TSE-PKI

Certificate Policy (CP) & Certification Practice Statement (CPS)

Deutsche Telekom Security GmbH

Version	06.00
Gültig ab	18.12.2025
Status	Freigegeben
Autor	Deutsche Telekom Security GmbH

Schutzklasse: öffentlich

Impressum

Herausgeber
Deutsche Telekom Security GmbH

Dateiname	Dokumentennummer	Dokumentenbezeichnung
CP_CPS_TSE-PKI.V6.0 - Draft.docx		Certificate Policy (CP) & Certification Practice Statement (CPS)

Version	Gültig ab	Status
V06.00	18.12.2025	Freigegeben

Autor	Inhaltlich geprüft von	Freigegeben von
Deutsche Telekom Security GmbH	Deutsche Telekom Security GmbH	Deutsche Telekom Security GmbH

Kurzinfo

In dem vorliegenden Dokument sind CP und CPS für die **TSE-PKI** zusammengefasst.

Es beschreibt das für den Betrieb der **TSE-PKI** erforderliche Sicherheitsniveau und beinhaltet Sicherheitsvorgaben sowie Erklärungen hinsichtlich technischer, organisatorischer und rechtlicher Aspekte.

Das Dokument orientiert sich an den dem internationalen Standard für Zertifizierungsrichtlinien RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework der Internet Society.

Änderungshistorie

Version	Stand	Autor/Bearbeiter	Kommentar
V1.0	02.10.2019	T-Systems	Freigegeben
V1.1	17.10.2019	T-Systems	Freigegeben.
V2.0	01.09.2020	Deutsche Telekom Security GmbH	OCSP wurde als optionale Leistung gekennzeichnet und das TSE-Zertifikatsprofil entsprechend angepasst. Bei Sperrlisten wurde ein Verfahren eingeführt, bei dem nicht aktivierte Zertifikate nach einer definierten Zeitspanne automatisch gesperrt werden (Abschnitt 3.2.2.3) Änderung der Zertifikatslaufzeiten von Root-CA und Sub-CA in Abschnitt 6.3.2 (Gültigkeitszeitraum von Zertifikaten und Schlüsselpaaren) und Anhang D. In Abschnitt A (Namensschema) wurde der Eintrag serial number aus den Namensschemata entfernt. Update von Abschnitt 6.7 (Validierungsmodell) Änderung des Firmennamens auf Deutsche Telekom Security GmbH Korrektur der Links von AuthorityInfoAccess in den Zertifikaten. Korrekturen bzgl. Rechtschreibung und Formatierung. Freigegeben
V2.1	28.10.2021	Deutsche Telekom Security GmbH	Internes Review Keine inhaltlichen Änderungen Überprüfung der Hyper-Links Korrekturen bezüglich Rechtschreibung und Formatierung Freigegeben
V3.0	24.10.2022	Deutsche Telekom Security	Internes Review Anpassung an TSE CA 2

Version	Stand	Autor/Bearbeiter	Kommentar
		GmbH	Korrekturen bezüglich Rechtschreibung und Formatierung Freigegeben
V3.9	17.10.2023	Deutsche Telekom Security GmbH	Empfehlungen aus dem Audit: • Erläuterung zu Sperrgrund „unspecified“ (Abschnitt 3.6) • Präzisierung zu Zertifikaten der Verwaltungs-PKI (Abschnitt 3.4) Inhaltlicher Prüfung und Korrekturen bezüglich Rechtschreibung und Formatierung
V4.0	18.10.2023	Deutsche Telekom Security GmbH	Freigegeben
V5.0	07.11.2024	Deutsche Telekom Security GmbH	Einführung von PostIdent-Verfahren als Alternative zur persönlichen Identifizierung mittels Ausweisdokument (siehe Abschnitte 3.2.2.2 und 4.2.1) Inhaltliche Prüfung Korrekturen bezüglich Rechtschreibung und Formatierung Freigegeben
V05.90	11.12.2025	Deutsche Telekom Security GmbH	Adressänderung wegen Umzug von Netphen nach Siegen Umsetzung der Empfehlungen E-01 bis E-04 aus dem Rezertifizierungsaudit vom 12.03.2025:

Version	Stand	Autor/Bearbeiter	Kommentar
			• E01 - PRC.Reg.8 Klarstellung, dass eine offline-Root-CA eingesetzt wird (Kapitel 1). • E02 - IR.Reg.11 Ergänzungen bezüglich Identifikation und Löschung von archivierten Daten (Anhang B). • E03 - PKS.Reg.4 Ergänzung bzgl. der Überprüfung der kryptographischen Eigenschaften der zu zertifizierenden Schlüssel und der Abweisung unzulässiger Schlüssel (Abschnitt 6.1.4). • E04 - SubC.Reg.1 Ergänzung von Angaben zum Sub-Unternehmer T-Systems International GmbH (Abschnitt 1.3.6). Korrekturen bezüglich Rechtschreibung, Versionsbezeichnung, Datenschutz und Formatierung
V06.00	17.12.2025	Deutsche Telekom Security GmbH	Freigegeben

Inhaltsverzeichnis

Tabellenverzeichnis

1 Einleitung

Mit der Verordnung zur Bestimmung der technischen Anforderungen an elektronische Aufzeichnungs- und Sicherungssysteme im Geschäftsverkehr (Kassensicherungsverordnung - KassenSichV) vom 26. September 2017 (BGBl. I S. 3515) werden die Anforderungen des § 146a der Abgabenordung (AO) präzisiert. Die Kassensicherungsverordnung legt u.a. fest:

- wie diese digitalen Grundaufzeichnungen zu speichern sind,
- wie die Anforderungen an eine einheitliche digitale Schnittstelle sind und
- wie die Anforderungen an die technische Sicherheitseinrichtung (TSE) sind.

Die Technische Richtlinie BSI TR-03153 „Technische Sicherheitseinrichtung für elektronische Aufzeichnungssysteme“ definiert verbindliche Vorgaben an die Technische Sicherheitseinrichtung, mit denen die digitalen Grundaufzeichnungen eines elektronischen Aufzeichnungssystems gemäß § 146a (1) der Abgabenordnung [AO] geschützt werden müssen.

Als Protokollierung wird der Prozess gemäß §2 [KassenSichV] bezeichnet, mit dem die Technische Sicherheitseinrichtung einen aufzuzeichnenden Vorgang des Aufzeichnungssystems bzw. einen Funktionsaufruf oder ein Ereignis der Technischen Sicherheitseinrichtung gegen nachträgliche, unerkannte Veränderungen schützt und die Existenz der Aufzeichnung zu einem bestimmten Zeitpunkt bestätigt.

Anwendungs- und Protokolldaten bilden in geeigneter Strukturierung den Input für die Prüfwertberechnung. Die (Anwendungsdaten,) Protokolldaten und der Prüfwert werden zusammen als abgesicherte (Anwendungs- und) Protokolldaten bezeichnet. Durch die Erzeugung der abgesicherten Protokolldaten werden die Anwendungsdaten mit den zugehörigen Protokolldaten abgesichert.

Der Hersteller der TSE MUSS Steuerpflichtigen ein Zertifikat über den zugehörigen öffentlichen Schlüssel für die Prüfwertverifikation bereitstellen. Nutzt der Hersteller der TSE externe Anbieter von Zertifikaten, welche zur Verifikation von Prüfwerten verwendet werden, MÜSSEN diese über ein Zertifikat nach [BSI-TR-03145-1] verfügen.

Die Zertifizierungsstelle MUSS durch geeignete Maßnahmen die Echtheit des TSE-(Sicherheits)-moduls und die Gültigkeit dessen CC-Zertifizierungen nach „PP-SMAERS“ [BSI-CC-PP-0107-2019] und „PP-CSP“ [BSI-CC-PP-0104-2019] / „PP-CSP-Light“ [BSI-CC-PP-0111-2019] und der BSI-TR-Zertifizierung nach „TSE“ [BSI-TR-03153] sicherstellen und diese Maßnahmen in ihrer Zertifizierungsrichtlinie (Certificate Policy) beschreiben.

Damit die Authentizität der Prüfwertverifikation gesichert ist, wird eine Public Key Infrastruktur für Technische Sicherheitseinrichtungen für elektronische Aufzeichnungssysteme (TSE-PKI) etabliert. Technisch wird der Authentizitätsnachweis der Schlüssel dabei über digitale X.509-Zertifikate aus der TSE-PKI realisiert.

Die Systemarchitektur der TSE-PKI wird in die folgenden drei Hierarchiestufen unterteilt:

- Die **Root-CA**, welche den Vertrauensanker der TSE-PKI darstellt. Sie ist daher besonders zu schützen und immer offline. Außerhalb der Zeiten ihrer Aufgabenerfüllung ist sie inaktiv.
- Die **Sub-CAs**, die zur Zertifizierung von Endnutzerschlüsseln dienen.
- Die **Endnutzer**, d.h. die TSE und Dritte. Dritte (z.B. Finanzbeamte) nutzen die TSE-Zertifikate, um die Authentizität der gesicherten Aufzeichnungen zu überprüfen.

Die in der TSE-PKI CP/CPS verwendeten Inhalte werden dem [RFC 2119] entsprechend mit folgenden deutschen Schlüsselworten beschrieben:

- **MUSS** bedeutet, dass es sich um eine normative Anforderung handelt.
- **DARF NICHT / DARF KEIN** bezeichnet den normativen Ausschluss einer Eigenschaft.
- **SOLLTE / EMPFOHLEN** beschreibt eine dringende Empfehlung. Es müssen triftige Gründe vorliegen, um die Empfehlung nicht umzusetzen, wobei die Entscheidung dazu unter Abwägung aller Auswirkungen auf den jeweiligen Betrieb getroffen werden muss.
- **SOLLTE NICHT / SOLLTE KEIN** kennzeichnet die dringende Empfehlung, eine Eigenschaft auszuschließen.
- **KANN / DARF** bedeutet, dass die Eigenschaften fakultativ oder optional sind.

Die Kapitel der TSE-PKI CP/CPS sind grundsätzlich als normativ anzusehen. Informative Kapitel werden explizit am Anfang gekennzeichnet.

Die in Kap. 1.5 genannte Organisation ist Betreiberin der TSE-PKI Root- und der Sub-CAs und erklärt, alle normativen Festlegungen des vorliegenden Dokuments zu erfüllen. Im Sinne eines CPS enthält das Dokument ggf. Erläuterungen zur Art und Weise der Erfüllung.

1.1 Überblick

Im vorliegenden Dokument sind die Certificate Policy (CP) und das Certification Practice Statement (CPS) der TSE-PKI zusammengefasst. Es wird im Weiteren auch kurz „TSE-PKI CP/CPS“ genannt. Die TSE-PKI CP/CPS beinhaltet Sicherheitsvorgaben sowie Erklärungen hinsichtlich technischer, organisatorischer und rechtlicher Aspekte.

Das Dokument richtet sich sowohl an den Betreiber der Root- und Sub-CA(s) als auch an die weiteren Teilnehmer und ist in Anlehnung an [RFC 3647] strukturiert und definiert. Nachfolgend wird die Struktur erläutert:

Nach der Einleitung (Kapitel 1) werden in Kapitel 2 zunächst die Verzeichnisdienste beschrieben. Hierunter fallen, neben der Darstellung der Verzeichnisse, Details dazu, welche Informationen durch die Root- und die Sub-CAs zu veröffentlichen sind.

In Kapitel 3 werden Regeln zur Authentifizierung der einzelnen Teilnehmer beschrieben. Hierzu gehören neben Details zur erstmaligen Identifizierung auch detaillierte Vorgaben zur Schlüsselerneuerung.

Kapitel 4 beschreibt die Betriebsanforderungen für den Zertifikatslebenszyklus (Ausgabe, Sperrung, Ablauf) sowie den Sonderfall der Außerbetriebnahme einer Sub-CA.

Kapitel 5 beschäftigt sich mit organisatorischen, betrieblichen und physikalischen Sicherheitsanforderungen für die Betriebsumgebungen der Root-CA, Sub-CA, TSE und DRITTE. Dabei wird u. a. auf Verfahrensanweisungen, Anforderungen an das Personal, Überwachungsanforderungen, die Organisation von Schlüsselwechseln, die Aufbewahrung von Schlüsseln, das Notfall-Management, die Behandlung von Sicherheitsvorfällen sowie Anforderungen an Maßnahmen bei einer Kompromittierung des Schlüsselmaterials eingegangen.

In Kapitel 6 werden technische Sicherheitsanforderungen wie die Erzeugung, die Lieferung, die Speicherung und das Management von Schlüsselpaaren definiert. Des Weiteren werden die Anforderungen an die einzusetzenden kryptografischen Module und Sicherheitsanforderungen für die Rechneranlagen spezifiziert.

Kapitel 7 beschreibt die Zertifikatsprofile für alle Teilnehmer der TSE-PKI.

In Kapitel 8 finden sich Bewertungsrichtlinien für die einzelnen Parteien, und das abschließende Kapitel 9 geht auf weitere rechtliche und finanzielle Regelungen ein.

Die Verantwortlichkeit für die TSE-PKI CP/CPS sowie den Betrieb der Root-CA obliegt dem in Kap. 1.5 genannten BETREIBER als Inhaber der Wurzelzertifikate der TSE-PKI.

1.2 Name und Identifizierung des Dokuments

Dieses Dokument ist die Certificate Policy (CP) und das Certification Practice Statement (CPS) der von Deutsche Telekom Security GmbH betriebenen TSE-PKI und kann über die folgenden Informationen identifiziert werden.

Identifikator	Wert
Titel	Certificate Policy und Certification Practice Statement TSE-PKI
Version	06.00
OID	1.3.6.1.4.1.7879.13.41

Tabelle 1: Identifikation des Dokuments

Dieses Dokument kann unter den folgenden Adressen bezogen werden:

http://docs.tse.telesec.de/cps/tse.htm

http://docs.tse.telesec.de/cps/tse.html

https://www.telesec.de/de/branchen-and-eco-systeme/fiskalisierung-kassengesetz/tse-pki

1.3 PKI-Teilnehmer

In diesem Unterkapitel werden die Teilnehmer (Zertifizierungsstellen, Registrierungsstellen, Antragsteller, Zertifikatsnehmer und Zertifikatsnutzer) der TSE-PKI aufgeführt. Die nachfolgende Tabelle zeigt einen Überblick über die PKI-Teilnehmer:

Instanz der PKI	Zertifizierungsstelle	Registrierungsstelle	Antragsteller	Zertifikatsnehmer	Zertifikatsnutzer
Root-CA	X	X		X	X
Sub-CA	X	X		X	X
TSE-Hersteller			X		
TSE				X	X
DRITTE					X

Tabelle 2: Übersicht der PKI-Teilnehmer

1.3.1 Zertifizierungsstellen

In diesem Unterkapitel werden nachfolgend die CAs der PKI beschrieben.

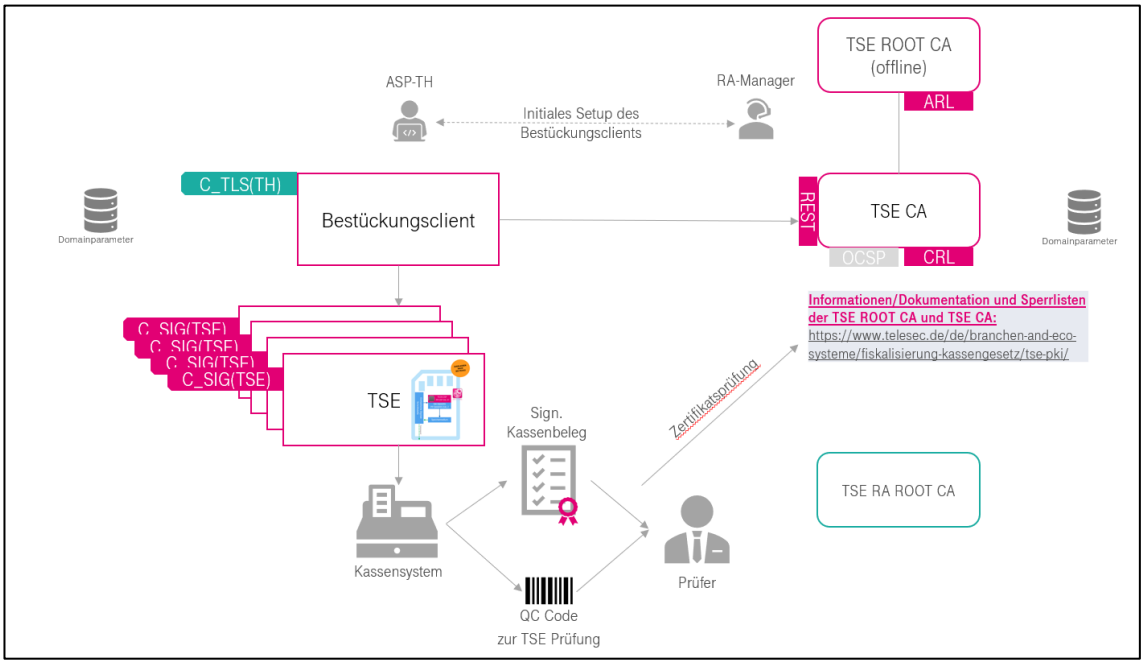

Abbildung 1: Übersicht über die TSE-PKI

1.3.1.1 Root-CA

Die Root-CA bildet den Vertrauensanker der TSE-PKI für die Berechtigung zur Ausstellung und Nutzung der Zertifikate und ist die Herausgeberin dieser TSE-PKI CP/CPS. Die Root-CA ist als Offline-CA konzipiert (siehe Abbildung 1). Sie ist immer offline, d.h. vollständig von allen Netzen getrennt und außerhalb der Zeiten, die sie für die Durchführung ihrer Aufgaben benötigt (u.a. Zertifizierung der TSE CA (Sub-CA)) inaktiv.

1.3.1.2 Sub-CA

Eine Sub-CA ist eine Instanz, welche von der Root-CA zur Ausstellung von Zertifikaten autorisiert wird und Zertifikate für die Endnutzer ausstellt.

1.3.2 Registrierungsstellen

Registrierungsstellen (Registration Authority, RA) führen vor der Ausstellung eines Zertifikats die zweifelsfreie Identifizierung des Antragstellers und die Authentifizierung der PKI-Rolle und der Identitätsdaten der ausführenden Personen für den Antragssteller durch.

Die Registrierungsstelle der TSE Root-CA bildet die TSE Root-RA. Diese ist für die Bearbeitung der initialen Registrierungen sowie der Wiederholungsanträge der Sub-CA zuständig.

Eine Sub-CA verfügt jeweils über eigene Registrierungsstellen (RA der Sub-CA). Diese sind für die initialen Registrierungen der Endnutzer zuständig.

1.3.3 Antragsteller

Bei der TSE-PKI gibt es die Besonderheit, dass die Registrierung der TSEs nicht über Einzelanträge wie bei Zertifikaten für Endnutzer erfolgt, sondern ein Mitarbeiter des

TSE-Herstellers die Rolle des „berechtigten Antragstellers“ in Form eines für den TSE-Hersteller ausgestellten C_TLS Zertifikates, erhält mit dem er über eine technische Schnittstelle an der dem C_TLS Zertifikat zugeordneten Domäne die Beantragung von C_{SIG}(TSE) durchführen muss.

1.3.4 Zertifikatsnehmer

Die nachfolgend beschriebenen PKI-Teilnehmer werden auch als Endnutzer oder Zertifikatsinhaber bezeichnet, da diese ihre Zertifikate nicht zur Ausstellung von Zertifikaten, sondern ausschließlich zur Erzeugung der abgesicherten Protokolldaten nutzen.

1.3.4.1 TSE

Bei einer TSE handelt es sich um eine technische Komponente (siehe [BSI-TR-03153]), die von einer Sub-CA mit Zertifikaten ausgestattet wird, welche für die Durchführung der definierten Prozesse benötigt werden. Ein TSE-Zertifikat ist immer genau einem Steuerpflichtigen zugeordnet.

1.3.5 Zertifikatsnutzer

Zertifikatsnutzer im Sinne dieser TSE-PKI CP/CPS sind alle natürlichen und juristischen Personen bzw. technischen Komponenten, die Zertifikate aus der TSE-PKI für die Erledigung von Geschäftsprozessen/Aufgaben verwenden.

1.3.6 Andere Teilnehmer

Teilnehmer (wie z.B. Endverbraucher oder Sub-Unternehmer), welche keine Verpflichtung im Rahmen dieser TSE-PKI CP/CPS eingegangen sind, sind nicht Bestandteil der TSE-PKI CP/CPS und werden daher nicht berücksichtigt.

Als Sub-Unternehmer der Deutsche Telekom Security GmbH für den Rechenzentrumsbetrieb inklusive der Bereitstellung der IT-Systeme fungiert die T-Systems International GmbH auf Basis einer individuellen „Vereinbarung zum Betrieb Trust Center”.

Alle darüberhinausgehenden im vorliegenden Dokument beschriebenen Services der TSE-PKI werden von der Deutsche Telekom Security GmbH betrieben.

Die Verantwortung für die durch das vorliegende Dokument festgelegten Anforderungen bezüglich der von T-Systems International GmbH bereitgestellten Services für die TSE-PKI liegt in der Verantwortung der Deutsche Telekom Security GmbH.

1.4 Verwendung von Zertifikaten

In diesem Abschnitt wird die erlaubte und verbotene Verwendung von Zertifikaten in der TSE-PKI definiert.

1.4.1 Erlaubte Verwendung von Zertifikaten

Jeder TSE-PKI-Teilnehmer benötigt für die Ausübung seiner PKI-Rolle entsprechende Zertifikate aus der TSE-PKI. Ein Teilnehmer, ausgenommen einer TSE, KANN über mehrere Zertifikate verfügen (siehe Abschnitt 4.1.1).

Das Schlüsselmaterial der TSE-PKI-Teilnehmer kann zur Erstellung von elektronischen Signaturen eingesetzt werden. Die Anwendungsfälle für den Einsatz der Schlüssel und Zertifikate einer TSE sind in der [BSI-TR-03153] beschrieben.

In den nachfolgenden Tabellen werden alle Zertifikate den unterschiedlichen PKI-Teilnehmern zugeordnet und der entsprechende Verwendungszweck erläutert. Alle weiteren Informationen können der [BSI-TR-03153] entnommen werden.

Root-CA

Zertifikat der Root-CA	Signiert durch	Verwendungszweck
C(Root)	Privater Schlüssel zu C(Root)	Vertrauensanker der TSE-PKI: Der öffentliche Schlüssel aus dem Zertifikat wird zur Überprüfung der Signatur von nachgeordneten Zertifikaten benötigt. Der zugehörige private Schlüssel wird für die Signatur von Sub-CA-, sowie von C(Root) und der ARL verwendet.

Tabelle 3: Zertifikate der Root-CA

Sub-CA

Zertifikat einer Sub-CA	Signiert durch	Verwendungszweck
C(Sub-CA)	Privater Schlüssel zu C(Root)	Der öffentliche Schlüssel aus dem Zertifikat wird zur Überprüfung der Signatur von nachgeordneten Zertifikaten benötigt, welche mit dem zum Zertifikat passenden privaten Schlüssel signiert wurden. Der zugehörige private Schlüssel wird für die Signatur von C_{SIG}(TSE)-Zertifikaten, der OCSP-Responder der Sub-CA und der CRL verwendet.
$C_{OCSP\text{-}S}$(Sub-CA)	Privater Schlüssel zu C(Sub-CA)	Mit Hilfe dieses Zertifikats kann die Signatur des optional nutzbaren OCSP-Responder (Sub-CA-OCSPR) verifiziert werden. Der zugehörige private Schlüssel wird für die Signatur der Sub-CA-OCSPR verwendet.

Tabelle 4: Zertifikate der Sub-CA

Zertifikate der Zertifikatsnehmer (außer Root-CA und Sub-CA)

Zertifikat eines Zertifikatsnehmers	Signiert durch	Verwendungszweck
C_{SIG}(TSE)	Privater Schlüssel zu C(Sub-CA)	Zertifikat zur Verifikation von Inhaltsdatensignaturen der entsprechenden TSE.

Tabelle 5: Zertifikate der Zertifikatsnehmer

Andere Zertifikate (nicht von der TSE-PKI bereitgestellt):

Für die Kommunikation der Ansprechpartner (ASP) in den unterschiedlichen Ebenen ist der Informationsaustausch mittels verschlüsselter und signierter E-Mails vorgesehen. Außerdem ist eine TLS-Kommunikation zwischen TSE-Hersteller (TH) / Bestückungsclient und Sub-CA vorgesehen, welche durch Zertifikate abgesichert werden muss. Diese Zertifikate werden nicht von der TSE-PKI bereitgestellt, die Anforderungen an diese Zertifikate sind in Tabelle 6 definiert.

Zertifikat eines Ansprechpartners	Verwendungszweck
$C_{S/MIME}$(ASP Root) $C_{S/MIME}$(ASP Sub-CA) $C_{S/MIME}$(ASP TH)	Zertifikat für den privaten Schlüssel, der vom Ansprechpartner der Root, einer Sub- CA, eines TH für die Signatur und Verschlüsselung der E- Mail-Kommunikation eingesetzt wird. Je nach Realisierung der ausstellenden CA KÖNNEN für die Signatur und die Verschlüsselung auch unterschiedliche Zertifikate eingesetzt werden. Es MUSS bei dem Zertifikat eine Zuordnung zwischen dem Ansprechpartner und den Angaben im Zertifikat möglich sein (personalisiertes bzw. persönliches Zertifikat). Der ergänzende Einsatz von Funktionspostfächern (Zugriff und Nutzung durch mehrere Anwender) ist nur zum Empfang von Mails gestattet, sofern die Kommunikation mit den identischen Mechanismen abgesichert wird (Funktionspostfach muss über ein entsprechendes Verschlüsselungszertifikat verfügen). Der Versand von allgemeinen bzw. öffentlichen Informationen kann optional auch unverschlüsselt erfolgen. Grundsätzlich kommen hier die Zertifikate zum Einsatz, welche durch den Ansprechpartner bereitgestellt werden.
$C_{SIG/TLS}$(TH)	Zertifikat für den privaten Schlüssel des Bestückungsclient des TSE-Herstellers. Das Zertifikat MUSS für die TLS-Verbindung zwischen Bestückungsclient und Sub-CA genutzt werden, sowie für die Signatur des Zertifikatsantrags.
C_{TLS}(Sub-CA)	Diese Zertifikate werden beim Aufbau des TLS-Kommunikationskanals zwischen Sub-CA und anderen Systemen eingesetzt.

Tabelle 6: Kommunikationszertifikate der Ansprechpartner

1.4.2 Verbotene Verwendung von Zertifikaten

Die Zertifikate MÜSSEN gemäß ihrem Verwendungszweck (siehe Abschnitt 1.4.1) eingesetzt werden.

1.5 Administration der TSE-PKI CP/CPS

Die für dieses Dokument verantwortliche Organisation ist die Deutsche Telekom Security GmbH. Die Deutsche Telekom Security GmbH kann über folgende Adresse kontaktiert werden:

Organisation	Deutsche Telekom Security GmbH
Abteilung	Trust Center & ID Security
Adresse	Koblenzer Straße 87-93 57072 Siegen
Fax	+49 391 580 137 801
E-Mail	tse-pki@telekom.de
Webseite	https://www.telesec.de/de/tse-pki

Tabelle 7: Kontaktadresse

1.5.1 Pflege der TSE-PKI CP/CPS

Jede aktualisierte Version der TSE-PKI CP/CPS wird den Anwendern unverzüglich über die angegebene Internetseite (siehe Tabelle 7) zur Verfügung gestellt.

Überdies wird über die Internetseite ein Changelog bereitgestellt, um Klarstellungen oder kleinere Änderungen zur TSE-PKI CP/CPS kurzfristig veröffentlichen zu können.

1.5.2 Zuständigkeit für das Dokument

Zuständig für die Erweiterung und/oder nachträgliche Änderungen dieser TSE-PKI CP/CPS ist die Deutsche Telekom Security GmbH als Betreiber der Root-CA.

1.5.3 Ansprechpartner / Kontaktperson

Siehe Tabelle 7.

1.5.4 Zuständiger für die Anerkennung eines CPS

Die TSE-PKI Root-CA kann für einzelne Sub-CAs bei Bedarf ein gesondertes CPS anerkennen.

1.5.5 CPS-Aufnahmeverfahren

Ein CPS der TSE-PKI MUSS konform zu den Sicherheitsanforderungen in dieser CP/CPS sein.

2 Verantwortlichkeit für Veröffentlichungen und Verzeichnisse

2.1 Verzeichnisse

Von der Root-CA sowie von allen Sub-CAs wird kein Verzeichnisdienst bereitgestellt.

2.2 Veröffentlichung von Informationen zur Zertifikatserstellung

2.2.1 Veröffentlichungen der Root-CA

Für die Root-CA wird eine Website eingerichtet, auf der sie folgende Informationen bereitstellen MUSS:

- Kontaktdaten der Root-CA
- Diese TSE-PKI CP/CPS
- Die aktuellen Zertifikate der Root-CA inklusive des SHA256 Hashs
- Sperrliste der Root-CA (Authority Revocation List, ARL)
- Link zu den allgemeinen Informationen des BSI zum Thema Technische Sicherheitseinrichtung (TSE) und den relevanten TRs
- Changelog zur TSE-PKI CP/CPS

2.2.2 Veröffentlichungen der Sub-CA

Für jede Sub-CA der TSE-PKI wird eine Web-Seite eingerichtet, welche mindestens die folgenden Informationen beinhalten MUSS:

- Kontaktdaten der Sub-CA
- Die aktuellen Zertifikate der Sub-CA inklusive der SHA256 Hashs.
- Sperrliste der Sub-CA (Certificate Revocation List, CRL).
- Die CP der Sub-CA; entweder das vorliegende Dokument oder eine hierzu kompatible separate CP mit folgenden Mindestanforderungen:
  - Die CP MUSS die Anforderungen und somit die Einhaltung dieser TSE-PKI Policy bestätigen.
  - Die CP MUSS die für die Bereitstellung und Verwaltung der Zertifikate notwendigen Prozesse grundsätzlich beschreiben. Diesbezüglich kann auch auf die entsprechenden Stellen in dieser TSE-PKI Policy verwiesen werden.

Die folgenden weiteren Informationen SOLLTEN bereitgestellt werden:

- Beschreibung des Antragsverfahrens von Zertifikaten unterhalb dieser Sub-CA
- Formulare zur Beantragung von Zertifikaten
- Informationen zu den zu erstellenden jeweiligen Zertifikatsrequests
- Informationen zum Sperrprozess von Zertifikaten

2.3 Zeitpunkt und Häufigkeit der Veröffentlichungen

Eine Sperrung wird nach Durchführung in der jeweiligen Root-CA / Sub-CA als solche wirksam.

Nach Ablauf der im Zertifikat eingetragenen Gültigkeit MUSS die CA für mindestens 10 weitere Jahre Auskunft über die Statusinformation des Zertifikats geben können. Siehe hierzu Kap. 7.3.

2.4 Zugriffskontrollen auf Verzeichnisse

Ein Verzeichnisdienst (z.B. LDAP-Server) wird in der TSE-PKI nicht benötigt.

3 Identifizierung und Authentifizierung

Dieses Kapitel enthält Informationen zu den Prozessen der Identifizierung und Authentifizierung, die dazu dienen, die Identität und die Berechtigung eines Antragstellers (**Sub-CA** oder **TSE)** vor dem Ausstellen eines Zertifikats feststellen zu können.

Das Profil eines Zertifikatsrequests für C_{SIG}(TSE) MUSS konform zu der Schnittstellendokumentation sein, die die Sub-CA dem TH im Rahmen von dessen Registrierung bereitstellt. Der TH MUSS diese Schnittstelle verwenden, um die von ihm gewünschten C_{SIG}(TSE) zu beantragen, zu beziehen und zu aktivieren.

3.1 Regeln für die Namensgebung

Hinsichtlich des Namensschemas MUSS der Bezeichner (CommonName (CN)) eines Zertifikats der TSE-PKI dem Profil gemäß Anhang A entsprechen.

3.1.1 Arten von Namen

Die Inhalte für die Identifikation des Zertifikatsinhabers (Subject) bzw. des Zertifikatsherausgebers (Issuer) der verschiedenen Zertifikate der TSE-PKI werden im Anhang A spezifiziert.

3.1.2 Notwendigkeit für aussagefähige Namen

Die Angaben der Zertifikatsinhaber MÜSSEN gemäß den Anforderungen aus Kapitel 3.1.1 in die Zertifikate aufgenommen werden.

3.1.3 Anonymität oder Pseudonymität von Zertifikatsnehmern

Der Zertifikatsnehmer DARF NICHT anonym sein oder Pseudonyme verwenden.

3.1.4 Eindeutigkeit von Namen

Die Angaben der Zertifikatsinhaber MÜSSEN gemäß den Anforderungen aus Kapitel 3.1.1 in die Zertifikate aufgenommen werden.

Eine Namensgleichheit (gleicher CN bei unterschiedlichem Zertifikatsnehmer) MUSS durch die CAs verhindert werden, entsprechend DARF eine CA einen CommonName NICHT mehrfach vergeben. Dies gilt neben dem CommonName auch für alle sonstigen Zertifikatsinhalte, welche dazu geeignet sind, den Zertifikatsnehmer eindeutig zu identifizieren.

Bei der Ausstellung von Zertifikaten ist ein Abgleich hinsichtlich der Eindeutigkeit von Namen zwischen den Sub-CAs nicht erforderlich.

Sollten zwei oder mehr Zertifikatsnehmer von einer CA den gleichen CN besitzen, besteht ein Konflikt, der gelöst werden MUSS. Es behält der Teilnehmer seinen CN, der zuerst sein erstes Zertifikat mit diesem CN erhalten hat. Sonstige Zertifikatsnehmer MÜSSEN sich ein neues Zertifikat mit einem anderem CN ausstellen lassen, um weiterhin an der TSE-PKI teilnehmen zu DÜRFEN.

3.2 Initiale Überprüfung zur Teilnahme an der PKI

Dieser Abschnitt enthält Informationen über die Identifizierungsprozeduren, d.h. die Prüfung der natürlichen Person als Vertreter des Unternehmens, und die Authentifizierungsprozeduren, d.h. die Prüfung der Anforderung und der Qualifikation des Unternehmens, für den initialen Zertifikatsantrag der unterschiedlichen Zertifikatsnehmer.

Bestandteil dieser Prozeduren sind auch die Prüfungen nach den Anforderungen aus Abschnitt 8.1.

Auf der **Root-Ebene** wird das Ausstellen des selbstsignierten C(Root) nicht betrachtet, da die Registrierungsstelle und der Betrieb für die Root-CA eine organisatorische Einheit bilden. Identifizierung und Authentifizierung sind auf Root-Ebene somit gegeben.

3.2.1 Methoden zur Überprüfung bzgl. Besitz des privaten Schlüssels

Falls der private Schlüssel zum Zeitpunkt der Request-Erstellung bereits technisch verwendbar ist, MUSS zum Nachweis des Besitzes des privaten Schlüssels der Zertifikatsrequest eine sogenannte innere Signatur aufweisen. Bei der Antragsprüfung MUSS diese innere Signatur durch die CA verifiziert werden, um sicherzustellen, dass der Antragsteller im Besitz des privaten Schlüssels ist.

Zusätzlich zur inneren Signatur ist eine sogenannte äußere Signatur in Form eines durch die Sub-CA festgelegten Key-Attestation-Verfahrens durchzuführen.

Falls der private Schlüssel zum Zeitpunkt der Request-Erstellung technisch noch nicht verwendbar ist, genügt es, den Besitz des privaten Schlüssels durch das Key-Attestation-Verfahren (äußere Signatur) nachzuweisen.

3.2.2 Authentifizierung von Organisationszugehörigkeiten

Die nachfolgenden Organisationen DÜRFEN innerhalb der TSE-PKI Zertifikatsanträge stellen. Hierbei wird speziell zwischen den Prozessen zur Ausgabe von Sub-CA Zertifikaten und von nachgeordneten Zertifikaten der TSE unterschieden.

3.2.2.1 Sub-CA

Alle Sub-CAs der TSE-PKI werden von der in Kap. 1.5 genannten Organisation selbst betrieben. Dies kann auch im Auftrag einer anderen Organisation geschehen, die dann im SubjectDN von C(Sub-CA) namentlich in Erscheinung tritt.

Zur initialen Autorisierung einer neuen Sub-CA MUSS das betreffende Unternehmen, welches im SubjectDN von C(Sub-CA) genannt werden soll, beim Betreiber der Root-CA authentifiziert werden. Außerdem MUSS mindestens ein bevollmächtigter Vertreter des Unternehmens beim Betreiber der Root-CA identifiziert und authentifiziert werden.

Notwendige Unterlagen und Daten für die Registrierung sind:

- Antragsschreiben zum Aufbau einer Sub-CA mit folgenden Daten bzw. beigefügten Informationen
  - Name der Firma bzw. der Institution
  - Anschrift des Unternehmens bzw. der Institution
  - Unternehmensnachweis (z.B. aktueller Auszug aus dem Handelsregister) oder Nachweis der Institution (durch ein entsprechendes Siegel der Institution)
  - Aussage zum Typ der geplanten Sub-CA (unternehmensintern oder -

übergreifend)

- Bei der Beauftragung eines Dienstleisters für den Betrieb einer Sub-CA MUSS der Betreiber eine Bestätigung des beauftragenden Unternehmens vorlegen, welches den Dienstleister zur Beantragung und zum Betrieb der Sub-CA berechtigt.
- Kontaktdaten der Ansprechpartner
- Bestätigung eines gesetzlichen Vertreters des Unternehmens bzw. der Leitung der Institution, in der der Vertreter des Betreibers berechtigt wird, den Antrag für die Sub-CA zu stellen und in der Sache dazu verbindliche Aussagen und Angaben zu machen.

– Persönliche/individuelle Zertifikate für die gesicherte E-Mail-Kommunikation der benannten Ansprechpartner ($C_{S/MIME}$(ASP Sub-CA)), ggf. inklusive der zur Verifikation erforderlichen Zertifikatskette.

– Certificate Policy der Sub-CA (siehe Abschnitt 2.2.2)

– Nachweis zum sicheren Betrieb der Sub-CA gemäß den Vorgaben zu den Anforderungen für die Teilnahme an der TSE-PKI (s. Tabelle 15).

3.2.2.2 TSE-Hersteller (TH)

Zur Aufnahme eines neuen TH in die TSE-PKI MÜSSEN das Unternehmen authentifiziert und mindestens ein bevollmächtigter Vertreter des TH bei dem Betreiber der ausgewählten Sub-CA identifiziert und authentifiziert werden.

Notwendige Unterlagen und Daten für die Registrierung sind:

– Antragsschreiben zur Ausgabe eines TH-Zertifikats mit folgenden Daten bzw. beigefügten Informationen

- Name der Firma bzw. der Institution
- Anschrift des Unternehmens bzw. der Institution
- Unternehmensnachweis (z.B. aktueller Auszug aus dem Handelsregister) oder Nachweis der Institution (durch ein entsprechendes Siegel der Institution)
- Kontaktdaten der Ansprechpartner (unter Beachtung einer Vertreterregelung)
- Bestätigung eines gesetzlichen Vertreters des Unternehmens bzw. der Leitung der Institution, in der der Vertreter des Betreibers berechtigt wird, den Antrag für den TH zu stellen und in der Sache dazu verbindliche Aussagen und Angaben zu machen.
- Informationen zu geplanten Antrags- und Zertifikatsdaten für die TSE-Signaturzertifikate (C_{SIG}(TSE)), zur Unterstützung der späteren Antragsprüfung. Die Sub-CA fordert die einzureichenden Informationen im Rahmen der TH-Registrierung an. Hierzu können bspw. zählen:
  – syntaktischer Aufbau des Chip-Typs (z.B. Response auf eine Device Attestation des TSE-Chips)
  – Öffentlicher Schlüssel des Attestation Keys je Chip-Typ
  – Geplanter Wert für SubjectDN.Organization
  – Geplanter Wert für SubjectDN.Country
  – Geplante Werte für SubjectDN.dnQualifier (TSE-SMAERS CC-Cert ID)

– Persönliche/individuelle Zertifikate für die gesicherte E-Mail-Kommunikation der benannten Ansprechpartner ($C_{S/MIME}$(ASP TH)) inklusive der zur Verifikation erforderlichen Zertifikatskette
– Der TH MUSS eine Erklärung zur Einhaltung der Sicherheitsvorgaben aus dieser TSE-PKI CP/CPS für die Teilnahme an der TSE-PKI (s. Tabelle 15) vorlegen.
– Identitätsnachweise für die bevollmächtigten Vertreter in Form eines Ausweisdokumentes oder via PostIdent-Verfahren.

Sollte ein Dienstleister für den Betrieb eines TH beauftragt werden, MUSS zusätzlich zu den genannten Unterlagen eine schriftliche Bestätigung durch den Auftraggeber mit Benennung der autorisierten Ansprechpartner vorgelegt werden.

Unabhängig von den Zertifikatsinhalten MUSS eine Sub-CA die Anträge und Zertifikate eines TH von den Anträgen und Zertifikaten sonstiger TH technisch unterscheiden können. Die Sub-CA richtet hierzu für jeden TH einen separaten Mandanten ein, dem sämtliche Anträge und Zertifikate des TH automatisch zugeordnet werden.

Der Sub-CA-Betreiber stellt dem TH eine technische Schnittstelle zur Verfügung, die er zur Beantragung von C_{SIG}(TSE) verwenden MUSS und zur Sperrung verwenden KANN. Der Sub-CA-Betreiber übergibt dem TH die technische Dokumentation dieser Schnittstelle spätestens nach erfolgreichem Abschluss der Registrierung.

Zur Nutzung dieser technischen Schnittstelle stellt der Sub-CA-Betreiber dem TH mindestens ein Zertifikat $C_{SIG/TLS}$(TH) aus, welches von einer internen Verwaltungs-PKI des Sub-CA-Betreibers signiert ist. Das Schlüsselmaterial für dieses Zertifikat wird vom Sub-CA-Betreiber generiert. Die Übergabe an den TH erfolgt im PKCS#12-Format. Außerdem wird das zugehörige PKCS#12-Passwort an den TH übergeben. Soweit keine persönliche Übergabe an den TH im Rahmen der Registrierung erfolgt, MÜSSEN KeyStore und Passwort in separaten verschlüsselten und signierten E-Mails unter Verwendung von $C_{S/MIME}$(ASP TH) für die Mail-Verschlüsselung und $C_{S/MIME}$(ASP Sub-CA) für die Mail-Signatur zugestellt werden.

3.2.2.3 TSE

Eine TSE kann selbst keine Zertifikate beantragen. Entsprechend beantragt ein berechtigter Antragsteller des TH als dritte Partei stellvertretend die Zertifikate C_{SIG}(TSE) für die TSE unter Verwendung der vom Sub-CA-Betreiber bereitgestellten technischen Schnittstelle.

Grundvoraussetzung für das Aufbringen von TSE-Zertifikaten ist, dass der TSE-Hersteller (TH) bei einer Sub-CA der TSE-PKI registriert ist (siehe Abschnitt 3.2.2.2) und dass der von ihm benannte Antragsteller über ein gültiges Zertifikat $C_{SIG/TLS}$(TH) und den zugehörigen privaten Schlüssel verfügt. Dabei MÜSSEN die Anforderungen aus Tabelle 15 eingehalten werden.

Der TH ist für die Einhaltung der Rahmenbedingungen verantwortlich und MUSS den Prozess gemäß den Vorgaben nachvollziehbar dokumentieren.

Der TH MUSS das Sicherheitsmodul in der TSE so ansteuern, dass darin ein Schlüsselpaar für das Zertifikat generiert wird. Für den Private Key des Schlüsselpaars MUSS anschließend entweder eine elektronische Signatur als Proof of Possession erzeugt werden, oder es muss das von der Sub-CA geforderte Key Attestation Verfahren durchlaufen werden. In allen Fällen MUSS die eingesetzte Nonce von der Sub-CA generiert und über die bereitgestellte Schnittstelle von ihr bezogen werden.

Gemäß der bereitgestellten Schnittstellendokumentation erzeugt der TH aus dem Schlüsselpaar, der Attestation Response, den TSE-Gerätekennungen und den eigenen

Identifikationsdaten einen Zertifikatsrequest. Der Antragsteller signiert diesen Request mit dem privaten Schlüssel von $C_{SIG/TLS}$(TH) als Autorisierungssignatur.

Der Zertifikatsrequest wird über einen gesicherten Kommunikationskanal an die Sub-CA gesendet. Hierbei muss der Antragsteller sein Zertifikat $C_{SIG/TLS}$(TH) als TLS-Client-Zertifikat verwenden; die Sub-CA muss C_{TLS}(Sub-CA) zur TLS-Serverauthentifizierung verwenden. Die Sub-CA MUSS das beim TLS-Handshake übermittelte TLS-Client-Zertifikat $C_{SIG/TLS}$(TH) zur Authentifizierung und Organisationszuordnung des berechtigten Antragstellers heranziehen und den gestellten Zertifikatsrequest dem jeweiligen TH zuordnen.

Die Sub-CA MUSS die äußere Signatur des Zertifikatsrequests prüfen und sicherstellen, dass sie mit demselben Schlüssel erzeugt wurde, der für die TLS-Client-Authentifizierung verwendet wurde. Die Sub-CA MUSS Gültigkeit und Sperrstatus des verwendeten $C_{SIG/TLS}$(TH) überprüfen.

Die Sub-CA MUSS den Zertifikatsantrag hinsichtlich ordnungsgemäßer Struktur und korrektem Inhalt überprüfen (siehe auch Kap. 3.2.4).

Die von der Sub-CA produzierten Zertifikate werden von dem TH geprüft und in die TSE eingebracht.

Die Zertifikate C_{SIG}(TSE) bleiben zunächst inaktiv, bis der TH gegenüber der Sub-CA deren erfolgreiche Installation im TSE gemeldet hat. Ein OCSP-Responder ist eine optionale Leistung der Sub-CA. Er MUSS – falls genutzt - für inaktive Zertifikate die Response „unknown“ liefern.

Bei technischen Fehlern im Ablauf des TSE-Personalisierungsprozesses KANN der TH den Prozess wiederholen, wenn noch kein Zertifikat für die TSE aktiviert wurde. Die Sub-CA DARF NICHT ein zweites Zertifikat für dasselbe TSE-Device aktivieren. Im Falle einer Wiederholung des Prozesses MUSS die Sub-CA das inaktive C_{SIG}(TSE) aus ihrem Datenbestand löschen, bevor ein neues Zertifikat für das TSE-Device ausgestellt wird.

Sobald der TH die erfolgreiche Installation des Zertifikats an die Sub-CA gemeldet hat, MUSS die Sub-CA das Zertifikat aktivieren, so dass der OCSP-Responder der Sub-CA – falls genutzt - die Response „good“ für das Zertifikat zurückliefern kann.

Wird ein ausgestelltes Zertifikat nicht innerhalb einer definierten Frist als aktiviert gemeldet, so wird es automatisch gesperrt und in die Sperrliste aufgenommen. Eine spätere Aktivierung ist damit nicht mehr möglich.

Aktivierte Zertifikate DÜRFEN NICHT von der CA gelöscht werden, wenn deren validNotAfter-Datum weniger als 10 Jahre in der Vergangenheit liegt.

3.2.3 Anforderungen zur Identifizierung und Authentifizierung des Zertifikats- Antragstellers

Ein Zertifikatsrequest DARF NICHT von einer Einzelperson (natürliche Person), sondern MUSS von einer Organisation (juristische Person) gestellt werden. Dies gilt insbesondere auch für die Zertifikatsrequests der TSE, die durch den TH zu übermitteln sind.

3.2.4 Ungeprüfte Angaben zum Zertifikatsnehmer

Die Registrierungsstelle MUSS die Angaben zum Zertifikatsnehmer in Zertifikatsrequests für C_{SIG}(TSE) gegen die eingereichten Unterlagen auf Korrektheit prüfen (siehe auch Abschnitt 3.2.2). Dies umfasst folgende Mindestanforderungen:

- Abgleich aller beantragten SubjectDN-Werte mit den bei der Registrierung des TH vereinbarten Werten, Wertebereichen und Bildungsregeln
- Prüfung des beantragten CN hinsichtlich korrekter Herleitung aus dem Public Key
- Prüfung der Authentizität des beantragten Schlüssels (Proof of Possession oder Key Attestation)
- Algorithmus und (bei ECC) Domainparameter des beantragten Schlüssels
- Prüfung der Schlüsselqualität (z.B., ob der Punkt auf der Kurve liegt)
- Prüfung der Eindeutigkeit des beantragten Schlüssels (keine Mehrfachzertifizierung)
- Prüfung der Eindeutigkeit von TSE-Gerätekennungen (keine Mehrfachzertifizierung)

Die detaillierten Prüfschritte werden in der Schnittstellendokumentation genannt, die die Sub-CA dem TH bereitstellt.

3.2.5 Prüfung der Berechtigung zur Antragstellung

Eine Validierung erfolgt gemäß der vertraglichen Beziehung zum Antragsteller.

3.2.6 Kriterien für den Einsatz interoperierender Systeme/Einheiten

Aktuell sind keine Kriterien definiert.

3.2.7 Aktualisierung / Anpassung der Zertifizierungsinformationen der Teilnehmer

Die für die Teilnehmer an der TSE-PKI geforderten Zertifizierungen (siehe Tabelle 8) können einem Überwachungszyklus unterliegen, für den z.B. ein Audit positiv abgeschlossen werden muss.

Die zertifikatsausgebende Stelle (Root- bzw. Sub-CA) muss von dem Zertifikatsnehmer rechtzeitig vor Ablauf der eingereichten Zertifikatsunterlagen über die Ergebnisse der Auditierung informiert werden und - soweit ausgestellt - auch das entsprechende Zertifikat zur Verfügung gestellt bekommen.

Sollte der Teilnehmer die Zertifizierung nicht mehr erhalten, so MUSS das Zertifikat / die Zertifikate aus der TSE-PKI gesperrt werden.

Informationen über relevante Änderungen, die beispielsweise

– eine Re-Zertifizierung (z.B. Wechsel des IT-Betriebs-Standorts)

erfordern, MUSS der Zertifikatsnehmer unverzüglich inklusive der entsprechenden Informationen zur Verfügung stellen. Dies gilt insbesondere für die Ergebnisse der Zertifizierung der Root- bzw. der Sub-CA.

Die CAs MÜSSEN entsprechend die Registrierungsdaten zu dem jeweiligen Teilnehmer aktualisieren.

3.2.8 Aktualisierung / Anpassung der Registrierungsinformationen der Teilnehmer

Jeder Teilnehmer an der TSE-PKI MUSS dem Betreiber der Root-CA bzw. dem Betreiber der entsprechenden Sub-CA unverzüglich mitteilen, falls sich Änderungen bzgl. seiner Registrierungsdaten ergeben (vgl. Abschnitt 4.7). Ergänzend SOLLTE der Betreiber der Root-CA sowie jeder Betreiber einer Sub-CA regelmäßig (z.B. jährliches Intervall) über die Ansprechpartner bei den Klienten anfragen, ob Änderungen an den Registrierungsdaten vorliegen.

3.3 Identifizierung und Authentifizierung von Anträgen auf Schlüsselerneuerung

3.3.1 Schlüsselerneuerung bei CA- und OCSP-Responder-Zertifikaten

Der Betreiber MUSS alle CA- und OCSP-Responder-Zertifikate der von ihm betriebenen Infrastrukturen fortlaufend überwachen und die Schlüsselerneuerung rechtzeitig veranlassen, um einen unterbrechungsfreien Betrieb zu gewährleisten. Die Verpflichtungen zur Veröffentlichung von Zertifikaten gemäß Kap. 2 sind hierbei zu beachten. Schlüsselerzeugung und Zertifikatsausstellung MÜSSEN jeweils im Vier-Augen-Prinzip erfolgen.

3.3.1.1 Schlüsselerneuerung von C(Root)

Die Schlüsselerneuerung von C(Root) erfolgt ohne formale Beantragung auf interne Veranlassung des Betreibers, weil hier Zertifikatsnehmer und Zertifikatsaussteller identisch sind.

3.3.1.2 Schlüsselerneuerung von C(Sub-CA)

Die Schlüsselerneuerung von C(Sub-CA) muss bei der Registration Authority der Root-CA („Root-RA“) beantragt werden. Die Ausstellung neuer Sub-CA-Zertifikate erfolgt ausschließlich im Auftrag der Root-RA. Die Beantragung erfolgt innerhalb der Organisation des Betreibers durch die Organisationseinheit, die für den Sub-CA-Betrieb verantwortlich ist.

Zur Antragstellung wird zunächst im HSM der Sub-CA ein neues Schlüsselpaar generiert. Die Sub-CA erzeugt einen PKCS#10-Request, der den Public Key des neuen Schlüsselpaars enthält und mit dem Private Key des neuen Schlüsselpaars signiert ist. Der PKCS#10-Request wird zusammen mit dem SubjectDN des bisherigen C(Sub-CA) an die Root-RA übergeben.

Wird die betreffende Sub-CA für eine andere Organisation betrieben, so muss die Root-RA aktuelle Unterlagen vom registrierten Ansprechpartner der auftraggebenden Organisation anfordern, um den Erneuerungsantrag prüfen zu können. Der Fortbestand des Vertrags mit der auftraggebenden Organisation und die Korrektheit des für C(Sub-CA) vorgesehenen SubjectDN sind zu verifizieren.

Der SubjectDN des neuen C(Sub-CA) wird von der Root-RA festgelegt. Hierzu wird der SubjectDN des bisherigen C(Sub-CA) wiederverwendet und die darin enthaltene SerialNumber um 1 erhöht. Für sonstige Änderungen am SubjectDN muss der Zertifikatsnehmer ein neues C(Sub-CA) beantragen.

Im Falle einer Genehmigung des Antrags wird der Antrag in der Root-CA weiterverarbeitet; hierbei erfolgt zunächst eine Prüfung der PKCS#10-Signatur. Das Zertifikat wird mit dem Schlüssel aus dem PKCS#10-Request und mit dem von der Root-RA festgelegten SubjectDN ausgestellt. Anschließend wird es organisationsintern an die Sub-CA übergeben. Dort wird das Zertifikat auf Korrektheit geprüft, importiert und mit dem privaten Schlüssel des PKCS#10-Requests zusammengeführt.

3.3.1.3 Schlüsselerneuerung von $C_{OCSP\text{-}S}$(Sub-CA)

Die Schlüsselerneuerung von $C_{OCSP\text{-}S}$(Sub-CA) erfolgt durch den CA-Betrieb der Sub-CA ohne formale Beantragung, weil Zertifikatsnehmer und Zertifikatsaussteller zur selben Organisationseinheit gehören.

3.3.1.4 Übergangsfristen Zertifikatswechsel

Zur technischen Abwicklung der Schlüsselerneuerung und Konfiguration der neu ausgestellten Zertifikate im CA-Betrieb gibt einen kurzen Zeitraum, in dem sowohl das „alte“ Zertifikat und das „neue“ Zertifikat parallel im CA-System konfiguriert sind, das „alte“ Zertifikat aber vorerst noch aktiv weiter betrieben wird. In Absprache mit den CA-Benutzern wird erst nach einer kurzen Übergangsfrist das „neue“ Zertifikat in Betrieb und das „alte“ Zertifikat außer Betrieb genommen. Der unterbrechungsfreie Betrieb muss aber jederzeit gewährleistet werden können. Dieses kann einer sofortigen Inbetriebnahme des neuen Zertifikats erfordern. Ab diesen Zeitpunkt ist es nicht mehr möglich Zertifikate/Signaturen vom „alten“ Zertifikat auszustellen. Die Übergangsfrist sollte möglichst kurzgehalten werden (maximal 3 Arbeitstagen). Ein aktiver Parallelbetrieb von beide Zertifikaten findet nicht statt.

3.3.2 Schlüsselerneuerung von C_{SIG}(TSE)

Nach der Aktivierung eines C_{SIG}(TSE) gemäß Kap. 3.2.2.3 sind keine Folgeanträge für das jeweilige TSE-Device zulässig. Nach Ablauf oder Sperrung von C_{SIG}(TSE) darf dieses vom TSE-Device nicht mehr weiter betrieben werden.

3.4 Überwachung der Zertifikate der Verwaltungs-PKI $C_{SIG/TLS}$(TH)

Der TSE-Hersteller stellt in der TSE-PKI eine Sonderrolle dar. Er muss zwar für die Prozesse in der TSE-PKI identifiziert werden (als berechtigter Antragsteller), jedoch erhält der TSE-Hersteller kein Zertifikat aus der TSE-PKI.

Die Registration Authority der Sub-CA hat jedoch dafür Sorge zu tragen, dass die von der internen Verwaltungs-PKI ausgestellten Zertifikate $C_{SIG/TLS}$(TH) fortlaufend

überwacht werden. Während der Vertragslaufzeit mit dem TSE-Hersteller veranlasst sie bei Bedarf rechtzeitig eine Neuausstellung dieser Zertifikate mit unverändertem SubjectDN. Diese werden dann wie in Kap. 3.2.2.2 dargestellt an die TSE-Hersteller übermittelt.

3.5 Identifizierung und Authentifizierung von Anträgen auf Schlüsselerneuerung (Nicht routinemäßiger Folgeantrag)

Eine Unterscheidung zwischen routinemäßigen und nicht-routinemäßigen Anträgen auf Schlüsselerneuerung ist in der TSE-PKI nicht vorgesehen.

3.6 Identifizierung und Authentifizierung von Anträgen auf Sperrung

Die Sperrung eines Zertifikats kann allgemein von den folgenden Beteiligten initiiert werden:

- Vom Zertifikatsnehmer selbst.
- Von der CA, die das jeweilige Zertifikat ausgestellt hat.
- Im Falle von C_{SIG}(TSE) kann die Sperrung nicht von der TSE als Zertifikatsnehmer, sondern stattdessen stellvertretend vom TH veranlasst werden. Der TH hat dazu folgende Möglichkeiten:
  - Sperrung über einen „Sperrservice ohne Sperrpasswort“

    Im Falle von C_{SIG}(TSE) kann die Sperrung durch den TH in der Rolle eines Sperrberechtigten beauftragt werden. Der TH bekommt von der Registration Authority der Sub-CA die Berechtigung zur Nutzung des „Sperrservice ohne Sperrpasswort“.

    Der Sub-CA-Betreiber stellt dem TH als Sperrberechtigten eine technische Schnittstelle zur Verfügung, die er zur Sperrung von C_{SIG}(TSE) ohne Angabe des Sperrkennworts verwenden KANN. Der Sub-CA-Betreiber übergibt dem Sperrberechtigten die technische Dokumentation dieser Schnittstelle spätestens nach erfolgreichem Abschluss der Registrierung.
  - Sperrung über einen „Sperrservice mit Sperrpasswort“

    Im Falle von C_{SIG}(TSE) kann die Sperrung auch durch Dritte über einen Sperr-Operator beauftragt werden. Der TH bekommt von der Registration Authority der Sub-CA die Berechtigung als Sperr-Operator zur Nutzung des „Sperrservice mit Sperrpasswort“.

    Der Sub-CA-Betreiber stellt dem TH als Sperr-Operator eine technische Schnittstelle zur Verfügung, die er zur Sperrung von C_{SIG}(TSE) unter Angabe des Sperrkennworts verwenden KANN. Der Sub-CA-Betreiber übergibt dem Sperr-Operator die technische Dokumentation dieser Schnittstelle spätestens nach erfolgreichem Abschluss der Registrierung.

    Das Sperrpasswort wird von der Sub-CA bei jeder Zertifikatsausstellung individuell generiert und zusammen mit dem ausgestellten Zertifikat an den TH übergeben. Durch Herausgabe des Sperrpassworts kann der TH seinerseits Dritte zur Initiierung einer Sperrung ermächtigen.

– Sperrung über den Sperrservice der Sub-CA

  Bei einer Sperrung von C_{SIG}(TSE) durch den TH über die Sub-CA MUSS eine mit $C_{S/MIME}$(ASP TH) signierte E-Mail oder ein vergleichbar abgesicherter Kommunikationskanal zur Übermittlung des Sperrauftrags verwendet werden. In diesem Fall darf die Sub-CA das Sperrpasswort für C_{SIG}(TSE) nicht verlangen.

Die Sub-CA MUSS vollständige und korrekte Sperraufträge für C_{SIG}(TSE) über die oben genannten Sperrservices entgegennehmen und ausführen.

Falls eine Sperrmöglichkeit durch Dritte vom TH nicht gewünscht ist, MUSS er dies der Sub-CA in einer signierten E-Mail schriftlich mitteilen und MUSS die von der CA generierten Sperrpassworte nach Erhalt verwerfen. Die Sub-CA darf in diesem Fall keine mit Passwort legitimierten Sperraufträge für C_{SIG}(TSE) dieses TSE-Herstellers entgegennehmen.

Bei einer Sperrung von C(Sub-CA) durch den Betreiber der Sub-CA MUSS eine mit $C_{S/MIME}$ (ASP Sub-CA) signierte E-Mail oder ein vergleichbar abgesicherter Kommunikationskanal zur Übermittlung des Sperrauftrags an den Betreiber der Root-CA verwendet werden.

Ein vollständiger Sperrauftrag MUSS folgende Informationen enthalten:

– Organisation, Name, Anschrift und E-Mail-Adresse des Absenders
– Zertifikatstyp
– Ausstellende Sub-CA bzw. Root-CA („IssuerDN“ des Zertifikats, siehe [RFC 5280])
– Zertifikats-Seriennummer („SerialNumber“ des Zertifikats, siehe [RFC 5280]; *nicht* SubjectDN.SN)
– Sperrgrund

  Folgende Sperrgründe sind möglich:

  – nicht spezifiziert
  – Schlüssel kompromittiert
  – CA kompromittiert
  – Angaben im Zertifikat nicht mehr aktuell
  – Zertifikat wird nicht mehr benötigt
  – Geschäftsaufgabe
  – Vorläufig gesperrt
  – Rechte wurden entzogen
  – Root Zertifikat kompromittiert

Ist dem Sperrenden der genaue Zeitpunkt für den Eintritt des Sperrgrundes bekannt, so KANN dieser bei der Sperrung angegebenen werden, ansonsten erfolgt der Eintrag in die Sperrliste ohne diesen Parameter.

Neben dem Sperrgrund MUSS als Erläuterung eine Beschreibung angegeben werden, die den Sperrgrund klar spezifiziert. Dies gilt auch für den Sperrgrund „nicht spezifiziert“.

Sperrlisten oder – sofern genutzt - OCSP MUSS von allen Teilnehmern zur Abfrage der Gültigkeit eines Zertifikats verwendet werden.

3.6.1 Initiative des Zertifikatsinhabers

Der Zertifikatsinhaber stellt im Rahmen des Betriebs einen Grund zur Sperrung des Zertifikats fest. Diese Gründe sind insbesondere

- eine Änderung der Zertifikatsdaten,
- eine Schlüsselkompromittierung oder
- die Einstellung des Betriebs.

Der Zertifikatsinhaber nutzt einen der in Kapitel 3.6 genannten Sperrservices und sperrt das Zertifikat.

Die Sperrung des jeweiligen Zertifikats MUSS über die CRL der zuständigen CA und – sofern genutzt - OCSP veröffentlicht werden und der Zertifikatsinhaber MUSS über den abgeschlossenen Sperrprozess im Rahmen des jeweiligen Sperrservices informiert werden.

Der Betreiber der Sub-CA KANN zusätzliche Verfahren zur Initiierung einer Sperrung anbieten. Diese MÜSSEN über eine authentisierte und integre Kommunikationsschnittstelle verfügen. Das Sicherheitsniveau muss mit dem der in Kap. 3.2.2.3 genannten Schnittstelle vergleichbar sein. Diese optionalen Verfahren MÜSSEN in dieser Certificate Policy aufgenommen werden.

3.6.1.1 Verantwortlichkeit für die Sperrung einer TSE

Für die Sperrung einer TSE und für die zusätzliche Erteilung von TSE-Sperrberechtigungen an Dritte ist der TH verantwortlich. Sofern Sperrpasswörter genutzt werden, hat der TH dafür Sorge zu tragen, das Sperrpasswort in geeigneter Form an die Parteien weitergegeben werden, die eine legitime Sperrberechtigung haben. Der TH MUSS die sperrberechtigte Partei über die sichere Handhabung und Speicherung der Sperrpasswörter informieren. Der TH MUSS zur Weitergabe der Sperrpasswörter geeignete Maßnahmen wie z.B. einen abgesicherten und integren Kommunikationskanal über eine verschlüsselte und signierte E-Mail verwenden.

3.6.2 Initiative des Betreibers der Certificate Authority

Der Betreiber der CA hat die Aufgabe, bei erkannten Schwachstellen alle Tätigkeiten durchzuführen, welche die Integrität und Sicherheit der PKI sicherstellen. Die Schwachstellen sind direkt nach Bekanntwerden der Root zu melden. Die Einleitung weiterer Schritte ist ggf. in Absprache mit der Root vorzunehmen. Mögliche Gründe sind beispielsweise

- ein erkannter Verstoß gegen Betriebsauflagen (insbesondere gegen die Anforderungen für die Teilnahme an der TSE-PKI (s. Tabelle 15),
- erkannte (erhebliche) Schwächen der eingesetzten Kryptografie oder Kryptoimplementierung,
- Änderungen in den zentralen Vorgaben (z.B. der [BSI-TR-03153]),
- Änderung der Zertifikatsdaten (z.B. des common name),
- eine erkannte Schlüsselkompromittierung oder
- die Einstellung des Betriebs bzw. die Außerbetriebnahme der betroffenen Komponente.

Sperrungen von Zertifikaten mit systemrelevanter Bedeutung (Sub-CA) MÜSSEN in Abstimmung mit der Root erfolgen.

Die Zertifikate einer TSE können in der eigenen Verantwortung durch den Betreiber der Sub-CA gesperrt werden. Sollten nach Ansicht des Betreibers der Sub-CA Sperrungen dieser Zertifikate systemrelevante Auswirkungen haben, so MUSS die Sub-CA die Root vorab informieren.

Zertifikate einer TSE, die in einem definierten Zeitraum nicht aktiviert wurden, werden automatisch gesperrt.

Eine Sperrung des jeweiligen Zertifikats MUSS über die Sperrliste und – sofern genutzt - den OCSP-Dienst der CA veröffentlicht werden. Der Zertifikatsinhaber sowie die Root (nur bei Sub-CA und TH) MÜSSEN über den abgeschlossenen Sperrprozess informiert werden.

Die Sperrliste (CRL) enthält ausschließlich die gesperrten TSE-Zertifikate. Die Sperrliste wird zum Schutz gegen Veränderungen mit dem CA-Zertifikat der TSE-PKI signiert, mit dem auch die TSE-Zertifikate ausgestellt werden. Entsprechend handelt es sich um eine sogenannte direkte Sperrliste.

3.7 Identifizierung und Authentifizierung von Anträgen auf Suspendierung

Die Suspendierung von Zertifikaten wird nicht unterstützt.

4 Betriebsanforderungen für den Zertifikatslebenszyklus

In diesem Kapitel werden die Prozeduren und Verantwortlichkeiten für den Lebenszyklus von Zertifikaten definiert. Dies umfasst insbesondere folgende Bereiche:

- Zertifikatsbeantragung,
- Verarbeitung von Zertifikatsanträgen und
- Zertifikatsausstellung.

Innerhalb der Prozesse des Zertifikatslebenszyklus MUSS die relevante personenbezogene Kommunikation verschlüsselt und signiert erfolgen, wofür individuelle/personenbezogene Zertifikate eingesetzt werden MÜSSEN. Für alle beteiligten Personen wird der Besitz von individuellen/persönlichen $C_{S/MIME}$(ASP)-Zertifikaten vorausgesetzt.

4.1 Zertifikatsantrag

In den folgenden Unterkapiteln wird definiert, wer ein Zertifikat in der TSE-PKI beantragen darf und welche Stelle für die Bearbeitung des Zertifikatsantrags verantwortlich ist.

4.1.1 Wer kann einen Zertifikatsantrag stellen?

Ein Zertifikatsrequest darf ausschließlich von einer Organisation gestellt werden. Befugte Organisationen sind TH oder der Sub-CA-Betreiber, die sich gemäß Abschnitt 3.2 identifiziert haben MÜSSEN.

Betreibt ein TH mehrere Instanzen des Clients für die Sub-CA-Schnittstelle, so KANN er sich entsprechend mehrere Zertifikate $C_{SIG/TLS}$(TH) von der Sub-CA ausstellen lassen, um jeden Client mit einem eigenen Zertifikat auszustatten.

Der Zertifikatsrequest für C_{SIG}(TSE) MUSS als Initialantrag (siehe Abschnitt 3.3) unter Nutzung der vorhandenen Zertifikate $C_{SIG/TLS}$(TH) und C_{TLS}(Sub-CA) bei der Sub-CA gestellt werden.

Die Zertifikate MÜSSEN eindeutig gekennzeichnet werden (siehe Anhang A).

4.1.2 Beantragungsprozess und Zuständigkeiten

Für die Bearbeitung eines Zertifikatsantrags ist die Registration Authority (RA) der jeweiligen CA verantwortlich.

4.2 Verarbeitung von initialen Zertifikatsanträgen

4.2.1 Durchführung der Identifizierung und Authentifizierung

Der Zertifikatsnehmer übergibt durch seinen benannten Ansprechpartner, je nach Definition im Abschnitt 3.2, die Unterlagen und Nachweise für die initiale Zertifikatsbeantragung an die RA einer CA.

Die RA-Mitarbeiter dieser CA prüfen die eingereichten Dokumente / Nachweise. Sollten die Unterlagen / Nachweise nicht vollständig oder fehlerhaft sein, informieren diese den ASP des Zertifikatsnehmers und fordern ihn zur Nachlieferung auf.

Sollte einer der benannten und identifizierten Mitarbeiter ausscheiden, MUSS sich mindestens ein neuer Vertreter im Rahmen eines persönlichen Termins oder via PostIdent-Verfahren (vergleichbar dem im Abschnitt 3.2 beschriebenen Prozess) bei der CA identifizieren lassen. Die Benennung des neuen Vertreters bzw. der neuen Vertreter sowie die Information über das Ausscheiden des bisherigen Vertreters MUSS von einem der benannten Ansprechpartner des Teilnehmers bestätigt werden.

Für die TSEs werden keine direkten Ansprechpartner benannt, da diese Aufgaben von den THs übernommen werden.

Bei allen Prozessen zur Beantragung, Ausgabe und Verwaltung der Zertifikate MUSS bei der TSE-PKI hinsichtlich der eingesetzten Kryptografie immer die aktuelle Version der [BSI-TR-03116-5] bei der Nutzung der Sub-CA Schnittstelle berücksichtigt werden. Zur Absicherung der Kommunikation via E-Mail S/MIME und TLS SOLLTEN die Vorgaben aus [BSI-TR-03116-4] berücksichtigt werden.

4.2.2 Annahme oder Ablehnung von initialen Zertifikatsanträgen bzw. TH-Registrierungen

Die vorliegenden bzw. nachgelieferten Unterlagen / Nachweise werden von den RA-Mitarbeitern gegen die Vorgaben aus der TSE-PKI CP/CPS der jeweiligen Certification Authority geprüft.

4.2.2.1 Annahme oder Ablehnung von Initialanträgen für C(Sub-CA)

Durch die RA MÜSSEN im Rahmen der Prüfung auch der vorliegende Zertifikatsrequest für das initiale C(Sub-CA) formal überprüft werden. Außerdem ist die Übereinstimmung des gedruckten Hashwerts in den Unterlagen mit denen der Zertifikatsrequests zu überprüfen.

Im Positivfall wird der Zertifikatsantrag formell freigegeben und der benannte Ansprechpartner per signierter E-Mail darüber informiert.

Im Negativfall MUSS der Zertifikatsantrag formell abgelehnt und der benannte Ansprechpartner per signierter E-Mail über die Ablehnung (incl. entsprechender Begründung) informiert werden. Der Beantragungsprozess ist mit diesem Schritt beendet und MUSS durch den Zertifikatsnehmer ggf. neu initiiert werden.

4.2.2.2 Annahme oder Ablehnung der Registrierung des TH

Im Positivfall erhält der benannte Ansprechpartner des TH per signierter E-Mail die Benachrichtigung, dass seine Registrierung abgeschlossen ist. In einer verschlüsselten Mail werden ihm seine Zugangszertifikate für die technische Schnittstelle der Sub-CA $C_{SIG/TLS}$(TH) zugestellt. In einer weiteren verschlüsselten Mail werden ihm die PKCS#12-Passworte für diese Zertifikate zugestellt.

Im Negativfall MUSS die Registrierung formell abgelehnt und der benannte Ansprechpartner des TH per signierter E-Mail über die Ablehnung (incl. entsprechender Begründung) informiert werden. Der Registrierungsprozess ist mit diesem Schritt beendet und MUSS durch den TH ggf. neu initiiert werden.

4.2.3 Fristen für die Bearbeitung von Zertifikatsanträgen

Die Ausstellung von Zertifikaten soll so schnell wie möglich durchgeführt werden.

4.2.4 Ausgabe von Zertifikaten

Bei TSE-Zertifikaten C_{SIG}(TSE) MUSS die Ausgabe über die technische Service-Schnittstelle der Sub-CA erfolgen. Über die Genehmigung der Anträge für C_{SIG}(TSE) wird automatisiert entschieden und das Zertifikat wird im Positivfall synchron zurückgeliefert.

Zugangszertifikate $C_{SIG/TLS}$(TH) für die technische Schnittstelle der Sub-CA werden jeweils per verschlüsselter und signierter E-Mail ausschließlich an den bekannten Ansprechpartner des TH versendet. Dasselbe gilt für den Versand der zugehörigen PKCS#12-Passworte.

Genehmigte Sub-CA-Zertifikate werden von der Root-CA per signierter E-Mail an den benannten Ansprechpartner der Sub-CA versendet. Der Versand KANN unverschlüsselt erfolgen.

4.2.5 Benachrichtigung des Zertifikatsnehmers über die Ausgabe des Zertifikats

Der Ansprechpartner SOLLTE nach der Ausstellung eines initialen Zertifikats per E-Mail informiert werden. Dies gilt nicht für C_{SIG}(TSE), da diese Zertifikate unter aktiver Beteiligung des Antragstellers über die technische Schnittstelle der Sub-CA ausgegeben werden.

4.3 Annahme von Zertifikaten

Bei den Endnutzer-Zertifikaten MUSS der Ansprechpartner des Zertifikatsnehmers nach Erhalt die Angaben im Zertifikat auf Korrektheit und Vollständigkeit prüfen. Um ein Zertifikat zurückzuweisen, MUSS der Ansprechpartner des Zertifikatsnehmers eine Nachricht an die CA schicken. In einer solchen Nachricht ist der Grund für die Verweigerung der Annahme anzugeben. Bei fehlerhaften Zertifikaten sind, soweit möglich, die fehlerhaften bzw. unvollständigen Einträge zu benennen.

Bei einer TSE kann diese Prüfung durch den TH automatisiert z.B. bei dem Erhalt oder der Einbringung der Zertifikate erfolgen.

Der Sub-CA Betreiber MUSS eine Kommunikationsschnittstelle für Fehlermeldungen bereitstellen. Die entsprechende Kommunikationsschnittstelle MUSS von der Sub-CA in der Sub-CA Policy definiert werden. Bei der Root-CA wird die Kontaktadresse auf der Web-Seite der Root-CA angegeben.

4.3.1 Veröffentlichung von Zertifikaten durch die CA

Eine Veröffentlichung von Zertifikaten in einem Verzeichnisdienst der jeweiligen CA ist nicht vorgesehen.

Root- und Sub-CA-Zertifikate und deren Hash-Werte werden auf der Website des CA-Betreibers veröffentlicht.

4.4 Verwendung von Schlüsselpaar und Zertifikat

4.4.1 Verwendung des privaten Schlüssels und des Zertifikats durch den Zertifikatsnehmer

C_{SIG}(TSE)-Zertifikate und die zugehörigen privaten Schlüssel MÜSSEN gemäß ihrem Verwendungszweck eingesetzt werden, d.h. im Rahmen der vorgeschriebenen Nutzung in der TSE gemäß [BSI-TR-03153].

Die privaten Schlüssel der CA-Zertifikate C(Root) und C(Sub-CA) dürfen ausschließlich zur Signatur der ausgegebenen Zertifikate gemäß Kap. 1.3 und zur Signatur von ARL/CRL verwendet werden.

Die privaten Schlüssel der OCSP-Responder-Zertifikate dürfen ausschließlich zur Signatur von OCSP-Responses verwendet werden.

Der TH darf die Zugangszertifikate $C_{SIG/TLS}$(TH) ausschließlich zur Signatur von Zertifikatsrequests für C_{SIG}(TSE) und für den TLS-Verbindungsaufbau mit der zuständigen Sub-CA verwenden. Er muss den privaten Schlüssel geheim halten und vor unbefugtem Zugriff angemessen schützen.

4.4.2 Verwendung des öffentlichen Schlüssels und des Zertifikats durch Zertifikatsnutzer

Die Verwendung des öffentlichen Schlüssels und des Zertifikats erfolgt gemäß [BSI-TR-03151].

Vor Verwendung des öffentlichen Schlüssels muss der Zertifikatsnutzer die Sperrlisten bzw. – sofern genutzt - OCSP der TSE-PKI nutzen, um die Gültigkeit des Zertifikats zu überprüfen.

4.5 Zertifikatserneuerung

Zertifikatserneuerung bedeutet das Ausstellen eines neuen Zertifikats für einen öffentlichen Schlüssel, der bereits zertifiziert wurde. Zertifikatserneuerungen DÜRFEN NICHT erfolgen.

4.6 Zertifizierung nach Schlüsselerneuerung

4.6.1 Bedingungen der Zertifizierung nach Schlüsselerneuerungen

Es gelten die Anforderungen aus Kapitel 3.3.

4.7 Änderungen am Zertifikat

Änderungen an den Zertifikatsinhalten, abgesehen vom Schlüsselmaterial, sind nicht vorgesehen. Sollte sich Änderungsbedarf ergeben, z.B. durch eine Umfirmierung eines Zertifikatsnehmers (d.h. die Änderung des Firmennamens oder der Gesellschaftsform), MUSS ein neues initiales Zertifikat gemäß Kapitel 3.2 beauftragt und das alte Zertifikat gesperrt werden.

4.8 Sperrung und Suspendierung von Zertifikaten

Zur Verantwortlichkeit der Initiierung der Sperrung eines Zertifikats siehe Kap. 3.6.

4.8.1 Sperrung

Alle Zertifikate werden über die von der Root- bzw. Sub-CA bereitgestellten Schnittstellen/Prozesse gesperrt. Eine Sperrung kann nicht zurückgenommen werden.

Alle Sperrungen MÜSSEN ereignisgesteuert nach Durchführung einer Sperrung umgesetzt werden.

4.8.2 Suspendierung

Eine Suspendierung von Zertifikaten wird nicht unterstützt.

4.8.3 Aktualisierungs- und Prüfungszeiten bei Sperrungen

Root-CA und Sub-CA bieten jeweils Sperrlisten an, die über die Sperrungen der ausgestellten Zertifikate Auskunft gibt.

Die Root-CA SOLL ihre ARL in einem Abstand von 6 Monaten (6 Monate mit 1 Monat Überlappung) ausstellen.

Die Sub-CA SOLL automatisiert täglich eine neue Sperrliste ausstellen (1 Tag mit 24 Stunden Überlappung).

Nach der Durchführung einer Sperrung MUSS ereignisgesteuert eine aktualisierte CRL innerhalb von 30 Minuten veranlasst und bereitgestellt werden.

4.9 Service zur Statusabfrage von Zertifikaten

Der Statusauskunftsdienst SOLLTE eine Verfügbarkeit von 7*24 Stunden haben.

4.10 Beendigung der Teilnahme

Die Beendigung der Teilnahme eines Zertifikatsnehmers kann durch diesen selbst oder die zugehörige CA eingeleitet werden.

Bei der Außerbetriebnahme einer TSE KANN das Zertifikat der TSE gesperrt werden. Die Sperrung MUSS der zugehörigen CA mitgeteilt werden.

4.11 Hinterlegung und Wiederherstellung von Schlüsseln

Die Root-CA und die Sub-CAs KÖNNEN eine Hinterlegung (z.B. für die Katastrophenfallvorsorge) gemäß den definierten Sicherheitsanforderungen durchführen. Der entsprechende Hinterlegungsprozess muss nachvollziehbar dokumentiert werden.

5 Organisatorische, betriebliche und physikalische Sicherheitsanforderungen

Die TSE-PKI CP/CPS spezifiziert technische und organisatorische Sicherheitsanforderungen an alle PKI-Teilnehmer, die im Kontext der PKI relevant sind, um die Sicherheit der PKI zu gewährleisten.

5.1 Generelle Sicherheitsanforderungen

In diesem Abschnitt werden die generellen Sicherheitsanforderungen an die PKI-Teilnehmer definiert. Diese bilden den Sicherheitsrahmen für die PKI-Teilnehmer. Hierauf aufbauend werden in dieser TSE-PKI CP/CPS erweiterte Sicherheitsanforderungen definiert.

Für die Einhaltung der generellen Sicherheitsanforderungen ist die Zertifizierung nach [ISO/IEC 27001] relevant. Eine ISO27001-Zertifizierung KANN nativ [ISO/IEC 27001] oder auf Basis von IT-Grundschutz (gemäß [BSI-Standard 200-2]) vorgenommen werden.

5.1.1 Erforderliche Zertifizierungen der PKI-Teilnehmer

Nachfolgend werden die durch die PKI-Teilnehmer zu erbringenden Zertifizierungen aufgelistet.

Root-CA: Die Root-CA bildet den Vertrauensanker der TSE-PKI. Die Zertifizierung nach [ISO/IEC 27001] MUSS vorhanden sein. Eine Zertifizierung nach [BSI-TR-03145-1] MUSS vorhanden sein, sofern diese TSE-PKI für TSE-Produkt mit TSE-CSP eines anderen Anbieters genutzt wird.

Sub-CA: Die Zertifizierung nach [ISO/IEC 27001] MUSS vorhanden sein und nachgewiesen werden. Eine Zertifizierung nach [BSI-TR-03145-1] MUSS vorhanden sein, sofern diese TSE-PKI für TSE-Produkt mit TSE-CSP eines anderen Anbieters genutzt wird.

TH: Ein TSE-Hersteller benötigt für sein TSE-Produkt eine Zertifizierung nach [BSI-TR-03153] und ein Common-Criteria-Zertifikat auf Basis von [BSI-CC-PP-0105-2019]. In der Produktionsumgebung des TSE-Herstellers werden die initialen Schlüssel im TSE-CSP generiert, die zugehörigen Zertifikate bei der TSE-PKI beantragt und auf die TSE aufgebracht werden.

TSE: Eine TSE MUSS über ein Common-Criteria-Zertifikat auf Basis von [BSI-CC-PP-0105-2019] sowie ein BSI-TR Zertifikat auf Basis von [BSI-TR-03153] verfügen.

5.1.2 Anforderungen an die Zertifizierung gemäß [ISO/IEC 27001]

Die Zertifizierung gemäß [ISO/IEC 27001] MUSS bei einer CA alle Geschäftsprozesse und IT-Systeme des Registrierungs- und Zertifizierungsbetriebs der betreffenden PKI-Infrastruktur umfassen. Hierbei muss von einem hohen Schutzbedarf ausgegangen werden.

5.2 Erweiterte Sicherheitsanforderungen

5.2.1 Betriebsumgebung und Betriebsabläufe:

Nachfolgend werden die Anforderungen an eine sichere Betriebsumgebung und an sichere Betriebsabläufe für Root-CA und Sub-CA definiert.

- **Objektschutz:** Die betrieblichen Prozesse MÜSSEN vor Störung geschützt werden.
- **Zutrittssicherheit:** Es MÜSSEN Vorkehrungen zur Sicherung des Zutritts vor Unbefugten zu den jeweiligen Betriebsräumen getroffen werden.
- **Geschäftsfortführung:** Die Wiederaufnahme der Betriebsabläufe sowie die Wiederherstellung der notwendigen Ressourcen (Personal, Technologie, Standort, Information) MÜSSEN nach einer Unterbrechung unverzüglich erfolgen.
- **Informationsträger:** Bei der Verarbeitung und Aufbewahrung von Informationen in IT-Systemen MUSS der Schutz vor unautorisiertem oder unbeabsichtigtem Gebrauch gewährleistet werden. Wenn nicht mehr benötigt, MUSS der Informationsträger sicher und unwiederherstellbar zerstört werden.
- **Brandschutz:** Es MÜSSEN bei den CAs Maßnahmen getroffen werden, die der Entstehung eines Brandes und der Ausbreitung von Feuer vorbeugen sowie wirksame Löscharbeiten ermöglichen.
- **Strom:** Eine gesicherte Stromversorgung einschließlich Redundanzkonzept für Strom SOLLTE bei den CAs gewährleistet werden.
- **Wasserschaden:** Die IT-Infrastruktur SOLLTE bei CAs gegen das Eintreten eines Wasserschadens geschützt werden.
- **Notfall-Management und Wiederherstellung:** Die CAs MÜSSEN ihre Systeme durch Backup-Mechanismen sichern, um die Wiederherstellung des Betriebs nach einer Störung oder einem Notfall zu ermöglichen. Nur vertrauenswürdiges Betriebspersonal SOLLTE Backup- und Wiederherstellungsprozesse durchführen.

5.2.2 Verfahrensanweisungen

Für den Betrieb der Root-CA und Sub-CA MÜSSEN folgende Verfahrensanweisungen umgesetzt werden:

- **Einhaltung von Verpflichtungen:** Basierend auf den verschiedenen Aufgaben MÜSSEN die Mitarbeiter die Pflichten entsprechend ihren Rollen bei ihren Tätigkeiten einhalten.
- **Vertreterreglung:** Für jede definierte Rolle MUSS ein Vertreter ernannt werden.
- **Verantwortungsbereiche:** Die Verantwortungsbereiche der Mitarbeiter MÜSSEN klar definiert werden. Für die Verantwortungsbereiche MÜSSEN klare Rollen definiert werden.
- **Vier-Augen-Prinzip:** Kritische Vorgänge erfordern die Einhaltung des Vier-Augen-Prinzips (siehe Definition in Anhang C). Nach Möglichkeit soll das Vier-Augen-Prinzip auch technisch durchgesetzt werden. Es ist immer zu dokumentieren, welche beiden Personen einen kritischen Vorgang durchgeführt haben.
- **Beschränkung der Anzahl Mitarbeiter:** Die Anzahl der Personen, die sicherheitsrelevante oder kritische Funktionen durchführen, MUSS auf die unbedingt notwendige Anzahl begrenzt sein.

- **Eskalationsmanagement:** Es MUSS ein gut definiertes und eindeutiges Eskalationsmanagement umgesetzt werden.

5.2.3 Personal

Der Betrieb der Root-CA und Sub-CA MUSS durch angemessen geschultes und erfahrenes Personal erfolgen. Insbesondere sollen folgende Anforderungen umgesetzt werden:

- **Rollen und Verantwortungen:** Die Rollen und Verantwortlichkeiten sind gemäß den Anforderungen in Kapitel 5.2.2 und [BSI-TR-03145-1] zu dokumentieren. In Bezug auf kritische Aufgaben/Funktionen bezüglich des Schlüssel- und Zertifikatsmanagement-Lebenszyklus MÜSSEN die Verantwortlichkeiten klar definiert werden.
- **Rollenbeschreibungen:** Für temporäres und permanentes Personal MÜSSEN Rollenbeschreibungen definiert werden, welche Aufgabentrennung, Mindestberechtigungen, Sicherheitsprüfungen, Verpflichtung zu Mitarbeiter- und Sensibilisierungsschulungen enthalten.
- **Einhaltung der ISMS-Anforderungen:** Das Personal MUSS administrative und betriebliche Verfahren und Prozesse im Einklang mit dem Standard ISO 27001 durchführen.
- **Qualifiziertes Personal:** Die CA MUSS Personal beschäftigen, welches über die erforderlichen Fachkenntnisse, Erfahrung und Qualifikation für das Aufgabenfeld und die angebotenen Dienste verfügt.
- **Sicherheitsüberprüfung:** Die CA MUSS sicherstellen, dass an kritischen und sicherheitsrelevanten Prozessen beteiligte Personen bezüglich der persönlichen Eignung geprüft und die Prüfung dokumentiert wurde.

5.2.4 Monitoring

Folgende Ereignisse MÜSSEN erkannt und aufgezeichnet bzw. dokumentiert werden: Root-CA und Sub-CA:

- Die aus der ISO27001 für den Betrieb, Prozesse und Infrastruktur relevanten Kontrollen
- Schlüsselmanagement (siehe Definition in Anhang C) auf dem Kryptografiemodul
- Nutzung des privaten Schlüssels der CA, insbesondere zur Erstellung von Zertifikaten
- Nicht routinemäßige Ausstellung von Zertifikaten
- Backup der privaten und öffentlichen Schlüssel und angemessene Maßnahmen für die Archivierung der öffentlichen Schlüssel MÜSSEN in der Zertifizierung nach [ISO/IEC 27001] nachgewiesen werden (siehe Anhang B).
- Es MUSS sichergestellt werden, dass unautorisierter oder unbeabsichtigter Gebrauch von PKI-relevanten Systemen erkannt wird.
- Regelmäßige Prüfung der Überwachungsmaßnahmen durch externe Auditoren.
- Remote-Anbindung über WAN: Mehrfach ungültige Login-Versuche über die WAN-Schnittstelle

5.2.5 Archivierung von Aufzeichnungen

Es MUSS sichergestellt sein, dass die Systeme über angemessene Archivierungsfunktionen verfügen. Die Zeiträume sind in Anhang B dokumentiert. Folgende Anforderungen MÜSSEN berücksichtigt werden:

Root-CA und Sub-CA:

- **Archivierung der relevanten Informationen zu öffentlichen Schlüsseln:** Die Beteiligten MÜSSEN sicherstellen, dass die relevanten Informationen zu den öffentlichen Schlüsseln des Zertifikates archiviert werden.

  Die zu archivierenden Informationen für öffentliche Schlüssel MÜSSEN enthalten:

  - Registrierungsinformationen
  - Essenzielle CA-Ereignisse (z.B. Generierung von Zertifikaten)
  - Schlüsselverwaltung
  - Zertifizierungsereignisse

  Für jedes Ereignis MUSS der Zeitpunkt der Archivierung präzise festgelegt werden.
- **Eindeutige Zuordnung von Zertifikaten:** Die Beteiligten MÜSSEN in der Lage sein, die jeweiligen Zertifikate eindeutig den registrierten Benutzern zuzuordnen.
- **Sicherstellen der Verfügbarkeit der Dienste:** Mit Hilfe einer angemessenen Archivierung klar definierter Daten der verbreiteten öffentlichen Zertifikatsschlüssel MUSS nach einer vollständigen Wiederherstellung die Verfügbarkeit der Dienste gewährleistet werden.
- **Aktualität, Integrität und Vertraulichkeit von Datenbanken:** Die Aktualität, Integrität und Vertraulichkeit der Datenbanken MÜSSEN gewährleistet sein, insbesondere bezüglich der Konsistenz der Datenbanken zur Verbreitung von Zertifikaten und der Datenbank zur Nutzer-Registrierung.
- **Tracking und Wiederherstellen von öffentlichen Schlüsseln:** Die Informationen, welche für das Tracking und die Wiederherstellung von öffentlichen Schlüsseln benötigt werden, MÜSSEN klar definiert werden.
- **Archivierung von Ereignissen:** Die wesentlichen Ereignisse, die archiviert werden, umfassen:

  - Zertifikatserstellung
  - Erneuerung und Aktualisierung der öffentlichen Zertifikats-Schlüssel
  - Ereignisse aus dem Incident- oder Notfall-Management bezüglich Zertifikats-relevanter Vorfälle.
- **Verlorene Schlüssel / Zertifikate:** Daten von verbreiteten Schlüsseln / Zertifikaten DÜRFEN NICHT wiederhergestellt werden. Es MÜSSEN neue Schlüssel / Zertifikate beantragt werden.

5.2.6 Schlüsselwechsel einer Zertifizierungsstelle

Der Schlüsselwechsel einer Zertifizierungsstelle kann einerseits geplant und andererseits ungeplant erfolgen:

- **Geplanter Schlüsselwechsel:** Im Fall eines planbaren Schlüsselwechsels einer Zertifizierungsstelle MÜSSEN die in Kapitel 5.2.7 beschriebenen Verfahren

berücksichtigt werden und entsprechende Prozesse vorhanden sein.

- **Ungeplanter Schlüsselwechsel:** Für den Fall, dass ein unvorhergesehener Schlüsselwechsel einer Zertifizierungsstelle notwendig ist, MÜSSEN entsprechende Verfahren im Notfallmanagement definiert werden.
- Sowohl ein geplanter als auch ein ungeplanter Schlüsselwechsel einer Zertifizierungsstelle MUSS gemäß dem **Vier-Augen-Prinzip** erfolgen.

5.2.7 Auflösen einer Zertifizierungsstelle

Root-CA: Die Root-CA kann nicht aufgelöst werden. Dies würde die Einstellung des gesamten Betriebs der TSE-PKI bedeuten.

Sub-CA: Wenn eine Sub-CA aufgelöst wird, MÜSSEN alle von ihr ausgestellten Zertifikate gesperrt werden. Insbesondere gelten folgende Anforderungen:

- **Übertragung der Aufgaben und Verpflichtungen:** Im Falle der Auflösung einer Sub-CA MÜSSEN deren Aufgaben und Verpflichtungen für eine Übergangszeit aufrechterhalten oder bei einer endgültigen Auflösung von einer Nachfolgeorganisation übernommen werden. Dies umfasst die Bereitstellung von Sperrinformationen für die Restlaufzeit und Archivierungszeitraum der ausgegebenen Zertifikate.
- **Informationspflicht:** Eine Sub-CA MUSS im Falle ihrer Auflösung alle beteiligten Teilnehmer sowie weitere Organisationen, mit denen Vereinbarungen bestehen, vor der Kündigung der Dienstleistung rechtzeitig informieren.
- **Zerstörung von Schlüssel- und Zertifikatsinformationen:** Nach Einstellung der Tätigkeiten MÜSSEN alle privaten Schlüssel einschließlich Zertifikatsinformationen und zugehörige Kundendaten zerstört werden.

5.2.8 Aufbewahrung der privaten Schlüssel

Alle Teilnehmer der TSE-PKI MÜSSEN folgende Anforderung umsetzen:

- **Kryptografiemodule:** Die Schlüssel MÜSSEN in vertrauenswürdigen Kryptografiemodulen gespeichert werden (siehe Abschnitt 6.2). Wenn private Schlüssel der Root-CA und Sub-CA aufbewahrt werden, MÜSSEN diese mit dem gleichen Schutzniveau, wie bei der Schlüsselerstellung verarbeitet werden.

Die Root-CA und Sub-CA MÜSSEN sicherstellen, dass folgende Anforderungen umgesetzt werden:

- **Schutz der Speichermedien:** Die Speichermedien MÜSSEN gegen nicht autorisierte Nutzung, Schäden durch Personen und weitere Bedrohungen (z.B. Feuer) gesichert werden (siehe auch 5.2.1).
- **Schlüsselaufbewahrung:** Die Speichermedien MÜSSEN sich in einem physisch und logisch hoch gesicherten Bereich befinden. Der Zutritt MUSS auf eine klar definierte Anzahl von Personen eingeschränkt werden.
- **Vertrauenswürdiges Personal:** Der private Schlüssel DARF NUR durch vertrauenswürdiges Personal erzeugt, gespeichert und für Signaturen verwendet werden.
- **Abfallbeseitigung:** Es MUSS sichergestellt werden, dass Abfälle nicht unberechtigt genutzt und vertrauliche Informationen veröffentlicht werden können.

– **Gehärtete IT-Systeme:** Es MUSS sichergestellt werden, dass die Anforderungen an gehärtete IT-Systeme und -Netzwerke sowie an die physische Sicherheit eingehalten werden. Eine Basis für umzusetzende Maßnahmen kann aus dem BSI-Grundschutzkatalog entnommen werden.

Der CSP innerhalb der TSE MUSS die Anforderungen gemäß [BSI-CC-PP-0104-2019] oder [BSI-CC-PP-0111-2019], ergänzt mit den Anforderungen aus [BSI-CC-PP-0107-2019] optional ergänzt mit [BSI-CC-PP-0108-2019] erfüllen.

5.2.9 Behandlung von Vorfällen und Kompromittierung

Nachfolgend wird beschrieben, wie bei Vorfällen und Kompromittierungen verfahren werden MUSS:

– Bei einer Kompromittierung oder einem begründeten Verdacht auf Kompromittierung eines privaten Schlüssels MUSS das zugehörige Zertifikat unverzüglich gesperrt und DARF NICHT wiederverwendet werden.

– Ein Fall von Kompromittierung sowie Verdachtsfälle MÜSSEN durch den Schlüsselinhaber dokumentiert werden.

– Jeder Verdacht auf Kompromittierung oder Missbrauch des privaten Schlüssels ist aufzuklären.

– Die Generierung neuer Schlüssel und Zertifikate MUSS überwacht und dokumentiert werden.

5.2.10 Meldepflichten

Bei Kompromittierung oder anderweitigen sicherheitsrelevanten Vorfällen MUSS eine Meldung aufbereitet und an die zuständige CA kommuniziert werden. Die Meldepflicht liegt auf Seiten des Zertifikatsnehmers.

Folgende Vorkommnisse sind Beispiele für eine Meldepflicht:

– Kompromittierung des privaten Schlüsselmaterials

– Verstoß gegen relevante Betriebsauflagen

– Betreiber der CA ist nicht mehr aktiv (Bsp.: Insolvenz)

– Aufforderung zur Sperrung eines Zertifikates

Folgende Angaben MÜSSEN der Meldung mindestens beigefügt werden:

– Was wurde kompromittiert bzw. was wurde betroffen?

– Wann ist das Vorkommnis passiert bzw. wann wurde der Vorfall bemerkt?

– Wer hat das Vorkommnis festgestellt?

– Ort des Vorkommnisses

– Wie ist das Vorkommnis vermutlich abgelaufen?

– Wenn schon eine Maßnahme durchgeführt wurde: Welche Maßnahmen wurden schon eingeleitet?

Root-CA:

Folgende Meldepflichten auf Seiten der Root erfolgen via Veröffentlichung über die ROOT-CA -Webseite (siehe Tabelle 7):

– Änderungen dieser TSE-PKI CP/CPS, welche insbesondere aus Änderungen an der

[BSI-TR-03153] oder der [BSI-TR-03145] resultieren können.

Jede Meldung MUSS nachvollziehbar dokumentiert werden und so abgelegt werden, dass die Meldung im Bedarfsfall vorgezeigt werden kann. Der Verfasser der Meldung MUSS eindeutig gekennzeichnet sein.

5.3 Notfall-Management

Die Root-CA und Sub-CA MÜSSEN gewährleisten, dass die Wiederherstellung des Normalbetriebs nach einer Störung oder nach einem Notfall innerhalb einer angemessenen Frist erfolgt. Notfall-Szenarien betreffen u.a.:

- Kompromittierung des privaten Schlüssels
- Entdeckte Schwachstellen in den verwendeten kryptografischen Verfahren
- Nichtverfügbarkeit von Sperrlisten

Insbesondere gelten folgende Anforderungen, welche erfüllt werden MÜSSEN:

- **Notfallmanagement:** Die Root-CA und Sub-CA MÜSSEN rechtzeitig angemessen auf Störungen oder Notfälle reagieren, um Schäden zu minimieren und den Geschäftsbetrieb zu gewährleisten.
- **Maßnahmenplanung:** Die Root-CA und Sub-CA MÜSSEN angemessene Maßnahmen für den Fall vorbereiten, dass relevante Algorithmen gebrochen oder Verfahren unsicher werden.
- **Kompromittierung:** Wenn die Vermutung besteht, dass Schlüsselmaterial kompromittiert ist, so DARF KEIN PKI-Teilnehmer dieses weiter nutzen.
- **Risikoreduktion / Schadensminderung**: Alle PKI-Teilnehmer SOLLTEN entsprechende Maßnahmen zur Minimierung von Risiken und Schäden anwenden.
- **Vermeidung von Vorfällen:** Alle PKI-Teilnehmer MÜSSEN angemessene Maßnahmen vorbereiten sowie die Ursachen von Vorfällen ermitteln, um diese in Zukunft zu vermeiden.
- **Notfallpläne:** Die Root-CA und Sub-CA MÜSSEN entsprechende Pläne vorbereiten, um die Geschäftsprozesse nach einem Notfall wiederherzustellen.
- **Backups**: Die Root-CA und Sub-CA MÜSSEN Backups von privaten und öffentlichen Schlüsseln, ausgestellten Zertifikaten und Sperrinformationen durchführen.
- **Vorgehen nach einer Störung:** Nach einer schweren Störung MÜSSEN alle PKI-Teilnehmer sicherstellen, dass die entstandene Sicherheitslücke geschlossen wird.

6 Technische Sicherheitsanforderungen

6.1 Erzeugung und Installation von Schlüsselpaaren

Jeder Zertifikatsnehmer MUSS sein eigenes Schlüsselpaar generieren.

6.1.1 Generierung von Schlüsselpaaren für die Zertifikate

Die PKI-Teilnehmer Root-CA und Sub-CA MÜSSEN sicherstellen, dass folgende Anforderungen umgesetzt werden:

- **Generierung im Vier-Augen-Prinzip:** Das Schlüsselpaar MUSS während der Schlüsselzeremonie im Vier- Augen-Prinzip unter Teilnahme des für den Schlüssel verantwortlichen Mitarbeiters generiert werden.
- **Generierung eines Schlüsselpaars:** Die zur Schlüsselgenerierung eingesetzten Kryptografiemodule MÜSSEN je nach TYP die in Kapitel 6.2 angegebenen Vorgaben erfüllen.
- Der **technische Zugriff auf die Schlüssel in den Kryptografiemodulen** aller Zertifikatsnehmer MUSS durch ein Geheimnis geschützt werden (Passwort, PIN, o.ä.), welches ausschließlich die jeweiligen Operatoren kennen. Der Zugriff auf das Kryptografiemodul, insbesondere zur Schlüsselerzeugung, MUSS auf ein Minimum an Operatoren beschränkt sein.

6.1.2 Lieferung privater Schlüssel

Die Erstellung der privaten Schlüssel für die TSE-Zertifikate erfolgt dezentral durch die Zertifikatsnehmer der TSE-PKI und innerhalb der TSE-CSP-Module. Daher erfolgt keine Lieferung der privaten Schlüssel.

6.1.3 Lieferung öffentlicher Zertifikate

Alle Zertifikate der TSEs können über die Einheitliche Digitale Schnittstelle (EDS) der TSE abgerufen werden. Die Zertifikate KÖNNEN zusätzlich in den jeweiligen Verzeichnissen der ausstellenden CAs abgelegt werden.

6.1.4 Schlüssellängen und kryptografische Algorithmen

Schlüssellängen und kryptografische Algorithmen der Schlüsselpaare MÜSSEN angemessene kryptografische Verfahren einhalten. Es werden ausschließlich ECC-basierte kryptographische Verfahren eingesetzt. Die zum jeweiligen Zeitpunkt konkret zu verwendenden kryptografischen Algorithmen und Schlüssellängen MÜSSEN der [BSI-TR-03116-5] entnommen werden.

Vor der Zertifikatserstellung für einen Schlüssel wird geprüft, dass

- die EC-Domänenparameter zulässig sind,
- der Public Key ein Punkt auf der Kurve ist und
- noch kein Zertifikat für den Public Key ausgestellt worden ist.

Unzulässige Schlüssel werden abgewiesen.

Bei der Erzeugung und Nutzung von statischen und temporären Schlüsseln im Rahmen der TSE-PKI MUSS ein Zufallsgenerator verwendet werden, der konform zu den Anforderungen aus [BSI-TR-03116-5] ist. Des Weiteren MUSS bei statischen Schlüsseln ein Kryptografiemodul gemäß Abschnitt 6.2 eingesetzt werden.

6.1.5 Festlegung der Parameter der Schlüssel und Qualitätskontrolle

- **Sichere Handhabung und Lagerung von Schlüsselmaterial:** Software- und Hardware-Komponenten zur Erzeugung, Handhabung und Lagerung der privaten Schlüssel MÜSSEN angemessene Maßnahmen zur sicheren Handhabung und Lagerung von Schlüsselmaterial einhalten.
- **Defektes Krypto-Modul (KM):** Im Falle eines defekten KM ist sicherzustellen, dass das Schlüssel-Backup sicher und im Vier-Augen-Prinzip in ein neues KM nach angemessenen Maßnahmen zur sicheren Handhabung und Lagerung von Schlüsselmaterial importiert wird.
- **Schutz vor Angriff auf den privaten Schlüssel:** Es MUSS sichergestellt werden, dass der private Schlüssel nicht von einem Angreifer für kryptografische Operationen missbraucht werden kann und dass angemessene Maßnahmen (siehe Abschnitt 6.2.3. bis 6.2.6) zur sicheren Handhabung und Lagerung von Schlüsselmaterial und gehärteten IT-Systemen und -Netzwerken eingehalten werden.
- **Unverschlüsselter / unberechtigter Export des privaten Schlüssels:** Es MUSS sichergestellt werden, dass der private Schlüssel nicht unverschlüsselt oder unberechtigt aus dem Schlüsselspeicher exportiert werden kann. Es MÜSSEN angemessene Maßnahmen zur sicheren Handhabung und Lagerung von Schlüsselmaterial eingehalten werden. Die zum jeweiligen Zeitpunkt konkret zu verwendenden kryptografischen Algorithmen und Schlüssellängen MÜSSEN den jeweils aktuellen Empfehlungen aus [BSI-TR-03116-5] entsprechen.

6.1.6 Verwendungszweck der Schlüssel

Die Schlüssel DÜRFEN ausschließlich für die in Kapitel 1.4.1 beschrieben Verwendungszwecke eingesetzt werden.

6.2 Sicherung des privaten Schlüssels und Anforderungen an kryptografische Module

Die Teilnehmer der TSE-PKI MÜSSEN Kryptografiemodule zur Generierung, Speicherung und Nutzung ihrer privaten Schlüssel zu ihren Zertifikaten aus der TSE-PKI verwenden. Die Sicherheitsanforderungen an Kryptografiemodule zum Schutz der privaten Schlüssel zu den Zertifikaten der TSE-PKI werden in Kapitel 6.2.10 definiert.

Neben dem Einsatz eines sicheren Kryptografiemodules MUSS auch ein sicherer Umgang mit den privaten Schlüsseln sichergestellt werden (Ausnahme TSE).

6.2.1 Mehrpersonen-Zugriffssicherung zu privaten Schlüsseln

Das Schlüsselmanagement bei Root-CA und Sub-CA MUSS im Vier-Augen-Prinzip, unter entsprechender Dokumentation und Protokollierung insbesondere der Rollen und eindeutiger Identifikation der teilnehmenden Personen, durchgeführt werden.

6.2.2 Ablage privater Schlüssel

Es MUSS sichergestellt werden, dass die Daten der privaten Schlüssel nach den Anforderungen aus Kapitel 5 zur sicheren Handhabung und Lagerung von Schlüsselmaterial gespeichert werden.

6.2.3 Backup privater Schlüssel

Die Root-CA und Sub-CA MÜSSEN sicherstellen, dass Maßnahmen zum sicheren Backup der privaten Schlüssel umgesetzt werden. Insbesondere MÜSSEN folgende Anforderungen eingehalten werden:

- Die Vorgaben aus 6.2.5 **Transfer** privater Schlüssel in oder aus kryptografischen Modulen MÜSSEN eingehalten werden.
- **Bestandteil des ISMS nach ISO 27001:** Die technischen Maßnahmen zum Backup privater Schlüssel MÜSSEN in der Auditierung nach [ISO/IEC 27001] berücksichtigt werden.
- **Sichere Schlüssel-Backups:** Die Durchführung von sicheren Backups der privaten Schlüssel MUSS nach den Vorgaben zur sicheren Handhabung und Lagerung von Schlüsselmaterial durchgeführt werden.
- **Durchführung des Schlüssel-Backups:** Das Schlüssel-Backup MUSS während der Schlüsselzeremonie gemäß dem Vier-Augen-Prinzip unter Teilnahme des für den Schlüssel verantwortlichen Mitarbeiters durchgeführt werden. Automatisierte Prozesse zur Übertragung der Schlüssel auf ein weiteres HSM (z.B. für ein Cold-Standby-Backup) DÜRFEN genutzt werden.
- **Schlüsselspeicherung:** Es MUSS sichergestellt werden, dass die Backup-Daten des öffentlichen Schlüssels nach den Vorgaben zur sicheren Handhabung und Lagerung von Schlüsselmaterial gespeichert werden.
- **Zugriff auf Backup-Daten:** Es MUSS sichergestellt werden, dass nur vertrauenswürdige Mitarbeiter Zugriff auf die Schlüsselspeicher- und Backup-Daten haben.

6.2.4 Archivierung privater Schlüssel

Es wird keine Archivierung gesperrter oder abgelaufener privater Schlüssel durchgeführt. Diese privaten Schlüssel MÜSSEN unter Beachtung der Einschränkungen aus Kapitel 6.2.9 zerstört werden (Ausnahme TSE).

6.2.5 Transfer privater Schlüssel in oder aus kryptografischen Modulen

- Der private Schlüssel KANN zwischen kryptografischen Modulen transferiert werden.
- Voraussetzung für den Transfer privater Schlüssel ist, dass nur Kryptografiemodule verwendet werden, welche die Anforderungen aus Abschnitt 6.2 erfüllen.
- Der private Schlüssel MUSS hierbei verschlüsselt und integritätsgesichert transferiert werden. Die Ver-/Entschlüsselung MUSS in den Kryptografiemodulen erfolgen.
- Der KEK zur Ver-/Entschlüsselung des privaten Schlüssels MUSS vertraulich und integritätsgesichert ausgetauscht werden.

– Bei der Durchführung eines manuellen Transfers MUSS das Vier-Augen-Prinzip eingehalten werden.

6.2.6 Speicherung privater Schlüssel in kryptografischen Modulen

– Grundsätzlich MÜSSEN die privaten Schlüssel eines PKI-Teilnehmers auf einem Kryptografiemodul gespeichert werden.

  Die einzige Ausnahme bilden die client- und serverseitigen TLS-Schlüssel bei Sub-CA und TH, die zur TLS-Authentisierung an der technischen Schnittstelle der Sub-CA verwendet werden. Hier KANN ein Kryptografiemodul eingesetzt werden.

– Auf einem HSM DÜRFEN private Schlüssel von Root-CA und Sub-CA gespeichert werden (Bsp.: es dürfen mehrere CA-Schlüssel auf demselben HSM gespeichert werden). Diese MÜSSEN aber in getrennten Sicherheitsdomänen (Trennung auf Anwendungsebene) verwaltet werden. Entsprechend MÜSSEN diese im HSM logisch getrennt sein.

6.2.7 Aktivierung privater Schlüssel

Die Aktivierung eines Schlüssels in einem Kryptografiemodul erfordert die Einhaltung des Vier-Augen-Prinzips.

6.2.8 Deaktivierung privater Schlüssel

Im deaktivierten Zustand der Schlüssel DÜRFEN diese NICHT genutzt werden können.

6.2.9 Zerstörung privater Schlüssel

Die privaten Schlüssel eines CA-Betreibers MÜSSEN in folgenden Fällen sicher und unwiederherstellbar zerstört werden:

– Der Gültigkeitszeitraum des CA-Schlüssels ist abgelaufen

– Der Schlüssel der CA wurde gesperrt.

Die Backups der Schlüssel MÜSSEN ebenfalls berücksichtigt werden.

Die Zerstörung der privaten Schlüssel MUSS durch einen sicheren Lösch-Mechanismus im Kryptografiemodul (falls vorhanden) oder durch die unwiederherstellbare mechanische Zerstörung erfolgen.

6.2.10 Beurteilung kryptografischer Module

6.2.10.1 Root-CA und Sub-CA

Die Root-CA bzw. Sub-CA MUSS sicherheitsüberprüfte oder zertifizierte Hardware-Sicherheitsmodule (HSM) oder Chipkarten einsetzen.

6.2.10.2 TSE

Bei einem TSE MUSS ein Kryptografiemodul eingesetzt werden, dass nach [BSI-CC-PP-0104-2019] bzw. [BSI-CC-PP-0111-2019] zertifiziert ist. Der TSE-Hersteller benötigt für sein Kryptografiemodul eine Bestätigung bzw. eine Sicherheitsaussage des Herstellers, dass diese Nachweise durch eine entsprechende Prüfstelle erbracht wurden.

Das Vorhandensein der Bestätigung zu dem vom PKI-Teilnehmer eingesetzten Kryptografiemodul MUSS vom TH bei der Einrichtung der technischen Service-Schnittstelle gegenüber der Sub-CA nachgewiesen werden.

6.3 Andere Aspekte des Managements von Schlüsselpaaren

6.3.1 Archivierung öffentlicher Schlüssel

Die Zertifikate eines Teilnehmers der TSE-PKI MÜSSEN inklusive der Statusdaten archiviert werden (siehe Anhang B).

6.3.2 Gültigkeitszeitraum von Zertifikaten und Schlüsselpaaren

Der Gültigkeitszeitraum von Zertifikaten wird wie folgt definiert:

- **TSE-CA Root-CA-Zertifikat C(Root):**
  - 30 Jahre für das erste Zertifikat und 15,5 Jahre für die Folgezertifikate
  - Die Root-CA-Zertifikate MÜSSEN unabhängig vom Gültigkeitszeitraum spätestens in dem hier angegebenen Intervall gewechselt werden:
    - Die Root-CA-Zertifikate werden nicht länger als 5 Jahre aktiv genutzt und danach über einen Zeitraum von 10,5 Jahren insbesondere nur für die Signatur der Sperrliste verwendet.
    - Sobald eine Root-CA über ein neues Zertifikat verfügt, MUSS dieses zum Ausstellen neuer Zertifikate verwendet werden.
- **TSE-CA Sub-CA-Zertifikat C(Sub-CA):**
  - 15 Jahre für das erste Zertifikat und 10,5 Jahre für die Folgezertifikate
  - Die Sub-CA-Zertifikate MÜSSEN unabhängig vom Gültigkeitszeitraum spätestens in dem hier angegebenen Intervall gewechselt werden:
    - Die Sub-CA-Zertifikate werden nicht länger als 3 Jahre aktiv genutzt und danach über einen Zeitraum von 7,5 Jahren insbesondere nur für die Signatur der Sperrliste verwendet.
    - Sobald eine Sub-CA über ein neues Zertifikat verfügt, MUSS dieses zum Ausstellen neuer Zertifikate verwendet werden.
- **TSE-CA End Entity-Zertifikate für OCSP-Responder C_{OCSP-S}(Sub-CA):**
  - Gültigkeitszeit des Zertifikats: 6 Monate
- **TSE-CA End Entity-Zertifikate für TSEs C_{SIG}(TSE):**
  - Gültigkeitszeit des Zertifikats: maximal 7,5 Jahre

6.4 Aktivierungsdaten

Die Aktivierungsdaten für die Kryptografiemodule MÜSSEN sicher aufbewahrt werden.

6.5 Sicherheitsanforderungen für die Rechneranlagen

Nachfolgend werden die Anforderungen an die Rechneranlagen definiert, die von den jeweiligen Root-CA und Sub-CA umgesetzt werden MÜSSEN:

- **Netzwerkkontrolle:** Es MÜSSEN entsprechende Maßnahmen umgesetzt werden, um das interne Netzwerk vom externen zu trennen und vor unbefugtem Zugriff zu schützen.
- **Intrusion Detection Systeme (IDS):** Der Einsatz von Intrusion-Detection-Systemen (IDS) im gesicherten Netzsegment MUSS berücksichtigt werden. Die Log-Dateien des IDS MÜSSEN regelmäßig kontrolliert werden.
- **System-Härtung:** Die CA-Server, die zur Erstellung von Zertifikaten verwendet werden, MÜSSEN gehärtet werden. Dies umfasst die Konfiguration und Einstellung der verwendeten Hardware- und Software-Komponenten.
- **System-Konfiguration:** Die Konfigurationsoptionen und -einstellungen DÜRFEN nur die minimal benötigten Funktionalitäten für den CA-Betrieb enthalten.
- **Netzwerk-Separierung:** Die Netzwerke, in denen sich die CA-Server befinden, MÜSSEN durch geeignete Maßnahmen geschützt werden.
- **Software-Updates:** Software-Updates MÜSSEN bei sicherheitsrelevanten Änderungen schnellstmöglich eingespielt werden, andere Updates SOLLTEN regelmäßig aktualisiert werden.
- **Vertraulichkeit und Integrität:** Die CA MUSS sensitive Daten vor unbefugtem Zugriff oder Veränderung schützen.
- **Logging und Audit-Trails:** Log-Dateien und Audit-Trails MÜSSEN regelmäßig geprüft werden, und automatisierte Benachrichtigungen MÜSSEN auf Abweichung vom vorgesehenen Betrieb hinweisen.
- **Speicherort von Log-Dateien:** Die Dateien der Audit-Trails SOLLEN NICHT auf dem CA-Server, der für die Verwaltung von Zertifikaten verwendet wird, gespeichert werden. Der Speicherort für Log-Dateien KANN temporär der CA-Server sein. Die Log-Dateien MÜSSEN dann regelmäßig auf einen anderen Speicherort ausgelagert werden.
- **Benutzerverwaltung:** Das System MUSS über eine angemessene Benutzerverwaltung verfügen.
- **Systemfunktionen:** Die CA MUSS den Zugriff auf die benötigten Systemfunktionen und Hilfsprogramme begrenzen.
- **Schutz vor Schadsoftware:** Die Integrität der System-Komponenten und Informationen MUSS gegen Viren, Schadsoftware sowie nicht zugelassene Programme geschützt werden.

6.6 Zeitstempel

Keine Anforderungen an Zeitstempel.

6.7 Validierungsmodell

Zur Validierung von C(Root), C(Sub-CA), den OCSP-Responder-Zertifikaten und C_{SIG}(TSE) MUSS ein hybrides Validierungsmodell angewandt werden. Dabei wird gefordert, dass alle Zertifikate im Zertifizierungspfad zum Zeitpunkt der Erzeugung der zu

prüfenden Signatur gültig waren. Somit ist sichergestellt, dass auch nach Ablauf der Zertifikatsgültigkeiten noch Signaturen von TSEs geprüft werden können. Zu diesem Zweck müssen CAen Sperrinformationen archivieren.

7 Profile für Zertifikate und Sperrlisten

7.1 Profile für Zertifikate und Zertifikatsrequests

Die Profile für die Zertifikate, die Zertifikatsrequests und das Namensschema sind in Anhang D spezifiziert.

7.1.1 Zugriffsrechte

Die erlaubte Funktion der Zertifikate wird über die Key-Usage-Extension definiert.

7.1.2 Zertifikatserweiterung

Die Certificate Extensions werden in Anhang D definiert.

7.2 Profile für Sperrlisten

Die TSE-PKI veröffentlicht Zertifikatssperrlisten gemäß des Standards X.509 Version 3. Die Root-CA und Sub-CA der TSE-PKI stellen Sperrlisten bereit. Der Verteilpunkt von Sperrlisten wird in der entsprechenden Erweiterung in ausgestellten Zertifikaten aufgenommen.

7.3 Profile für OCSP-Dienste

Die Profile für die OCSP-Responder-Signaturzertifikate sind in Anhang D spezifiziert.

Die OCSP-Responder-Zertifikate enthalten eine OCSP NoCheck-Extension, d.h. der OCSP-Client wird angewiesen, den Sperrstatus des OCSP-Signer-Zertifikats nicht per OCSP-Request zu überprüfen. Muss ein OCSP-Signer-Zertifikat als „nicht mehr vertrauenswürdig“ betrachtet werden, so MUSS der CA-Betreiber es unverzüglich außer Betrieb nehmen und MUSS den OCSP-Responder mit einem neu ausgestellten OCSP-Signer-Zertifikat bestücken.

Der zuständige OCSP-Responder SOLLTE durch Verwendung der ArchiveCutoff-OCSP-Extension (siehe [RFC 6960]) dokumentieren, bis wann er die Statusinformation für das Zertifikat bereithalten wird.

.

8 Überprüfung und andere Bewertungen

In diesem Kapitel werden die Überprüfungen definiert, die den Teilnehmern der TSE-PKI als Auflage im Rahmen ihrer Antragszeit und Nutzung der TSE-PKI auferlegt werden.

8.1 Inhalte, Häufigkeit und Methodik

8.1.1 Beantragung Teilnahme an TSE-PKI

Folgende Anforderungen MÜSSEN bei Beantragung der Teilnahme an der TSE-PKI erfüllt werden. Detaillierte Informationen sind in Kapitel 5.1 zu finden.

Antrag für Teilnahme als	**Nachweis**		**Überprüfung der Nachweise**	**Wichtung**
Sub-CA	oder	ISO27001-Zertifizierung nativ der Sub-CA	Zertifizierter ISO27001 Lead Auditor	Voraussetzung
		ISO27001-Zertifizierung nach BSI Grundschutz der Sub-CA	BSI-akkreditierter ISO27001 Lead Auditor	
	Optional: Zertifizierung nach [BSI-TR-03145-1]		Zertifizierter [BSI-TR-03145-1] Auditor	
TSE	CC-Zertifizierung entsprechend [BSI-CC-PP-0105] mit einem CSP gemäß [BSI-CC-PP-0104/0111]		CC-Zertifizierungsverfahren	Voraussetzung
	Zertifizierung entsprechend [TR3153]		Prüfstelle	

Tabelle 8: Anforderungen für die Teilnahme an der TSE-PKI

8.1.2 Wirkbetrieb

Die vorausgesetzten Nachweise/Zertifizierungen (siehe Kapitel 8.1.1) MÜSSEN im Wirkbetrieb auf Basis des jeweiligen Prüf-/Zertifizierungsschemas aufrechterhalten werden.

Sollte eine Zertifizierung nicht mehr gültig sein, so MUSS dies der zuständigen CA umgehend mitgeteilt werden (siehe Kapitel 3.2.7).

Sollte eine Sub-CA eine geänderte Version ihrer Certificate Policy veröffentlichen, so MUSS die Root hierüber einen der benannten Ansprechpartner mittels verschlüsselter und signierter E-Mail informiert werden.

8.2 Reaktionen auf identifizierte Vorfälle

Die Reaktionen auf identifizierte Vorfälle sind in Kapitel 5.2.10 Meldepflichten definiert.

9 Sonstige finanzielle und rechtliche Regelungen

9.1 Preise

An die Betreiber von Sub-CA-Instanzen werden keine preislichen Anforderungen gestellt.

9.2 Finanzielle Zuständigkeiten

Die Root-CA und Sub-CA obliegt der finanziellen Zuständigkeit der Deutsche Telekom Security GmbH und damit den entsprechenden Regelungen der Deutsche Telekom Security GmbH.

Sofern dedizierte Sub-CAs von Deutsche Telekom Security GmbH für andere TSE-Hersteller betrieben werden, werden die finanziellen Zuständigkeiten im jeweiligen Vertrag geregelt.

A Namensschema

Bei C_{SIG}(TSE) MUSS als CommonName der HEX-codierte SHA256-Hash des Public Keys verwendet werden. Der Hash ist über die DER-codierte Struktur SubjectPublicKeyInfo zu bilden.

Die Common Names (CN) der übrigen TSE-PKI Teilnehmer MÜSSEN folgendem Schema entsprechen: **‘<org>.<function>[.<extension>]‘**.

Durch die Registrierungsprozesse MUSS von den CAs sichergestellt werden, dass die PKI-Teilnehmer die Common Names (Funktionskennzeichnung ‘<function>‘) entsprechend ihrer PKI-Rolle zugewiesen bekommen.

Eine Sub-CA MUSS sicherstellen, dass ein Common Name in Kombination mit der Sequenznummer unter dem Issuer Common Name der Sub-CA bei Endnutzer-Zertifikaten (bzw. bei einem Zertifikatstripel) ausschließlich einmal vergeben wird, um die Eindeutigkeit dieser Zertifikate in der TSE-PKI zu gewährleisten. Des Weiteren MUSS die Root sicherstellen, dass jede Sub-CA einen anderen Common Name erhält.

Tabelle 9 beschreibt die Bestandteile der CN für die übrigen Teilnehmer der TSE-PKI:

Namensteil	Bedeutung	Länge, Kodierung, Ausnahmen
<org>	Kürzel der Identität/Organisation	Länge max. 48 Zeichen, erstes Zeichen muss ein Buchstabe oder eine Ziffer sein.
<function>	Funktionskennzeichnung innerhalb der TSE-PKI	Länge max. 4 Zeichen. Feste Werte: CA
<extension>	Erweiterung, zusätzliche Informationen	Länge max. 10 Zeichen. Optional, z.B. für leichteres Auffinden in Listen. Zwingend vorgegebene Werte bei CAs gemäß Tabelle 10 (Root-CA) und Tabelle 11 (Sub-CA).

Tabelle 9: Namensschema (Kodierung Common Name)

Grundsätzliche Festlegungen:

- Die Länge des CN ist auf 64 Zeichen begrenzt.
- Die Kodierung ist ‘Printable String‘.
- Die zulässigen Zeichen sind: „0...9“, „a...z“, „A...Z“, „-“ (keine Leerzeichen).
- Der Punkt („.“) ist ausschließlich als Trennzeichen zwischen den Namensteilen zulässig und MUSS bei Vorhandensein im Namen des Zertifikatsinhabers weggelassen oder durch ein „-“ ersetzt werden.
- Die Leserichtung ist von links nach rechts (parsen, z.B. nach dem ersten Punkt immer ‘<function>‘).
- Endnutzer KÖNNEN auf Basis der <extension> eine bessere Unterscheidbarkeit der von Ihnen genutzten Zertifikate herbeiführen. In dieser <extension> kann, nach der einmaligen Registrierung, eine individuelle Nummerierung oder z.B. ein Bezug auf einen Verwaltungsbereich (Kürzel Ortsangabe etc.) erfolgen.

Eine Erweiterung des Namensschemas ist möglich durch die Nutzung/Vorgabe weiterer Funktionsbezeichnungen und die Flexibilität der Nutzung der zusätzlichen Informationen in der optionalen Erweiterung.

Das Kürzel der Identität (<org>) wird durch den Zertifikatsinhaber festgelegt und sollte:

- kurz,
- sprechend (Identität erkennbar) und
- eindeutig sein.

Ausnahmen bzw. Festlegungen für das Kürzel der Identität (<org>):

Root-CA: „TSE-Root“

Die Zertifikate der Wirkumgebung haben das in den folgenden Tabellen angegebene Namensschema[3].

A.1 Root-CA

Die Zertifikate der Root-CA haben folgendes Namensschema:

C(Root)

Attribut Typ	Kürzel	Vorgabe	Wert	Erläuterung
common name	CN	mandatory	„<Root name> “	Name der Root-CA
organisation	O	mandatory	„<Organisation>“	Name der Organisation
organisational unit	OU	optional	„<Organisational Unit>“	Name der Organisationseinheit
country	C	mandatory	„<LC>“	Zwei Zeichen Ländercode gemäß [ISO 3116 ALPHA-2], für Deutschland „DE“

Tabelle 10: Namensschema Zertifikat C(Root)

A.2 Sub-CA

Die Zertifikate der Sub-CA haben folgendes Namensschema:

C(Sub-CA)

Attribut Typ	Kürzel	Vorgabe	Wert	Erläuterung
common name	CN	mandatory	“<Sub-CA name>“	Eindeutiger Name der Sub-CA.
organisation	O	mandatory	„<Organisation>“	Name der Organisation
organisational unit	OU	optional	„<Organisational Unit>“	Name der Organisationseinheit
country	C	mandatory	„<LC>“	Zwei Zeichen Ländercode gemäß [ISO 3116 ALPHA-2], für Deutschland „DE“

Tabelle 11: Namensschema der Sub-CA-Zertifikate

$C_{OCSPS-S}$(Sub-CA)

Attribut Typ	Kürzel	Vorgabe	Wert	Erläuterung
common name	CN	mandatory	„<OCSP-Signer name>“	Kennzeichnung als OCSP-Signer
organisation	O	mandatory	„<Organisation>“	Name der Organisation
organisational unit	OU	optional	„<Organisational Unit>“	Name der Organisationseinheit
country	C	mandatory	„<LC>“	Zwei Zeichen Ländercode gemäß [ISO 3116 ALPHA-2], für Deutschland „DE“

Tabelle 12: Namensschema Zertifikat C_{OCSP-S}(Sub-CA)

A.3 TSE

TSE haben folgendes Namensschema:

Attribut Typ	Kürzel	Vorgabe	Wert	Erläuterung
common name	CN	mandatory	„<serialnumber>“	Seriennummer des Geräts (SHA256-Hash des Public Keys in HEX-Codierung)[1]
organisation	O	mandatory	„<Organisation>“	Name der Organisation entsprechend der Master Domäne
country	C	mandatory	„<LC>“	Zwei Zeichen Ländercode gemäß [ISO 3116 ALPHA-2]
dnQualifier	dnQualifier	mandatory	„<TSE-SMAERS CC-Cert ID>“	Wert des BSI CC Zertifikats (z.B. „BSI-DSZ-CC-1121-2019“ oder „BSI-DSZ-CC-1121-V2“)

Tabelle 13: Namensschema Zertifikat C_{SIG}(TSE)

[1] SHA256-Hash über die DER-Bytes der SubjectPublicKeyInfo-Struktur des Zertifikats

B Archivierung

Die folgende Tabelle gibt die Archivierungszeiträume für die unterschiedlichen Zertifikate der TSE-PKI Teilnehmer wieder.

Die Speicherung bzw. auch die Bereitstellung der Zertifikate KANN in dem LDAP-Verzeichnis der Sub-CA erfolgen (diese Option wird jedoch aktuell nicht genutzt), wobei die anderen Teilnehmer von der eigenverantwortlichen Speicherung der Zertifikate nicht befreit werden.

Teilnehmer	Archivierungsort	Zertifikatstyp	Archivierungsdauer
Root-CA	Zertifikatsspeicher	C(Root)	Zertifikatslaufzeit + 10 ½ Jahre
Sub-CA	Zertifikatsspeicher	C(Sub-CA)	Zertifikatslaufzeit + 10 ½ Jahre
		C_{TLS}(Sub-CA)	
TSE	Zertifikatsspeicher	C_{SIG}(TSE)	Zertifikatslaufzeit + 10 ½ Jahre
ASP Root, ASP Sub-CA, ASP TH	Zertifikatsspeicher	$C_{S/MIME}$(ASP Root) $C_{S/MIME}$(ASP Sub-CA) $C_{S/MIME}$(ASP TH)	Zertifikatslaufzeit + 2 ½ Jahre
TH	Zertifikatsspeicher	$C_{SIG/TLS}$(TH)	Zertifikatslaufzeit + 10 ½ Jahre

Tabelle 14: Archivierung von Zertifikaten

Nach Ablauf der Archivierungsdauer können die Zertifikate vernichtet werden.

Weitere Daten, die im Zusammenhang mit Kundenbeziehungen erstellt werden, wie z.B.

- Kundendaten
- Vertragsdaten
- Schriftwechsel mit Kunden
- Registrierungsdaten des TSE-Herstellers und dessen berechtigter Personen
- Liefer- und Abrechnungsdaten

werden in einer Kundenakte in Papierform und/oder elektronischer Form verwaltet und archiviert.

Die Archivierung in der Kundenakte erfolgt für die Dauer der Teilnahme des Kunden an der TSE-PKI.

Nach Beendigung der Teilnahme ist die Kundenakte für 10 Jahre zu archivieren. Anschließend kann diese vernichtet werden.

C Definitionen

Begriff	Beschreibung
Ansprechpartner	Der Ansprechpartner (auch ASP oder Vertreter genannt) ist im Rahmen der operativen Tätigkeit der Vertreter des Unternehmens in Richtung der CA-Instanz und darf in dessen Namen die Entscheidungen treffen bzw. die Anträge autorisieren.
Antragsteller	Der Antragsteller im Sinne dieses Dokumentes ist das Unternehmen, welches die Zertifikate für den Betrieb einer Sub-CA, eines TH bei der zuständigen CA-Instanz anfordert.
Vier-Augen-Prinzip	Parallele Gegenkontrolle durch eine zweite Person bei der Durchführung eines Vorgangs. Die eindeutige Identifikation und Rolle der teilnehmenden Mitarbeiter MUSS protokolliert werden. Das Vier-Augen-Prinzip KANN organisatorisch so umgesetzt werden, dass bei diesem Prozess zwei unterschiedliche Personen beteiligt sein MÜSSEN, die nicht zeitgleich gemeinsam am gleichen Ort agieren MÜSSEN.
Schlüsselmanagement	Verwaltung von Schlüsseln (insbesondere Erzeugung, Speicherung und Löschung bzw. Zerstörung von Schlüsseln)
Hinterlegung von Schlüsseln	Sichere Verwahrung einer Kopie eines Schlüssels an einem Zweitort.
Zerstörung von Schlüsseln	Zerstörung des Schlüssels durch einen sicheren Löschmechanismus im Kryptografiemodul. Dieser wird i.d.R. durch ein Überschreiben mit einem vorgegebenen Wert oder durch das interne dauerhafte Sperren aller Zugriffe auf den Schlüssel realisiert. Verfügt das Kryptografiemodul nicht über einen entsprechen Löschmechanismus, muss eine unwiederherstellbare mechanische Zerstörung erfolgen.
PKI-Rolle	Die PKI-Rolle beschreibt die Funktionsklasse eines PKI-Teilnehmers in der TSE-PKI. Folgende PKI-Rollen sind in der TSE-PKI vorhanden: Root-CA, Sub-CA, und TSE. Ein PKI-Teilnehmer ist eine Instanz seiner PKI-Rolle.
Sequenznummer	SERIAL NUMBER des Distinguished Name, siehe Anhang A
Serialnumber	serialNumber Feld des Zertifikats

Tabelle 15: Definitionen

D Zertifikatsprofile

D.1 TSE-CA Root-CA-Zertifikat C(Root)

TBSCertificate von C(Root)

- **Version**
  - „v3“
- **SerialNumber**
  - zufällig
  - bitLength (Entropie): 126 Bit
- **Signature**
  - gleicher Wert wie im Feld SignatureAlgorithm
- **Issuer**
  - entspricht Subject (da Root-CA-Zertifikat)
- **Validity**
  - Gültigkeitszeit des Zertifikats: (siehe Kapitel 6.3.2)
- **Subject**
  - Namensschema Zertifikat C(Root): (siehe Tabelle 10)
- **SubjectPublicKeyInfo**
  - Algorithm:
    - id-ecPublicKey, OID: 1.2.840.10045.2.1
    - namedCurve: brainPoolP384r1, OID: 1.3.36.3.3.2.8.1.11
  - subjectPublicKey:
    - ECPoint (uncompressed)
  - öffentlicher Schlüssel des Zertifikats

X.509-Extensions von C(Root)

- **SubjectKeyIdentifier**
  - OID: 2.5.29.14
  - Kritisch: nein
  - zur Identifikation eines Zertifikats mit einem bestimmten öffentlichen Schlüssel
- **KeyUsage**
  - OID: 2.5.29.15
  - Kritisch: ja
  - spezifiziert, wofür der zertifizierte Schlüssel verwendet werden darf
  - Gesetzte Bits
    - KeyCertSign
    - cRLSign

- **BasicConstraints**
  - OID: 2.5.29.19
  - Kritisch: ja
  - Gibt an, ob es sich um ein EE- oder CA-Zertifikat handelt.
  - CA-Flag: true
  - pathLengthConstraint: 1

SignatureAlgorithm von C(Root)

- Signaturalgorithmus
  - ECDSAwithSHA384 (1.2.840.10045.4.3.3)

SignatureValue von C(Root)

- ECDSA-Signatur des Zertifikats im ANSI X9.62-Format

D.2 TSE-CA Sub-CA-Zertifikat C(Sub-CA)

TBSCertificate von C(Sub-CA)

- **Version**
  - „v3“
- **SerialNumber**
  - zufällig
  - bitLength (Entropie): 126 Bit
- **Signature**
  - gleicher Wert wie im Feld SignatureAlgorithm
- **Issuer**
  - entspricht dem Subject des Issuer-Zertifikats TSE-CA Root-CA-Zertifikat (siehe Kapitel A.1)
- **Validity**
  - Gültigkeitszeit des Zertifikats: (siehe Kapitel 6.3.2)
- **Subject**
  - Namensschema der Sub-CA-Zertifikate: (siehe Tabelle 11)
- **SubjectPublicKeyInfo**
  - Algorithm:
    - id-ecPublicKey, OID: 1.2.840.10045.2.1
    - namedCurve: brainPoolP384r1, OID: 1.3.36.3.3.2.8.1.11
  - subjectPublicKey:
    - ECPoint (uncompressed)
  - öffentlicher Schlüssel des Zertifikats

X.509-Extensions von C(Sub-CA)

- **AuthorityKeyIdentifier**
  - OID: 2.5.29.35
  - Kritisch: nein
  - keyIdentifier
  - zur Unterscheidung verschiedener öffentlicher Schlüssel desselben Zertifikats-Issuers
- **CRLDistributionPoints**
  - OID:2.5.29.31
  - Kritisch: nein
  - Verteilpunkt für Sperrlisten
  - uniformResourceIdentifier: beinhaltet URL, unter der die Sperrliste der ausstellenden CA abgerufen werden kann.
- **SubjectKeyIdentifier**

- OID: 2.5.29.14
- Kritisch: nein
- zur Identifikation eines Zertifikats mit einem bestimmten öffentlichen Schlüssel

KeyUsage

- OID: 2.5.29.15
- Kritisch: ja
- spezifiziert, wofür der zertifizierte Schlüssel verwendet werden darf.
- Gesetzte Bits
  - KeyCertSign
  - cRLSign

CertificatePolicies

- OID: 2.5.29.32
- Kritisch: nein
- enthält Informationen über die CP, nach der das Zertifikat ausgestellt wurde und gibt die Bezugsquelle der CP an
- Policy-OID: 1.3.6.1.4.1.7879.13.41
- CPSuri im Feld policyQualifiers: beinhaltet URL, unter der die CPS abgerufen werden kann.

BasicConstraints

- OID: 2.5.29.19
- Kritisch: ja
- Gibt an, ob es sich um ein EE- oder CA-Zertifikat handelt.
- CA-Flag: true
- pathLengthConstraint: 0

AuthorityInfoAccess

- OID: 1.3.6.1.5.5.7.1.1
- Kritisch: nein
- Gibt Formate und Bezugspunkte für weitere Informationen an, die von der CA bereitgestellt werden
- caIssuers: wird gesetzt und verweist auf das ausstellende Zertifikat

SignatureAlgorithm von C(Sub-CA)

Signaturalgorithmus

- ECDSAwithSHA384 (1.2.840.10045.4.3.3)

SignatureValue von C(Sub-CA)

ECDSA-Signatur des Zertifikats im ANSI X9.62-Format

D.3 TSE-CA End Entity-Zertifikate für OCSP-Responder

Dies betrifft die Zertifikate $C_{OCSP\text{-}S}$(Sub-CA).

TBSCertificate von $C_{OCSP\text{-}S}$(Sub-CA)

- **Version**
  - „v3“
- **SerialNumber**
  - zufällig
  - bitLength (Entropie): 126 Bit
- **Signature**
  - gleicher Wert wie im Feld SignatureAlgorithm
- **Issuer**
  - entspricht dem Subject des Issuer-Zertifikats für den OCSP-Responder der Sub-CA: TSE-CA Sub-CA-Zertifikat (siehe Kapitel A.2)
- **Validity**
  - Gültigkeitszeit des Zertifikats: (siehe Kapitel 6.3.2)
- **Subject**
  - Namensschema Zertifikat $C_{OCSP\text{-}S}$(Sub-CA): (siehe Tabelle 12)
- **SubjectPublicKeyInfo**
  - Algorithm:
    - id-ecPublicKey, OID: 1.2.840.10045.2.1
    - namedCurve: brainPoolP384r1, OID: 1.3.36.3.3.2.8.1.11
  - subjectPublicKey:
    - ECPoint (uncompressed)
  - öffentlicher Schlüssel des Zertifikats

X.509-Extensions von $C_{OCSP\text{-}S}$(Sub-CA)

- **AuthorityKeyIdentifier**
  - OID: 2.5.29.35
  - Kritisch: nein
  - keyIdentifier
  - zur Unterscheidung verschiedener öffentlicher Schlüssel desselben Zertifikats-Issuers
- **SubjectKeyIdentifier**
  - OID: 2.5.29.14
  - Kritisch: nein
  - zur Identifikation eines Zertifikats mit einem bestimmten öffentlichen Schlüssel
- **KeyUsage**
  - OID: 2.5.29.15

- Kritisch: ja
- spezifiziert, wofür der zertifizierte Schlüssel verwendet werden darf
- Gesetzte Bits
  - DigitalSignature

- **ExtendedKeyUsage**
  - OID: 2.5.29.37
  - Kritisch: nein
  - Value: 1.3.6.1.5.5.7.3.9 (OCSP Signing)
- **OCSP-NoCheck**
  - OID: 1.3.6.1.5.5.7.48.1.5
  - Kritisch: nein
- **CertificatePolicies**
  - OID: 2.5.29.32
  - Kritisch: nein
  - Enthält Informationen über die CP, nach der das Zertifikat ausgestellt wurde, und gibt die Bezugsquelle der CP an
  - Policy-OID: 1.3.6.1.4.1.7879.13.41
  - CPSuri im Feld policyQualifiers: beinhaltet URL, unter der die CPS abgerufen werden kann.
- **BasicConstraints**
  - OID: 2.5.29.19
  - Kritisch: nein
  - Gibt an, ob es sich um ein EE- oder CA-Zertifikat handelt.
  - CA-Flag: false
  - pathLengthConstraint: nicht gesetzt
- **AuthorityInfoAccess**
  - OID: 1.3.6.1.5.5.7.1.1
  - Kritisch: nein
  - Gibt Formate und Bezugspunkte für weitere Informationen an, die von der CA bereitgestellt werden
  - caIssuers: wird gesetzt und verweist auf das ausstellende Zertifikat

SignatureAlgorithm von $C_{OCSP\text{-}S}$(Sub-CA)

- Signaturalgorithmus
  - ECDSAwithSHA384 (1.2.840.10045.4.3.3)

SignatureValue von $C_{OCSP\text{-}S}$(Sub-CA)

- ECDSA-Signatur des Zertifikats im ANSI X9.62-Format

D.4 TSE-CA End Entity-Zertifikate für TSEs C_{SIG}(TSE)

TBSCertificate von C_{SIG}(TSE)

- **Version**
  - „v3“
- **SerialNumber**
  - zufällig
  - bitLength (Entropie): 126 Bit
- **Signature**
  - gleicher Wert wie im Feld SignatureAlgorithm
- **Issuer**
  - entspricht dem Subject des Issuer-Zertifikats TSE-CA Sub-CA-Zertifikat (siehe Kapitel A.2)
- **Validity**
  - Gültigkeitszeit des Zertifikats: (siehe Kapitel 6.3.2)
- **Subject**
  - Namensschema Zertifikat C_{SIG}(TSE): (siehe Tabelle 13)
- **SubjectPublicKeyInfo**
  - Algorithm:
    - id-ecPublicKey, OID: 1.2.840.10045.2.1
    - namedCurve: brainPoolP384r1, OID: 1.3.36.3.3.2.8.1.11
  - subjectPublicKey:
    - ECPoint (uncompressed)
  - öffentlicher Schlüssel des Zertifikats
- **IssuerUniqueID**
  - entfällt
- **SubjectUniqueID**
  - entfällt

X.509-Extensions von C_{SIG}(TSE)

- **AuthorityKeyIdentifier**
  - OID: 2.5.29.35
  - Kritisch: nein
  - keyIdentifier
  - zur Unterscheidung verschiedener öffentlicher Schlüssel desselben Zertifikats-Issuers

- **CRLDistributionPoints**
  - OID:2.5.29.31
  - Kritisch: nein
  - Verteilpunkt für Sperrlisten
  - uniformResourceIdentifier: beinhaltet URL, unter der die Sperrliste der ausstellenden (Sub-) CA abgerufen werden kann.
- **SubjectKeyIdentifier**
  - OID: 2.5.29.14
  - Kritisch: nein
  - zur Identifikation eines Zertifikats mit einem bestimmten öffentlichen Schlüssel
- **KeyUsage**
  - OID: 2.5.29.15
  - Kritisch: ja
  - spezifiziert, wofür der zertifizierte Schlüssel verwendet werden darf
  - Gesetzte Bits
    - DigitalSignature
- **CertificatePolicies**
  - OID: 2.5.29.32
  - Kritisch: nein
  - Enthält Informationen über die CP, nach der das Zertifikat ausgestellt wurde und gibt die Bezugsquelle der CP an
  - Policy-OID: 1.3.6.1.4.1.7879.13.41
  - CPSuri im Feld policyQualifiers: beinhaltet URL, unter der die CPS abgerufen werden kann.
- **BasicConstraints**
  - OID: 2.5.29.19
  - Kritisch: ja
  - Gibt an, ob es sich um ein EE- oder CA-Zertifikat handelt.
  - CA-Flag: false
  - pathLengthConstraint: nicht gesetzt
- **AuthorityInfoAccess**
  - OID: 1.3.6.1.5.5.7.1.1
  - Kritisch: nein
  - Gibt Formate und Bezugspunkte für weitere Informationen an, die von der CA bereitgestellt werden
  - Optional - sofern genutzt - OCSP-URL

- o caIssuers: beinhaltet URL, unter der die Sperrliste der ausstellenden CA abgerufen werden kann.

SignatureAlgorithm von C_{SIG}(TSE)

- Signaturalgorithmus (nach BSI-TR-03116-5)
  - o ECDSAwithSHA384 (1.2.840.10045.4.3.3)
  - o SHA-384
  - o BrainpoolP384r1

SignatureValue von C_{SIG}(TSE)

- ECDSA-Signatur des Zertifikats im ANSI X9.62-Format

Literaturverzeichnis

AO	Abgabenordnung in der Fassung der Bekanntmachung vom 1. Oktober 2002 (BGBl. I S. 3866; 2003 I S. 61), die zuletzt durch Artikel 10 des Gesetzes vom 11. Juli 2019 (BGBl. I S. 1066) geändert worden ist
BSI-KLC-SR	BSI, Key Lifecycle Security Requirements, Version 1.0.2, 02.11.2018
BSI-CC-PP-0104-2019	BSI, Common Criteria Protection Profile: Cryptographic Service Provider (CSP), Version 0.9.8
BSI-CC-PP-0105-2019	BSI, Common Criteria Protection Profile: Security Module Application for Electronic Record-keeping Systems (SMAERS), Version 0.7.5
BSI-CC-PP-0107-2019	BSI, Common Criteria Protection Profile: Protection Profile Configuration Cryptographic Service Provider – Time Stamp Service and Audit (PPC-CSP-TS-Au), Version 0.9.5
BSI-CC-PP-0108-2019	BSI, Common Criteria Protection Profile: Protection Profile Configuration Cryptographic Service Provider – Time Stamp Service, Audit and Clustering (PPC-CSP-TS-Au-Cl), Version 0.9.4
BSI-CC-PP-0111-2019	BSI, Common Criteria Protection Profile: Cryptographic Service Provider Light (CSP-Light), Version 0.9.8
BSI-STD-200-1	BSI-Standard 200-1: Managementsysteme für Informationssicherheit (ISMS), Version 1.0, Oktober 2017,
BSI-STD-200-2	BSI-Standard 200-2: IT-Grundschutz-Methodik, Version 1.0, Oktober 2017,
BSI-STD-200-3	BSI-Standard 200-3: Risikomanagement, Version 1.0, Oktober 2017,
BSI-STD-100-4	BSI-Standard 100-4: Notfallmanagement, Version 1.0, November 2008
BSI-TR-02102-1	BSI, Technische Richtlinie BSI TR-02102, Kryptographische Verfahren: Empfehlungen und Schlüssellängen, Stand 2019
BSI-TR-03111	BSI, Technical Guideline BSI TR-03111, Elliptic Curve Cryptography, Version 2.1, 1.6.2018
BSI-TR-03116-4	BSI, Technische Richtlinie BSI TR-03116, Kryptographische Vorgaben für Projekte der Bundesregierung, Teil 4: Kommunikationsverfahren in Anwendungen, Stand 2019
BSI-TR-03116-5	BSI, Technische Richtlinie BSI TR-03116, Kryptographische Vorgaben für Projekte der Bundesregierung, Teil 5: Anwendungen der Secure Element API, Stand 2019
BSI-TR-03145-1	BSI, Technical Guideline BSI TR.03145, Secure CA operation, Part 1: Generic requirements for Trust

	Centers instantiating as Certification Authority (CA) in a Public-Key Infrastructure (PKI) with security level 'high', Version 1.1,
BSI-TR-03151	BSI, Technical Guideline BSI TR-03151, Secure Element API (SE API), Version 1.0.1, 20. December 2018
BSI-TR-03153	BSI, Technische Richtlinie BSI TR-03153, Technische Sicherheitseinrichtung für elektronische Aufzeichnungssysteme, Version 1.0.1, 20. Dezember 2018
ISO 3116 ALPHA-2	ISO: Codes for countries and their subdivisions, ALPHA-2 coding,
ISO/IEC 27001	ISO/IEC 27001:2013, Information technology — Security techniques — Information security management systems — Requirements, ISO/IEC JTC 1/SC 27, 2013
CC1	Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, CCMB-2017-04-001, Version 3.1, Revision 5, April 2017
CC2	Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2017-04-002, Version 3.1, Revision 5, April 2017
CC3	Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components; CCMB-2017-04-003, Version 3.1, Revision 5, April 2017
KassenSichV	Kassensicherungsverordnung vom 26. September 2017 (BGBl. I S. 3515)
RFC 2119	IETF: Key words for use in RFCs to Indicate Requirements Levels,
RFC 3647	IETF: Internet X.509 Public Key Infrastructure, Certificate Policy and Certification Practices Framework
RFC 5280	IETF: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, 2008
RFC 6960	IETF: X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP, 2013

Tabelle 16: Referenzen

Stichwort- und Abkürzungsverzeichnis

Abkürzung	Begriff
ASP	Ansprechpartner (des Unternehmens)
BSI	Bundesamt für Sicherheit in der Informationstechnik
CA	Certificate Authority
CC	Common Criteria
CER	Canonical Encoding Rules (Format zur Zertifikatscodierung)
CN	Common Name
CP	Certificate Policy
CPS	Certificate Practice Statement
CRL	Certificate Revocation List (Zertifikatssperrliste)
DRG	(Funktionsklasse für Zufallsgeneratoren)
DN	Distinguished Name
ENC	Encryption / Verschlüsselung
HSM	Hardware Sicherheitsmodul
ISMS	Information Security Management System
ISO	International Organization of Standardization
KEK	Key Encyption Key
KM	Krypto Modul
TSE-PKI	KassenSichV – Public Key Infrastructure
OCSP	Online Certificate Status Protocol
PKI	Public Key Infrastructure
PP	Protection Profile
RA	Registration Authority
SHA	Secure Hash Algorithm
S/MIME	Secure/Multipurpose Mail Extension
TH	TSE-Hersteller
TLS	Transport Layer Security (Protokoll zur Verschlüsselung einer Datenüber-tragung)
TR	Technische Richtlinie
TSE	Technische Sicherheitseinrichtung
X.509	ITU-T-Standard für eine Public-Key-Infrastruktur

Tabelle 17: Abkürzungen