durch den Freigabe-Ansprechpartner, der die hierfür erforderlichen Überprüfungen durchführt. Andernfalls erfolgt der Rückruf durch den Zertifikatsinhaber oder den ursprünglichen Auftraggeber selbst.

Für den Rückruf sind die in Kap. 0 Ergänzend und konkretisierend dazu gelten die Ausführungen der Arbeitsanleitung „Prüfung von Zertifikatsanträgen“.

Allgemeines festgelegten Kommunikationswege einzuhalten.

Es können hiervon abweichende Regelungen vertraglich vereinbart sein.

Für die Überprüfung einer Rückrufanforderung sind exakte Angaben erforderlich, die es erlauben, das Zertifikat zweifelsfrei festzustellen.

© Finanz Informatik Technologie Service
Dokumentenvorlage: Version 2.0 vom Juli 2015

8.9 Class 2-Zertifikate

Die Prüfung der Zertifikatsrequests der Class 2 Zertifikate kann in Form von RA an andere Organisationen innerhalb und außerhalb von FI-TS übertragen werden.

Eine automatisierte Ausstellung von Class 2-Zertifikaten ist nicht vorgesehen.

8.9.1 Registrierung

Für die Zertifizierung eines öffentlichen Schlüssels als Class 2-Zertifikat müssen die gleichen Prüfungsschritte wie für Class 1 durchlaufen werden.

Abweichend dazu ist die automatisierte Ausstellung von Zertifikaten nicht zulässig.

Das Organisations-Feld und das Country-Feld dürfen im Unterschied zu Class1- Zertifikaten nicht leer sein – die Objektklassen CN, O und C müssen stets gesetzt sein.

Die Beauftragung von Zertifikaten erfolgt über einen Prozess in einem Workflow-Management-System (z.B. ARS oder Service Now). In diesen Workflow-Prozess sind die erforderlichen Freigaben eingearbeitet.

Die Prüfungen können teilautomatisiert oder manuell erfolgen. Eine voll automatisierte Ausstellung allerdings ist nicht zulässig.

Das FI-TS Trustcenter ist grundsätzlich befugt, zweckdienliche Änderungen vor der Signatur vorzunehmen.

Sind alle Kriterien erfüllt, wird das Zertifikat erstellt und entsprechend dem Auftrag bereitgestellt.

Sind eine oder mehrere Kriterien nicht erfüllt, wird der Zertifikatsrequest abgelehnt und der Auftraggeber informiert. Die Information des Auftraggebers kann sowohl durch das FI-TS Trustcenter als auch den Freigabe-Ansprechpartner erfolgen. Für eine erneute, korrigierte Beantragung muss der komplette Antragsprozess erneut durchlaufen werden.

8.9.2 Erneuerung

Die Rezertifizierung bzw. Erneuerung eines existierenden Zertifikats muss explizit beantragt werden. Eine automatische Rezertifizierung findet nicht statt.

Die Rezertifizierung wird nach dem gleichen Verfahren wie die Erstregistrierung durchgeführt.

Ca. 6 bis 8 Wochen vor dem Ablauf eines Class 2-Zertifikates erfolgt eine Information über das Ticketsystem von FI-TS an den Auftraggeber.

8.9.3 Rückruf eines Zertifikats

Sofern für die Organisation eines Zertifikatsinhabers eine RA definiert ist, erfolgt der Rückruf eines Zertifikates durch den Freigabe-Ansprechpartner, der die hierfür erforderlichen Überprüfungen durchführt. Andernfalls erfolgt der Rückruf durch den Zertifikatsinhaber selbst.

Für den Rückruf sind grundsätzlich die in Kap. 0 Ergänzend und konkretisierend dazu gelten die Ausführungen der Arbeitsanleitung „Prüfung von Zertifikatsanträgen“.

Allgemeines festgelegten Kommunikationswege einzuhalten. In Notfällen kann der Freigabeverantwortliche einen Rückruf über den Incidentmanagementprozess von FI-TS veranlassen. Die vereinbarten Arbeitsunterlagen sind in diesem Fall auf dem vereinbarten Wege nachzureichen.

Es können hiervon abweichende Regelungen vertraglich vereinbart sein.

Für die Überprüfung einer Rückrufanforderung sind exakte Angaben erforderlich, die es erlauben, das Zertifikat zweifelsfrei festzustellen.

© Finanz Informatik Technologie Service
Dokumentenvorlage: Version 2.0 vom Juli 2015

8.10 Class 3-Zertifikate

Diese Zertifikate dürfen nur über das FI-TS Trustcenter selbst beantragt und ausgestellt werden. Die Prüfung der Aufträge durch RAs außerhalb von FI-TS ist nicht zulässig.

Für Class 3-Zertifikate wird derzeit kein Einsatzszenario gesehen. Diese Klasse wird daher momentan nicht bedient; es kann jedoch jederzeit eine Class 3 CA gebildet werden.

8.10.1 Registrierung

Für die Zertifizierung eines öffentlichen Schlüssels als Class 3-Zertifikat sind folgende Kriterien notwendig:

1. Bei dieser Zertifikatsklasse erfolgen grundsätzlich die gleichen Prüfungsschritte wie für Class 2.

Abweichend bzw. ergänzend gelten folgende Regelungen:

2. Die Ausstellung dieser Zertifikate kann nur durch autorisierte Personen (PKI-Hauptadministratoren) innerhalb von FI-TS erfolgen. Eine Übertragung an andere RA ist ausgeschlossen.
3. Die Korrektur fehlerhafter Felder ist nicht zulässig. Ggf. muss ein neuer Request erstellt werden.
4. Der Zertifikatsrequest inklusive aller Parameter wird durch das FI-TS Trustcenter mit dem Antragsteller und dem zuständigen Freigabe-Ansprechpartner telefonisch verifiziert.
5. Alle Prüfungsschritte müssen manuell erfolgen – Automationen und Teilautomationen sind nicht zulässig.

Sind alle Kriterien erfüllt, wird das Zertifikat erstellt und entsprechend dem Auftrag bereitgestellt.

Sind eine oder mehrere Kriterien nicht erfüllt, wird der Zertifikatsrequest abgelehnt und der Auftraggeber informiert. Die Information des Auftraggebers kann sowohl durch das FI-TS Trustcenter als auch den Freigabe-Ansprechpartner erfolgen. Für eine erneute, korrigierte Beantragung muss der komplette Antragsprozess erneut durchlaufen werden.

Der zuständige Freigabe-Ansprechpartner wird über die Ausstellung des Zertifikats informiert.

8.10.2 Erneuerung

Die Rezertifizierung bzw. Erneuerung eines existierenden Zertifikats muss gemäß den oben festgelegten Antragswegen explizit beantragt werden. Eine automatische Rezertifizierung findet nicht statt.

Die Rezertifizierung wird nach dem gleichen Verfahren wie die Erstregistrierung durchgeführt.

Ca. 6 bis 8 Wochen vor dem Ablauf eines Class 3-Zertifikates erfolgt eine Information über das Ticketsystem von FI-TS an den Auftraggeber.

8.10.3 Rückruf eines Zertifikats

Der Rückruf erfolgt durch den Zertifikatsinhaber selbst.

Für den Rückruf sind die in Kap. 0 Ergänzend und konkretisierend dazu gelten die Ausführungen der Arbeitsanleitung „Prüfung von Zertifikatsanträgen“.

Allgemeines festgelegten Kommunikationswege einzuhalten. Lediglich in Notfällen kann der Freigabeverantwortliche einen Rückruf über den Incidentmanagementprozess von FI-TS veranlassen. Die vereinbarten Arbeitsunterlagen sind in diesem Fall auf dem vereinbarten Wege nachzureichen.

Es können hiervon abweichende Regelungen vertraglich vereinbart sein.

Für die Überprüfung einer Rückrufanforderung sind neben der exakten Bezeichnung des Zertifikates mindestens die Angabe des Namens, der Telefonnummer und der Email-Adresse des Zertifikatsinhabers notwendig. Darüber hinaus können weitere Daten angefordert werden, die zur Identifizierung des Nutzers dienen.

© Finanz Informatik Technologie Service
Dokumentenvorlage: Version 2.0 vom Juli 2015

Der Rückruf des Zertifikats wird vom FI-TS Trustcenter durch telefonische Rücksprache mit dem zuständigen Freigabe-Ansprechpartner des Kunden/Mandanten überprüft, bevor das Zertifikat widerrufen wird.

Der zuständige Freigabe-Ansprechpartner wird über den Rückruf des Zertifikats informiert.

© Finanz Informatik Technologie Service
Dokumentenvorlage: Version 2.0 vom Juli 2015

8.11 Ausstellung weiterer Sub-CAs

Weitere Sub-CAs können von den Wurzelinstanzen des FI-TS Trustcenters ausgestellt werden. Da die Anforderungen in diesem Umfeld sehr individuell sind, werden hier nur die minimalen Sicherheitsanforderungen an den Ausstellungsprozess der zu signierenden CA definiert. Außerdem wird der Beauftragungsprozess beschrieben.

Beispiele für derartige CAs sind CA-Zertifikate für den Einsatz in einer windows-basierten CA, für die Ausstellung von Zertifikaten zur Email-Verschlüsselung oder für individuelle Kunden-CAs.

Als Sub-CA Zertifikate werden ausschließlich X.509 V3 Zertifikate ausgestellt.

Soweit über dieses Dokument hinausgehende Festlegungen notwendig sind, wird für eine Sub-CA ein Policy-Dokument erstellt, in dem z.B. der Einsatzzweck der auszustellenden Zertifikate definiert wird. Dort kann auch geregelt sein, ob ggf. eine Schlüsselhinterlegung stattfindet oder Details zu den erforderlichen Prozessen.

8.11.1 Antragstellung

Zur Einrichtung einer Sub-CA ist die Vorlage einer Zertifizierungsrichtlinie (Policy) erforderlich oder es muss festgelegt sein, nach welcher der drei in diesem Dokument beschriebenen Policies (Klassen) die Sub-CA arbeiten soll.

Eine ggf. neu zu schaffende Richtlinie muss die Kriterien unter Kap. 8.11.3 Anforderungen an die Richtlinie erfüllen. Ebenso sind die technischen Anforderungen gem. Kap. 0 und der Richtlinie „Zertifikate im FI-TS Trustcenter“ zu erfüllen.

Nach Prüfung der entsprechenden Dokumente und ggf. eines Audits der Umgebung wird der Request unterschrieben.

Die Laufzeit dieser Zertifikate beträgt i.d.R. mindestens 10 Jahre, maximal bis zum Laufzeitende der Root-CA.

Eine Schlüsselerneuerung bzw. Erneuerung von CA-Zertifikaten ist nicht vorgesehen. Wenn die Schlüssel oder Zertifikate einer CA nicht weiter verwendet werden sollen oder können, wird eine neue Zertifizierungsinstanz aufgebaut.

8.11.2 Technische Anforderungen

Die Sicherheit des privaten Schlüssels der CA entscheidet letztlich über die Sicherheit der gesamten Sub-CA Instanz. Daher ist eine kryptographisch sichere Erzeugung und Speicherung dieses Schlüssels von großer Bedeutung. Diese Sicherheit kann nur durch spezielle kryptographische Hardware vollständig gewährleistet werden. Es ist allerdings auch bekannt, dass nicht alle Systeme eine solche Hardware unterstützen und deren Einsatz auch nicht immer wirtschaftlich zu vertreten ist.

Weicht eine Sub-CA von der Anforderung ab, so ist in deren Policy eine Beschreibung des eingesetzten Systems, eine Risikobetrachtung mit Identifikation der Restrisiken und eine Übernahme der Risiken aufzuführen.

Der Umgang mit Schlüsselmaterial muss dabei stets nach den in den Richtlinien „ISR_Kryprografie“ und „ISR_Sichere-Kommunikation“ festgelegten Standards erfolgen.

8.11.3 Anforderungen an die Richtlinie

Sofern eine neu einzurichtende CA nicht nach den Kriterien der in dieser Richtlinie definierten Klassen arbeitet, muss eine neue Policy erstellt werden. Die Policy der CA muss folgende Punkte festlegen:

1. Beschreibung der relevanten Prozesse, mindestens zur Beauftragung und Sperrung der CA
2. Beauftragungsweg für Zertifikate und Rückrufe
3. Methoden zur Identifikation des Antragstellers
4. Kommunikationswege
5. Informationen über die Veröffentlichung der Sperrlisten

© Finanz Informatik Technologie Service
Dokumentenvorlage: Version 2.0 vom Juli 2015

6. Technische Beschreibung der verwendeten Systeme
7. Risikobetrachtung

Änderungen an der Policy oder an den verwendeten Systemen sind dem FI-TS Trustcenter vorab mitzuteilen. Das Trustcenter hat das Recht, das Sub-CA Zertifikat zu sperren, sollten die Anforderungen aus diesem Dokument nicht mehr erfüllt sein.

© Finanz Informatik Technologie Service
Dokumentenvorlage: Version 2.0 vom Juli 2015

9 Betriebliche Anforderungen für den Lebenszyklus eines Zertifikats

9.1 Berechtigung für Beantragung eines Zertifikats

Berechtigt für die Beantragung eines Zertifikats sind nur Angehörige von Organisationen, die die PKI-Dienstleistung des FI-TS Trustcenters erworben haben.

9.2 Kriterien für Interoperation mit anderen CAs

Eine Zusammenarbeit mit anderen CAs findet nicht statt.

9.3 Zeiträume für Bearbeitung von Anträgen

Für die Bearbeitung von Anträgen durch das FI-TS Trustcenter sind folgende Zeiten festgelegt:

	Class 1	**Class 2**	**Class 3**
Erstregistrierung	7 Arbeitstage[1]	7 Arbeitstage	10 Arbeitstage
Rezertifizierung	7 Arbeitstage[2]	7 Arbeitstage	10 Arbeitstage
Rückruf	1 Arbeitstag	1 Arbeitstag	4 Stunden

Verzögerungen, die durch den Kunden bzw. den Antragsteller verursacht werden, sind in den o.g. Zeiten nicht enthalten.

Werden Zertifikate in großen Mengen beauftragt oder sind Zertifikate in großen Mengen zu sperren, müssen einvernehmliche Absprachen getroffen werden. Typischerweise werden derartige Aufträge binnen 20 Arbeitstagen erledigt.

Hiervon abweichende Zeiträume sind vertraglich zu vereinbaren.

Es gelten die mit den Kunden vereinbarten Servicezeiten basierend auf den allgemeinen Servicezeiten von FI-TS.

9.4 Ende der Subskription

Endet der Vertrag eines Kunden – gleich aus welchem Grund -, so werden mit Ablauf des Vertrages alle Zertifikate dieses Kunden automatisch und ohne Rücksprache für ungültig erklärt. Eine Information der Zertifikatsnehmer erfolgt dabei nicht.

Abweichungen von dieser Regelung sind vertraglich zu vereinbaren.

9.5 Schlüsselhinterlegung und Schlüsselwiederherstellung

Eine Schlüsselhinterlegung und eine Schlüsselwiederherstellung werden vom FI-TS Trustcenter nicht unterstützt.

9.5.1 Schlüsselhinterlegungs- und Wiederherstellungspolicy und Prozeduren

Findet keine Anwendung.

9.5.2 Session-Schlüssel Kapselungs- und Wiederherstellungspolicy und Prozeduren

Findet keine Anwendung.

[1] sofern keine vollautomatischen Ausstellungsprozesse eingerichtet sind.

[2] sofern keine vollautomatischen Ausstellungsprozesse eingerichtet sind.

© Finanz Informatik Technologie Service
Dokumentenvorlage: Version 2.0 vom Juli 2015

10 Sicherheitsmaßnahmen für die Bereiche Infrastruktur, Management, und Betrieb

Die allgemeinen Maßnahmen orientieren sich an den Vorgaben der Normen ISO 27001 und dem Rahmenwerk des SIZ „Der sichere IT Betrieb (SITB)“.

10.1 Physikalische Sicherheitsmaßnahmen

10.1.1 Lage und Sicherungsmaßnahmen der Gebäude

Die Komponenten der PKI sind in den Rechenzentren von FI-TS untergebracht.

10.1.2 Zutritt

Nur autorisierte Personen haben Zutritt zu den Rechenzentren von FI-TS. Die Räume der Rechenzentren sind videoüberwacht.

10.1.3 Stromversorgung und Klimaanlage

Die Rechenzentren von FI-TS sind mit einer Notstromversorgung ausgestattet und klimatisiert.

10.1.4 Gefährdungspotential durch Wasser

In den Rechenzentren von FI-TS wurden Vorkehrungen gegen Überschwemmung und Wassereinbruch getroffen.

10.1.5 Feuerschutzmaßnahmen

Die Rechenzentren von FI-TS sind mit Rauchmeldern und Löscheinrichtungen gemäß den gesetzlichen Anforderungen ausgestattet.

10.1.6 Lagerung von Backupmedien

Alle Daten werden innerhalb der Rechenzentren von FI-TS gelagert. FI-TS betreibt mehrere räumlich voneinander getrennte Rechenzentren. Ein ausgereiftes Backup-Konzept ermöglicht eine Spiegelung der wichtigsten Systeme und Daten in Echtzeit.

10.2 Betriebliche Sicherheitsmaßnahmen

10.2.1 Rollenkonzept des FI-TS Trustcenters

Für den Betrieb des FI-TS Trustcenters werden unterschiedliche interne und externe Rollen definiert. Diese Rollen beschreiben die Tätigkeiten, die durch den einer Rolle zugeordneten Personenkreis durchgeführt werden darf.

Die Rollen sind an verschiedene Rahmenbedingungen gebunden:

- Unvereinbarkeit: Unvereinbare Rollen dürfen nicht von ein und derselben Person wahrgenommen werden.
- Aufgabentrennung: Bestimmte Tätigkeiten müssen in unterschiedlichen Rollen ausgeführt werden. Durch diese Trennung wird bei bestimmten Aufgaben ein 4-Augen-Prinzip gewährleistet.

10.2.2 Identifizierung und Authentisierung für die Rollen

Die Kommunikation zwischen FI-TS Trustcenter und Freigabe-Ansprechpartnern erfolgt über das Workflow-System von FI-TS, das mindestens eine Passwort-Authentisierung der einzelnen Nutzer erfordert.

10.3 Personelle Sicherheitsmaßnahmen

10.3.1 Anforderungen an die Qualifizierung

Die Mitarbeiter des FI-TS Trustcenters und die Freigabe-Ansprechpartner müssen mit folgenden Themen vertraut sein:

- die Dokumentation zum FI-TS Trustcenter

© Finanz Informatik Technologie Service
Dokumentenvorlage: Version 2.0 vom Juli 2015

- den am Schluss dieser Richtlinie genannten mitgeltenden Unterlagen
- den entsprechenden Passagen des SIZ-Rahmenwerkes „Sicherer IT-Betrieb“ bzw. der ISO Normen 27001 und 27002

Jeder Freigabe-Ansprechpartner muss mit den Validierungsprozessen für Zertifikate innerhalb seines Unternehmens vertraut sein.

10.3.2 Qualifizierungsmaßnahmen

Die Mitarbeiter des FI-TS Trustcenters und die Freigabe-Ansprechpartner werden im Bereich PKI weitergebildet. Welche Art und Häufigkeit der Weiterbildung erforderlich ist, richtet sich allgemein nach dem Stand der Technik und den beim FI-TS Trustcenter eingesetzten Verfahren.

Für die Freigabe-Ansprechpartner liegt die Verantwortung für die Weiterbildung bei dem jeweiligen Kunden, zu dem der Freigabe-Ansprechpartner gehört.

10.3.3 Anforderungen an externe Dienstleister

Für Mitarbeiter externer Dienstleister gelten die Bedingungen des SIZ-Rahmenwerkes „Sicherer IT-Betrieb“ bzw. der ISO Normen 27001 und 27002.

10.4 Audit Logging Prozeduren

10.4.1 Klassen von Events, die aufgezeichnet werden

10.4.1.1 RA

- Booten und Shutdown der RA-Systeme
- Starten und Stoppen der RA-Software
- Account-Management
- Zugriff auf die RA-Software, einschließlich unautorisierter Zugriffsversuche
- Anforderungen von Zertifikaten und zugehörige Informationen, die zwischen Nutzer und RA ausgetauscht werden.
- Anforderung von Zertifikatswiderrufen und zugehörige Informationen, die zwischen Nutzer und RA ausgetauscht werden.
- Prozeduren zur Überprüfung der Identität des Zertifikatsanfordernden (Workflow-System)

10.4.1.2 CA

- Booten und Shutdown der CA-Systeme
- Starten und Stoppen der CA-Software
- Account-Management
- Zugriff auf die CA-Software, einschließlich unautorisierter Zugriffsversuche
- Ausstellung von Zertifikaten
- Zertifikatswiderruf
- Ausstellung von CRLs

10.4.2 Aufbewahrungsfrist der Audit Log-Daten

Die Log-Daten werden mindestens 2 Monate vorgehalten. Anschließend werden sie archiviert (s.a. 10.5).

10.4.3 Schutz der Audit Log-Daten

Nur autorisiertes Personal von FI-TS darf auf die Audit Log-Daten zugreifen.

10.4.4 Sicherung der Audit Log-Daten

Die Sicherung der Audit Log-Daten erfolgt kontinuierlich.

© Finanz Informatik Technologie Service
Dokumentenvorlage: Version 2.0 vom Juli 2015

10.4.5 System, das die Audit-Daten sammelt (extern oder intern)

Das System, das Auditdaten sammelt und zur Verfügung stellt, kann unabhängig von der CA-Software laufen.

10.4.6 Information über Verursacher von Audit-Daten

Die Verursacher von Audit-Daten werden nicht über die Audit-Daten informiert, die durch ihre Aktionen erzeugt wurden.

10.4.7 Vulnerability Assessments

Die Mitarbeiter des FI-TS Trustcenters und die Freigabe-Ansprechpartner der Kunden müssen sensibilisiert sein, Anzeichen, die auf eine Störung der Integrität des FI-TS Trustcenters und seiner Prozesse hindeuten, zu erkennen und zu melden. Jede festgestellte mögliche Schwachstelle muss im Rahmen eines Vulnerability Assessments überprüft werden.

10.5 Datenarchivierung

10.5.1 Klassen von Daten, die archiviert werden

- Zertifikatsbeauftragungen und zugehörige Informationen, die zwischen Nutzer und RA bzw. CA ausgetauscht werden, sind innerhalb des FI-TS Workflow-Systems festgehalten. Bei automatisiert stattfindenden Zertifizierungsvorgängen findet dies keine Anwendung.
- Ausgestellte Zertifikate bleiben innerhalb der PKI-Datenbanken auch nach Widerruf oder Ablauf gespeichert.
- Zertifikatswiderrufe und zugehörige Informationen, die zwischen Nutzer und RA bzw. CA ausgetauscht werden, sind innerhalb des FI-TS Workflow-Systems festgehalten.
- Versionen der System-Konfiguration der CAs werden für 3 Jahre (maximale Laufzeit der Nutzer-Zertifikate) aufbewahrt.
- Audit-Daten aus 10.4.1
- Versionen dieser und der Richtlinie „Zertifikate im FI-TS Trustcenter“ werden im Rahmen des Dokumentenmanagements archiviert.
- Zertifikatsrequests werden nur kurzzeitig archiviert.

Nicht archiviert werden

- Veröffentlichte CRLs
- Private Signaturschlüssel der PKI.

10.5.2 Aufbewahrungsfrist für archivierte Daten

Digitale Zertifikate des FI-TS Trustcenters und Daten, die zur Beantragung oder dem Widerruf von Zertifikaten von Bedeutung sind, werden bis zwei Jahre nach Gültigkeitsende bzw. dem Revoke-Datum aufbewahrt.
Alle anderen Auditdaten werden 5 Jahre aufbewahrt.

10.5.3 Schutz der archivierten Daten

Die digital archivierten Daten werden nicht verschlüsselt gespeichert. Zugriff auf diese Daten haben nur autorisierte Personen des FI-TS Trustcenters.

10.5.4 Sicherung der archivierten Daten

s. 10.4.4

10.5.5 Zeitstempel für archivierte Daten

Alle archivierten Daten sind mit einem Zeitstempel zu versehen.

10.5.6 Lokation des Archives (intern oder extern)

s. 10.4.5

© Finanz Informatik Technologie Service
Dokumentenvorlage: Version 2.0 vom Juli 2015

10.5.7 Abläufe um Daten aus dem Archiv zu erhalten und diese zu verifizieren

Die archivierten Daten sind gemäß den Richtlinien Abschnitt 13.1 zu behandeln.

10.6 Kompromittierung und Desaster-Recovery

10.6.1 Abläufe im Fall der Kompromittierung oder eines Sicherheitsvorfalls im Bereich des FI-TS Trustcenters

Im Falle der Kompromittierung des Schlüsselmaterials oder eines Sicherheitsvorfalls im Bereich des FI-TS Trustcenters ist der FI-TS Krisenprozess anzustoßen, das Problem zu analysieren und gegebenenfalls neues Schlüsselmaterial für die CAs des FI-TS Trustcenters zu generieren.

Die Nutzer sind über diese Aktionen zu informieren.

Alle zu ergreifenden Maßnahmen sind von den Umständen des Falles abhängig. Die grundlegende Vorgehensweise ist:

1 Umfang und Art der Kompromittierung ermitteln und beheben

   Die privaten Schlüssel der CAs des FI-TS Trustcenters sind erheblich gesichert. Im ersten Schritt muss deshalb ermittelt werden, aufgrund welcher Gegebenheiten die Schlüssel kompromittiert werden konnten. Nur wenn die Ursache bekannt und dauerhaft behoben ist, können die folgenden Schritte eingeleitet werden.

2 Information der betroffenen Kunden

   Alle betroffenen Kunden (Zertifikatsinhaber) müssen direkt informiert werden. Darin muss ein Hinweis auf die folgenden Schritte 4 bis 6 mit dem dafür vorgesehenen Zeitrahmen enthalten sein.

3 Generierung einer neuen Root-CA

   Es wird eine neue Root-CA nach den geltenden Vorgaben erzeugt und vollumfänglich bereitgestellt. Alle erforderlichen Intermediate-Instanzen werden ebenfalls neu erstellt und aus der neuen Root-CA signiert. Die CRLs der neuen Instanzen werden veröffentlicht.

4 Vertrauen der Kunden herstellen

   Betroffene Kunden müssen der neuen Root-CA und den davon signierten Zwischenzertifikaten das Vertrauen aussprechen und diese parallel in den Zertifikatsspeichern hinterlegen bzw. die Hinterlegung beauftragen, damit die neu auszustellenden Nutzer-Zertifikate den ihnen zugedachten Zweck erfüllen können.

5 Neuausstellung der Nutzer-Zertifikate

   Die Nutzer-Zertifikate werden vom Kunden neu beauftragt und aus der neuen Infrastruktur neu ausgestellt. Sobald der Austausch vollzogen ist, werden die Zertifikate in der alten kompromittierten Infrastruktur durch Eintrag in die CRL gesperrt. Über die Zertifikatsdatenbank und die CRL kann jeweils der Bearbeitungsgrad des Austauschs kontrolliert werden. Die Bearbeitungsreihenfolge ist grundsätzlich:

   i) Server-Zertifikate
   ii) Client-Zertifikate
   iii) andere Zertifikate

6 Bereinigung der Zertifikatsspeicher

   Sobald alle noch benötigten Nutzer-Zertifikate neu erstellt wurden, müssen die CA-Zertifikate der kompromittierten Root-CA einschl. der damit signierten Zwischenzertifikate aus allen Zertifikatsspeichern entfernt werden. Dieser Prozess kann für Standard Clients weitestgehend automatisiert erfolgen, muss jedoch sorgfältig vorgenommen werden. Schließlich verbleiben von der alten Struktur aus kompromittiertem Root- und allen davon ausgestellten Zwischenzertifikaten nur noch die CRLs. Diese Sperrlisten sollten jetzt vollständig sein, d.h. sie enthalten alle ursprünglich signierten Nutzer-Zertifikate als Sperreintrag und sie sollten für die Restlaufzeit der Zwischenzertifikate abrufbar sein.

© Finanz Informatik Technologie Service
Dokumentenvorlage: Version 2.0 vom Juli 2015

10.6.2 Abläufe im Fall von defekter Hardware, Software oder Daten

- Bei Ausfall der primären PKI-Hardware wird auf die entsprechende Backup-Hardware geschwenkt.
- Bei Verlust oder Beschädigung von Software oder Daten werden die betroffenen Teile der PKI mit dem letzten Sicherungsstand wieder aufgesetzt und auf der Basis der Änderungsinformationen wieder auf den aktuellen Stand unmittelbar vor der Beschädigung überführt.
- Die Abläufe erfolgen im Rahmen des Backupkonzepts für zentrale Hardware von FI-TS.

10.6.3 Möglichkeiten des Weiterbetriebs nach einer Krise

Über den Weiterbetrieb nach einer Krise wird im Rahmen des FI-TS Krisenprozesses entschieden.

10.7 Beendigung des CA- oder RA-Dienstes

Der Dienst des FI-TS Trustcenters kann an eine andere Organisation übertragen werden. In diesem Fall werden alle Zertifikatsinhaber bzw. Kunden mit einem Vorlauf von sechs Monaten informiert. Die neue Organisation sollte dieser Zertifizierungsrichtlinie und der zugehörigen Zertifikatsrichtlinie entsprechen.

Bei Beendigung des Dienstes durch FI-TS werden die Kunden ebenfalls mit einem Vorlauf von sechs Monaten benachrichtigt.

© Finanz Informatik Technologie Service
Dokumentenvorlage: Version 2.0 vom Juli 2015

11 Technische Sicherheitsmaßnahmen

11.1 Schlüsselerzeugung und Installation

11.1.1 Schlüsselerzeugung

Die Schlüssel der Root-CAs sowie die Schlüssel der Class 1 CAs, Class 2 CAs und Class 3 CAs werden ausschließlich durch autorisiertes Personal des FI-TS Trustcenters im 4-Augen-Prinzip erzeugt. Die Erzeugung des Schlüsselmaterials erfolgt nach Möglichkeit in spezieller kryptographischer Hardware.

Die Schlüssel spezieller untergeordneter CAs werden entsprechend den in den jeweiligen Policies festgelegten Verfahren erzeugt. Das 4-Augen-Prinzip ist dabei stets zu wahren und es ist sicherzustellen, dass keine einzelne Person Kenntnis des gesamten privaten Schlüssels im Klartext erlangen kann.

Schlüsselmaterial für spätere Zertifikatsinhaber kann in bestimmten Fällen und auf Anforderung durch das FI-TS Trustcenter erzeugt werden. Dabei kommen der kryptographisch sichere Zufallszahlengenerator des Hardware Security Module oder geeignete Software-Mechanismen zum Einsatz.

Zum Anwender werden diese Schlüssel verschlüsselt übertragen; dies geschieht beispielsweise in einem pkcs#12-Container. Die Übermittlung des verwendeten Passworts erfolgt entweder über einen gesicherten oder einen getrennten Kanal. Als gesicherter Kanal werden z.B. das Workflow-System von FI-TS mit dem korrespondierenden Auftragstyp und speziell gesicherten Feldern oder verschlüsselte Emails betrachtet.

Eine Schlüsselhinterlegung für Nutzer-Zertifikate findet nicht statt, eine Wiederherstellung von Schlüsseln ist demzufolge nicht möglich. Nähere Details können vertraglich festgelegt sein.

11.1.2 Übergabe des öffentlichen Schlüssels an den Aussteller von Zertifikaten

Das FI-TS Trustcenter akzeptiert Zertifikatsanforderungen im pkcs#10-Format (base64-codiert, pem, s. RFC 2986).

Die Übertragung der Anforderungen geschieht mit dem Workflow-System von FI-TS, soweit keine anderslautenden Vereinbarungen bestehen.

11.1.3 Veröffentlichung von CA-Zertifikaten für Zertifikatsnutzer

Siehe Richtlinie „Zertifikate im FI-TS Trustcenter“

11.1.4 Schlüssellängen

Siehe Richtlinie „Zertifikate im FI-TS Trustcenter“

11.1.5 Parameter für die Generierung von öffentlichen Schlüsseln und Qualitätsprüfung

Siehe Richtlinie „Zertifikate im FI-TS Trustcenter“

11.1.6 Verwendungszweck der Schlüssel

Siehe Richtlinie „Zertifikate im FI-TS Trustcenter“

11.2 Sicherheitsmaßnahmen zum Schutz des privaten Schlüssels und kryptographische Methoden

11.2.1 Standards und Schutzmaßnahmen der genutzten kryptographischen Methoden

Die eingesetzte kryptographische Hardware entspricht mindestens FIPS140-1 LEVEL 4

11.2.2 Hinterlegung des privaten Schlüssels

Die privaten Schlüssel des FI-TS Trustcenters werden grundsätzlich nur in kryptographischer Hardware gehalten und darüber hinaus auf IT-Systemen nicht hinterlegt. Soweit dies für bestimmte CAs nicht möglich ist, wird das Schlüsselmaterial so implementiert, dass es nicht exportierbar ist.

© Finanz Informatik Technologie Service
Dokumentenvorlage: Version 2.0 vom Juli 2015

11.2.3 Sicherung des privaten Schlüssels

Die Sicherung der privaten Schlüssel des FI-TS Trustcenters erfolgt im Rahmen eines gesonderten Verfahrens, das im 4-Augen-Prinzip durchgeführt und zusätzlich unter Aufsicht eines Auditors durchgeführt wird.

Das dazu eingesetzte Verfahren ist im Rahmen eines besonderen Fachkonzeptes dokumentiert, vertraulich und wird nicht veröffentlicht.

11.2.4Archivierung des privaten Schlüssels

Siehe 11.2.3.

11.2.5 Übermittlung des privaten Schlüssels in oder aus einem Verschlüsselungsmodul

Siehe 11.2.3.

11.2.6 Speicherung von privaten Schlüsseln in Verschlüsselungsmodulen

Siehe 11.2.3.

11.2.7 Aktivierungs- und Deaktivierungsmethode für den privaten Schlüssel

Die Aktivierung des privaten Schlüssels erfolgt durch die an einen Nutzer gebundenen Rechte, die er nach erfolgreicher Authentisierung zugewiesen bekommt.

11.2.8 Löschen des privaten Schlüssels

Die privaten Schlüssel des FI-TS Trustcenters werden grundsätzlich nicht gelöscht. Es kann entschieden werden, dass private Schlüssel von IT-Systemen entfernt werden, wenn die betr. CA über einen längeren Zeitraum hinweg inaktiv ist – sofern die Löschung technisch möglich ist. „Über einen längeren Zeitraum hinweg inaktiv“ bedeutet hier, dass alle ausgestellten Nutzer-Zertifikate entweder abgelaufen oder seit mindestens 1 Jahr gesperrt sein müssen. Im Übrigen siehe 11.2.3.

11.3 Weitere Aspekte des Managements von Schlüsselpaaren

11.3.1 Archivierung des öffentlichen Schlüssels

Siehe 10.5

11.3.2 Gültigkeitszeitraum für Zertifikate und Nutzungszeitraum für ein Schlüsselpaar

Siehe Richtlinie „Zertifikate im FI-TS Trustcenter“.

11.4 Maßnahmen zur Computersicherheit

11.4.1 Spezifische technische Anforderungen an die Computersicherheit

- Die Entschlüsselung der privaten Schlüssel des FI-TS Trustcenters findet grundsätzlich innerhalb spezieller kryptographischer Module statt. Kryptographische Operationen mit den privaten Schlüsseln des FI-TS Trustcenters werden grundsätzlich in speziellen kryptographischen Modulen durchgeführt.
- Die Schlüssel spezieller untergeordneter CAs werden mit den Krypto-Modulen des jeweiligen Betriebssystems entschlüsselt und genutzt.
- Der Zugriff auf kryptographische Operationen mit den privaten Schlüsseln des FI-TS Trustcenters erfordert dedizierte Berechtigung der Nutzer.

11.4.2 Bemessung der Computersicherheit

Ein formales Rating der Computersicherheit findet nicht statt.

11.5 Zeitstempel

Die Systeme des FI-TS Trustcenters laufen mit einer zur Physikalisch-Technischen Bundesanstalt synchronen Zeit.

© Finanz Informatik Technologie Service
Dokumentenvorlage: Version 2.0 vom Juli 2015

12 Audits

12.1 Häufigkeit der Audits

Ein Audit findet mindestens einmal pro Jahr statt.

12.2 Identität/Qualifikation des Auditors

Der Auditor nimmt keine weiteren Aufgaben im operativen Betrieb des FI-TS Trustcenters wahr.

12.3 Umfang des Audits

Es werden alle Instanzen, Rollen, Prozesse, Personen, Protokolle und Log-Dateien des Trustcenters stichprobenartig überprüft.

12.4 Maßnahmen nach Feststellung von Mängeln

Werden Mängel festgestellt, werden sofort geeignete Maßnahmen zu deren Beseitigung eingeleitet. Falls die Sicherheit des Trustcenters gefährdet ist, wird der Betrieb bis zur Beseitigung der Mängel eingestellt.

12.5 Veröffentlichung der Ergebnisse des Audits

Die Ergebnisse des Audits bzw. der Mängelbeseitigung werden nicht veröffentlicht.

© Finanz Informatik Technologie Service
Dokumentenvorlage: Version 2.0 vom Juli 2015

13 Sonstige Bestimmungen

Es gelten die Allgemeinen Geschäftsbedingungen von FI-TS in der jeweils aktuellen Version.

Informationen über die Gebühren für Leistungen des FI-TS Trustcenters werden auf Anfrage erteilt.

Das FI-TS Trustcenter gewährleistet, dass alle Zertifikate entsprechend dieser Zertifizierungsrichtlinie und der zugehörigen Zertifikatsrichtlinie ausgestellt werden.

Die RAs bzw. die Freigabe-Ansprechpartner gewährleisten, dass die Identität der Zertifikatsinhaber bzw. die Zuordnung von Zertifikaten zu den darin beschriebenen Objekten zum Zeitpunkt der Ausstellung überprüft wurde.

Für die Ausstellung eines Zertifikates, das auf falschen oder fehlerhaften Daten einer externen RA beruht, haftet ausschließlich die externe RA und nicht das FI-TS Trustcenter. Eine Haftung des FI-TS Trustcenters ist in diesem Fall ausgeschlossen.

Der Zertifikatsinhaber ist für die Benutzung seines Zertifikates allein verantwortlich; FI-TS übernimmt keinerlei Verantwortung für Rechtsgeschäfte, die mit Einsatz eines Zertifikates getätigt werden.

13.1 Datenschutz

Im Rahmen des Betriebs des Trustcenters werden persönliche Daten erhoben. Diese werden nach dem BDSG und der Datenschutz-Policy von FI-TS in ihrer jeweils gültigen Fassung behandelt.

13.1.1 Vertrauliche Informationen

Alle persönlichen Daten, die nicht im Zertifikat enthalten sind, gelten als vertrauliche Informationen. Ausnahmen stellen solche Informationen dar, deren Veröffentlichung der Eigentümer der Information zugestimmt hat und die zum Auffinden oder zur eindeutigen Kennzeichnung eines Zertifikates dienen. Diese sind Name, Vorname, Nutzerkennungen, Geräteidentifikationen.

13.1.2 Nicht vertrauliche Informationen

Alle Daten, die im Zertifikat enthalten sind, **gelten als nicht vertraulich**. Dies gilt insbesondere auch für alle Fälle, wenn im Zertifikat Namen, Vornamen, Mail-Adressen usw. enthalten sind. Entsprechend der Nutzung des Zertifikates können alle darin enthaltenen Informationen öffentlich werden. Des weiteren sind Informationen, die für die Überprüfung eines Zertifikats benötigt werden, generell nicht vertraulich und werden veröffentlicht. Insbesondere gelten Informationen zur Sperrung eines Zertifikates (Seriennummer, Zeitpunkt, Ursache u.ä.) als öffentliche Informationen.

Ferner gelten jene Informationen als nicht vertraulich, die zwar nicht im Zertifikat enthalten sind, deren Veröffentlichung der Eigentümer der Information aber explizit zugestimmt hat und die zum Auffinden oder zur eindeutigen Kennzeichnung eines Zertifikates vorgesehen sind.

Das FI-TS Trustcenter behält sich vor, nicht vertrauliche Informationen zu veröffentlichen.

13.1.3 Informationen zur Sperrung von Zertifikaten

In einer CRL werden die Seriennummer eines gesperrten Zertifikates sowie der Zeitpunkt und ggf. Ursache der Sperrung veröffentlicht.

Der Zertifikatsinhaber wird über die zuständige RA informiert, wenn sein Zertifikat gesperrt wird. Die RA und der Inhaber werden auch informiert, wenn ein Zertifikat aus einem anderen als von ihm angegebenem Grund gesperrt wurde oder wenn die von ihm beauftragte Sperrung abgelehnt wurde.

13.1.4 Aushändigung von Informationen nach gerichtlicher Anforderung

Bei gerichtlicher oder behördlicher Anforderung werden nach Prüfung der Rechtsgrundlagen und vorgelegten Beschlüsse alle angeforderten Informationen ausschließlich der anfordernden Behörde übergeben. Die betroffenen Zertifikatsinhaber werden, falls zulässig, informiert.

© Finanz Informatik Technologie Service
Dokumentenvorlage: Version 2.0 vom Juli 2015

13.1.5 Herausgabe bzw. Löschung von Informationen nach Aufforderung durch den Eigentümer der Information

Fordert ein Eigentümer von vertraulichen oder personenbezogenen Daten das FI-TS Trustcenter auf, diese Daten herauszugeben bzw. zu löschen, wird das FI-TS Trustcenter diese dem Eigentümer übergeben bzw. löschen, soweit dem keine rechtlichen, vertraglichen oder sicherheitstechnischen Rahmenbedingungen entgegenstehen.

13.1.6 Weitere Umstände für die Weitergabe von vertraulichen Informationen

Vertrauliche und personenbezogene Informationen werden außer den im Abschnitt 13.1 genannten Gründen unter keinen anderen Umständen weitergegeben.

13.2 Regelung der Urheberrechte und der Eigentumsrechte

Die Root-CA-Zertifikate, deren Sub-CA-Zertifikate sowie die privaten und öffentlichen Schlüssel der CA des FI-TS Trustcenters sind Eigentum von FI-TS.

Die Zertifikate, die für die Zertifikatsinhaber ausgestellt wurden, sowie die dazugehörigen privaten und öffentlichen Schlüssel sind Eigentum der jeweiligen Inhaber.

13.3 Individuelle Vereinbarungen und Kommunikation zwischen den beteiligten Parteien

Änderungen oder Ergänzungen dieser Richtlinie bedürfen zu ihrer Wirksamkeit der Schriftform. Dies gilt auch für eine Änderung oder Aufhebung des Schriftformerfordernisses selbst. Mündliche Nebenabreden bestehen nicht.

13.4 Zugrundeliegende gesetzliche Bestimmungen

Der Betrieb des FI-TS Trustcenters, diese Zertifikatspolicy und die Zertifizierungspolicy unterliegen dem Recht der Bundesrepublik Deutschland unter Ausschluss des UN-Kaufrecht (CISG).

Das FI-TS Trustcenter stellt keine qualifizierten Zertifikate im Sinne des deutschen Signaturgesetzes aus.

© Finanz Informatik Technologie Service
Dokumentenvorlage: Version 2.0 vom Juli 2015

14 Internes Kontrollsystem (IKS)

14.1 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

14.2 Zuordnung der Kontrollziele, -verfahren und -ergebnisse

Kontrollziel	Kontrollverfahren	Kontrollergebnis	Bemerkungen
Siehe oben	Alle Kontrollverfahren werden ausführlich im Kapitel 10 „Sicherheitsmaßnahmen für die Bereiche Infrastruktur, Management, und Betrieb“ beschrieben	Alle Kontrollergebnisse werden ausführlich im Kapitel 10 „Sicherheitsmaßnahmen für die Bereiche Infrastruktur, Management, und Betrieb“ beschrieben	

© Finanz Informatik Technologie Service
Dokumentenvorlage: Version 2.0 vom Juli 2015

15 Anhang

15.1 Definitionen

Begriff	Definition
Freigabe-Ansprechpartner	Namentlich definierte Gruppen von Personen eines Kunden/Mandanten, die berechtigt sind, einen Zertifikatsrequest von Auftraggebern 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	Als Kunde/Mandant bestehen zwei mögliche 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.
Zertifikatsnutzer	Der Zertifikatsnutzer ist diejenige Person oder Organisation, die anhand eines Zertifikats die Authentizität eines Kommunikationspartners feststellt und überprüfen kann.
Certication Revocation List	Hierbei handelt es sich eine Liste 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.

15.2 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

© Finanz Informatik Technologie Service
Dokumentenvorlage: Version 2.0 vom Juli 2015

URI	Uniform Ressource Identifier
USB	Universal Serial Bus
VPN	Virtual Private Network
X.509	ISO Standard zum Format digitaler Zertifikate

© Finanz Informatik Technologie Service
Dokumentenvorlage: Version 2.0 vom Juli 2015