finanz informatik
technologie service

# Richtlinie

# Zertifizierung 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 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 Internet “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: Richtlinie Zertifizierung im FI-TS-Trustcenters

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 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 gellten 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 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.<br>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.<br>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 (FI-TS) 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 Einführung

Ein Zertifikat ist eine elektronische Bescheinigung, mit der ein öffentlicher kryptografischer 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 kryptografischen 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 Organisationen* (jur. Personen) müssen in allen Fällen die Angaben des Unternehmens oder der Institution enthalten.
- *Zertifikate für Personen* müssen immer Angaben zu der Organisation enthalten, zu der die Person gehört. Personenzertifikate sind demnach immer einer Person zugeordnet.
- *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 Endteilnehmer. 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 Nutzerzertifikate 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. So bestehen z.B. die „Finanz Informatik Technologie Service F04 *Class2* CA G1“ und die „Finanz Informatik Technologie Service F04 *Class2* CA G2“. Diese CAs unterliegen den gleichen 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 von Endteilnehmern 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.

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 Freigabeansprechpartner 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 der 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 Bankenumfeld aus.

Zertifikate werden für Organisationen, Personen oder Geräte ausgestellt.

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

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

### 4.1.4 Zertifikatsnutzer

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

### 4.1.5 Weitere Teilnehmer

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

#### 4.1.5.1 Freigabeansprechpartner

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

#### 4.1.5.2 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
- Endnutzer-Zertifikate

#### 4.2.1 Zulässige Nutzungszwecke

1. Root-CA Zertifikate: Root-Zertifikate dürfen ausschließlich zur Signierung untergeordneter CA-Zertifikate verwendet werden. Endutzer-Zertifikate dürfen damit *nicht* signiert werden.
2. Sub-CA Zertifikate: Die Zertifikate untergeordneter CAs ("Sub-CA") werden zur Signierung von Zertifikaten für Endnutzer 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).
3. Endnutzerzertifikate: 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.

### 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 zum FI-TS Trustcenter 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
- CA-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 Endteilnehmern 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.

# 5 Generelle Vorschriften

Dieser Abschnitt beschreibt sowohl die Verpflichtungen der Betreiber des FI-TS Trustcenter als auch der Endteilnehmer. Durch diese Vorschriften soll ein hohes Sicherheitsniveau und damit ein hohes Maß an Vertrauen zwischen den beteiligten Parteien gewährleistet 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 Endteilnehmer gemäß den Anforderungen zuverlässig zu prüfen.

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

Die RAs sind verpflichtet, jeden Auftrag zur Erstellung von Zertifikaten,, der an die CA weitergeleitet wird, zu dokumentieren. Dies gilt nicht für automatisierte Verfahren.

Kommt eine RA außerhalb von FI-TS den hier aufgeführten Verpflichtungen nicht nach, so haftet FI-TS nicht für die dadurch entstandenen 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 Freigabeansprechpartners

Der Freigabeansprechpartner ist verpflichtet, die ihm gemäß den Vereinbarungen zugeordneten Aufgaben zuverlässig durchzuführen und zu dokumentieren.

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

## 5.4 Verpflichtungen des Zertifikatsinhabers

Der Endteilnehmer, 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 Zwecke und mit angemessener Vorsicht einzusetzen.

Der Endteilnehmer 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 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.

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 Daten,

- die im Zertifikat selbst enthalten sind oder
- zur Überwachung benötigt werden (z.B. geänderter Ansprechpartner bei Server-Zertifikaten).

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

Der Zertifikatsinhaber darf das Zertifikat und die zugehörigen Schlüssel nur zu den im Zertifikat definierten Verwendungszwecken nutzen.

## 5.5 Verpflichtungen des Zertifikatsnutzer

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

# 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 der betr. CA-Zertifikate 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 anhand ihrer Key-Usage bzw. Extended Key-Usage unterschieden. Kombinationen mehrer Key-Usages und Extended Key-Usages sind in grundsäztlich zulässig.

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 zwei Typen unterschieden:

- Root-Zertifikate: Diese Zertifikate sind selbstsigniert. Sie dienen ausschließlich zur Ausstellung von Intermediate CA-Zertifikaten.
- Intermediate CA-Zertifikate für Sub-CAs: Diese Zertifikate sind vom FI-TS Trustcenter Root-Zertifikat unterzeichnet. Sie dienen grundsätzlich der Ausstellung von Endnutzer-Zertifikaten.
- Intermediate-Zertifikate können auch für Policy-CAs ausgestellt werden. In diesen Fällen werden mit den CA-Zertifikaten ausschließlich weitere CA-Zertifikate für Sub-CAs ausgestellt.

CA-Zertifikate sind von folgenden Merkmalen bestimmt:

1. Regulatorische Anforderungen
   - Zugehörigkeit zu genau einer Zertifikatsklasse
2. Technische Anforderungen
   - Schlüssellänge
   - Signaturalgorithmus
   - „Scope“ einer CA z.B. aufgrund von Netzwerkeinschränkungen bei Nutzung von Auto-Enrollment-Funktionen

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.

Der Widerruf eines CA-Zertifikates, der aufgrund eines kompromittierten CA-Schlüssels erforderlich wird, erfolgt im Rahmen des FI-TS Krisenprozesses.

## 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 (Class-1-Zertifikate) ausgegeben.

## 7.4 Client-Zertifikate für Personen

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

Client-Zertifikate für natürliche Personen können in Verbindung mit entsprechenden Key-Usages darüber hinaus zur Verschlüsselung oder Signatur von Dokumenten oder Emails genutzt werden.

Client-Zertifikate werden manuell, halbautomatisch oder automatisiert ausgegeben.

## 7.5 Sonstige Zertifikate

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

# 8 Identifizierung und Authentisierung

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

## 8.1 Allgemeines

Für die Identifizierung und Authentisierung am FI-TS Trustcenter ist ein Verfahren festgelegt, das diese beiden Schritte in die Verantwortung der Kunden/Mandanten übergeben kann und das eine vertrauenswürdige Kommunikation zwischen dedizierten Ansprechpartnern auf beiden Seiten voraussetzt.

Auf der Seite des Kunden/Mandanten werden im Rahmen einer RA sogenannte Freigabeansprechpartner 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/Mandaten den Zertifikatsrequest bzw. den Zertifikatswiderruf an das FI-TS Trustcenter weiter.

Für die Weiterleitung ist das Workflow-System (ARS) von FI-TS vorgesehen:

Der (künftige) Zertifikatsinhaber erstellt einen Auftrag zur Zertifikatserstellung oder den -widerruf. Diese Zertifikatsanforderung oder Zertifikatsrückruf wird vom Freigabeansprechpartner überprüft und ggf. genehmigt. Nach der Genehmigung wird der Auftrag automatisch an das Trustcenter weitergeleitet. Dieses stellt dann 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 Freigabeansprechpartner mehrere Zertifikatsrequests oder die Zertifikatswiderrufe in einem Auftrag zusammenfassen und diesen genehmigt weiterleiten.

## 8.2 Namenkonventionen

### 8.2.1 Allgemeines

Es gelten die Vorgaben der Richtlinie „Zertifikate im FI-TS-Trustcenter“.

### 8.2.2 Wiedererkennung, Authentisierung und die Rolle von Schutzmarken

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

## 8.3 Methoden zur Überprüfung des Besitzes der privaten Schlüssel

Die RA kann vom Endteilnehmer 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 Endteilnehmer ein Zertifikat anfordert, das als Bestandteil den Namen einer juristischen Person enthält, muss im Vorfeld auf der Basis eines 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

Änderungen von Zertifikatsinhalten sind 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 auch eine Übergangszeit vereinbart werden, während der beide Zertifikate gültig sind. Dies erleichtert eine Migration. Dieser Zeitraum sollte nicht länger als fünf Arbeitstage andauern.

## 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-Funkionen bestimmt. Alle Prüfungsschritte beschränken sich daher auf solche Aspekte, die automatisiert durchführbar sind.

### 8.8.1 Registrierung

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

1. Der Common Name (CN, „Betreff“) muss den Konventionen der jeweils gültigen Zertifikatsrichtlinie entsprechen und den anfordernden Kunden/Mandanten zuordenbar sein.
2. Wenn eine Domain (Top-Level-Domain und Second-Level-Domain, z.B. example.de) öffentlich registriert ist, bedarf es einer schriftlichen Autorisierung durch den Inhaber der Domain, damit das Zertifikat ausgestellt werden darf. Hierfür besteht ein entsprechender Vordruck, der durch den admin-c der Domain unterzeichnet werden muß.
3. Das Organisations-Feld (O) muß mit einem Wert belegt sein, der zur Domain des gewählten CN paßt. Es darf insbesondere kein Widerspruch zu einer bestehenden Domain-Registrierung und der Belegung des Feldes bestehen.
   Erlaubte Werte sind eine Kurzform oder der juristische Name zur Bezeichnung der Organisation.
4. Das Country-Feld (C) muß zum Hauptsitz oder einer Niederlassung der Organisation passen.
5. Alle übrigen Felder sind optional und werden nicht geprüft.
6. Die Beauftragungen für Zertifikate muss gemäß dem für den jeweiligen Kunden/Mandanten definierten Antragsverfahren durchgeführt sein.
   Soweit nichts anderes vereinbart ist, 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 Freigabeansprechpartners.
   b. Grundsätzlich erfolgt die Zertifikatsausstellung per Request. Liegt ein Request vor, muß er im Workflowsystem übermeittelt 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 übermittel werden.

   Die Überprüfung der Parameter erfolgt in der Regel durch den Freigabeansprechpartner.

   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 Endnutzer informiert. Die Information des Endnutzers erfolgt in der Regel durch den Freigabeansprechpartner, kann aber auch durch das FI-TS-Trustcenter erfolgen. Für die erneute, korrigierte Beantragung muss der komplette Antragsprozess erneut durchlaufen werden.

   Die Dokumentation des Ablaufs erfolgt durch die in 8.1 beschriebenen Verfahren.

   Der entsprechende Freigabeansprechpartner wird über die Ausstellung des Zertifikats informiert.

7. Alternativ zur vorstehend beschriebenen manuellen Beauftragung und Prüfung können Zertifikate auch voll automatisiert auf Grundlage dafür vorgesehner Protokolle ausgestellt werden. Es gelten dann folgende Kriterien:
    a. Zu 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.

### 8.8.2 Erneuerung

Die Rezertifizierung eines existierenden Zertifikats muss explizit beaftragt werden. Eine automatische Rezertifizierung findet nicht statt.

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

### 8.8.3 Rückruf eines Zertifikats

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

Für den Rückruf sind die in Kap. 8.1 Allgemeines festgelegten Kommunikationswege einzuhalten.

Es können hiervon abweichende Regelungen vertraglich vereinbart sein.

Für die Überprüfung einer Rückrufanforderung sind neben der exakten Bezeichnung des Zertifikates (CN) auch die Angabe der ausstellenden CA und der Seriennummer notwendig.

## 8.9 Class 2-Zertifikate

Die Prüfung dieser Zertifikatrequests 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.

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

Die Prüfungen können teilautomatisiert oder manuell erfolgen. Eine voll automatisierte Ausstellung 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 Endnutzer informiert. Die Information des Endnutzers erfolgt in der Regel durch den Freigabe-Ansprechpartner, kann aber auch durch das FI-TS-Trustcenter erfolgen. Für die erneute, korrigierte Beantragung muss der komplette Antragsprozess erneut durchlaufen werden.

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

### 8.9.2 Erneuerung

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

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

### 8.9.3 Rückruf eines Zertifikats

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

Für den Rückruf sind grundsätzlich die in Kap. 8.1 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.

Der Freigabeansprechpartner legt die Bedingungen zur Sperrung eines Zertifikates in seiner Organisation fest.

Für die Überprüfung einer Rückrufanforderung sind neben der exakten Bezeichnung des Zertifikates mindestens die Angabe des Namens (CN) auch die Angabe der ausstellenden CA und der Seriennummer notwendig. Darüber hinaus können weitere Daten angefordert werden, die zur Identifizierung des Nutzers dienen.

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

## 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 vonFI-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.

### 8.10.1Registrierung

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 Freigabeansprechpartner 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 Endnutzer informiert. Die Information des Endnutzers erfolgt in der Regel durch den Freigabe-Ansprechpartner, kann aber auch durch das FI-TS Trustcenter erfolgen. Für die erneute, korrigierte Beantragung muss der komplette Antragsprozess erneut durchlaufen werden.

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

### 8.10.2Erneuerung

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

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

### 8.10.3Rückruf eines Zertifikats

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

Für den Rückruf sind die in Kap. 8.1 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.

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

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

## 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 Microsoft-PKI, 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 Zerifizierungsrichtlinie (Policy) erforderlich oder es mußfestgelegt 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 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 Zertifiate 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 sinnvoll 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 im Sicherheitskonzept K108 – Schlüsselmanagement festgelegten Standards erfolgen.

### 8.11.3 Anforderungen an die Richtlinie

Die Richtlinie der CA muss folgende Punkte festlegen:

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

# 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** |
|---|---|---|---|
| Erstregistierung | 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 Zertifikatein großen Menghen zu sperren, müssen einvernehmliche Abschrachen 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] Wert gilt für nicht-automatisierte Signierungsprozesse

[2] Wert gilt für nicht-automatisierte Signierungsprozesse

# 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 des Rechenzentrums 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 aller Systeme und Daten in Echtzeit.

## 10.2 Betriebliche Sicherheitsmaßnahmen

### 10.2.1 Rollenkonzept des FI-TS-Trustcenter

Für den Betrieb des FI-TS-Trustcenter 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 innerhalb einer Rolle müssen von unterschiedlichen Personen ausgeführt werden. Durch diese Trennung wird bei bestimmten Aufgaben ein vier Augenprinzip gewährleistet.

### 10.2.2 Identifizierung und Authentisierung für die Rollen

Die Kommunikation zwischen FI-TS Trustcenter und Freigabeansprechpartnern 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

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

#### 10.3.2 Qualifizierungsmaßnahmen

Die Mitarbeiter des FI-TS Trustcenters und die Freigabeansprechpartner werden regelmäßig im Bereich PKI weitergebildet.

Ein Freigabeansprechpartner muss mit den Validierungsprozessen für Zertifikate innerhalb seines Unternehmens vertraut sein.

Für die Freigabeansprechpartner liegt die Verantwortung für die Weiterbildung bei den jeweiligen Kunden, zu dem der Freigabeansprechpartner 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 aufgetauscht werden.
- Anforderung von Zertifikatswiderrufen und zugehörige Informationen die zwischen Nutzer und RA aufgetauscht 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 für 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-Logdaten zugreifen.

#### 10.4.4 Sicherung der Audit Log-Daten

Die Sicherung der Audit-Log-Daten erfolgt kontinuierlich.

#### 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 Freigabeansprechpartner 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 Zertifikate für Endteilnehmer) 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 archviert 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 aufgewahrt.
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

### 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 Trustcenter 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 durch 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.

5 Neuausstellung der Endzertifikate

Die Endzertifikate 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 Endzertifikate neu erstellt wurden, müssen die CA-Zertifikate der kompromittierte Root-CA einschl. derdamit 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 Endzertifikate als Sperreintrag und sie sollten für die Restlaufzeit der Zwischenzertifikate abrufbar sein.

### 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.

### 10.6.3Möglichkeiten 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.

# 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 Vier-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 Vier-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 Nutzer kann in bestimmten Fällen und auf Anforderung durch das FI-TS Trustcenter erzeugt werden. Dabei kommt 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 FI-TS mit dem ARS-Auftragstyp Zertifikate mit seinen speziell gesicerten Feldern oder verschlüsselte Emails betrachtet..

Eine Schlüsselhinterlegung findet nicht statt, eine Widerherstellung von Schlüsseln ist nicht möglich. Nähere Details werden vertraglich festgelegt.

### 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 Zertifikatsrichtlinie des FI-TS Trustcenter

### 11.1.4 Schlüssellängen

Siehe Zertifikatsrichtlinie des FI-TS Trustcenter

### 11.1.5 Parameter für die Generierung von öffentlichen Schlüsseln und Qualitätprüfung

Siehe Zertifikatsrichtlinie des FI-TS Trustcenter

### 11.1.6 Verwendungszweck der Schlüssel

Siehe Zertifikatsrichtlinie des FI-TS Trustcenter

## 11.2 Sicherheitsmaßnahmen zum Schutz des privaten Schlüssels und kryptografische Methoden

### 11.2.1 Standards und Schutzmaßnahmen der genutzten kryptografischen Methoden

Die eingesetzte kryptografische 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 kyptographischer Hardware gehalten und darüber hinaus auf IT-Systemen nicht hinterlegt.

#### 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 dokumentiert, vertraulich und wird nicht veröffentlicht.

#### 11.2.4 Archivierung 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 gebunden Rechte, die er nach erfolgreicher Authentisierung zugewiesen bekommt.

#### 11.2.8 Löschen des privaten Schlüssels

Die privaten Schlüssel des FI-TS Trustcenters werden nicht gelöscht. 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 Zertifikatsrichtlinie des FI-TS Trustcenters

### 11.4 Maßnahmen zur Computersicherheit

#### 11.4.1 Spezifische technische Anforderungen an die Computersicherheit

- Die Entschlüsselung der privaten Schlüssel des FI-TS Trustcenters findet innerhalb spezieller kryptographischer Module statt. Kryptographische Operationen mit den privaten Schlüsseln des FI-TS Trustcenters werden ausschließlich in speziellen kryptographischen Modulen durchgeführt.
- Die Schlüssel spezieller untergeordneter CAs werden mit den Kypto-Modulen des jeweiligen Betriebssystems entschlüsselt.
- Der Zugriff auf kryptografische 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 Trustcenter laufen mit einer zur Physikalisch-Technischen Bundesanstalt synchronen Zeit.

# 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.

# 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 Zertifikatsnutzer - 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 Endteilnehmer 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 aktuellen gültigen Version behandelt.

### 13.1.1 Vertrauliche Informationen

Alle persönlichen Daten, die nicht im Zertifikat enthalten sind (Ausnahme: Zertifikatssperrung, Zeitpunkt der Sperrung), gelten als vertrauliche Informationen. Eine Ausnahme stellen die 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. Informationen, die für die Überprüfung eines Zertifikats benötigt werden, sind generell nicht vertraulich und werden veröffentlicht.

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 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 Endteilnehmer werden, falls zulässig, informiert.

#### 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 an Endteilnehmer ausgestellt wurden, sowie die privaten und öffentlichen Schlüssel der Endteilnehmer sind Eigentum der jeweiligen Endteilnehmer.

### 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 Zugrunde liegende 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.

# 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 | |

# 16 Anhang

## 16.1 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 | Als Kunde/Mandant bestehen zwei mögliche Gruppen:<br>intern: Eine OE von FI-TS, die die Berechtigung hat, das FI-TS Trustcenter zu nutzen, der Antragsweg ist über ARS festgelegt.<br>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.<br>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 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. |

## 16.2 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 |