Certificate Policy der DARZ.CA

Inhalt

Certificate Policy der DARZ.CA

Dokumenteninformationen

Bearbeitungsvermerk

	Name und Funktion	Version	Datum	Unterschrift
Erstellt von:	Franziska Gimbel	2.8	28.05.2020	
Geprüft von:	Jürgen Henzler	2.8	28.05.2020	
Genehmigt von:	Jürgen Henzler	2.8	28.05.2020	
Rücknahme durch:				

Änderungshistorie

Datum	Bearbeiter	Version	Änderungsgrund / Änderungen
23.06.2017	Jan Keppler	0.1	Initialisierung
17.08.2017	Lisa Weinand	1.0	Anpassung der Dokumentenstruktur
11.04.2018	Rüdiger Heusel Andreas Schneider	2.0 2.1 2.2	* Korrekturen gemäß „Empfehlungen und Abweichungen – Audit TR 03145 – DARZ GmbH“ vom 14.08.2017 entsprechend Anforderung des BSI * Einfügen der OID der DARZ GmbH * Überprüfung und Anpassung an die Certificate Policy der Smart Metering PKI Version 1.1.1 Datum: 09.08.2017 unter Berücksichtigung des Change Log des BSI (ChangeLog SM-Test-PKI Aktualisiert: 2018-02-21 und ChangeLog SM-Root-CA Aktualisiert: 2018-03-01) * Ersetzen des Begriffes DARZ1-PKI durch DARZ.CA
04.05.2018	Rüdiger Heusel Andreas Schneider	2.3	* Korrekturen gemäß SM-PKI der Root
24.05.2018	Rüdiger Heusel Andreas Schneider	2.4	* Anpassung der CP an CP-SM-PKI (Rückmeldungen SM-PKI Root-CA I)
25.05.2018	Rüdiger Heusel Andreas Schneider	2.5	* Anpassung der CP an CP-SM-PKI (Rückmeldungen SM-PKI Root-CA II)
14.01.2020	Jürgen Henzler Franziska Gimbel	2.6	* Anpassung der CP an CP-SM-PKI (Rückmeldungen SM-PKI Root-CA III)
20.01.2020	Jürgen Henzler Franziska Gimbel	2.7 2.7.1 2.7.2	* Anpassung der CP an CP-SM-PKI (Rückmeldungen SM-PKI Root-CA III)
28.05.2020	Jürgen Henzler Franziska Gimbel	2.8	* Anpassung CP entsprechend der Empfehlungen im 2. Überwachungsaudit TR03145 (Kapitel 5.2.1 & 4.7)

Gleichstellungshinweis

In folgendem Dokument wird für die Beschreibung von Aufgaben, Funktionen oder Rollen aus Vereinfachungsgründen die männliche Schreibweise gewählt. Mit der gewählten Schreibweise werden in diesem Dokument alle Geschlechter angesprochen, denen Aufgaben, Funktionen oder Rollen zugeordnet werden, ohne eine Wertung ihres Geschlechts, ihrer physischen oder psychischen Fähigkeiten, oder eine sonstige Wertung vorzunehmen.

1. Einleitung

Die volatile Stromerzeugung aus erneuerbaren Energien erfordert es, Netze, Erzeugung und Verbrauch von verschiedenen Energien wie Strom oder Gas effizient und intelligent miteinander zu verknüpfen. Dabei muss die fluktuierende Stromerzeugung aus erneuerbaren Energien und der Stromverbrauch bedarfs- und verbrauchsorientiert durch intelligente Netze und technische Systeme ausbalanciert werden.

Zur Unterstützung dieses Ziels werden intelligente Messsysteme (Smart Metering Systems) eingesetzt, die dem Letztverbraucher eine höhere Transparenz über den eigenen Energieverbrauch bieten und die Basis dafür schaffen, seinen Energieverbrauch an die Verfügbarkeit von Energie anzupassen. Die zentrale Kommunikationseinheit des intelligenten Messsystems stellt das Smart Meter Gateway (SMGW oder im Folgenden auch Gateway genannt) in den Haushalten der Letztverbraucher dar. Diese Einheit trennt das Weitverkehrsnetz (WAN), d. h. das Netz zu den Backendsystemen von Smart Meter Gateway Administratoren (GWA) und externen Marktteilnehmern (EMT), von dem im Haushalt befindlichen Heimnetz (HAN) und den lokal angebundenen Zählern im metrologischen Netz (LMN). Die Hauptaufgaben des SMGW bestehen dabei in der technischen Separierung der angeschlossenen Netze, der sicheren Kommunikation in diese Netze, der Erfassung, Verarbeitung und Speicherung empfangener Messwerte verschiedener Zähler, der sicheren Weiterleitung der Messwerte an die Backendsysteme externer autorisierter Marktteilnehmer im WAN sowie der Verarbeitung von Administrationstätigkeiten durch den jeweiligen GWA.

Zur Absicherung der Kommunikation im WAN ist eine gegenseitige Authentisierung der Kommunikationspartner erforderlich. Die Kommunikation erfolgt dabei stets über einen verschlüsselten und integritätsgesicherten Kanal. Zudem werden Daten vom SMGW vor der Übertragung zur Integritätssicherung signiert und zur Gewährleistung des Datenschutzes für den Endempfänger verschlüsselt.

Damit die Authentizität und die Vertraulichkeit bei der Kommunikation der einzelnen Marktteilnehmer untereinander gesichert sind, wird eine Smart Metering Public Key Infrastruktur (SM-PKI) etabliert. Technisch wird der Authentizitätsnachweis der Schlüssel dabei über digitale X.509-Zertifikate aus der SM-PKI realisiert. Die Systemarchitektur der SM-PKI ist in der (TR-3109-4) spezifiziert. Sie wird in die folgenden drei Hierarchiestufen unterteilt:

- Die **Root-CA**, welche den hoheitlichen Vertrauensanker der SM-PKI darstellt.
- Die **Sub-CAs** die zur Zertifizierung von Endnutzerschlüsseln dienen
- Die **Endnutzer**, d.h. die SMGW, GWA, GWH und EMT. Diese Teilnehmer bilden die untere Ebene der SM-PKI und nutzen ihre Zertifikate zur Kommunikation miteinander und insbesondere zum Aufbau gesicherter Verbindungen zu den SMGW.

Die DARZ GmbH betreibt in diesem Kontext eine Sub-CA, die im Folgenden als **DARZ.CA** bezeichnet wird. Vor diesem Hintergrund entspricht die in diesem Dokument genannte Sub-CA der **DARZ.CA**.

Das vorliegende Dokument stellt die Zertifizierungsrichtlinie (CP) inkl. der Erklärung zum Zertifizierungsbetrieb (CPS) der **DARZ.CA** (Sub-CA der DARZ GmbH) dar und beinhaltet Sicherheitsvorgaben sowie Beschreibungen technischer, organisatorischer und rechtlicher Aspekte.

Die **DARZ.CA** CP/CPS unterwirft sich der CP-SM-PKI und beschreibt die Vorgaben der **DARZ.CA** und deren Umsetzung.

Die in der CP 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 SM-PKI Policy sind grundsätzlich als normativ anzusehen. Informative Kapitel werden explizit

am Anfang gekennzeichnet.

1.1 Überblick

Das Dokument richtet sich an alle Teilnehmer der SM-PKI und insbesondere an Hersteller (GWH), Administratoren (GWA) und weitere Teilnehmer (EMT), die Zertifikate der **DARZ.CA** nutzen oder benötigen.
Die Gliederung erfolgt nach dem Muster des Standards RFC 3647.

Die Verantwortlichkeit für die **DARZ.CA** obliegt der DARZ GmbH.

1.2 Name und Identifizierung des Dokuments

Identifikator	Wert
Titel	Certificate Policy und Certificate Practice Statement der DARZ.CA (Sub-CA der DARZ GmbH)
Version	2.7.2.
Datum	20.01.2020
OID	**1.3.6.1.4.1.51695.1.1**

1.3 PKI-Teilnehmer

1.3.1 Zertifizierungsstellen

DARZ.CA ist eine Instanz, welche von der Root-CA zur Ausstellung von Zertifikaten autorisiert wird und Zertifikate für ihre Kunden ausstellt.

Neben dem Wirksystem der DARZ.CA betreibt die DARZ GmbH für die DARZ GmbH auch die DARZ-Test.CA. Diese stellt für Testzwecke (z. B. Erst-Registrierung und zum Test systemkritischer Vorgänge, wie dem Wechsel des Vertrauensankers) die erforderlichen Funktionaltäten bereit. Die technische Infrastruktur der DARZ-Test.CA entspricht der Wirkumgebung der DARZ.CA. Beide Plattformen sind informationstechnisch voneinander getrennt. Die verwendeten Schlüssel sind in beiden Plattformen unterschiedlich.

Der Betreiber der DARZ.CA ist die DARZ GmbH, Julius-Reiber-Strasse 11, 64293 Darmstadt.

1.3.2 Registrierungsstellen

Die **DARZ.CA** verfügt über eine Registrierungsstelle (RA der **DARZ.CA**). Diese ist für die initialen Registrierungen, sowie die Folgeanträge der Endnutzer zuständig. Im Rahmen der initialen Registrierung wird eine zweifelsfreie Identifizierung des Antragsstellers und die Authentifizierung der PKI-Rolle und der Identitätsdaten der ausführenden Personen festgestellt.

Das Registrierungsverfahren ist in Abschnitt 3.2 dargestellt.

Die Grundlage für die Prozesse der RA bildet dieses Dokument sowie die Vorgaben der CP-SM-PKI.

1.3.3 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 Absicherung der Kommunikation verwenden.

1.3.3.1 SMGW

Bei einem SMGW handelt es sich um eine technische Komponente (Kommunikationseinheit eines intelligenten Messsystems, siehe (TR-03109-1), die von der DARZ.CA mit Zertifikaten ausgestattet werden kann, welche für die Durchführung der definierten Prozesse und Kommunikationsverbindungen benötigt werden. Ein SMGW wird immer von einem GWA verwaltet.

1.3.3.2 Gateway-Administrator

Ein Gateway-Administrator (GWA) ist für die Verwaltung der ihm zugeordneten SMGWs verantwortlich. Ein Gateway-Administrator (GWA) kann von der DARZ.CA Zertifikate erhalten, mit denen dieser insbesondere die Beantragung und Verwaltung der

Wirkzertifikate der SMGWs durchführen kann, die Administration der SMGWs durchführen kann und den Datenaustausch mit den anderen Teilnehmern der SM-PKI (z.B. EMT) absichern kann.

1.3.3.3 Gateway-Hersteller

Ein Hersteller von Gateway-Komponenten (GWH) kann von der DARZ.CA Zertifikate erhalten, mit denen dieser insbesondere die Prozesse zur Beantragung und Verwaltung von Gütesiegelzertifikaten für SMGWs durchführen kann.

1.3.3.4 Externer Marktteilnehmer

Ein externer Marktteilnehmer (EMT) kann von der DARZ.CA Zertifikate erhalten, mit denen dieser insbesondere mit den SMGWs sicher kommunizieren kann. Überdies kann der Datenaustausch mit den anderen Teilnehmern der SM-PKI (z.B. einem GWA) abgesichert werden.

Ein EMT, welcher ein SMGW nutzt, um über dieses nachgelagerte Gerät (Controllable Local Systems, CLS) anzusprechen, wird als aktiver EMT bezeichnet. Die entsprechenden Anwendungsfälle zur Steuerung von CLS an der HAN-Schnittstelle durch einen EMT sind in der (TR-03109-1) definiert.

Ein EMT, welcher keine nachgelagerten Geräte (CLSs) anspricht bzw. steuert, sondern nur Daten empfängt, um auf Basis dieser Informationen die eigenen Geschäftsprozesse fortzuführen, wird als passiver EMT bezeichnet.

Ein Unternehmen (muss nicht selbst EMT sein) kann die Abwicklung der Kommunikation mit den SMGWs inkl. dem zugehörigen Zertifikatsmanagement auch als Dienstleistung anbieten. Dieses Unternehmen würde somit das EMT-Frontend des Auftraggebers realisieren. Bei dem Aufbau einer solchen Systemstruktur muss darauf geachtet werden, dass die Übermittlung der Daten von dem Dienstleister zu dem Auftraggeber ein vergleichbares Sicherheitsniveau zu den in der (TR-03116-3) definierten Sicherheitsmechanismen einhält.

Betreut ein solcher Dienstleister mehrere Auftraggeber, so muss eine klare Trennung zwischen den Auftraggebern erfolgen. Die Trennung kann durch technische und/oder organisatorische Maßnahmen realisiert erfolgen.

1.3.4 Zertifikatsnutzer

Zertifikatsnutzer im Sinne dieser DARZ.CA Policy sind alle natürlichen und juristischen Personen bzw. technischen Komponenten, die Zertifikate aus der SM-PKI, insbesondere auch Zertifikate aus der DARZ.CA, für die Erledigung von Geschäftsprozessen/Aufgaben verwenden.

1.3.5 Andere Teilnehmer

Andere Teilnehmer - wie beispielsweise Endverbraucher – welche keine Verpflichtungen im Rahmen der DARZ.CA Policy eingegangen sind, sind nicht Bestandteil dieser DARZ.CA Policy und werden daher nicht berücksichtigt.

1.4 Verwendung von Zertifikaten

1.4.1 Erlaubte Verwendung von Zertifikaten

Die im Rahmen der DARZ.CA ausgestellten Zertifikate dürfen innerhalb der SM-PKI für alle Verfahren genutzt werden, die von den im Zertifikat enthaltenen Schlüsselverwendungszwecken ermöglicht werden. Die Anwendungsfälle für den Einsatz der Schlüssel und Zertifikate sind in der (CP-SM-PKI) und (TR-3109-4) beschrieben.
Die DARZ.CA erstellt Zertifikats-Sets (TLS, ENC, SIG) für die SM-PKI Teilnehmer GWA, GWH, SMGW sowie EMT und das DARZ.CA CA-TLS Zertifikat.
Teilnehmer bzw. Zertifikatinhaber sind selbst für die Nutzung in den Anwendungsprogrammen zuständig, sowie für die Prüfung, ob die damit möglichen Anwendungen deren Sicherheitsanforderungen genügen.

1.4.2 Verbotene Verwendung von Zertifikaten

Die private Verwendung der Zertifikate ist untersagt.
Geschäftspartner dürfen die Zertifikate nicht ohne die Genehmigung der DARZ.CA über die in Ziffer 1.4.1 beschriebene Verwendung hinaus im Zusammenhang mit Geschäftsangelegenheiten mit Dritten nutzen.

1.5 Administration der Policy

1.5.1 Pflege der Policy

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

Organisation	DARZ GmbH
Abteilung	IT-Services
Adresse	Julius-Reiber-Straße 11, D-64293 Darmstadt
Telefon	+49 6151 8762-100
E-Mail	info@da-rz.de
Webseite	www.da-rz.de

Diese CP wird im Intranet und auf der Homepage der DARZ GmbH veröffentlicht.
Eine Weitergabe an andere Organisationen ist vorgesehen, damit eine unabhängige Überprüfung der Arbeitsweise der DARZ.CA möglich ist.

1.5.2 Zuständigkeit für das Dokument

Die Verwaltung dieses Dokuments erfolgt durch die DARZ GmbH. Jede aktualisierte Version des Dokuments wird den Anwendern unverzüglich über die angegebene Internetseite (siehe 1.5) zur Verfügung gestellt.

1.5.3 Ansprechpartner/Kontaktperson

Organisation	DARZ GmbH
Abteilung	IT-Services
Person	Jürgen Henzler
Adresse	Julius-Reiber-Straße 11, D-64293 Darmstadt
Telefon	+49 6151 8762-100
E-Mail	j.henzler@da-rz.de
Webseite	www.da-rz.de

1.5.4 Zuständiger für die Anerkennung eines CPS

Diese CP wird durch die verantwortliche Organisation (s. Kap. 1.5.1) überprüft und ist Bestandteil der Betriebsdokumentation der DARZ.CA.

1.5.5 CPS-Aufnahmeverfahren

Entfällt.

2. Verantwortlichkeit für Veröffentlichungen und Verzeichnisse

2.1 Verzeichnisse

Die DARZ GmbH stellt die Informationen zur DARZ.CA auf der Homepage
− unter https://www.da-rz.de/de/ueber-darz/unternehmen/PKI/ sowie im Intranet (Zugriff nur für Beschäftigte der DARZ GmbH sowie deren externe Mitarbeiterinnen und Mitarbeiter) zur Verfügung.

2.2 Veröffentlichung von Informationen zur Zertifikatserstellung

Die DARZ GmbH veröffentlicht folgende Informationen:

- Kontaktdaten der DARZ.CA
- DARZ.CA-Zertifikate mit Hash (SHA 256)
- Parameter zur Einrichtung eines Zugriffs auf die Sperrliste bzw. das LDAP-Verzeichnis
- Formulare
- Erläuterungen zum Sperrverfahren
- Zertifizierungsrichtlinie (CP)
- Hinweis zur erfolgreichen Teilnahme am Testsystem

2.3 Zeitpunkt und Häufigkeit der Veröffentlichungen

Für die Veröffentlichung von DARZ.CA-Zertifikaten, Sperrlisten sowie CP gelten die folgenden Intervalle:

Alle von der DARZ.CA ausgestellten Zertifikate	Unmittelbar nach Ausstellung
Sperrlisten	Nach Suspendierungen/Sperrungen, sonst turnusmäßig
CP	Nach Erstellung bzw. Aktualisierung

Nach Ablauf der im Zertifikat eingetragenen Gültigkeit wird der Eintrag aus der Sperrliste entfernt.

2.4 Zugriffskontrollen auf Verzeichnisse

Der lesende Zugriff auf die unter den Ziffern 2.1 und 2.2 aufgeführten Informationen ist nicht eingeschränkt. Der schreibende Zugriff liegt im Verantwortungsbereich der DARZ.CA.

3. Identifizierung und Authentifizierung

3.1 Regeln für die Namensgebung

3.1.1 Arten von Namen

Der Name der ausgestellten Zertifikate (Distinguished Name = DN) richtet sich nach den Vorgaben des Standards X.509 und dem Namensschema gemäß Anhang A der CP-SM-PKI.

3.1.2 Notwendigkeit für aussagefähige Namen

Die Angaben der Zertifikatsinhaber werden gemäß den Anforderungen aus Kapitel 3.1.1 der CP-SM-PKI in die Zertifikate aufgenommen.

3.1.3 Anonymität oder Pseudonymität von Zertifikatsnehmern

Anonymität oder Pseudonymität in Namen von Zertifikaten ist nicht erlaubt.

3.1.4 Eindeutigkeit von Namen

Die Angaben der Zertifikatsinhaber werden gemäß den Anforderungen aus Kapitel 3.1.1 in die Zertifikate der DARZ.CA aufgenommen. Eine Namensgleichheit (gleicher CN bei unterschiedlichem Zertifikatsnehmer) wird durch die DARZ.CA verhindert, entsprechend vergibt die DARZ.CA einen CN NICHT mehrfach. Sollten zwei oder mehr Zertifikatsnehmer der DARZ.CA den gleichen CN wünschen, wird dieser Konflikt gelöst. Es behält der Teilnehmer seinen CN, der zuerst sein initiales Zertifikat mit diesem CN von der DARZ.CA erhalten hat. Der oder die anderen Zertifikatsnehmer lassen sich ein Zertifikat mit einem anderen CN ausstellen, um an der DARZ.CA teilnehmen zu dürfen.

3.1.5 Anerkennung, Authentifizierung und die Rolle von Markennamen

Im Rahmen der Beantragung von Zertifikaten für Geschäftspartner dürfen nur solche Marken oder Warenzeichen als Teil des Zertifikatseintrags für die im Antrag anzugebende Firma bzw. Behörde verwendet werden, zu deren Verwendung diese berechtigt sind. Diese Berechtigung wird jedoch bei der Registrierung nicht geprüft.
Die DARZ.CA bietet insbesondere keine Prozeduren zur Auflösung von Markenstreitigkeiten an. Diese sind zwischen den daran beteiligten Unternehmen ggf. durch markenrechtliche oder wettbewerbsrechtliche Maßnahmen im Zivilrechtsweg zu lösen. Falls der DARZ.CA ein rechtskräftiges Urteil vorgelegt wird, das die Unrechtmäßigkeit der Verwendung einer Marke oder eines Warenzeichens feststellt, wird das Zertifikat gesperrt.

3.2 Initiale Überprüfung zur Teilnahme

3.2.1 Methoden zur Überprüfung bzgl. Besitz des privaten Schlüssels

Zum Nachweis des Besitzes des privaten Schlüssels beinhaltet ein Zertifikatsrequest gemäß (TR-03109-4) eine sogenannte innere Signatur.

Hierdurch wird bei der Antragsprüfung durch Verifikation der inneren Signatur mit dem im Zertifikatsrequest enthaltenen zugehörigen öffentlichen Schlüssel durch die DARZ.CA geprüft, dass der Antragsteller im Besitz des privaten Schlüssels ist.

3.2.2 Authentifizierung von Organisationszugehörigkeiten

3.2.2.1 EMT

Zur Aufnahme eines neuen EMT in die **DARZ.CA** wird das Unternehmen durch Registration Authority (RA) der **DARZ.CA** authentifiziert. Notwendige Unterlagen und Daten für die Registrierung sind:

- Antragsschreiben zur Ausgabe eines EMT-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)
- Bei der Beauftragung eines Dienstleisters für den Betrieb des EMT legt der Betreiber eine Bestätigung des Unternehmens vor, die den Dienstleister zur Beantragung und zum Betrieb für den EMT berechtigt.
- Bestätigung der Geschäftsführung des Unternehmens bzw. der Leitung der Institution, in der der Vertreter des Unternehmens berechtigt wird, den Antrag für den EMT 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 EMT)) inklusive der zur Verifikation erforderlichen Zertifikatskette.

- Erklärung zur Nutzung des EMT-Zertifikats
  - Aus der Erklärung wird nachvollzogen, welche Funktionen und Aufgabe ein EMT wahrnehmen will. Es geht daraus insbesondere hervor, ob es sich um einen aktiven oder passiven EMT handelt.
- Erklärung zur Einhaltung der Sicherheitsvorgaben aus der DARZ.CA Policy.
  - Der passive EMT reicht eine Erklärung zur Einhaltung der Sicherheitsvorgaben aus dieser DARZ.CA Policy mit ein. Die Sicherheitsvorgaben bestehen darin, dass der passive EMT über ein Sicherheitskonzept verfügt (s. Tabelle 15 der CP-SM-PKI).
  - Der aktive EMT erbringt den Nachweis des sicheren Betriebs gemäß den Vorgaben zu den Anforderungen für die Teilnahme an der **DARZ.CA** (s. Tabelle 15 der CP-SM-PKI).
- Der Hashwert (SHA 256) des initialen Zertifikatsrequest-Pakets für das Signatur (C_{Sig}(EMT)), das Verschlüsselungs- (C_{Enc}(EMT)) und das TLS-Zertifikat (C_{TLS}(EMT)) des EMT (gemäß (TR-03109-4)) wird in gedruckter Form inklusive der Information zum Format der Darstellung mit der Bestätigung durch die Unterschrift des Bevollmächtigten vorgelegt. Der Hashwert wird dabei über die binär-codierte Request-Datei gebildet, welche das Zertifikatsrequest-Paket gemäß (TR-03109-4) enthält, und als base64-codierter Ausdruck in diesem Prozess verwendet.
- Bestätigung der erfolgreichen Test-Teilnahme
  - Vor der initialen Identifizierung und Authentifizierung ist die Registrierung, Zertifikatsbeantragung-, -erneuerung und -sperrung von EMT-Zertifikaten unterhalb der **DARZ-Test.CA** (siehe Abschnitt 1.3.1) erfolgreich erprobt worden. Die erfolgreiche Teilnahme wird von einem Ansprechpartner der **DARZ-Test.CA** per signierter E-Mail bestätigt.

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

3.2.2.2 GWA

Zur Aufnahme eines neuen GWA in die **DARZ.CA** wird das Unternehmen authentifiziert und mindestens zwei bevollmächtigte Vertreter des GWA werden persönlich bei der Registration Authority (RA) der **DARZ.CA** identifiziert und authentifiziert. Der Ortstermin wird durch den Ansprechpartner (oder seine interne Vertretung) der **DARZ.CA** (s. Kapitel 1.5.3 und Kapitel 4.1.2) koordiniert und abgestimmt.

Notwendige Unterlagen und Daten für die Registrierung sind:

- Antragsschreiben zur Ausgabe eines GWA-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 der Geschäftsführung des Unternehmens bzw. der Leitung der Institution, in der der Vertreter des Unternehmens berechtigt wird, den Antrag für den GWA 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 GWA)) inklusive der zur Verifikation erforderlichen Zertifikatskette
- Erklärung zur Einhaltung der Sicherheitsvorgaben aus dieser DARZ.CA Policy

- Nachweise über die Einhaltung der Vorgaben zu den Anforderungen für die Teilnahme an der **DARZ.CA** (s. Tabelle 15 der CP-SM-PKI)

- Bestätigung der erfolgreichen Testteilnahme
  - Vor der initialen Identifizierung und Authentifizierung ist die Registrierung, Zertifikatsbeantragung-, -erneuerung und -sperrung von GWA- und SMGW-Zertifikaten unterhalb der **DARZ-Test.CA** (siehe Abschnitt 1.3.1) erfolgreich erprobt worden. Die erfolgreiche Teilnahme wird von einem Ansprechpartner der**DARZ-Test.CA** per signierter E-Mail bestätigt.
- Der Hashwert (SHA 256) des initialen Zertifikatsrequest-Pakets für das Signatur-(C_{Sig}(GWA)), das Verschlüsselungs-(C_{Enc}(GWA)) und das TLS- Zertifikat (C_{TLS}(GWA)) des GWA (gemäß (TR-03109-4)) wird in gedruckter Form inklusive der Information zum Format der Darstellung mit der Bestätigung durch die Unterschrift des Bevollmächtigten vorgelegt. Der Hashwert wird dabei über die binär-codierte Request-Datei gebildet, welche das Zertifikatsrequest-Paket gemäß (TR-03109-4) enthält, und als base64-codierter Ausdruck in diesem Prozess verwendet. Die eigentlichen Zertifikatsrequests können zusätzlich im Rahmen dieses Termins als Dateien übergeben.
  - Es wird empfohlen die Zertifikatsrequests vorab der **DARZ.CA** zuzusenden, so dass vor dem Termin eine Überprüfung auf Konformität erfolgen kann.

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

3.2.2.3 GWH

Zur Aufnahme eines neuen GWH in die **DARZ.CA** wird das Unternehmen authentifiziert und mindestens zwei bevollmächtigte Vertreter des GWH persönlich bei der Registration Authority (RA) der **DARZ.CA** identifiziert und authentifiziert.
Der Ortstermin wird durch den Ansprechpartner (oder seinen interne Vertretung) der **DARZ.CA** (s. Kapitel 1.5.3 und Kapitel 4.1.2) koordiniert und abgestimmt.

Notwendige Unterlagen und Daten für die Registrierung sind:

- Antragsschreiben zur Ausgabe eines GWH 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 der Geschäftsführung des Unternehmens bzw. der Leitung der Institution, in der der Vertreter des Unternehmens berechtigt wird, den Antrag für den GWH 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 GWH)) inklusive der zur Verifikation erforderlichen Zertifikatskette
- Erklärung zur Einhaltung der Sicherheitsvorgaben aus dieser DARZ.CA Policy
  - Zusätzlich wird durch den GWH der Nachweis über den sicheren Betrieb gemäß den Vorgaben zu den Anforderungen für die Teilnahme an der DARZ.CA (s. Tabelle 15 der CP-SM-PKI) vorgelegt.
- Bestätigung der erfolgreichen Testteilnahme
  - Vor der initialen Identifizierung und Authentifizierung ist die Registrierung, Zertifikatsbeantragung-, -erneuerung und -sperrung von GWH und SMGW-Gütesiegelzertifikaten unterhalb der DARZ-Test.CA (siehe Kapitel 1.3.1) erfolgreich erprobt worden. Die erfolgreiche Teilnahme wird von einem Ansprechpartner der DARZ-Test.CA per signierter E-Mail bestätigt.
- Der Hashwert (SHA 256) des initialen Zertifikatsrequest-Pakets für das Signatur-(C_{Sig}(GWH)), das Verschlüsslungs-(C_{Enc}(GWH)) und das TLS-Zertifikat(C_{TLS}(GWH)) des GWH (gemäß (TR-03109-4)) wird in gedruckter Form inklusive der Information zum Format der Darstellung mit der Bestätigung durch die Unterschrift des Bevollmächtigten vorgelegt. Der Hashwert wird dabei über die binär-codierte Request-Datei gebildet, welche das Zertifikatsrequest-Paket gemäß (TR-03109-4) enthält, und als base64-codierter Ausdruck in diesem Prozess verwendet. Die eigentlichen Zertifikatsrequests KÖNNEN zusätzlich im Rahmen dieses Termins als Dateien übergeben werden.
  - Es wird empfohlen die Zertifikatsrequests vorab der **DARZ.CA** zuzusenden, so dass vor dem Termin eine Überprüfung auf Konformität erfolgen kann.

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

3.2.2.4 SMGW

Das SMGW kann selbst keine Zertifikate beantragen. Entsprechend beantragt eine dritte Partei stellvertretend für das SMGW die Zertifikate, siehe [TR03109-4]. Hierbei wird zwischen der Beantragung der Gütesiegelzertifikate und der Zertifikate für die Wirkumgebung unterschieden.

- Im Rahmen der Produktion werden durch den GWH gemäß den definierten und geprüften Prozessen (siehe Anforderungen in Kapitel 8.1) Gütesiegelzertifikate aufgebracht, welche in den nachfolgenden Prozessen zur Verifikation der Komponente verwendet werden.
- Bei der Integration des SMGWs in die Wirkumgebung müssen die Gütesiegelzertifikate vom GWA durch Wirkzertifikate ersetzt werden.

Aufbringen der Gütesiegelzertifikate
Grundvoraussetzung für das Aufbringen von Gütesiegel-Zertifikaten aus der **DARZ.CA** ist, dass der GWH bei der **DARZ.CA** registriert ist (siehe Abschnitt 3.2.2.3) und über gültige Zertifikate verfügt. Dabei werden die Anforderungen aus Tabelle 15 der CP-SM-PKI eingehalten.

Der GWH ist für die Einhaltung der Rahmenbedingungen verantwortlich und wird den Prozess gemäß den Vorgaben nachvollziehbar dokumentieren. Der GWH steuert das Sicherheitsmodul im SMGW so an, dass darin die drei Schlüsselpaare für die Gütesiegelzertifikate generiert werden. Das SMGW erzeugt daraus zusammen mit den eigenen Identifikationsdaten je Schlüsselpaar einen Zertifikatsrequest. Der GWH exportiert die drei Requests und bildet mit weiteren relevanten Daten daraus einen gemeinsamen Datensatz (Zertifikatsrequest-Paket, siehe (TR-03109-4). Das Zertifikatsrequest-Paket wird mit dem C_{Sig}(GWH) signiert (Autorisierungssignatur, vgl. (TR-03109-4)) und an die **DARZ.CA** über einen gesicherten Kommunikationskanal gesendet.

Die von der **DARZ.CA** produzierten Gütesiegelzertifikate werden von dem GWH geprüft und in das SMGW eingebracht.

Austausch der Gütesiegelzertifikate gegen Wirkzertifikate
Grundvoraussetzung für den Austausch der Gütesiegelzertifikate gegen Wirkzertifikate aus der **DARZ.CA** ist, dass der für das SMGW zuständige GWA bei der **DARZ.CA** registriert ist (siehe Abschnitt 3.2.2.2) und über gültige Zertifikate verfügt. Bei den SMGWs sind die Gütesiegelzertifikate im Rahmen der Personalisierung nach der (TR-03109-1) beim erstmaligen Kontakt mit dem GWA durch Wirkzertifikate zu ersetzen.

Zum Austausch der Gütesiegelzertifikate durch Wirkzertifikate kommuniziert das SMGW mit dem GWA:

- Aufbau eines sicheren TLS-Kanals zwischen SMGW und GWA unter Zuhilfenahme der aufgebrachten TLS-Gütesiegelzertifikate.
- Generierung neuer SMGW-Schlüsselpaare für TLS, Signatur und Verschlüsselung durch das Sicherheitsmodul des SMGW.
- Generierung der Zertifikatsrequests durch das SMGW gemäß (TR-03109-4) Die Zertifikatsrequests sind mit einer äußeren Signatur (siehe (TR-03109-4)) versehen, um die Authentizität des SMGW nachzuweisen.
- Senden der Zertifikatsrequests an den GWA. Der GWA prüft die Zertifikatsrequests. Neben der syntaktischen Prüfung des Requests werden auch die Gütesiegelzertifikate auf Gültigkeit geprüft. Nur wenn beide Prüfungen ein positives Ergebnis haben, werden für dieses SMGW Zertifikate beantragt.
- Der GWA erzeugt aus den drei Zertifikatsrequests und weiteren relevanten Daten ein Zertifikatsrequest-Paket (siehe (TR-03109-4)), welches dann mit dem C_{Sig}(GWA) signiert wird (Autorisierungssignatur, siehe (TR-03109-4)).Durch diese Signatur autorisiert der GWA die Beantragung.
- Das signierte Zertifikatsrequest-Paket wird über die per TLS-Kanal gesicherte Web-Service-Schnittstelle an die **DARZ.CA** gesendet.
- Die Authentizität des Zertifikatsrequest-Pakets wird durch die **DARZ.CA** geprüft (siehe (TR-03109-4)). Es werden ausschließlich für authentische SMGWs Zertifikate ausgestellt, deren Beantragung durch den zugehörigen GWA autorisiert wurde.
- Die Zertifikate werden von der **DARZ.CA** erzeugt und über die Web-Service-Schnittstelle an den GWA übertragen.
- Der GWA prüft die Zertifikate und installiert diese auf dem SMGW (vgl. (TR-03109-4)).

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 SMGWs, die durch den GWH bzw. GWA zu übermitteln sind.

3.2.4 Ungeprüfte Zertifikatsnehmerangaben

Die Registrierungsstelle überprüft beim EMT, GWA, und GWH die Angaben zum Zertifikatsnehmer im Zertifikatsrequest gegen die eingereichten Unterlagen auf Korrektheit (vergl. Kapitel 3.2.2).

3.2.5 Prüfung der Berechtigung zur Antragstellung

Siehe Kapitel 3.2

3.2.6 Kriterien für den Einsatz interoperierender Systeme/Einheiten

Nicht zutreffend.

3.2.7 Aktualisierung/Anpassung der Zertifizierungsinformationen der Teilnehmer

Die für die Teilnehmer an der **DARZ.CA** geforderten Zertifizierungen (s. Tabelle 15 der CP-SM-PKI) unterliegen in der Regel einem jährlichen Überwachungszyklus, für das z.B. ein Audit positiv abgeschlossen werden muss.

Die **DARZ.CA** muss von dem Zertifikatsnehmer rechtzeitig vor Ablauf der eingereichten Zertifikatsunterlagen über die Ergebnisse der Auditierung informiert und soweit ausgestellt auch das entsprechende Zertifikat zur Verfügung gestellt bekommen. Sollte der Teilnehmer die Zertifizierung nicht mehr erhalten, so wird das Zertifikat bzw. werden die Zertifikate aus der **DARZ.CA** gesperrt. Informationen über relevante Änderungen, die beispielsweise

- eine Erst-Zertifizierung (z.B. Wechsel vom passiven EMT zum aktiven EMT)
  oder
- eine Re-Zertifizierung (z. B. Wechsel des IT-Betriebs-Standorts)

erfordern, muss der Zertifikatsnehmer unverzüglich inklusive der entsprechenden Informationen und besonders die Ergebnisse der Zertifizierung der **DARZ.CA** zur Verfügung stellen.

Die **DARZ.CA** aktualisiert anschließend die entsprechenden Registrierungsdaten.

3.2.8 Aktualisierung/Anpassung der Registrierungsinformationen der Teilnehmer

Änderungen der Registrierungsinformationen sind der DARZ.CA unverzüglich mitzuteilen.

3.3 Identifizierung und Authentifizierung von Anträgen auf Schlüsselerneuerung (Routinemäßiger Folgeantrag)

Nach der initialen Zertifikatsausstellung erfolgen sogenannte Folgeanträge. Diese werden ebenso wie die initialen Zertifikatsanträge zweifelsfrei von der **DARZ.CA** identifiziert und authentisiert. Bei einer Schlüsselerneuerung (Folgeantrag zu einem bestehenden Zertifikat) ist zu beachten, dass von dem Antragsteller immer ein neuer Schlüssel erstellt wird.

Ein Zertifikatsinhaber ist dafür verantwortlich, rechtzeitig, d.h. vor dem Ablauf aller Zertifikate, neue Zertifikate zu beantragen (vgl. (TR-03109-4)). Dies gilt insbesondere für Zertifikate (Gütesiegelzertifikate und Wirkzertifikate) für SMGWs. Der Zeitpunkt ist so zu wählen, dass die neuen Zertifikate rechtzeitig in die Systeme eingebracht werden können, so dass der Betrieb ohne Beeinträchtigungen fortgeführt werden kann. Beim GWA, GWH und EMT kann es nach der Ausstellung des neuen Zertifikats zu einem temporären Betrieb mit mehreren gleichzeitig gültigen Zertifikaten kommen. Diese Phase dient dazu, allen relevanten Komponenten rechtzeitig das neue Zertifikat bekanntzumachen. Der Antragsteller besitzt einen privaten Schlüssel des dem Betreiber zugeordneten TLS-Zertifikats, mit dem die Absicherung des Kommunikationskanals durchgeführt werden muss. Das Zertifikat zu diesem Schlüssel darf weder gesperrt noch abgelaufen sein. Der zu übermittelnde Zertifikatsrequest (unabhängig von dem Zertifikatstyp) bzw. das Zertifikatsrequest-Paket ist mit dem zuletzt gültigen Signaturschlüssel signiert worden, und das zugehörige Zertifikat ist noch gültig und nicht gesperrt.

Bei den SMGWs werden die Folgeanträge durch den GWA gestellt, die Absicherung der Zertifikatsrequests erfolgt dabei über dessen TLS-Zertifikat und durch die Signatur mit seinem Signaturschlüssel (Autorisierungssignatur, siehe (TR-03109-4)). Überdies wird über die äußere Signatur die Echtheit des SMGW nachgewiesen, siehe (TR-03109-4).

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

3.4.1 Allgemein

Um einem nicht routinemäßigen Folgeantrag (vgl. Abschnitt 3.3) handelt es sich, wenn mindestens eine der folgenden Bedingungen erfüllt ist:

- Der Antragssteller besitzt kein gültiges TLS-Zertifikat für die Beantragung.
- Der Zertifikatsrequest ist nicht mit der gültigen Signatur des vorherigen Signaturschlüssels (äußere Signatur, vgl. (TR-03109-4) versehen.

Entsprechend ist eine der beiden Absicherungen eines Folgeantrags nicht gegeben. Daher kann der zuvor beschriebene Regelprozess (routinemäßiger Folgeantrag) nicht genutzt werden. Die weitere Vorgehensweise unterscheidet sich anhand der dem Antragsteller zu diesem Zeitpunkt noch zur Verfügung stehenden Sicherheitsmerkmale.

Beide Absicherungen fehlen
Sind beide Absicherungen (gültiges TLS-Zertifikat und gültige äußere Signatur) nicht gegeben, wird ein neues initiales Zertifikatsrequest-Paket im Rahmen einer erneuten initialen Identifizierung des PKI-Teilnehmers vergleichbar Kapitel 3.2 übergeben.

Ungültiges TLS-Zertifikat
Kann keine Authentifikation mittels TLS-Zertifikat (Webservice) gegenüber der **DARZ.CA** mehr erfolgen, wird die Übermittlung des Zertifikatsrequests über einen anderen gesicherten Kanal (z.B. eine verschlüsselte und signierte E-Mail des benannten ASP des Zertifikatsnehmers) durchgeführt. Bei der Beantragung wird immer auch ein neues TLS-Zertifikat beantragt. Dies ist auf Endnutzer-Ebene automatisch gegeben, da hier immer ein Zertifikatstripel beantragt wird. Durch die Erneuerung des TLS-Zertifikats können dann wieder routinemäßige Folgeanträge über den TLS-abgesicherten Webservice gestellt werden. Die Beantragung von Zertifikaten erfolgt, unabhängig vom Kommunikationskanal, immer über Zertifikatsrequest-Pakete gemäß (TR-03109-4).

Ungültige „Äußere Signatur“(z.B. ungültiges Signatur-Zertifikat)
Kann die Autorisation des Zertifikatsrequests nicht mehr über Signatur mit einem vorherigen noch gültigen Signaturschlüssel erfolgen, wird ein neues initiales Zertifikatsrequest-Paket (identisch mit dem Zertifikatsrequest bei der ersten Beantragung der Zertifikate) übermittelt.

Verfügt der PKI-Teilnehmer noch über ein gültiges TLS-Zertifikat wird das neue initiale Zertifikatsrequest-Paket hiermit signiert und über einen gesicherten Kanal an die **DARZ.CA** übermittelt. Zusätzlich wird ebenfalls über einen gesicherten Kanal (z.B. eine verschlüsselte und signierte E-Mail des benannten ASP des Zertifikatsnehmers) der Hashwert des Zertifikatspaketes zum Abgleich und zur Autorisation zugesendet. Die Hashwerte (SHA 256) werden dabei über die binär-codierte Request-Datei gebildet, welche das Zertifikatsrequest-Paket gemäß (TR-03109-4) enthält, und als base64-codierter Ausdruck in einer [ISO19005-1] konformen Datei versendet wird.

Nach einem positiven Abgleich des Hashwertes durch die Mitarbeiter der **DARZ.CA** werden die Zertifikate zur Verfügung gestellt. Der erfolgreiche Abgleich des Hashwertes wird durch die **DARZ.CA** mit Angabe der beteiligten Personen dokumentiert.

Sonderfall SMGW
Die beschriebenen Verfahren für einen nicht routinemäßigen Folgeantrag können nicht auf ein SMGW angewendet werden. Bei einem SMGW muss der verantwortliche GWA darauf achten, dass dieses immer über gültige Zertifikate verfügt.

3.4.2 Schlüsselerneuerung nach Sperrungen

Nach einer Sperrung eines Zertifikates können bestehende Zertifikate weiterhin genutzt werden.
Es können weitere Folgezertifikate beantragt werden.
Nach der Sperrung aller Zertifikate muss immer ein komplett neues Initial Request gestellt werden.

3.5 Identifizierung und Authentifizierung von Anträgen auf Sperrung

Die Sperrung eines Zertifikates kann von den folgenden Beteiligten initiiert werden:

- dem Zertifikatsinhaber

- der **DARZ.CA**
- der Root CA

Bei einer Sperrung wird dafür folgende Informationen an die **DARZ.CA** von einem benannten Ansprechpartner der o.a. Beteiligten mittels signierter und verschlüsselter E-Mail (S/MIME) oder einem vergleichbar abgesicherten Kommunikationskanal übermittelt:

- Zertifikatstyp
- Identifier (commonName (CN)) der DARZ.CA: **DARZ.CA**
- Zertifikatsnummer (Der Wert des Felds “SerialNumber“ des Zertifikats, siehe (TR-03109-4))
- Sperrgrund (siehe auch Kapitel 4.8)
- Zeitpunkt, ab dem das Zertifikat als unsicher/gesperrt einzustufen ist (wenn kein Zeitpunkt angegeben wird, wird das Zertifikat mit dem Zeitpunkt des Eintrages in die Sperrliste gesperrt)

3.5.1 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 benannte Ansprechpartner sendet in diesem Fall eine mittels seinem $C_{S/MIME}$ (ASP) signierte E-Mail an die **DARZ.CA**. Diese prüft die Authentizität der Information, den Sperrwunsch auf Durchführbarkeit und Beteiligung der SM-PKI Root. Sperrungen von Zertifikaten mit systemrelevanter Bedeutung erfolgen in Abstimmung mit der SM-PKI Root.

Die Sperrung des jeweiligen Zertifikats wird über die Sperrliste die **DARZ.CA** veröffentlicht, und der Zertifikatsinhaber wird über den abgeschlossenen Sperrprozess per signierter E-Mail informiert.

3.5.1.1 Verantwortlichkeit für die Sperrung eines SMGW

Bei den SMGWs wird die Berechtigung zur Sperrung der Zertifikate von dem zuständigen GWH (nur Gütesiegelzertifikate) bzw. GWA (Gütesiegel- und Wirkzertifikate) wahrgenommen.

Voraussetzung für die manuelle Übertragung der technischen Verantwortlichkeit ist, dass der GWH den GWA, an den übertragen werden soll, bei der zugehörigen **DARZ.CA** bekannt gemacht hat. Dieses erfolgt mittels eines Formulars, welches über den Download-Bereich (siehe Kapitel 1.5.3: Kontaktadresse CP/CPS DARZ.CA) bezogen werden kann. Das vom registrierten Ansprechpartner unterschriebene Formular ist elektronisch – mit den notwendigen Zertifikaten (laut Formular, z. B. C_{TLS} (GWA)…) – an die **DARZ.CA** (siehe Kapitel 4.1.1: Kontaktadresse DARZ.CA Registration Authority (RA)) zu übermitteln.

Der manuelle Vorgang muss über einen sicheren Kommunikationskanal erfolgen (z.B. signierte E-Mail). Die **DARZ.CA** prüft die Angaben des GWH, indem ein sicherer Kanal (S/MIME) zum GWA aufgebaut wird. Das Ergebnis wird dem GWH mitgeteilt. Ein GWA kann Gütesiegelzertifikate nur dann sperren, wenn seine technische Verantwortlichkeit für das betreffende SMGW in der **DARZ.CA** registriert ist. Zur Durchführung einer Übertragung der Verantwortlichkeit kann der GWH die Webservice-Schnittstelle der **DARZ.CA** nutzen, alternativ kann er einen entsprechend abgesicherten, etablierte Kommunikationskanal (z.B. signierte E-Mail) verwenden.

Falls der GWH die Webservice-Schnittstelle nutzen möchte, so erstellt er einen Datensatz gemäß (TR-03109-4), in welchem er eines oder mehrere SMGWs und den dafür zuständigen GWA benennt. Diesen Datensatz signiert er mit dem privaten Schlüssel von C_{Sig}(GWH) und sendet ihn per Web-Service an die **DARZ.CA**. Die Übertragung der technischen Verantwortlichkeit an den GWA ist mit sofortiger Wirkung gültig, sobald die **DARZ.CA** den Datensatz erfolgreich verarbeitet hat.
Durch die Übertragung der technischen Verantwortlichkeit erhält der GWA die Berechtigung, die Gütesiegelzertifikate der betreffenden SMGWs zu sperren. Um Wirkzertifikate für das SMGW beantragen zu können, ist dieser Schritt nicht erforderlich.
Die Übertragung der technischen Verantwortlichkeit für SMGWs kann je SMGW nur einmalig vom zuständigen GWH initiiert werden. Der GWA wird von der **DARZ.CA** per signierter E-Mail an die zuvor benannten Ansprechpartner informiert, sobald die Übertragung der Verantwortlichkeit abgeschlossen wurde.

3.5.1.2 Sperrung eines SMGW

Die Sperrung eines SMGW-Zertifikats muss über die Web-Service-Schnittelle der DARZ.CA als Paket (enthält Zertifikatstripel, siehe (TR-03109-4) beantragt werden. Die **DARZ.CA** prüft bei der Bearbeitung von Sperranträgen für Gütesiegelzertifikate, ob der Absender und Unterzeichner des Sperrantrags für die zu sperrenden Zertifikate technisch verantwortlich ist. Wurde die technische Verantwortlichkeit für Gütesiegelzertifikate an einen GWA übertragen, so ist dieser alleinig sperrberechtigt. In allen anderen Fällen ist diejenige Instanz sperrberechtigt, die die Zertifikate beantragt hat. Im Ausnahmefall (z.B. Web-Service-Schnittstelle steht nicht zur Verfügung) kann die Sperrung auch über einen entsprechend abgesicherten, etablierten Kommunikationskanal (z.B. signierte E-Mail) erfolgen.

3.5.2 Initiative der Certificate Authority

Die **DARZ.CA** hat die Aufgabe, bei erkannten Schwachstellen alle Tätigkeiten durchzuführen, welche die Integrität und Sicherheit der PKI sicherstellen. Die Schwachstellen werden direkt nach Bekanntwerden der SM-PKI Root gemeldet. Die Einleitung weiterer Schritte wird ggf. in Absprache mit der SM-PKI Root vorgenommen. Mögliche Gründe sind beispielsweise

- ein erkannter Verstoß gegen Betriebsauflagen (insbesondere gegen die Anforderungen für die Teilnahme an der **DARZ.CA** (s. Tabelle 15 der CP-SM-PKI),
- erkannte (erhebliche) Schwächen in der eingesetzten Kryptographie oder Kryptoimplementierung,
- Änderungen in den zentralen Vorgaben (z.B. der (TR-03109-4)),
- Änderung der Zertifikatsdaten (z.B. des Organisationsnamens),
- eine erkannte Schlüsselkompromittierung oder
- die Einstellung des Betriebs bzw. die Außerbetriebnahme der betroffenen Komponente.

Sperrungen von Zertifikaten mit systemrelevanter Bedeutung (das Sub-CA Zertifikat der **DARZ.CA** selbst und GWA) erfolgen in Abstimmung mit der SM-PKI Root. Die Zertifikate eines SMGW, GWH oder eines EMT können in der eigenen Verantwortung durch die **DARZ.CA** gesperrt werden. Sollten nach Ansicht des Betreibers der **DARZ.CA** Sperrungen dieser Zertifikate systemrelevante Auswirkungen haben, so informiert die **DARZ.CA** die Root vorab (siehe auch Kapitel 4.8.1).

Eine Sperrung des jeweiligen Zertifikats wird über die Sperrliste der **DARZ.CA** veröffentlicht. Der Zertifikatsinhaber sowie die SM-PKI Root (nur bei **DARZ.CA** und GWA) werden über den abgeschlossenen Sperrprozess informiert.

3.6 Identifizierung und Authentifizierung von Anträgen auf Suspendierung

Die Suspendierung der Wirk-Zertifikate eines SMGW MUSS vom zugehörigen GWA durchgeführt werden.
Bei einer Suspendierung müssen dafür folgende Informationen an die **DARZ.CA** übermittelt werden:

- Ausstellende Sub-CA
- Zertifikatsnummer (Der Wert des Felds “SerialNumber“ des Zertifikats, siehe (TR-03109-4))
- Der Sperrgrund „certificateHolde“ gemäß (RFC5280)
- Begründung für die Suspendierung gemäß Kapitel 4.8

Die Suspendierung MUSS über die Web-Service-Schnittelle der **DARZ.CA** beantragt werden. Im Ausnahmefall (z.B. Web-Service-Schnittstelle steht nicht zur Verfügung) kann dies auch über einen entsprechend abgesicherten, etablierten Kommunikationskanal (z.B. signierte E-Mail) durchgeführt werden. Eine Suspendierung eines SMGW muss immer als Paket (enthält Zertifikatstripel) erfolgen, siehe (TR-03109-4)).

Eine Suspendierung des jeweiligen Zertifikats wird über die Sperrliste der **DARZ.CA** veröffentlicht. Der für das SMGW zuständige GWA wird über den abgeschlossenen Suspendierungsprozess von der **DARZ.CA** informiert; hierzu ist die Veröffentlichung der Sperrliste hinreichend.

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 (initiale Beantragung und Folgeantrag),
- Verarbeitung von Zertifikatsanträgen und
- Zertifikatsausstellung.

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

E-Mails ohne sicherheitskritischen Inhalt können ggf. auch ohne Signatur und Verschlüsselung an zentrale Postfächer versendet werden.

4.1 Zertifikatsantrag

In den folgenden Unterkapiteln wird definiert, wer ein Zertifikat bei der **DARZ.CA** beantragen darf und welche Organisationseinheit für die Bearbeitung des Zertifikatsantrags verantwortlich ist.

4.1.1 Wer kann einen Zertifikatsantrag stellen?

Ein Zertifikatsantrag darf ausschließlich von einer Organisation gestellt werden. Befugte Organisationen sind GWA, GWH oder EMT, die sich gemäß Abschnitt 3.2 an der **DARZ.CA** identifiziert haben müssen.

Ein Endnutzer (nicht SMGW) kann sofern erforderlich, weitere Zertifikate bzw. Zertifikatstripel siehe (TR-03109-4) für sich beantragen (z.B. für Lastmanagement oder Ausfallsicherheit). Der Zertifikatsrequest muss als Folgeantrag (siehe Kapitel 3.3) unter Nutzung der vorhandenen Zertifikate bei der **DARZ.CA** gestellt werden. Die weiteren Zertifikate/Zertifikatstripel müssen eindeutig gekennzeichnet werden (siehe Anhang A der (CP-SM-PKI)). Die Eindeutigkeit von Zertifikaten erfolgt aus der Kombination von Common Name, der Sequenznummer im Subject-DN, der Seriennummer des Zertifikats und dem Issuer-DN (Herausgeber/CA).

4.1.2 Beantragungsprozess und Zuständigkeiten

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

Die Kontaktadresse zur Koordinierung lautet wie folgt:
DARZ GmbH
Julius-Reiber-Strasse 11
64293 Darmstadt
RA-DARZ.CA@da-rz.de

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 der **DARZ.CA**.

Die RA-Mitarbeiter der **DARZ.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 und damit die erforderliche Anzahl von mindestens zwei Ansprechpartnern unterschritten werden, muss mindestens ein neuer Vertreter benannt werden (vergleichbar dem im Abschnitt 3.2 beschriebenen Prozess). Die Benennung des neuen Vertreters bzw. der neuen Vertreter sowie das Ausscheidens des bisherigen Vertreters muss vom Geschäftsführer analog zu Abschnitt 3.2 des Teilnehmers bestätigt werden.

Für die SMGWs werden keine direkten Ansprechpartner benannt, da diese Aufgaben von den GWAs bzw. von den GWHs übernommen werden.

Bei allen Prozessen der Beantragung, Ausgabe und Verwaltung der Zertifikate wird seitens der **DARZ.CA** hinsichtlich der eingesetzten Kryptografie immer die aktuelle Version der (TR-03116-3) bei der Nutzung des Webservice bzw. wird die (TR-03116-4) zur Absicherung der E-Mail-Kommunikation via S/MIME berücksichtigt.

4.2.2 Annahme oder Ablehnung von initialen Zertifikatsanträgen

Die vorliegenden bzw. nachgelieferten Unterlagen / Nachweise werden von den RA-Mitarbeitern gegen die Vorgaben dieser CP/CPS der **DARZ.CA** geprüft.

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

Durch die RA werden im Rahmen der Prüfung auch der vorliegende Zertifikatsrequest für die initialen Zertifikate formal und die Übereinstimmung der gedruckten Hashwerte in den Unterlagen mit denen der Zertifikatsrequests überprüft.

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

4.2.3 Fristen für die Bearbeitung von Zertifikatsanträgen

Die in den nachfolgenden Abschnitten aufgeführten Zeiten sind als Richtwerte für die einzelnen Arbeitsschritte bei der initialen Ausgabe von Zertifikaten anzusehen. Die Ausgabe von Folgezertifikaten bzw. Ersatzzertifikaten nach der Sperrung von Zertifikaten können von den angegebenen Werten situationsabhängig abweichen.

4.2.3.1 Ausgabe von initialen Endnutzer-Zertifikaten

Die Bearbeitung der Zertifikatsanträge gliedert sich in folgende Arbeitsschritte:

Arbeitsschritt	Beschreibung des Arbeitsschrittes	Zeitrahmen
1	Start des Beantragungsprozesses durch den Endnutzer (GWA, GWH oder EMT)	-
2	Kontaktaufnahme zur Terminvereinbarung durch die DARZ.CA	3 Arbeitstage (Die DARZ.CA ermöglicht dabei einen Termin (für Arbeitsschritt 3) innerhalb der nachfolgenden 3 Arbeitstage)
3	Übergabe der Dokumente / Nachweise ggf. im Rahmen eines persönlichen Termins	-
4	Vorprüfung der Unterlagen und Rückmeldung an den Endnutzer	1 Kalenderwoche
(5 – optional)	Nachlieferungsfrist für den Endnutzer	3 Kalenderwochen
6	Prüfung der Unterlagen durch die DARZ.CA inkl. Rückmeldung an den Endnutzer	1 Kalenderwoche
7	Ausstellung der Zertifikate für Endnutzer	2 Arbeitstage

TABELLE 1: ZEITABLAUF FÜR DIE INITIALE AUSGABE VON ENDNUTZER-ZERTIFIKATEN (GWA, GWH, EMT)

Für die Einhaltung der hier definierten Zeiträume ist eine fristgerechte und fachliche Lieferung / Mitwirkung der Endnutzer Voraussetzung. Sollten sich die Lieferungen /Zuarbeiten der Endnutzer verzögern, können sich die Zeiten verlängern.

4.2.4 Ausgabe von Zertifikaten

Die Ausgabe von SMGW-Zertifikaten erfolgt ausschließlich über die Web-Service-Schnittstelle. Bei Endnutzer-Zertifikaten erfolgt, abgesehen von den initialen Zertifikaten, die Ausgabe über die Web-Service-Schnittstelle (EMT Folgezertifikate können auch über die anderen definierten Schnittstellen, wie E-Mail, ausgegeben werden). Die initialen Zertifikate werden immer, Folgezertifikate alternativ per E-Mail an den Ansprechpartner gesendet. Der Versand per E-Mail kann unverschlüsselt erfolgen.

4.2.5 Benachrichtigung des Zertifikatsnehmers über die Ausgabe des Zertifikats

Der Ansprechpartner wird nach der Ausstellung eines initialen Zertifikats der **DARZ.CA** - ausser SMGW - per signierter und verschlüsselter E-Mail (S/MIME) hierüber informiert. Die initialen Zertifikate werden als Anlage ebenfalls übermittelt.

4.3 Annahme von Zertifikaten

Bei den Endnutzer-Zertifikaten prüft der Ansprechpartner des Zertifikatsnehmers nach Erhalt die Angaben im Zertifikat auf Korrektheit und Vollständigkeit. Um ein Zertifikat zurückzuweisen, schickt der Ansprechpartner des Zertifikatsnehmers eine signierte und verschlüsselte Email-Nachricht an die **DARZ.CA**. 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 einem SMGW kann diese Prüfung durch den GWH oder den GWA automatisiert z.B. bei dem Erhalt oder der Einbringung der Zertifikate erfolgen. Die **DARZ.CA** nimmt Fehlermeldungen unter der Mailadresse RA-DARZ.CA@da-rz.de entgegen.

4.3.1 Veröffentlichung von Zertifikaten durch die CA

Alle ausgestellten Zertifikate werden direkt nach der Ausstellung in dem Verzeichnisdienst der DARZ.CA veröffentlicht.

4.4 Verwendung von Schlüsselpaar und Zertifikat

4.4.1 Verwendung des privaten Schlüssels und des Zertifikats durch den Zertifikatsnehmer

Zertifikate und die zugehörigen privaten Schlüssel werden gemäß ihrem Verwendungszweck laut (TR-03109-4) eingesetzt.

4.4.2 Verwendung des öffentlichen Schlüssels und des Zertifikats durch Zertifikatsnutzer

Die Verwendung des öffentlichen Schlüssels und des Zertifikats erfolgt gemäß [TR-03109-4].

4.5 Zertifikatserneuerung

Eine Zertifikatserneuerung auf Basis des bestehenden Schlüsselpaares ist nicht zugelassen.

4.6 Zertifizierung nach Schlüsselerneuerung

4.6.1 Bedingungen der Zertifizierung nach Schlüsselerneuerung

Es gelten die Anforderungen aus Kapitel 3.3.

4.6.2 Wer darf Zertifikate für Schlüsselerneuerungen beantragen?

Jeder Teilnehmer der **DARZ.CA** muss darauf achten, rechtzeitig vor Ablauf der Zertifikatslaufzeit ein neues Schlüsselpaar zu generieren und ein Zertifikat zu beantragen. Für ein SMGW liegt die Verantwortung beim zuständigen GWA.

4.6.3 Bearbeitung von Zertifikatsanträgen für Schlüsselerneuerungen

Es gibt zwei unterschiedliche Arten der Folgeanträge:

- Folgeanträge über eine automatisierte Web-Service-Schnittstelle, vgl. (TR-03109-4), oder
- Folgeanträge über eine abgesicherte E-Mail-Kommunikation

Folgeanträge über eine automatisierte Schnittstelle (synchroner Betrieb)
Hier wird über eine gesicherte TLS Verbindung (siehe (TR-03116-3)) ein Zertifikatsrequest gemäß (TR-03109-4) an die **DARZ.CA** gesendet. Die **DARZ.CA** beantwortet diesen Zertifikatsrequest synchron, so dass die beantragten Zertifikate unmittelbar in der Response enthalten sind. Eine zeitverzögerte Zustellung (asynchroner Betrieb) der Zertifikate per Webservice wird seitens der **DARZ.CA** nicht unterstützt.

Folgeanträge über eine abgesicherte E-Mail Kommunikation
Bei einem Folgeantrag wird der Zertifikatsrequest gemäß (TR-03109-4) vom benannten Ansprechpartner des Zertifikatsnehmers an die **DARZ.CA** in einer verschlüsselten und signierten E-Mail gesendet.

Unabhängig von der gewählten Kommunikationsverbindung wird bei einem routinemäßigen Antrag gemäß Kapitel 3.3 gehandelt und das Zertifikat wird seitens der **DARZ.CA** direkt ausgestellt. Bei einem nicht routinemäßigen Folgeantrag wird wie in Abschnitt 3.4 beschrieben verfahren.

4.6.4 Benachrichtigung des Zertifikatsnehmers über die Ausgabe eines Nachfolgezertifikats

Der Beantragende wird durch die Zustellung des Nachfolgezertifikats seitens der **DARZ.CA** informiert. Die sonstigen Teilnehmer der **DARZ.CA** werden grundsätzlich nicht individuell über die Ausgabe von Zertifikaten zur Schlüsselerneuerung informiert. Eine Benachrichtigung erfolgt nur über die Veröffentlichung im Verzeichnisdienst (siehe Abschnitt 4.6.7).

4.6.5 Verhalten für die Annahme von Zertifikaten für Schlüsselerneuerungen

Bei den GWA/GWH/EMT-Zertifikaten muss der Ansprechpartner des Zertifikatsnehmers nach Erhalt die Angaben im Zertifikat auf Korrektheit und Vollständigkeit prüfen. Um ein Zertifikat zurückzuweisen, schickt der Ansprechpartner des Zertifikatsnehmers eine Nachricht an die **DARZ.CA**. 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 einem SMGW kann diese Prüfung durch den GWH oder den GWA automatisiert z.B. bei dem Erhalt oder der Einbringung der Zertifikate erfolgen. Die **DARZ.CA** stellt eine Kommunikationsschnittstelle für Fehlermeldungen bereit. (vgl. Kapitel 4.3)
.

4.6.6 Veröffentlichung von Zertifikaten für Schlüsselerneuerungen durch die CA

Siehe Kapitel 4.3.1.

4.6.7 Benachrichtigung anderer PKI-Teilnehmer über die Ausgabe eines Nachfolgezertifikats

Siehe Kapitel 4.3.1.

4.7 Änderungen am Zertifikat

Änderungen an den Zertifikatsinhalten, abgesehen vom individuellen privaten Schlüsselmaterial, sind nicht zulässig. Dies entspricht dem durch die TR03145 vorgegebenen Konzept des „Rekeyings“. 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 Abschnitt 3.2 beauftragt und das alte Zertifikat gesperrt werden.

4.8 Sperrung und Suspendierung von Zertifikaten

Eine Sperrung eines Zertifikates kann eingeleitet werden durch den Zertifikatsnehmer, die DARZ.CA und die Root. Im Falle von SMGW-Wirkzertifikaten kann diese auch vom GWA durchgeführt werden. Im Falle von SMGW-Gütesiegelzertifikaten kann diese vom GWH, bzw. nach Übergabe der Sperrberechtigung an den GWA, vom GWA durchgeführt werden.

4.8.1 Sperrung

Sperrungen von GWA, GWH und EMT Zertifikaten können von den jeweiligen registrierten Ansprechpartnern bei der DARZ GmbH.CA per verschlüsselter E-Mail angefordert werden

Ein Zertifikat muss gesperrt werden, wenn mindestens einer der folgenden Gründe eintritt:

- Die im Zertifikat enthaltenen Angaben sind nicht oder nicht mehr gültig.
- Der private Schlüssel wurde kompromittiert.
- Der Zertifikatsnehmer ist nicht mehr berechtigt, das Zertifikat zu nutzen.
- Der Zertifikatsnehmer benötigt das Zertifikat nicht mehr.
- Der Zertifikatsnehmer hält Verpflichtungen gemäß dieses CP bzw. des CPS nicht ein.
- Die DARZ.CA stellt ihren Zertifizierungsbetrieb ein. In diesem Fall werden sämtliche von der DARZ.CA ausgestellten Zertifikate gesperrt.
- Der private Schlüssel der ausstellenden oder einer übergeordneten Root-CA wird kompromittiert. In diesem Fall werden sämtliche von diesen CA’s ausgestellte Zertifikate gesperrt.

- Die Algorithmen, die Schlüssellänge oder die Gültigkeitsdauer des Zertifikates bieten keine ausreichende Sicherheit mehr. Die DARZ.CA behält sich vor, die betreffenden Zertifikate zu sperren.

Der Sperrservice der RA kann auch telefonisch kontaktiert werden. Hierzu werden im Rahmen der Erstregistrierung die Kontaktdaten ausgetauscht und ein Sperrkennwort vereinbart. Dieses ist bei einem telefonischen Sperrwunsch seitens des Kunden zu nennen. Der RA Mitarbeiter prüft das Kennwort auf Übereinstimmung.

Eine Sperrung des GWA Zertifikates hat systemrelevante Bedeutung und muss daher in Abstimmung mit der SM-PKI Root erfolgen. Der Sperrwunsch des Kunden, wenn nicht seitens der **DARZ.CA** initiiert, wird zunächst seitens der **DARZ.CA** entgegengenommen, geprüft und danach per signierter Email an die SM-PKI Root CA als beteiligte Instanz übermittelt. Nach Zustimmung wird das Zertifikat im Vier-Augenprinzip gesperrt und der Kunde hierüber informiert.

Alle Anträge zum zu sperrenden Zertifikat müssen folgende Angaben beinhalten:

- SerialNumber
- Subject-DN
- Zertifikatstyp (GWA/GWH/EMT/SMGW Güte- oder Wirkzertifikat)
- Sperrgrund

Ist dem Sperrenden der genaue Zeitpunkt für den Eintritt des Sperrgrundes bekannt, so muss dieser bei der Sperrung angegebenen werden, ansonsten erfolgt der Eintrag in die Sperrliste ohne diesen Parameter. Alle Teilnehmer der **DARZ.CA** müssen gemäß (TR-03109-4) immer die aktuelle Sperrliste verwenden. In besonderen Fällen (Erstinbetriebnahme oder auf Aufforderung einer CA-Instanz) müssen neben den regelmäßigen Aktualisierungen die Sperrlisten auch anlassbezogen abgefragt werden.

4.8.2 Sperrung und Suspendierung von SMGW-Zertifikaten

Bei SMGW-Wirkzertifikaten (nicht jedoch bei SMGW-Gütesiegelzertifikaten) kann alternativ zur Sperrung auch die Suspendierung durch den GWA erfolgen. Die Suspendierung stellt einen Spezialfall der Sperrung dar. Suspendierte Zertifikate werden in die Sperrliste aufgenommen und speziell gekennzeichnet (siehe (TR-03109-4)). Bei diesen Zertifikaten kann die Sperrung innerhalb eines begrenzten Zeitraums der Suspendierung von 30 Tagen vorübergehend wieder zurückgenommen werden, um neue Zertifikate zu erhalten und somit wieder in den Wirkbetrieb aufgenommen zu werden. Nach 30 Tagen wird ein einmal suspendiertes Zertifikat endgültig gesperrt. Initiiert der Zertifikatsnehmer eine Suspendierung, so muss er dies an einen Ansprechpartner der **DARZ.CA** mittels signierter E-Mail als Sicherheitsvorfall melden (siehe auch Kapitel 5.2.10). Hierbei muss der Grund für die Suspendierung genannt werden. Die **DARZ.CA** dokumentiert diese Begründung. Dies gilt auch für Suspendierungen, welche über die Webservice-Schnittstelle in Auftrag gegeben wurden. Wird seitens des Zertifikatsnehmers der Grund für die Suspendierung des SMGW-Wirkzertifikates nicht innerhalb von 7 Kalendertagen an die **DARZ.CA** übermittelt, wird dieser an seine Informationspflicht gegenüber der **DARZ.CA** informiert. Sollte ab dem Zeitpunkt der Erinnerung innerhalb von 3 Arbeitstagen keine Begründung für die Suspendierung via S/MIME eingehen, wird dieser Umstand als Sicherheitsvorfall an die SM-PKI Root nach Kapitel 5.2.10 kommuniziert.

Eine Suspendierung von SMGW-Zertifikaten wird beispielsweise bei unklaren Sachverhalten genutzt, wenn die Vertrauenswürdigkeit eines SMGW in Frage gestellt wird. Liegen belastbare Erkenntnisse vor, dass das SMGW nicht mehr vertrauenswürdig ist, muss die Kennzeichnung als suspendiert in der Sperrliste entfernt werden (siehe (TR-03109-4)). Eine Rücknahme der Sperrung ist dann nicht mehr möglich.

Eine Suspendierung ermöglicht eine Prüfung, inwieweit das betroffene Gerät weiter verwendet werden kann.

Im Positivfall (SMGW ist weiterhin vertrauenswürdig) KANN der GWA innerhalb der Suspendierungsdauer die Suspendierung zurücknehmen, um anschließend mittels Zertifikatsrequest neue Zertifikate für das SMGW beantragen zu können. Dabei werden die suspendierten Zertifikate für die Neubeantragung temporär von der Sperrliste entfernt. Die Rücknahme der Suspendierung erfolgt, ebenso wie die Suspendierung, durch den GWA über die von der **DARZ.CA** angebotene Schnittstelle (Webservice, alternativ durch per S/MIME verschlüsselte und signierte E-Mail). Anschließend muss der GWA sicherstellen, dass die -vorübergehend wieder gültigen- SMGW-Zertifikate ausschließlich für die Neubeantragung verwendet werden. Sobald die neuen Zertifikate auf dem SMGW installiert sind, MUSS der GWA die alten Zertifikate endgültig sperren lassen, so dass diese wieder in die Sperrliste eingetragen werden.

Die **DARZ.CA** prüft in diesem Fall

- die Signatur des GWA als Nachweis für die Rechtmäßigkeit zur Ausgabe der neuen Zertifikate und
- die Signatur des SMGW‘s als Nachweis, dass das Gerät neue Zertifikate beziehen darf.

Sind die Bedingungen erfüllt, werden die neuen Zertifikate erstellt und sind durch den GWA in das SMGW einzubringen. Der Entscheidungsprozess für die Beauftragung der neuen Zertifikate muss vom GWA sorgfältig und nachvollziehbar dokumentiert werden.

Dieser Zusatzschritt wird bei den SMGW vorgenommen, um ggf. einen zum Zeitpunkt des Auftretens nicht nachweisbaren Verdacht des Verlusts der Vertrauenswürdigkeit des SMGW-Zertifikats innerhalb eines angemessenen Zeitraums untersuchen zu können.
Suspendierte Zertifikate müssen von allen Teilnehmern der **SM-PKI** als gesperrte Zertifikate behandelt werden.

Der Zertifikatsnehmer kann die Sperrung seines eigenen Zertifikates jederzeit beantragen, auch wenn keiner oben genannten Gründe vorliegt. Suspendierungen sind nur bei SMGW-Wirkzertifikaten zulässig.

Die DARZ.CA führt die Sperrung oder Suspendierung des Zertifikates durch und veröffentlicht die entsprechende Sperrliste. Der Zertifikatsnehmer wird über die Sperrung des Zertifikates unterrichtet.

4.8.3 Aktualisierungs- und Prüfungszeiten bei Sperrungen

In der folgenden Tabelle sind die minimal erforderlichen Aktualisierungs- und Prüfungszeiten der Sperrlisten für die einzelnen **DARZ.CA** Teilnehmer definiert. Es wird zwischen regelmäßigen Aktualisierungen, verursacht durch den Ablauf der Gültigkeitszeit einer Sperrliste, und anlassbezogenen Aktualisierungen, verursacht durch die Sperrung von Zertifikaten, unterschieden. Voraussetzung für die anlassbezogene Aktualisierung ist, dass die **DARZ.CA** wie in Tabelle 2 definiert erreichbar ist.

Nach Eintreffen eines Antrags für eine Sperrung wird dieser von der **DARZ.CA** unverzüglich geprüft. Ist der Antrag valide wird dieser zeitlich, wie in Tabelle 2 definiert, umgesetzt.

Die Gültigkeit einer Sperrliste darf max. 3 Tage länger sein, als das in Tabelle 2 definierte Aktualisierungsintervall.

Sollte eine Sperrliste nicht verfügbar bzw. abrufbar sein, wird ersatzweise mit der zuletzt bekannten Sperrliste weitergeprüft. Die **DARZ.CA** wird hierüber unverzüglich informiert. Diese stellt dann auf anderem Wege eine aktuelle Sperrliste zur Verfügung. Steht nach 3 Tagen immer noch keine aktualisierte Sperrliste zur Verfügung, wird die Root-CA informiert.

PKI-Teilnehmer	Regelmäßige Aktualisierung der Sperrliste	Erreichbarkeit für Sperrungen	Anlassbezogene Aktualisierung der Sperrliste	Abruf der Sperrliste	Prüfung der Zertifikate auf Sperrung
Sub-CA	Innerhalb von 7 Tagen	Täglich	Unverzüglich	Täglich	Täglich
Endnutzer (außer SMGW)	Entfällt (Erstellt keine Sperrliste)	Entfällt	Entfällt (Erstellt keine Sperrliste)	Täglich	Bei jeder Verwendung
Endnutzer SMGW	Entfällt (Erstellt keine Sperrliste)	Entfällt	Entfällt (Erstellt keine Sperrliste)	Täglich durch GWA bzw. anlassbezogen	Täglich durch GWA bzw. anlassbezogen

TABELLE 2: ZEITLICHE ANFORDERUNGEN BEI SPERRUNGEN

4.9 Service zur Statusabfrage von Zertifikaten

Die DARZ.CA unterhält derzeit keinen Dienst zur Statusabfrage von Zertifikaten. Die Bereitstellung von Sperrlisten ist in Kapitel 2 geregelt.

4.10 Beendigung der Teilnahme

Die Beendigung der Teilnahme eines Zertifikatsnehmers kann durch den Zertifikatsnehmer selbst oder die **DARZ.CA** eingeleitet werden.

Die Beendigung gliedert sich in drei Schritte:

- Information der Zertifikatsnutzer, die direkt von einer Beendigung der Teilnahme des Zertifikatsinhabers betroffen sind, durch den Zertifikatsinhaber. Es wird hierbei durch den Zertifikatsinhaber jedes Unternehmen (EMT, GWH und GWA) informiert, welches im Rahmen der Nutzung der Zertifikate mit dem Zertifikatsinhaber in Kontakt stand.
- Austausch der von der Sperrung betroffenen Zertifikate, so dass ein kontinuierlicher Betrieb gewährleistet werden kann (hierzu erfolgt eine entsprechende Abstimmung zwischen den Beteiligten bezüglich des dazu notwendigen Zeitrahmens. Ausgenommen hiervon ist die Sperrung von Zertifikaten aufgrund von Gefahren für den sicheren Betrieb der **DARZ.CA bzw. der SM-PKI**).
- Sperrung aller Zertifikate des Zertifikatsnehmers sowie entsprechende Kennzeichnung der $C_{S/MIME}$ (ASP) Zertifikate der benannten Ansprechpartner zum betroffenen Zertifikatsnehmer, so dass die Nutzung der Zertifikate für eine vertrauliche und authentische Kommunikation unterbunden wird.

Bei der Außerbetriebnahme eines SMGWs werden die Zertifikate des SMGW gesperrt. Die Sperrung MUSS der **DARZ.CA** über deren Webservice-Schnittelle mitgeteilt werden (siehe (TR-03109-4)).

4.11 Hinterlegung und Wiederherstellung von Schlüsseln

Eine Schlüsselhinterlegung- und wiederherstellung der DARZ.CA ist vorgesehen. Eine Schlüsselhinterlegung- und wiederherstellung durch die DARZ.CA wird für PKI-Teilnehmer unterhalb der DARZ.CA nicht angeboten.

5. Organisatorische, betriebliche & physikalische Sicherheitsanforderungen

5.1 Generelle Sicherheitsanforderungen

DARZ GmbH besitzt eine gültige ISO27001-Zertifizierung und erfüllt alle aufgelisteten Sicherheitsanforderungen. DARZ GmbH als Betreiber der DARZ.CA hat zusätzlich eine Zertifizierung nach TR-03145.

5.1.1 Erforderliche Zertifizierungen der PKI-Teilnehmer

Die Zertifizierung nach ISO/IEC 27001 sowie eine Zertifizierung nach TR-03145 gelten für den Betrieb der DARZ.CA mit. Zertifizierungen weiterer PKI-Teilnehmer werden durch die DARZ.CA überprüft.

- GWA : TR-03109-6
- GWH : Common-Criteria-Zertifikat auf Basis von [BSI-CC-PP-0073]
- Aktiver EMT : ISO27001 nativ oder ISO27001-Zertifizierung nach BSI Grundschutz

Der Nachweis der Zertifizierung eines SMGW wird durch den GWA überprüft.

5.1.2 Anforderungen an die Zertifizierung gemäß ISO/IEC 27001

Die Zertifizierung gemäß ISO/IEC 27001 umfasst alle Geschäftsprozesse und IT-Systeme des Registrierungs- und Zertifizierungsbetriebs der betreffenden PKI-Infrastruktur. Es wurde von einem hohen Schutzbedarf ausgegangen. Die Überprüfung der Anforderungen aus TR-03145 und der CP-SM-PKI Policy ist vor Inbetriebnahme erfolgt.

5.2 Erweiterte Sicherheitsanforderungen

5.2.1 Betriebsumgebung und Betriebsabläufe

Lage und Gebäude

Die DARZ.CA wird innerhalb eines zutrittsgesicherten Bereiches mit einem weiteren separaten Sicherheitsbereich betrieben. Sie unterhält darüber hinaus verschiedene Sicherheitsanlagen zur Hinterlegung von Produktiv- und Backup-Systemen und –Medien. Der Sicherheitsbereich sowie die Sicherheitsanlagen sind an die zentrale Alarmleitstelle des Gebäudes angebunden. Zudem ist der Sicherheitsbereich an ein lokales optisches und akustisches Alarmsystem angeschlossen.

Zutritt

Der räumliche Zutritt erfolgt über ein mehrstufiges Zutrittskontrollsystem. Zu dem Sicherheitsbereich der DARZ.CA ist ausschließlich das dort produktiv tätige PKI-Betriebspersonal zutrittsberechtigt. Es wird ein ausweisbezogenes Login mit biometrischer Bestätigung durchgeführt.

Strom, Heizung und Klimaanlage

Die Installation zur Stromversorgung entspricht den erforderlichen Normen. Eine Notstromversorgung über Dieselgeneratoren ist vorhanden. Eine Klimatisierung des Sicherheitsbereiches ist vorhanden.

Gefährdung durch Wasser

Die Räume verfügen über einen angemessenen Schutz vor Wasserschäden.

Brandschutz

Die Richtlinien für den Brandschutz werden eingehalten. Die Räume sind über Rauchmelder an die Brandmeldeanlage angeschlossen und enthalten eine automatische Löschanlage. Handfeuerlöscher sind in angemessener Anzahl vorhanden.

Aufbewahrung von Datenträgern

Sämtliche Datenträger mit Software sowie tagesaktuelle Sicherungen werden in mehrfachen Ausfertigungen als Original- und Backup-Versionen vorgehalten und in unterschiedlichen Gebäudeabschnitten (Gebäude/Orte) sicher aufbewahrt. Darüber hinaus werden der Gesamtbestand außer Kraft gesetzter Software sowie alte Datensicherungen in einem Archiv hinterlegt.

Sämtliche Datenträger werden mehrstufig in anwendungsbezogenen Stahlkassetten, die sich in Tresorschränken, welche sich wiederum in Tresoranlagen befinden, sicher hinterlegt.

Datenvernichtung

Elektronische Datenträger werden vor Ort sachgerecht zerstört und entsorgt. Papierdatenträger werden vor Ort mittels Aktenvernichtern sachgerecht zerstört und entsorgt.

Desaster Backup

Eine externe Sicherung von Daten, außerhalb der DARZ.CA, bei anderen Dienstleistern findet nicht statt.

5.2.2 Verfahrensanweisungen

Es wird im Rahmen eines Rollenkonzeptes sichergestellt, dass Verantwortungsbereiche klar definiert sind, dass einzelne Personen nicht unbemerkt Veränderungen an sicherheitskritischen Komponenten der DARZ.CA vornehmen können und private Schlüssel einsehen, generieren oder manipulieren können. Die Namen der am Prozess der Generierung sowie Auslieferung von Schlüsseln und Zertifikaten beteiligten Personen werden protokolliert.

Rollenbeschreibungen

Head of CA operations	Trägt die umfassende Verantwortung für das gesamte CA-Geschäft
CA Operator	Generiert Schlüsselpaare, Zertifikate und Sperrlisten
RA Operator	Verwaltet die Registrierungen, Suspendierungen und Sperrungen
IT Security Officer	Plant und überwacht die Implementierung von Sicherheitsmaßnahmen die gesamte CA Betreffend, einschließlich aller technischen, organisatorischen und physikalischen Maßnahmen
System Administrator	Verantwortlich für die Konfiguration und Instandhaltung der IT Infrastruktur einschließlich der Netzwerke, Datenbanken und Server
Access Manager	Verwaltet Rollen, technische und organisatorische Zugangsberechtigungen und die befugten Personen
Revisor	Interner Auditor, zuständig für die regelmäßige Überprüfung von Logdaten, Datenbanken und Papierdokumentationen der CA auf Unregelmäßigkeiten gemäß der internen Auditplanung

Für jede definierte Rolle wurde ein Vertreter ernannt. Der aktuelle Ansprechpartner wird wie unter Kapitel 2.1 beschrieben im Internet veröffentlicht. Die interne Vertretung wird nur im Intranet der DARZ GmbH veröffentlicht.

Die DARZ.CA setzt im Produktionsbetrieb für den Umgang mit hochsicherheitskritischen Zugangsmedien und kryptographischen Schlüsselmaterialien und Zertifikaten ein durchgängiges Vier-Augen-Prinzip ein.

Das Konzept sieht vor, dass die Hinterlegung, der Zugriff und der Einsatz der hochsicheren Zugangsmedien stets vom PKI-Betriebspersonal im Vier-Augen-Prinzip wahrgenommen werden. Darüber hinaus wird der gesamte Prozess der Generierung von kryptographischem Schlüsselmaterial und Zertifikaten bis zur Weitergabe im Vier-Augen-Prinzip durchgeführt. Das durchgängige Vier-Augen-Prinzip setzt die Dokumentation der Rollenverteilung der am Generierungsprozess beteiligten Personen in verschiedenen zu erstellenden sowie systembedingt erzeugten Protokollen voraus.

Identifizierung und Authentifizierung jeder Rolle

Das Rollenkonzept wird durch technische und organisatorische Maßnahmen umgesetzt. Die Identifizierung und Authentifizierung der Rollen erfolgt

- beim Zutritt zu Sicherheitsbereichen und Tresoren bzw.
- beim Zugriff auf Wertschränke oder sicherheitskritische Systeme und Anwendungen

mit Hilfe von SmartCards, Hardwaretoken, Benutzerkennungen und Passwörtern. Die Rollenverteilung wird in verschiedenen zu erstellenden sowie systembedingt erzeugten Protokollen dokumentiert.

Das Rollenkonzept stellt die Trennung von bestimmten Rollen und Aufgaben sicher, um zu verhindern, dass eine Person allein einen Schlüssel erzeugen oder ein Zertifikat ausstellen und weitergeben kann.

5.2.3 Personal

Die DARZ.CA setzt im Betrieb erfahrenes Personal ein, das über die erforderlichen IT-Kenntnisse und spezifischen Kenntnisse des CA-Betriebs verfügt.

Von allen Mitarbeitern des Betreibers der DARZ.CA (DARZ GmbH) liegt ein polizeiliches Führungszeugnis, ohne Einträge, welche eine Eignung für die Tätigkeit in Frage stellen, vor.

Das mit dem Betrieb der DARZ.CA betraute Personal wird regelmäßig und anlassbezogen geschult. Es ist hinsichtlich der Sicherheitsrelevanz seiner Arbeit sensibilisiert.

Schulungen und Fortbildungen werden insbesondere bei der Einführung neuer Richtlinien, IT-Systeme und IT-Verfahren durchgeführt.

Das PKI-Betriebspersonal wird in allen Bereichen des CA-Betriebes eingesetzt.

Unerlaubte Handlungen, die die Sicherheit der DARZ.CA gefährden oder gegen Datenschutzbestimmungen verstoßen, werden über die Personalstellen disziplinarisch geahndet bzw. strafrechtlich verfolgt.

Dem Personal des Betreibers der DARZ.CA stehen zum ordnungsgemäßen Betrieb der PKI folgende Dokumente zur Verfügung:

- Certificate Policy (CP) inkl. Certification Practice Statement (CPS) (mit diesem Dokument)
- Betriebshandbücher
- Benutzeranleitungen
- Dienstvorschriften und –anweisungen
- Relevante ISO27001-Dokumente
- Aktive Betreiberverträge und mögliche Zusatzdokumente welche die Zusammenarbeit definieren und abgrenzen

5.2.4 Monitoring

Die nachfolgenden Ereignisse werden protokolliert und dokumentiert:

- Systeminitialisierung
- Zertifizierungsanträge
- Registrierung der Benutzer
- Schlüsselerzeugung für CA
- Zertifikatserstellung für CA
- Datensicherungen für CA
- Zertifikatsveröffentlichung CA
- Nutzung des privaten Schlüssels und des Zertifikates
- Sperranträge
- Sperrung eines Zertifikates
- Erstellung einer Sperrliste
- Veröffentlichung einer Sperrliste

Darüber hinaus werden Störfälle und besondere Betriebssituationen erfasst. (ITIL-basiertes Incident-Management System)

Die Ordnungsmäßigkeit des Zertifizierungsbetriebes wird im Rahmen der risikoorientierten Prüfungen des Bereiches Revision des Betreibers vorgenommen. Bei Verdacht auf Unregelmäßigkeiten wird eine umgehende Prüfung veranlasst.

5.2.5 Archivierung von Aufzeichnungen

Sämtliche Daten, die für den Zertifizierungsprozess relevant sind werden archiviert. Die Archivierung wird bei der betriebsverantwortlichen Stelle der DARZ.CA vorgenommen. Die Archive werden gegen Zugriff, Manipulation und Vernichtung geschützt. Die Aufbewahrungszeiten orientieren sich an gesetzlichen Fristen, den Grundsätzen der Revisionssicherheit sowie weiteren internen Regelungen.

Die Protokolldaten werden zusammen mit anderen relevanten Daten einem regelmäßigen Backup unterzogen. Protokolle auf Papier werden in verschließbaren Schränken verwahrt.

Datensicherungen werden arbeitstäglich nach der Durchführung von

- Schlüsselausgaben
- Sperrungen von Zertifikaten
- der Erstellung von Sperrlisten

durchgeführt. Sie werden als Original- und Backupdatensicherungen vorgenommen und sicher in unterschiedlichen Gebäudebrandabschnitten hinterlegt.

5.2.6 Schlüsselwechsel der DARZ.CA

Der Schlüsselwechsel der DARZ.CA kann einerseits geplant und andererseits ungeplant erfolgen:

- Geplanter Schlüsselwechsel: Im Fall eines planbaren Schlüsselwechsels werden die Verfahren entsprechend der (CP-SM-PKI) berücksichtigt und entsprechend der vorhanden Prozesse abgearbeitet.
- Ungeplanter Schlüsselwechsel: Für den Fall, dass ein unvorhergesehener Schlüsselwechsel der DARZ.CA notwendig ist, sind entsprechende Verfahren im Notfallmanagement, welches Bestandteil der Betriebsdokumentation ist, definiert.
- Sowohl ein geplanter als auch ein ungeplanter Schlüsselwechsel der DARZ.CA erfolgt gemäß dem Vier-Augen-Prinzip.

5.2.7 Auflösen der Zertifizierungsstelle

Im Fall der Einstellung des Betriebes der DARZ.CA werden die nachfolgenden Maßnahmen ergriffen:

- Abstimmung der Auflösung mit der SM-PKI-Root
- falls mit der SM-PKI-Root vereinbart, werden alle Aufgaben der SubCA an eine Nachfolgeorganisation übertragen
- andernfalls werden deren Aufgaben und Verpflichtungen für die Restlaufzeit aufrechterhalten
- Information aller Zertifikatsnehmer sowie vertrauenden Parteien mit einer Vorlauffrist von mindestens drei Monaten.
- Vernichtung der privaten Schlüssel der Zertifizierungsstellen nach Einstellung der Tätigkeiten.
- Veröffentlichung der entsprechenden CA- und Root-CA-Sperrlisten.

5.2.8 Aufbewahrung der privaten Schlüssel

Kryptografiemodule	: Die Schlüssel sind in vertrauenswürdigen Kryptografie-Modulen gespeichert.
Schutz der Speichermedien	: siehe Kapitel 5.2.1 Betriebsumgebung.
Schlüsselaufbewahrung	: die Speichermedien befinden sich im physisch und durch technisch-organisatorische Maßnahmen hochgesicherten Bereich, der Zutritt ist auf eine klar definierte Zahl von Personen beschränkt.
Vertrauenswürdiges Personal	: der private Schlüssel wird durch vertrauenswürdiges Personal erzeugt, gespeichert und verwendet
Abfallbeseitigung	: es ist sichergestellt, dass Abfälle nicht unberechtigt genutzt und vertrauliche Informationen nicht veröffentlicht werden können
Gehärtete IT-Systeme	: eine Zertifizierung auf Basis ISO27001 liegt vor

5.2.9 Behandlung von Vorfällen und Kompromittierungen

Das Verfahren zur Behandlung von Sicherheitsvorfällen und Kompromittierungen von privaten Schlüsseln wird von der zuständigen Stelle für IT-Sicherheitsvorfälle festgelegt.

Werden innerhalb der Zertifizierungsstelle fehlerhafte oder manipulierte Rechner, Software und/oder Daten festgestellt, die Auswirkungen auf die Prozesse der Zertifizierungsstelle haben, wird der Betrieb des entsprechenden Systems unverzüglich eingestellt.

Das System wird unter Verwendung der Software sowie der Datensicherungen neu aufgesetzt und nach Überprüfung in einem sicheren Zustand in Betrieb genommen. Das fehlerhafte oder modifizierte System wird analysiert. Bei Verdacht einer vorsätzlichen Handlung werden gegebenenfalls rechtliche Schritte eingeleitet.

Falls Zertifikate mit fehlerhaften Angaben generiert wurden, wird der Zertifikatsinhaber unverzüglich informiert und das Zertifikat von der Zertifizierungsstelle gesperrt.

Bei Kompromittierung oder einem begründeten Verdacht auf Kompromittierung eines privaten Schlüssels ist das jeweilige Zertifikat unverzüglich zu sperren. Bei systemkritischen Zertifikaten ist die SM-PKI Root zu beteiligen. Alle betroffenen Zertifikatsinhaber werden umgehend benachrichtigt.

5.2.10 Meldepflichten

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

Bei der Kompromittierung eines GWA oder GWH muss zusätzlich die SM-PKI Root durch die DARZ.CA informiert werden.
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 oder Suspendierung 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?

Bei Eintreten von sicherheitskritischen Ereignissen unterrichtet die DARZ.CA die zuständige Stelle für IT-Sicherheitsvorfälle der DARZ GmbH.

5.3 Notfall-Management

Eine Wiederaufnahme des Zertifizierungsbetriebes nach einer Katastrophe ist Bestandteil der Notfallplanung und kann innerhalb kurzer Zeit erfolgen, sofern die Sicherheit des Betriebes der DARZ.CA gegeben ist.

6. Technische Sicherheitsmaßnahmen

6.1 Erzeugung und Installation von Schlüsselpaaren

6.1.1 Generierung von Schlüsselpaaren für die Zertifikate

Die Schlüsselpaare der **DARZ.CA** als Zertifikatsnehmer (C_{TLS}(Sub-CA)) werden zentral im Sicherheitsbereich der DARZ.CA auf IT-Systemen ohne Netzwerkanschluss offline im Vier-Augen-Prinzip erstellt.

6.1.2 Lieferung privater Schlüssel

Die Erstellung der privaten Schlüssel erfolgt dezentral durch die Zertifikatsnehmer der DARZ.CA. Daher erfolgt keine Lieferung der privaten Schlüssel.

6.1.3 Lieferung öffentlicher Zertifikate

Alle Zertifikate werden nach der Erstellung sofort im Verzeichnis der **DARZ.CA** abgelegt und sind somit für alle PKI-Teilnehmer zugänglich.

6.1.4 Schlüssellängen und kryptografische Algorithmen

Die CA-Schlüssel der DARZ.CA sind konform zu den Anforderungen aus [TR-03116-3]. Ebenso werden die zum jeweiligen Zeitpunkt konkret zu verwendenden kryptografischen Algorithmen und Schlüssellängen durch die [TR-03116-3] bestimmt.

6.1.5 Festlegung der Parameter der öffentlichen Schlüssel und Qualitätskontrolle

Es gelten die Vorgaben aus der Certificate Policy der SM-PKI Root.

6.1.6 Verwendungszweck der Schlüssel

Die Schlüssel werden ausschließlich für die in Kapitel 1.4.1 beschrieben Verwendungszwecke eingesetzt. Der Verwendungszweck ist in der jeweils aktuellen Fassung der (TR-03109-4) konkretisiert.

6.2 Sicherung des privaten Schlüssels und Anforderungen an kryptografische Module

Die Teilnehmer der **DARZ.CA** verwenden Kryptografiemodule zur Generierung, Speicherung und Nutzung ihrer privaten Schlüssels zu ihren Zertifikaten aus der **DARZ.CA**. Die Sicherheitsanforderungen an Kryptografiemodule zum Schutz der privaten Schlüssel zu den Zertifikaten werden in Kapitel 6.2.10 definiert.

Neben dem Einsatz eines sicheren Kryptografiemodules muss auch ein sicherer Umgang mit den privaten Schlüsseln sichergestellt werden. Daher müssen die Anforderungen an den Lebenszyklus und die Einsatzumgebung aus (KeyLifeSec) – Security Level 2 eingehalten werden (Ausnahme SMGW).

Für die **DARZ-Test.CA** werden Kryptografiemodule gemäß (CP-SM-PKI) Anhang C1 eingesetzt, welche baugleich zu dem für die **DARZ.CA** verwendeten Modell ist.

6.2.1 Mehrpersonen-Zugriffssicherung zu privaten Schlüsseln

Die privaten Schlüssel einer CA sind durch ein Vier-Augen-Prinzip geschützt.

6.2.2 Ablage privater Schlüssel

Es ist sichergestellt, 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

Es liegt ein kryptographisch gesichertes Backup der privaten CA-Schlüssel vor. Der Zugriff erfolgt im Vier-Augen-Prinzip. Die Anforderungen in Kapitel 6.2.3 der CP-SM-PKI werden erfüllt.

6.2.4 Archivierung privater Schlüssel

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

6.2.5 Transfer privater Schlüssel in oder aus kryptografischen Modulen

Ein Transfer privater CA-Schlüssel erfolgt nur zu Backup- oder Wiederherstellungszwecken in verschlüsselter Form und im Vier-Augen-Prinzip.

6.2.6 Speicherung privater Schlüssel in kryptografischen Modulen

Grundsätzlich werden die privaten Schlüssel der **DARZ.CA** auf einem Kryptografiemodul gespeichert.

- Die einzige Ausnahme bilden die client- und serverseitigen TLS-Schlüssel der **DARZ.CA**, die zur TLS-Authentisierung an der Web-Service-Schnittelle (siehe (TR-03116-3) und am Verzeichnisdienst verwendet werden.
- Die privaten Schlüssel der **DARZ-Test.CA** - Umgebung werden von der Produktivumgebung (DARZ.CA) getrennt.

6.2.7 Aktivierung privater Schlüssel

Die Aktivierung des privaten CA-Schlüssels ist nur im Vier-Augen-Prinzip möglich.

6.2.8 Deaktivierung privater Schlüssel

Es ist technisch sichergestellt, dass deaktivierte Schlüssel nicht genutzt werden können.

6.2.9 Zerstörung privater Schlüssel

Die privaten Schlüssel der **DARZ.CA** werden in folgenden Fällen sicher und unwiederherstellbar zerstört:

- Der Gültigkeitszeitraum des **DARZ.CA**-Schlüssels ist abgelaufen
- Der Schlüssel der **DARZ.CA** wurde gesperrt.

Die Backups der Schlüssel werden ebenfalls berücksichtigt.

Die Zerstörung der privaten Schlüssel erfolgt durch einen sicheren Lösch-Mechanismus im Kryptografiemodul. Für diesen Prozess gelten die Anforderungen aus(KeyLifeSec).

Die ENC-Schlüssel sind von dieser Anforderung ausgenommen. Diese dürfen nur noch für die Entschlüsselung abgelegter Daten genutzt werden, mit dem Ziel einer Umschlüsselung auf den aktuellen ENC-Schlüssel. Sollte der ENC-Schlüssel nicht mehr zur Umschlüsselung erforderlich sein, wird dieser ebenfalls zerstört.

6.2.10 Beurteilung kryptographischer Module

Die Anforderungen in Kapitel 6.2.10 der CP-SM-PKI werden erfüllt.

6.3 Andere Aspekte des Managements von Schlüsselpaaren

6.3.1 Archivierung öffentlicher Schlüssel

Sämtliche von der DARZ.CA erstellten öffentlichen Schlüssel werden inklusive der Statusdaten in der Datenbank der Zertifizierungsstelle archiviert.

6.3.2 Gültigkeitsperioden von Zertifikaten und Schlüsselpaaren

Der Gültigkeitszeitraum von Zertifikaten und Schlüsseln wird in [TR-03109-4] definiert. Unabhängig vom Gültigkeitszeitraum müssen die folgenden Zertifikate spätestens in dem hierzu angegebenen Intervall gewechselt werden.

- GWA-Zertifikate (TLS/ENC/SIG) alle 3 Jahre.
- Alle sonstigen Endnutzerzertifikate (TLS/ENC/SIG) alle 2 Jahre.
- SubCA alle 2 Jahre

6.4 Aktivierungsdaten

Im Rahmen der DARZ.CA ist der Zugriff auf die privaten Schlüssel der Zertifizierungsstelle kryptografisch und durch ein Vier-Augen-Prinzip geschützt.

Die Aktivierungsdaten für die Kryptografiemodule werden sicher aufbewahrt.

6.5 Sicherheitsanforderungen für die Rechneranlagen

Die Sicherheitsanforderungen für Rechneranlagen der CP-SM-PKI gemäß Kapitel 6.5 werden erfüllt.

6.6 Zeitstempel

Ein Zeitstempeldienst wird nicht angeboten.

6.7 Validierungsmodell

Die Zertifikatsvalidierung richtet sich nach den Anforderungen der [TR-03109-4].
Die CA- und Teilnehmerzertifikate sind zu validieren.

7. Profile für Zertifikate und Sperrlisten

7.1 Profile für Zertifikate und Zertifikatsrequests

Die Profile für die Zertifikate und die Zertifikatsrequests sind in [TR-03109-4] spezifiziert. Das Namensschema zu den Zertifikaten ist in Anhang A der CP-SM-PKI definiert.

Die Struktur der Sperrlisten, das Sperrmanagement (Veröffentlichung, Aktualisierung und Sperrlistenvalidierung) wird in der jeweils aktuellen Fassung der [TR-03109-4] definiert.

7.1.1 Zugriffsrechte

Die erlaubte Funktion der Zertifikate wird über die Key-Usage-Extension definiert (siehe [TR-03109-4]).

7.1.2 Zertifikatserweiterung

Die Certificate Extensions werden in der jeweils aktuellen Fassung der (TR-03109-4) definiert und in der **DARZ.CA** analog umgesetzt.

7.2 Profile für Sperrlisten

Die Anforderungen an die Sperrlisten (Certification Revocation List, CRL)-Profile werden in der jeweils aktuellen Fassung der (TR-03109-4) definiert und in der **DARZ.CA** analog umgesetzt.

7.3 Profile für OCSP Dienste

OCSP wird durch DARZ.CA nicht unterstützt.

8. Überprüfungen der CA und andere Bewertungen

8.1 Inhalte, Häufigkeit und Methodik

Die Arbeitsprozesse der Zertifizierungsstelle sowie der an der Registrierung beteiligten Stellen werden regelmäßig bzw. anlassbezogen überprüft.
Die Audits des technischen Aufbaus der PKI und der operativen Abläufe werden in regelmäßigen Abständen durch die interne Revision nach den in der DARZ GmbH für solche Vorgänge festgelegten Regeln durchgeführt. Die Ergebnisse der Audits werden nicht veröffentlicht. Grundsätzlich werden interne Audits und Prüfungen in regelmäßigen Abständen vorgenommen.

Die internen Prüfungen werden durch den Zentralbereich Revision der DARZ GmbH, sowie die Leitung der DARZ.CA vorgenommen. Die Prüfer verfügen über das Know-how sowie die notwendigen Kenntnisse auf dem Gebiet Public Key Infrastructure (PKI), um die Prüfungen vornehmen zu können.

Der Prüfer darf nicht in den Produktionsprozess der DARZ.CA eingebunden sein. Eine Selbstüberprüfung ist nicht erlaubt.

Es können alle für die PKI relevanten Bereiche überprüft werden. Die Prüfungsinhalte obliegen dem Prüfer.

Die DARZ GmbH stellt eine Testumgebung DARZ-Test.CA bereit, welche die Antragssteller (GWA,GWH,EMT) zum Test der Funktionalitäten der SM-PKI durchlaufen müssen, bevor diese Teilnehmer der SM-PKI werden können, siehe Kapitel 3.2.

8.2 Reaktionen auf identifizierte Vorfälle

Festgestellte Mängel müssen in Abstimmung zwischen Zertifizierungsstelle und Prüfer zeitnah beseitigt werden (siehe Kapitel 5.2.10). Der Prüfer wird über die Beseitigung der Mängel informiert.

9. Sonstige finanzielle und rechtliche Angelegenheiten

9.1 Preise

Preise für SubCA Dienstleistungen werden auf Anfrage zur Verfügung gestellt.

9.2 Finanzielle Zuständigkeiten

Der Angebotswunsch zur Teilnahme und Fragen zu den finanziellen Konditionen können wir Ihnen auf Anfrage gerne zur Verfügung stellen.

10. Vertraulichkeitsgrad von Geschäftsdaten

10.1.1 Definition von vertraulichen Informationen

Alle Informationen und Daten über Zertifikatsinhaber und Teilnehmer der DARZ.CA, die nicht unter Ziffer 10.1.2 fallen, werden als vertrauliche Informationen eingestuft.

10.1.2 Informationen, die nicht zu den vertraulichen Informationen gehören

Alle Informationen und Daten, die in herausgegebenen Zertifikaten und Sperrlisten explizit (z. B. E-Mail-Adresse) oder implizit (z. B. Daten über die Zertifizierung) enthalten sind oder davon abgeleitet werden können, werden als nicht vertraulich eingestuft.

10.1.3 Zuständigkeiten für den Schutz vertraulicher Informationen

Die DARZ.CA trägt die Verantwortung für Maßnahmen zum Schutz vertraulicher Informationen.

10.2 Schutz personenbezogener Daten

10.2.1 Datenschutzkonzept

Die Speicherung und Verarbeitung von personenbezogenen Daten richtet sich nach den gesetzlichen Datenschutzbestimmungen.

10.2.2 Als persönlich behandelte Daten

Jegliche Daten über Zertifikatsnehmer und Teilnehmer der DARZ.CA werden vertraulich behandelt.

10.2.3 Daten, die nicht als persönlich behandelt werden

Es gelten die Bestimmungen in Ziffer 10.1.2.

10.2.4 Zuständigkeiten für den Datenschutz

Die DARZ.CA trägt die Verantwortung für Maßnahmen zum Schutz personenbezogener Daten.

10.2.5 Hinweis und Einwilligung zur Nutzung persönlicher Daten

Der Zertifikatsinhaber stimmt der Nutzung von personenbezogenen Daten durch die DARZ.CA zu, soweit dies zur Leistungserbringung erforderlich ist. Darüber hinaus können alle Informationen veröffentlicht werden, die als nicht vertraulich behandelt werden.

10.2.6 Auskunft gemäß rechtlicher oder staatlicher Vorschriften

Die DARZ.CA richtet sich bei der Speicherung und Verarbeitung von personenbezogenen Daten nach den gesetzlichen Datenschutzbestimmungen. Eine Offenlegung findet gegenüber staatlichen Instanzen nur bei Vorliegen entsprechender Entscheidungen in Übereinstimmung mit den geltenden Gesetzen statt.

10.2.7 Andere Bedingungen für Auskünfte

Es sind keine weiteren Umstände für eine Veröffentlichung vorgesehen.

10.3 Geistiges Eigentumsrecht

Die DARZ GmbH ist Urheber dieses Dokumentes. Das Dokument kann unverändert an Dritte weitergegeben werden.

10.4 Zusicherungen und Garantien

10.4.1 Zusicherungen und Garantien der CA

Die DARZ.CA verpflichtet sich, den Bestimmungen der Zertifizierungsrichtlinie (CP) und den Regelungen für den Zertifizierungsbetrieb (CPS) zu folgen.

10.4.2 Zusicherungen und Garantien der RA

Die DARZ.CA verpflichtet sich, den Bestimmungen der Zertifizierungsrichtlinie (CP) und den Regelungen für den Zertifizierungsbetrieb (CPS) zu folgen.

10.4.3 Zusicherungen und Garantien der Zertifikatsnehmer

Die Zertifikatsnehmer sind zur Einhaltung der Bestimmungen der Zertifizierungsrichtlinie (CP) und den Regelungen für den Zertifizierungsbetrieb (CPS) verpflichtet.

10.4.4 Zusicherungen und Garantien der Zertifikatsnutzer

Die Zertifikatsnutzer sind zur Einhaltung der Bestimmungen der Zertifizierungsrichtlinie (CP) und den Regelungen für den Zertifizierungsbetrieb (CPS) verpflichtet.

10.4.5 Zusicherungen und Garantien anderer PKI-Teilnehmer

Von der DARZ.CA beauftragte Dienstleister (z. B. Betreiber von Verzeichnisdiensten) werden auf die Einhaltung dieser Zertifizierungsrichtlinie (CP) und den Regelungen für den Zertifizierungsbetrieb (CPS) verpflichtet.

10.5 Gewährleistungen

Grundsätzlich wird keine Gewährleistung übernommen. Die DARZ GmbH garantiert nicht die Verfügbarkeit der Leistungen der PKI.

10.6 Haftungsbeschränkungen

Verletzt die DARZ GmbH bei der Vertragsdurchführung schuldhaft eine vertragswesentliche Pflicht, die hierfür im Einzelfall von besonderer Bedeutung ist, so haftet sie für den dadurch entstehenden Schaden. Bei einfacher Fahrlässigkeit ist die Haftung der DARZ GmbH auf den vertragstypischen Schaden beschränkt.
Für die Verletzung sonstiger Pflichten haftet die DARZ GmbH nur bei grobem Verschulden. Gegenüber Kaufleuten und öffentlichen Verwaltungen gilt die Haftungsbeschränkung des Absatzes 1 Satz 2 auch bei grober Fahrlässigkeit einfacher Erfüllungsgehilfen.
Vorstehende Haftungsausschlüsse und -begrenzungen finden keine Anwendung auf die Haftung für Schäden aus der Verletzung des Lebens, des Körpers oder der Gesundheit; insofern haftet die DARZ GmbH nach den gesetzlichen Bestimmungen.
Im Falle einer Haftung der DARZ GmbH nach den vorstehenden Absätzen bestimmt sich der Haftungsumfang entsprechend § 254 BGB danach, wie das Verschulden der DARZ GmbH im Verhältnis zu anderen Ursachen an der Entstehung des Schadens mitgewirkt hat.

10.7 Schadensersatz

Bei der unsachgemäßen Verwendung des Zertifikats und dem zugehörigen privaten Schlüssel oder einer Verwendung des Schlüsselmaterials beruhend auf fälschlichen oder fehlerhaften Angaben bei der Beantragung ist die DARZ GmbH von der Haftung freigestellt.

10.8 Gültigkeitsdauer und Beendigung

10.8.1 Gültigkeitsdauer

Diese Zertifizierungsrichtlinie (CP) und die Regelungen für den Zertifizierungsbetrieb (CPS) treten an dem Tag in Kraft, an dem sie veröffentlicht werden.

10.8.2 Beendigung

Dieses Dokument ist so lange gültig, bis es durch eine neue Version ersetzt wird oder der Betrieb der DARZ.CA eingestellt wird.

10.8.3 Auswirkung der Beendigung und Weiterbestehen

Von den Konsequenzen der Aufhebung dieser Zertifizierungsrichtlinie (CP) und den Regelungen für den Zertifizierungsbetrieb (CPS) bleibt die Verantwortung zum Schutz vertraulicher Informationen und personenbezogener Daten unberührt.

10.9 Individuelle Mitteilungen und Absprachen mit Teilnehmern

In dieser Zertifizierungsrichtlinie werden keine entsprechenden Regelungen getroffen.

10.10 Ergänzungen

10.10.1 Verfahren für Ergänzungen

Änderungen der Zertifizierungsrichtlinie (CP) und den Regelungen für den Zertifizierungsbetrieb (CPS) werden rechtzeitig vor ihrem Inkrafttreten veröffentlicht.

10.10.2 Benachrichtigungsmechanismen und –fristen

Die Zertifikatsinhaber werden rechtzeitig vor dem Inkrafttreten auf die Änderung der Zertifizierungsrichtlinie (CP) und den Regelungen für den Zertifizierungsbetrieb (CPS) per signierter E-Mail hingewiesen.
Das Einverständnis von Geschäftspartnern mit den Änderungen gilt als erteilt, wenn der DARZ.CA bis zum Zeitpunkt des Inkrafttretens keine gegenteilige Erklärung mit signierter E-Mail zugeht. Auf diese Folge wird die DARZ.CA bei dem Hinweis auf die Änderung besonders aufmerksam machen. Sollte ein Geschäftspartner den Änderungen vor dem Zeitpunkt des Inkrafttretens in Form einer signierten E-Mail widersprechen, kommt es zu einem Klärungsgespräch zwischen dem Geschäftspartner und der DARZ GmbH. Sollte der Kunde die aktualisierte CP weiterhin nicht akzeptieren, wird die Sperrung aller Kundenzertifikate entsprechend Kap. 4.8 eingeleitet.
Beschäftigten der DARZ GmbH gegenüber gilt die im Intranet bekannt gemachte jeweils aktuelle Fassung.

10.10.3 Bedingungen für OID Änderungen

Der Richtlinienbezeichner ändert sich bis zum Ende der Gültigkeit der zugehörigen Zertifizierungsinstanz nicht.

10.11 Verfahren zur Schlichtung von Streitfällen

Die Anrufung eines Schiedsverfahrens liegt im Ermessen der DARZ GmbH.

10.12 Zugrunde liegendes Recht

Der Gerichtsstand ist Darmstadt.

10.13 Einhaltung geltenden Rechts

Es gilt deutsches Recht. Die von der DARZ.CA ausgestellten Zertifikate sind nicht konform zu qualifizierten Zertifikaten gemäß Signaturgesetz.

10.14 Sonstige Bestimmungen

10.14.1 Vollständigkeitserklärung

Alle Regelungen in dieser Zertifizierungsrichtlinie (CP) und Regelungen für den Zertifizierungsbetrieb (CPS) gelten zwischen der DARZ.CA und den Zertifikatsinhabern. Die Ausgabe einer neuen Version ersetzt alle vorherigen Versionen. Mündliche Vereinbarungen bzw. Nebenabreden sind nicht zulässig.

10.14.2 Abgrenzungen

Eine Abtretung von Rechten ist nicht vorgesehen.

10.14.3 Salvatorische Klausel

Sollten einzelne Bestimmungen dieser Zertifizierungsrichtlinie unwirksam sein oder werden, so lässt dies den übrigen Inhalt der Zertifizierungsrichtlinie unberührt. Auch eine Lücke berührt nicht die Wirksamkeit der Zertifizierungsrichtlinie im Übrigen. Anstelle der unwirksamen Bestimmung gilt diejenige wirksame Bestimmung als vereinbart, welche der ursprünglich gewollten am nächsten kommt oder nach Sinn und Zweck der Zertifizierungsrichtlinie geregelt worden wäre, sofern der Punkt bedacht worden wäre.

10.14.4 Vollstreckung (Anwaltsgebühren und Rechtsmittelverzicht)

Rechtliche Auseinandersetzungen, die aus dem Betrieb der DARZ.CA herrühren, obliegen den Gesetzen der Bundesrepublik Deutschland.
Erfüllungsort und Gerichtsstand ist Darmstadt.

10.14.5 Höhere Gewalt

Die DARZ GmbH übernimmt keine Haftung für die Verletzung einer Pflicht sowie für Verzug oder Nichterfüllung im Rahmen dieser Zertifizierungsrichtlinie (CP) und den Regelungen für den Zertifizierungsbetrieb (CPS), sofern das zugrundeliegende Ereignis außerhalb ihrer Kontrolle (z. B. höhere Gewalt, Kriegshandlungen, Netzausfälle, Brände, Erdbeben und andere Katastrophen) resultiert.

11. Abkürzungen

DARZ.CA	Sub-CA der DARZ GmbH innerhalb der SM-PKI-CP
DARZ-Test.CA	Test Sub-CA der DARZ GmbH innerhalb der SM-PKI-CP
BSI	Bundesamt für Sicherheit in der Informationstechnologie
CA	Certification Authority, Zertifizierungsinstanz
CN	Common Name (Bestandteil des Distinguished Name)
CP	Certificate Policy; Zertifizierungsrichtlinie einer PKI
CPS	Certification Practice Statement, Regelungen für den Zertifizierungsbetrieb
CRL	Certificate Revocation List, Sperrliste
DN	Distinguished Name
EMAIL	Email address (Bestandteil des Distinguished Name)
Hardwaretoken	Hardware zur Speicherung von privaten Schlüsseln
LDAP	Light Directory Access Protocol, Verzeichnisdienst
O	Organization (Bestandteil des Distinguished Name)
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OU	Organizational Unit (Bestandteil des Distinguished Name)
PKI	Public Key Infrastructure
RFC	Request for Comment, Dokumente für weltweite Standardisierungen
RFC 3647	Dieser RFC dient der Beschreibung von Dokumenten, die den Betrieb einer PKI beschreiben
Root-CA	oberste Zertifizierungsinstanz einer PKI
SHA 256	Secure Hash Algorithm No.2 Version
S/MIME	Secure Multipurpose Internet Mail Extensions, Standard für sichere E-Mail
Sperrliste	signierte Liste einer CA, die gesperrte Zertifikate enthält
TLS	Transport Layer Security (Protokoll zur Verschlüsselung einer Datenübertragung)
x.509v1	Zertifizierungsstandard
Zertifikat	sichere Zuordnung von öffentlichen Schlüsseln zu einem Teilnehmer

12. Literaturverweise

BSI-CC-PP-0073 (2014)	*Protection Profile für the Gateway of a Smart Metering System (Smart Meter Gateway PP),* Version 1.3. Bonn: BSI.
CP-SM-PKI (2017)	*Certificate Policy der Smart Metering PKI Version 1.1.1 (09.08.2017).* Bonn: BSI.
ISO/IEC 27001 (2015)	*IT-Sicherheitsverfahren – Informationssicherheits-Managementsysteme – Anforderungen.* DIN.
TR-03109-1 (2019)	*Anforderungen an die Interoperabilität der Kommunikationseinheit eines intelligenten* Messsystems. Version 1.0.1 (16.01.2019) Bonn: BSI.
TR-03109-4 (2017)	*Technische Richtlinie - Public Key Infrastruktur für Smart Meter Gateways Version 1.2.1 (09.08.2017).* Bonn: BSI.
TR-03109-6 (2015)	*Smart Meter Gateway Administration. Version 1.0 (26.11.2015)* Bonn: BSI.
TR-03116-3 (2019)	*Kryptographische Vorgaben für Projekte der Bundesregierung; Teil 3: Intelligente Messsysteme. Stand 2019 (11.01.2019)* Bonn: BSI.
TR-03145 (2017)	*Secure Certification Authority operation. Version 1.1 (27.03.2017)* Bonn: BSI.