Bundesamt
für Sicherheit in der
Informationstechnik

Certificate Policy der Smart Metering PKI

Version 1.1

Datum: 09.12.2016

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: +49 22899 9582-0

E-Mail: smartmetering-pki@bsi.bund.de
Internet: https://www.bsi.bund.de

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

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 ist, 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-03109-4] 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.

Das vorliegende Dokument beschreibt die Certificate Policy (CP) der SM-PKI, im Weiteren auch SM-PKI Policy genannt. Die SM-PKI Policy dient dazu, die technischen, personellen und organisatorischen Sicherheitsanforderungen für die Ausstellung von Zertifikaten in der SM-PKI zu beschreiben.

Die HAN-Zertifikate gemäß der [TR-03109-1] werden nicht mit der hier beschriebenen SM-PKI ausgestellt und verwaltet und werden aus diesem Grund in diesem Dokument nicht behandelt.

Die in der SM-PKI Policy 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 sowohl an die Betreiber der Root- oder einer Sub-CA als auch an die weiteren Teilnehmer und ist in Anlehnung an [RFC 3647] strukturiert und definiert. Nachfolgend wird die Struktur erläutert:

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

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

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

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

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

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

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

Die Verantwortlichkeit für die SM-PKI Policy sowie den Betrieb der Root obliegt dem Bundesamt für Sicherheit in der Informationstechnik (BSI) als Inhaber der Wurzelzertifikate der SM-PKI (siehe Gesetz zur Digitalisierung der Energiewende [GDEW]).

Das BSI behält sich vor, komplette Aufgaben oder Teilaufgaben von beauftragten Unternehmen ausführen zu lassen.

1.2 Name und Identifizierung des Dokuments

Dieses Dokument ist die Certificate Policy (CP) der deutschen Smart Metering PKI (SM-PKI) und kann über die folgenden Informationen identifiziert werden.

Identifikator	Wert
Titel	Certificate Policy der Smart Metering-PKI
Version	1.1
OID	0.4.0.127.0.7.3.4.1.1.1

Tabelle 1: Identifikation des Dokuments

Dieses Dokument kann unter https://www.bsi.bund.de/ bezogen werden.

1.3 PKI-Teilnehmer

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

Instanz der PKI	Zertifizierungsstelle	Registrierungsstelle	Zertifikatsnehmer	Zertifikatsnutzer
Root-CA	X	X	X	X
Sub-CA	X	X	X	X
GWA			X	X
GWH			X	X
EMT			X	X
SMGW			X	X

Tabelle 2: Übersicht der PKI-Teilnehmer

Unternehmen können mit ihrer Organisation mehrere Instanzen der SM-PKI wahrnehmen. Voraussetzung ist eine klare technische und organisatorische Separierung der Aufgabenbereiche sowie die Erfüllung aller Sicherheitsvorgaben der jeweiligen Instanz (siehe dazu auch die Maßnahmen zur Trennung der Instanzen im Kapitel 6.2.6). Zusätzlich MUSS bei den ausführenden Personen der Unternehmen darauf geachtet werden, dass kein Interessenkonflikt bei der Erfüllung der Aufgaben auftreten kann.

Entsprechend MUSS jede Instanz in einer Organisation je nach zugrundeliegender PKI-Rolle (siehe Tabelle 15) über ein ISMS und ein Rollen- und Rechtekonzept, oder eine vergleichbare Sicherheitsorganisation/-dokumentation, verfügen. Hierbei MUSS technisch und oder organisatorisch sichergestellt werden, dass die Trennung der Instanzen hinsichtlich der Durchführung der SM-PKI relevanten Prozesse, insbesondere die Beantragung und Ausstellung von Zertifikaten, nicht umgangen werden kann.

1.3.1 Zertifizierungsstellen

In diesem Unterkapitel werden nachfolgend die CAs der PKI beschrieben.

Neben dem Wirksystem MUSS eine CA in der SM-PKI für Testzwecke (z.B. bei der Erst-Registrierung und zum Test systemkritischer Vorgänge wie dem Wechsel des Vertrauensankers) auch jeweils eine Test-CA bereitstellen. Mit den Test-CAs wird eine Test-PKI (genannt SM-Test-PKI) betrieben, Details zu den Anforderungen an diese Systeme sind in dem Anhang C definiert.

Die technische Infrastruktur der Test-CA MUSS funktional der einer Wirk-CA entsprechen. Hierbei MUSS die Test-CA informationstechnisch von der Wirk-CA getrennt sein, und die verwendeten Schlüssel MÜSSEN unterschiedlich sein.

Nachfolgend werden die unterschiedlichen Bestandteile der CAs der Smart Metering PKI erläutert. In der folgenden Abbildung ist dargestellt, wo die verschiedenen CA-Systeme miteinander verbunden sind:

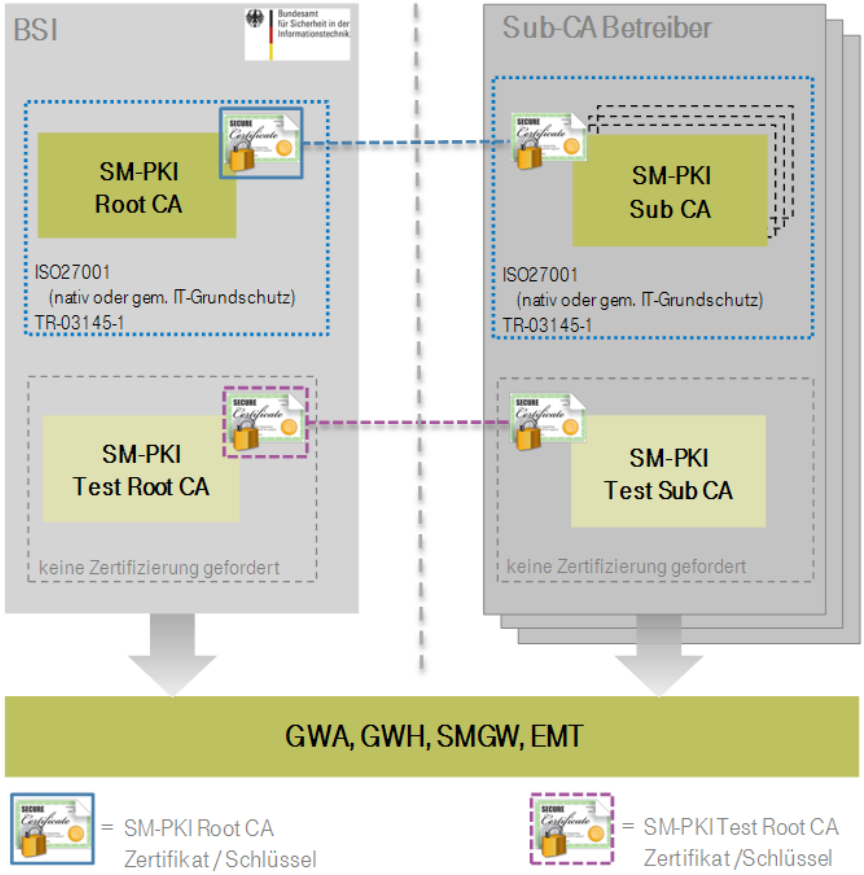

Abbildung 1: Schaubild der CA-Systeme der SM-PKI

1.3.1.1 Root-CA

Die Root-CA bildet den nationalen Vertrauensanker der SM-PKI für die Berechtigung zur Ausstellung und Nutzung der Zertifikate und ist der Herausgeber dieser SM-PKI Policy.

1.3.1.2 Sub-CA

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

Der Betrieb einer Sub-CA kann auf unterschiedliche Arten erfolgen, die in der [TR-03109-4] beschrieben sind. Diese SM-PKI Policy definiert Sicherheitsvorgaben für den Betrieb einer Sub-CA.

1.3.2 Registrierungsstellen

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

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

Eine Sub-CA verfügt jeweils über eigene Registrierungsstellen (RA der Sub-CA). Diese sind für die initialen Registrierungen sowie die Wiederholungsanträge der Endnutzer zuständig. Die Grundlage für die Prozesse der RA bilden die Vorgaben dieser SM-PKI Policy.

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 einer Sub-CA mit Zertifikaten ausgestattet wird, 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 (siehe [TR-03109-6]).

Ein GWA erhält von einer oder mehreren Sub-CA Zertifikate, mit denen dieser insbesondere

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

Ein GWA KANN die Verwaltung von SMGWs gemäß [TR-03109-6] als Dienstleistung anbieten. Hierzu KANN der GWA ein bereits vom ihm genutztes Zertifikat verwenden, auch wenn aus diesem nicht der Auftraggeber hervorgeht. Werden Teile des GWAs durch Dienstleister realisiert, so MUSS dies im ISMS des GWA und des Auftraggebers abgebildet werden und [TR-03109-6] konform sein.

1.3.3.3 Gateway-Hersteller

Ein Hersteller von Gateway-Komponenten (GWH) erhält von einer Sub-CA der SM-PKI Zertifikate, 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) erhält von einer Sub-CA der SM-PKI Zertifikate, 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 Geräte (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 werden.

Für die Kommunikation kann der Dienstleister ein bereits vom ihm genutztes Zertifikat verwenden, auch wenn aus diesem nicht der Auftraggeber hervorgeht. Alternativ kann er auch je Auftraggeber ein individuelles Zertifikat nutzen, wobei hierbei auf die Trennung der auftraggeberspezifischen Schlüssel in unterschiedlichen Verwaltungsbereichen des Kryptographiemoduls zu erfolgen hat. Die Verwaltungsbereiche müssen jeweils durch ein eigenes Geheimnis geschützt werden.

1.3.4 Zertifikatsnutzer

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

1.3.5 Andere Teilnehmer

Teilnehmer (wie z.B. Endverbraucher), welche keine Verpflichtung im Rahmen dieser SM-PKI Policy eingegangen sind, sind nicht Bestandteil der SM-PKI Policy und werden daher nicht berücksichtigt. Ergeben sich beispielsweise durch die internationale Anbindung anderer Infrastrukturen weitere Teilnehmer, so MÜSSEN sowohl deren PKI-Rollen als auch deren Interaktionen den Sicherheitsanforderungen aus dieser SM-PKI Policy entsprechen.

1.4 Verwendung von Zertifikaten

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

1.4.1 Erlaubte Verwendung von Zertifikaten

Jeder SM-PKI-Teilnehmer benötigt für die Ausübung seiner PKI-Rolle entsprechende Zertifikate aus der SM-PKI. Ein Teilnehmer KANN über mehrere Zertifikate bzw. Zertifikatstriple (siehe [TR-03109-4]) verfügen (siehe Abschnitt 4.1.1).

Das Schlüsselmaterial der SM-PKI-Teilnehmer kann zur Authentisierung, zur Verschlüsselung und zur Erstellung von elektronischen Signaturen eingesetzt werden. Die Anwendungsfälle für den Einsatz der Schlüssel und Zertifikate beim SMGW sind in der [TR-03109] beschrieben.

In den nachfolgenden Tabellen werden alle Zertifikate den unterschiedlichen PKI-Teilnehmern zugeordnet und der entsprechende Verwendungszweck erläutert. Alle weiteren Informationen können der [TR-03109-4] entnommen werden.

Root-CA:

Zertifikat der Root-CA	Signiert durch	Verwendungszweck
C(Root)	Privater Schlüssel zu C(Root)	Vertrauensanker der SM-PKI: Der öffentliche Schlüssel aus dem Zertifikat wird zur Überprüfung der Signatur von nachgeordneten Zertifikaten benötigt. Der zugehörige private Schlüssel wird für die Signatur von Sub-CA-, sowie von C(Root)-, Link-C(Root)-, C_{CRL-S}(Root)- und C_{TLS-S}(Root)-Zertifikaten verwendet.
Link-C(Root)	Privater Schlüssel zu C(Root)	Das Link-C(Root)-Zertifikat dient zur Echtheitsprüfung eines neuen C(Root). Mit diesem Zertifikat kann das aktuelle C(Root) mit dem vorherigen C(Root) verifiziert werden (gilt nicht für die initiale Root, da dieser Prozess erst ab dem ersten „Folgezertifikat“ genutzt werden kann).
C_{CRL-S}(Root)	Privater Schlüssel zu C(Root)	Mit Hilfe dieses Zertifikats kann die Signatur der Sperrliste (Root-CA-CRL) verifiziert werden. Der zugehörige private Schlüssel wird für die Signatur der Root-CA-CRL verwendet.
C_{TLS-S}(Root)	Privater Schlüssel zu C(Root)	Dieses Zertifikat wird bei der Verifikation der C_{TLS}(Root)-Zertifikate und der Sperrliste (Root-TLS-CRL) verwendet. Der zugehörige private Schlüssel wird für die Signatur von $C_{TLS,Root}$(Sub-CA)-Zertifikaten, C_{TLS}(Root)-Zertifikaten und der Root-TLS-CRL verwendet.
C_{TLS}(Root)	Privater Schlüssel zu C_{TLS-S}(Root)	Diese Zertifikate werden beim Aufbau des TLS-Kommunikationskanals (siehe [TR-03116-3]) zwischen Root und anderen Systemen eingesetzt.

Tabelle 3: Zertifikate der Root-CA

Sub-CA:

Zertifikat einer Sub-CA	Signiert durch	Verwendungszweck
C(Sub-CA)	Privater Schlüssel zu C(Root)	Der öffentliche Schlüssel aus dem Zertifikat wird zur Überprüfung der Signatur von nachgeordneten Zertifikaten benötigt, welche mit dem zum Zertifikat passenden privaten Schlüssel signiert wurden. Der zugehörige private Schlüssel wird für die Signatur von GWA, GWH, EMT, SMGW-,C_{TLS}(Sub-CA)-Zertifikaten und der Sperrliste der Sub-CA verwendet.
$C_{TLS,Root}$(Sub-CA)	Privater Schlüssel zu C_{TLS-S}(Root)	Diese Zertifikate werden beim Aufbau des TLS-Kommunikationskanals (siehe [TR-03116-3]) zwischen Sub-CA und der Root für das Zertifikatsmanagement eingesetzt.
C_{TLS}(Sub-CA)	Privater Schlüssel zu C(Sub-CA)	Diese Zertifikate werden beim Aufbau des TLS-Kommunikationskanals (siehe [TR-03116-3]) zwischen Sub-CA und anderen Systemen eingesetzt.

Tabelle 4: Zertifikate der Sub-CA

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

Zertifikat eines Zertifikatsnehmers	Signiert durch	Verwendungszweck
C_{TLS}(EMT) C_{TLS}(GWA) C_{TLS}(GWH) C_{TLS}(SMGW)	Privater Schlüssel zu C(Sub-CA)	Zertifikat des entsprechenden Endnutzers zur Authentisierung beim Kommunikationspartner und zum Aufbau einer TLS-Verbindung (siehe [TR-03116-3]). Das Zertifikat C_{TLS}(GWA) wird zudem auch für die Authentifikation am Sicherheitsmodul des SMGW verwendet.
C_{Enc}(EMT) C_{Enc}(GWA) C_{Enc}(GWH) C_{Enc}(SMGW)	Privater Schlüssel zu C(Sub-CA)	Zertifikat zur Verschlüsselung von Inhaltsdaten für den entsprechenden Endnutzer.
C_{Sig}(EMT) C_{Sig}(GWA) C_{Sig}(GWH) C_{Sig}(SMGW)	Privater Schlüssel zu C(Sub-CA)	Zertifikat zur Verifikation von Inhaltsdatensignaturen des entsprechenden Endnutzers.

Tabelle 5: Zertifikate der Zertifikatsnehmer

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

Für die Kommunikation der Ansprechpartner (ASP) in den unterschiedlichen Ebenen ist der Informationsaustausch mittels verschlüsselter und signierter E-Mails vorgesehen. Diese Zertifikate werden nicht von der SM-PKI bereitgestellt, die Anforderungen an diese Zertifikate sind in Tabelle 6 definiert: :

Zertifikat einer Ansprechpartners	Verwendungszweck
$C_{S/MIME}$(ASP Root) $C_{S/MIME}$(ASP Sub-CA) $C_{S/MIME}$(ASP GWA) $C_{S/MIME}$(ASP GWH) $C_{S/MIME}$(ASP EMT)	Zertifikat für den privaten Schlüssel, der vom Ansprechpartner der Root, einer Sub-CA, eines GWA, eines GWH, eines EMT für die Signatur und Verschlüsselung der E-Mail-Kommunikation eingesetzt wird. Je nach Realisierung der ausstellenden CA KÖNNEN für die Signatur und die Verschlüsselung auch unterschiedliche Zertifikate eingesetzt werden. Es MUSS bei dem Zertifikat eine Zuordnung zwischen dem Ansprechpartner und den Angaben im Zertifikat möglich sein (personalisiertes bzw. persönliches Zertifikat). Der ergänzende Einsatz von Funktionspostfächern (Zugriff und Nutzung durch mehrere Anwender) ist nur zum Empfang von Mails gestattet, sofern die Kommunikation mit den identischen Mechanismen abgesichert wird (Funktionspostfach muss über eine entsprechendes Verschlüsselungszertifikat verfügen). Der Versand von allgemeinen bzw. öffentlichen Informationen kann optional auch unverschlüsselt erfolgen. Es wird EMPFOHLEN, dass Zertifikate den Anforderungen der [TR-03116-4] entsprechen. Grundsätzlich kommen hier die Zertifikate zum Einsatz, welche durch den Ansprechpartner bereitgestellt werden. Vor dem Ablauf des personenbezogenen Zertifikats muss der Ansprechpartner ein neues Zertifikat zur Verfügung stellen, so dass durchgehend ein sicherer Kommunikationskanal bereitgestellt wird. Die Übermittlung des neuen Zertifikats erfolgt dabei mittels einer mit dem alten, noch gültigen Zertifikat signierten E-Mail (alternativ mit einer entsprechenden E-Mail eines anderen Ansprechpartners).

Tabelle 6: Kommunikationszertifikate der Ansprechpartner

1.4.2 Verbotene Verwendung von Zertifikaten

Die Zertifikate MÜSSEN gemäß ihres Verwendungszwecks (siehe Abschnitt 1.4.1) eingesetzt werden.

1.5 Administration der SM-PKI Policy

Die für dieses Dokument verantwortliche Organisation ist das Bundesamt für Sicherheit in der Informationstechnik (BSI). Das BSI kann über folgende Adresse kontaktiert werden:

Organisation	Bundesamt für Sicherheit in der Informationstechnik
Abteilung	Sichere elektronische Identitäten, Zertifizierung und Standardisierung
Adresse	Godesberger Allee 185 – 189 53175 Bonn
Fax	+49 22899 9582 5477
E-Mail	smartmetering-pki@bsi.bund.de
Webseite	https://www.bsi.bund.de/SM-PKI

Tabelle 7: Kontaktadresse

1.5.1 Pflege der SM-PKI Policy

Jede aktualisierte Version der SM-PKI Policy wird den Anwendern unverzüglich über die angegebene Internetseite (siehe 1.5) zur Verfügung gestellt.

Überdies wird über die Internetseite ein Changelog bereitgestellt, um Klarstellungen oder kleinere Änderungen zur SM-PKI Policy oder zu [TR-03109-4] kurzfristig veröffentlichen zu können.

1.5.2 Zuständigkeit für das Dokument

Zuständig für die Erweiterung und oder die nachträgliche Änderungen dieser SM-PKI Policy ist die Root.

1.5.3 Ansprechpartner / Kontaktperson

Siehe Tabelle 7.

1.5.4 Zuständiger für die Anerkennung eines CPS

Ein CPS (Certificate Practice Statement) einer CA ist ein Dokument, welches Bestandteil der Betriebsdokumentation ist.

1.5.5 CPS-Aufnahmeverfahren

Ein CPS der SM-PKI MUSS konform zu dieser CP sein.

2 Verantwortlichkeit für Veröffentlichungen und Verzeichnisse

2.1 Verzeichnisse

Von der Root-CA sowie von allen Sub-CAs MUSS jeweils ein Verzeichnisdienst gemäß [TR-03109-4] bereitstellt werden.

Zusätzlich MUSS von der Root-CA und allen Sub-CAs jeweils eine auf deren Verantwortungsbereich beschränkte Sperrliste erzeugt werden, in der alle gesperrten Zertifikate während ihres Gültigkeitszeitraums aufgeführt sind.

2.2 Veröffentlichung von Informationen zur Zertifikatserstellung

2.2.1 Veröffentlichungen der Root-CA

Die Root-CA MUSS über ihre Webseiten folgende Informationen bereitstellen:

- Kontaktdaten der Root
- Diese SM-PKI Policy
- Die aktuellen Zertifikate der Root-CA inklusive der SHA256 Hashs
- Parameter zur Einrichtung eines Zugriffs auf die Sperrliste bzw. auf das LDAP-Verzeichnis
- Beschreibung des Antragsverfahrens für eine Sub-CA Berechtigung
- Formular zur Beantragung einer Sub-CA Berechtigung
- Informationen zu den zu erstellenden Sub-CA Zertifikatsrequests
- Informationen zum Sperrprozess für Sub-CA Zertifikate
- Hinweise zur Teilnahme an der Testinfrastruktur (Test-PKI)
- Link zu den allgemeinen Informationen des BSI zum Thema Smart Metering und den relevanten TRs
- Changelog zur SM-PKI Policy und [TR-03109-4]

2.2.2 Veröffentlichungen der Sub-CA

Eine Sub-CA MUSS über eine Web-Seite verfügen, welche die folgenden Informationen beinhaltet:

- Kontaktdaten der Sub-CA
- Die aktuellen Zertifikate der Sub-CA inklusive der SHA256 Hashs. Das Format, in dem die Zertifikate und Hashs vorliegen, muss angegeben werden.
- Parameter zur Einrichtung eines Zugriffs auf die Sperrliste bzw. das LDAP-Verzeichnis
- Certificate Policy der Sub-CA mit folgenden Mindestanforderungen:
  - Die CP MUSS die Anforderungen und somit die Einhaltung dieser SM-PKI Policy bestätigen.
  - Die CP MUSS die für die Bereitstellung und Verwaltung der Zertifikate notwendigen Prozesse grundsätzlich beschreiben. Diesbezüglich kann auch auf die entsprechenden Stellen in dieser SM-PKI Policy verwiesen werden.

- Die CP MUSS die für den Betrieb verantwortlichen Bereiche / Ansprechpartner benennen.

Die folgenden weiteren Informationen SOLLTEN bereitgestellt werden:

– Beschreibung des Antragsverfahrens von Zertifikaten unterhalb dieser Sub-CA

– Formulare zur Beantragung von Zertifikaten

– Informationen zu den zu erstellenden jeweiligen Zertifikatsrequests

– Informationen zum Sperrprozess von Zertifikaten

– Hinweise zur Teilnahme am Testsystem

2.3 Zeitpunkt und Häufigkeit der Veröffentlichungen

Alle Zertifikate innerhalb der SM-PKI MÜSSEN unmittelbar nach der Ausstellung im jeweiligen LDAP-Verzeichnis veröffentlicht werden.

Eine Sperrung oder Suspendierung wird nach Durchführung durch eine Veröffentlichung in der jeweiligen Sperrliste der Root-CA / Sub-CA als solche wirksam. Eine Aufnahme in die Sperrliste sowie deren Veröffentlichung erfolgt gemäß den in der Tabelle 10 festgelegten Zeiten.

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

2.4 Zugriffskontrollen auf Verzeichnisse

Der lesende Zugriff auf die LDAP-Verzeichnisdienste MUSS auf die an der SM-PKI teilnehmenden Organisationen beschränkt werden[1]. Dies wird über eine zertifikatsbasierte Authentisierung am jeweiligen Verzeichnisdienst mittels der TLS-Zertifikate der Zertifikatsnehmer gemäß der Anforderungen aus [TR-03116-3] sichergestellt.

Ein Verzeichnisdienst in der SM-PKI dient ausschließlich der Aktualisierung von angefragten Zertifikaten. Ein Massenabruf von Zertifikaten DARF NICHT erfolgen. Es wird EMPFOHLEN, den Verzeichnisdienst so zu konfigurieren, dass die Anzahl der zurückgegebenen Suchergebnisse geeignet begrenzt ist. Die Rahmenbedingungen für die Abfrage und insbesondere die Suche von Zertifikaten aus dem Verzeichnis der Sub-CA werden in der jeweiligen Certificate Policy der Sub-CA dokumentiert.

Der lesende Zugriff auf die Sperrlisten einer CA MUSS ohne Authentifikation und ohne Einschränkungen erfolgen können.

1 Ein SMGW verfügt über keine Schnittstellen zu den Verzeichnisdiensten, so dass diese Zertifikate für den Zugriff auch nicht freigeschaltet werden müssen.

3 Identifizierung und Authentifizierung

Dieses Kapitel beschreibt die durchzuführenden Prozeduren, um die Identität und die Berechtigung eines Antragstellers (**Sub-CA**, **EMT, GWA, GWH** oder **SMGW)** vor dem Ausstellen eines Zertifikats festzustellen.

Das Profil eines Zertifikatsrequests MUSS konform zu [TR-03109-4] sein.

3.1 Regeln für die Namensgebung

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

3.1.1 Arten von Namen

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

3.1.2 Notwendigkeit für aussagefähige Namen

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

3.1.3 Anonymität oder Pseudonymität von Zertifikatsnehmern

Der Zertifikatsnehmer DARF NICHT anonym sein oder Pseudonyme verwenden.

3.1.4 Eindeutigkeit von Namen

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

Eine Namensgleichheit (gleicher CN bei unterschiedlichem Zertifikatsnehmer) MUSS durch die CAs verhindert werden, entsprechend DARF eine CA einen CN NICHT mehrfach vergeben.

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

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

3.1.5 Anerkennung, Authentifizierung und die Rolle von Markennamen

Die Eintragung der Firmennamen MÜSSEN gemäß den Vorgaben aus Kapitel 3.1.1 auf Basis der Identität, die im Rahmen der initialen Überprüfung in das erste Zertifikat übernommen wurde, erfolgen.

3.2 Initiale Überprüfung zur Teilnahme an der PKI

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

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

Auf der **Root-Ebene** wird das Ausstellen des selbstsignierten C(Root) sowie der $C_{CRL\text{-}S}$(Root), $C_{TLS\text{-}S}$(Root), C_{TLS}(Root) und Link-C(Root)-Zertifikate nicht betrachtet, da die Registrierungsstelle und der Betrieb für die Root eine organisatorische Einheit bilden. Somit ist eine Identifizierung und Authentifizierung auf Root-Ebene gegeben.

3.2.1 Methoden zur Überprüfung bzgl. Besitz des privaten Schlüssels

Zum Nachweis des Besitzes des privaten Schlüssels MUSS ein Zertifikatsrequest gemäß [TR-03109-4] eine sogenannte innere Signatur beinhalten.

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

3.2.2 Authentifizierung von Organisationszugehörigkeiten

Die nachfolgenden Organisationen DÜRFEN innerhalb der SM-PKI Zertifikatsanträge stellen. Hierbei wird speziell zwischen den Prozessen zur Ausgabe von Sub-CA Zertifikaten und von nachgeordneten Zertifikaten der EMT, GWA, GWH und SMGW unterschieden.

3.2.2.1 Sub-CA

Zur initialen Autorisierung einer neuen Sub-CA MÜSSEN das Unternehmen authentifiziert und mindestens zwei bevollmächtigte Vertreter des Betreibers persönlich bei dem Betreiber der Root-CA identifiziert und authentifiziert werden.

Notwendige Unterlagen und Daten für die Registrierung sind:

- Antragsschreiben zum Aufbau einer Sub-CA mit folgenden Daten bzw. beigefügten Informationen
  - Name der Firma bzw. der Institution
  - Anschrift des Unternehmens bzw. der Institution
  - Unternehmensnachweis (z.B. aktueller Auszug aus dem Handelsregister) oder Nachweis der Institution (durch ein entsprechendes Siegel der Institution)
  - Aussage zum Typ der geplanten Sub-CA (unternehmensintern oder -übergreifend)
  - Bei der Beauftragung eines Dienstleisters für den Betrieb einer Sub-CA MUSS der Betreiber eine Bestätigung des beauftragenden Unternehmens vorlegen, welches den Dienstleister zur Beantragung und zum Betrieb der Sub-CA berechtigt.
  - Kontaktdaten der Ansprechpartner (unter Beachtung einer Vertreterregelung)
  - Bestätigung der Geschäftsführung des Unternehmens bzw. der Leitung der Institution, in der der Vertreter des Betreibers berechtigt wird, den Antrag für die Sub-CA zu stellen und in der Sache dazu verbindliche Aussagen und Angaben zu machen.
- Persönliche/individuelle Zertifikate für die gesicherte E-Mail-Kommunikation der benannten Ansprechpartner ($C_{S/MIME}$(Sub-CA)), ggf. inklusive der zur Verifikation erforderlichen Zertifikatskette.
- Certificate Policy der Sub-CA (siehe Abschnitt 2.2.2)
- Nachweis zum sicheren Betrieb der Sub-CA gemäß den Vorgaben zu den Anforderungen für die Teilnahme an der SM-PKI (s. Tabelle 15).
- Bestätigung der erfolgreichen Testteilnahme (ausgestellt von der Test-Root-CA)

  - Vor der initialen Identifizierung und Authentifizierung MUSS der Betrieb der Sub-CA im Rahmen einer Testteilnahme unterhalb der Test-Root-CA (siehe Abschnitt 1.3.1) erfolgreich erprobt worden sein. In diesem Test MÜSSEN mindestens eine Zertifikatsbeantragung und eine Zertifikatssperrung erfolgreich durchlaufen werden. Die erfolgreiche Teilnahme wird von einem Ansprechpartner der Test-Root-CA per signierter E-Mail bestätigt.

– Die Hashwerte (SHA 256) der initialen Zertifikatsrequests für das Signatur- (C(Sub-CA)) und das TLS-Zertifikat ($C_{TLS,Root}$(Sub-CA)) der Sub-CA (gemäß [TR-03109-4]) MÜSSEN in gedruckter Form inklusive der Information zum Format der Darstellung mit der Bestätigung durch die Unterschrift des Bevollmächtigten vorgelegt werden. 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 dem Root-Betreiber vorab zuzusenden, so dass vor dem Termin eine Überprüfung auf Konformität erfolgen kann.

3.2.2.2 EMT

Zur Aufnahme eines neuen EMT in die SM-PKI MUSS durch den Sub-CA-Betreiber eine Authentifikation des Unternehmens erfolgen.

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 MUSS der Betreiber eine Bestätigung des Unternehmens vorlegen, 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 Betreibers 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 ($C_{S/MIME}$(EMT)) inklusive der zur Verifikation erforderlichen Zertifikatskette.
– Erklärung zur Nutzung des EMT-Zertifikats
  - Aus der Erklärung MUSS nachvollzogen werden können, welche Funktionen und Aufgaben ein EMT wahrnehmen will. Es MUSS daraus insbesondere hervorgehen, ob es sich um einen aktiven oder passiven EMT handelt.
  - Möchte ein passiver EMT nachträglich auch die Aufgaben eines aktiven EMTs (siehe Abschnitt 1.3.3.4) wahrnehmen oder möchte ein aktiver EMT nur noch als passiver EMT auftreten, so MUSS das Unternehmen dies der Sub-CA rechtzeitig und eigenverantwortlich mitteilen und die entsprechenden Unterlagen vorlegen.

  - Die Aufgaben des aktiven EMT dürfen erst vom Antragssteller mit dem bestehenden Zertifikat ausgeübt werden, wenn die erfolgreiche Registrierung als aktiver EMT von der Sub-CA bestätigt wurde. Die Bestätigung MUSS per signierter E-Mail an den registrieren Ansprechpartner gesendet werden.
  - Die zusätzlichen Auflagen für den Betrieb des aktiven EMT fallen erst weg, wenn der Rollenwechsel von der Sub-CA bestätigt wurde. Die Bestätigung MUSS per signierter E-Mail an den registrieren Ansprechpartner gesendet werden.
- Erklärung zur Einhaltung der Sicherheitsvorgaben aus dieser SM-PKI Policy
  - Der EMT MUSS eine Erklärung zur Einhaltung der Sicherheitsvorgaben aus dieser SM-PKI Policy mit einreichen.
  - Der EMT MUSS den Nachweis des sicheren Betriebs gemäß den Vorgaben zu den Anforderungen für die Teilnahme an der SM-PKI (s. Tabelle 15) erbringen.
- Bestätigung der erfolgreichen Testteilnahme (ausgestellt von der entsprechenden Test-Sub-CA)
  - Vor der Wirkbetriebsaufnahme MÜSSEN die Prozesse zum Zertifikatsmanagement (insbesondere Registrierung, Zertifikatsbeantragung, -erneuerung, -sperrung) mit der Test-Sub-CA des jeweiligen Sub-CA-Betreibers erfolgreich durchgeführt worden sein. Die erfolgreiche Teilnahme wird von einem Ansprechpartner der Test-Sub-CA per signierter E-Mail bestätigt.
- 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]) MUSS in gedruckter Form inklusive der Information zum Format der Darstellung mit der Bestätigung durch die Unterschrift des Bevollmächtigten zugesendet werden. 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.

3.2.2.3 GWA

Zur Aufnahme eines neuen GWA in die SM-PKI MUSS das Unternehmen authentifiziert werden, und mindestens zwei bevollmächtigte Vertreter des GWA MÜSSEN persönlich bei dem Betreiber der ausgewählten Sub-CA identifiziert und authentifiziert werden.

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 Betreibers 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 ($C_{S/MIME}$(GWA)) inklusive der zur Verifikation erforderlichen Zertifikatskette
- Nachweise über die Einhaltung der Vorgaben zu den Anforderungen für die Teilnahme an der SM-PKI (s. Tabelle 15)

– Bestätigung der erfolgreichen Testteilnahme
  - Vor der Wirkbetriebsaufnahme MÜSSEN die Prozesse zum Zertifikatsmanagment (insbesondere Registrierung, Zertifikatsbeantragung, -erneuerung, -sperrung) von GWA- und SMGW-Zertifikaten mit der Test-Sub-CA (siehe Abschnitt 1.3.1) des ausgewählten Sub-CA-Betreibers erfolgreich durchgeführt worden sein. Die erfolgreiche Teilnahme wird von einem Ansprechpartner der Test-Sub-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]) MUSS in gedruckter Form inklusive der Information zum Format der Darstellung mit der Bestätigung durch die Unterschrift des Bevollmächtigten vorgelegt werden. 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, Zertifikatsrequests dem Sub-CA-Betreiber vorab zuzusenden, so dass vor dem Termin eine Überprüfung auf Konformität erfolgen kann.

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

3.2.2.4 GWH

Zur Aufnahme eines neuen GWH in die SM-PKI MÜSSEN das Unternehmen authentifiziert und mindestens zwei bevollmächtigte Vertreter des GWH persönlich bei dem Betreiber der ausgewählten Sub-CA identifiziert und authentifiziert werden.

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 Betreibers 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 ($C_{S/MIME}$(GWH)) inklusive der zur Verifikation erforderlichen Zertifikatskette
– Der GWH MUSS eine Erklärung zur Einhaltung der Sicherheitsvorgaben aus dieser SM-PKI Policy für die Teilnahme an der SM-PKI (s. Tabelle 15) vorlegen.
– Bestätigung der erfolgreichen Testteilnahme
  - Vor der Wirkbetriebsaufnahme MÜSSEN die Prozesse zum Zertifikatsmanagment (insbesondere Registrierung, Zertifikatsbeantragung, -erneuerung, -sperrung) von GWH und SMGW-Gütesiegelzertifikaten mit der Test-Sub-CA (siehe Abschnitt 1.3.1) des ausgewählten Sub-CA Betreibers erfolgreich durchgeführt worden sein. Die erfolgreiche Teilnahme wird von einem Ansprechpartner der Test-Sub-CA per signierter E-Mail bestätigt.

– Der Hashwert (SHA 256) des initialen Zertifikatsrequest-Pakets für das Signatur- (C_{Sig}(GWH)), das Verschlüsselungs- (C_{Enc}(GWH)) und das TLS-Zertifikat (C_{TLS}(GWH)) des GWH (gemäß [TR-03109-4]) MUSS in gedruckter Form inklusive der Information zum Format der Darstellung mit der Bestätigung durch die Unterschrift des Bevollmächtigten vorgelegt werden. 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, Zertifikatsrequests dem Sub-CA-Betreiber vorab zuzusenden, so dass vor dem Termin eine Überprüfung auf Konformität erfolgen kann.

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

3.2.2.5 SMGW

Das SMGW kann selbst keine Zertifikate beantragen. Entsprechend beantragt eine dritte Partei stellvertretend für das SMGW die Zertifikate, siehe [TR-03109-4]. 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 ist, dass der GWH bei einer Sub-CA registriert ist (siehe Abschnitt 3.2.2.4) und über gültige Zertifikate verfügt. Dabei MÜSSEN die Anforderungen aus Tabelle 15 eingehalten werden.

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

Der GWH MUSS das Sicherheitsmodul im SMGW so ansteuern, 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 von dem GWH ausgewählte Sub-CA über einen gesicherten Kommunikationskanal gesendet.

Die von der Sub-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 ist, dass der für das SMGW zuständige GWA bei einer Sub-CA registriert ist (siehe Abschnitt 3.2.2.3) 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 einer sicheren TLS-Verbindung (siehe [TR-03116-3]) 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 MÜSSEN mit einer äußern Signatur (siehe [TR-03109-4]) versehen sein, um die Authentizität des SMGW nachzuweisen.
- Senden der Zertifikatsrequests an den GWA.
- Der GWA prüft die Zertifikatsrequests. Neben der syntaktischen Prüfung des Requests MÜSSEN auch die Gütesiegelzertifikate auf Gültigkeit geprüft werden. Nur wenn beide Prüfungen ein positives Ergebnis haben, DÜRFEN für dieses SMGW Wirkzertifikate beantragt werden.
- 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 MUSS über die per TLS-Verbindung gesicherte Web-Service-Schnittstelle an die Sub-CA gesendet werden.
- Die Authentizität des Zertifikatsrequest-Pakets MUSS durch die Sub-CA geprüft werden (siehe [TR--03109-4]. Es DÜRFEN ausschließlich für authentische SMGWs Wirkzertifikate ausgestellt werden, deren Beantragung durch den zugehörigen GWA autorisiert wurde.
- Die Wirkzertifikate werden von der Sub-CA erzeugt und über die Web-Service-Schnittstelle an den GWA übertragen
- Der GWA prüft die Wirkzertifikate 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 Angaben zum Zertifikatsnehmer

Die Registrierungsstelle MUSS die Angaben zum Zertifikatsnehmer im Zertifikatsrequest gegen die eingereichten Unterlagen auf Korrektheit prüfen (siehe Abschnitt 3.2.2).

3.2.5 Prüfung der Berechtigung zur Antragstellung

Siehe Abschnitt 3.2.

3.2.6 Kriterien für den Einsatz interoperierender Systeme/Einheiten

Aktuell sind keine Kriterien definiert.

3.2.7 Aktualisierung / Anpassung der Zertifizierungsinformationen der Teilnehmer

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

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

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

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 Root- bzw. der Sub-CA zur Verfügung stellen.

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

3.2.8 Aktualisierung / Anpassung der Registrierungsinformationen der Teilnehmer

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

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

Nach der initialen Zertifikatsausstellung erfolgen sogenannte Folgeanträge. Diese MÜSSEN ebenso wie die initialen Zertifikatsanträge zweifelsfrei von der jeweiligen CA identifiziert und authentisiert werden.

Bei einer Schlüsselerneuerung (Folgeantrag zu einem bestehenden Zertifikat) ist zu beachten, dass von dem Antragsteller immer ein neuer Schlüssel erstellt werden MUSS.

Ein Zertifikatsinhaber ist dafür verantwortlich, rechtzeitig, d.h. vor dem Ablauf aller Zertifikate, neue Zertifikate zu beantragen (vgl. [TR-03109-4]). Dies MUSS insbesondere bei den Zertifikaten (Gütesiegelzertifikate und Wirkzertifikate) für SMGWs beachtet werden. Der Zeitraum MUSS so gewählt werden, 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 zwei gleichzeitig gültigen Zertifikaten kommen. Diese Phase dient dazu, allen relevanten Komponenten rechtzeitig das neue Zertifikat mitzuteilen.

Der Antragsteller besitzt einen privaten Schlüssel des dem Betreiber zugeordneten TLS-Zertifikats, mit dem die Absicherung des Kommunikationskanals durchgeführt wird. 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 MUSS über die äußere Signatur die Echtheit des SMGW nachgewiesen werden, siehe [TR-03109-4].

Nach der erfolgreichen Prüfung eines routinemäßigen Folgeantrags erfolgt die Ausstellung des beantragten Zertifikats.

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 vorher beschriebene Regelprozess (routinemäßiger Folgeantrag) nicht genutzt werden. Die weitere Vorgehensweise unterscheidet sich anhand der dem Antragsteller zu diesem Zeitpunkt noch zur Verfügung stehenden Sicherheitsmechanismen.

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

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

Ungültige „Äußere Signatur“(z.B. ungültiges Signatur-Zertifikat)

Kann die Autorisation des Zertifikatsrequests nicht mehr über Signatur mit einem vorherigen, noch gültigen Signaturschlüssel erfolgen, MUSS ein neues initiales Zertifikatsrequest-Paket (identisch mit dem Zertifikatsrequest bei der ersten Beantragung der Zertifikate) übermittelt werden.

Verfügt der PKI-Teilnehmer noch über ein gültiges TLS-Zertifikat MUSS das neue initiale Zertifikatsrequest-Paket hiermit signiert und über einen gesicherten Kanal an die CA übermittelt werden.

Zusätzlich wird ebenfalls über einen gesicherten Kanal (z.B. eine verschlüsselte und signierte E-Mail des benannten ASP des Zertifikatsnehmers) der Hashwert des Zertifikats-Pakets 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 [ISO 19005-1] konformen Datei versendet wird.

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

Sonderfall SMGW

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

3.4.2 Schlüsselerneuerung nach Sperrungen

Das weitere Vorgehen zur Identifizierung und Authentifizierung eines PKI-Teilnehmers nach einer Sperrung ist davon abhängig, welche seiner Zertifikate von der Sperrung betroffen sind. Der PKI-Teilnehmer MUSS auf Basis der ihm zur Verfügung stehenden gültigen Zertifikate, einen Folgeantrag gemäß des vorangegangenen Unterkapitels stellen, um seine gesperrten Zertifikate durch neue gültige Zertifikate zu ersetzen. Ein Endnutzer MUSS immer ein neues Zertifikatstripel beantragen, wenn eines seiner Zertifikate gesperrt wurde.

3.5 Identifizierung und Authentifizierung von Anträgen auf Sperrung

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

- dem Zertifikatsinhaber oder
- der Root-CA bzw. der ausstellenden Sub-CA.

Bei einer Sperrung MÜSSEN dafür folgende Informationen an die Root- bzw. die Sub-CA von einem benannten Ansprechpartner mittels signierter E-Mail oder einem vergleichbar abgesicherten Kommunikationskanal übermittelt werden:

- Zertifikatstyp
- Ausstellende Sub-CA bzw. Root-CA
- Zertifikatsnummer (Der Wert des Felds “SerialNumber“ des Zertifikats, siehe [TR-03109-4])
- Sperrgrund
- Zeitpunkt, ab dem das Zertifikat als unsicher/gesperrt einzustufen ist (optional, nur wenn genauer Zeitpunkt bekannt ist)

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 den Betreiber der CA. Dieser prüft die Authentizität der Information und sperrt das Zertifikat.

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

Bei den SMGWs wird die Berechtigung zur Sperrung der Zertifikate von dem zuständigen GWH (nur Gütesiegelzertifikate) bzw. GWA (Gütesiegel- und Wirkzertifikate) wahrgenommen. Der GWH überträgt den Besitz der Gütesiegel-Zertifikate an den entsprechenden GWA (neuer Besitzer des SMGW). Die Übergabe MUSS rechtssicher dokumentiert werden. Damit ein GWA ein Gütesiegel-Zertifikat sperren kann, MUSS dieser den Besitzübergang gegenüber der Sub-CA über diese Dokumentation nachweisen. Die Sperrung eines SMGW MUSS über die Web-Service-Schnittelle der Sub-CA als Paket (enthält Zertifikatstripel, siehe [TR-03109-4].) 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) erfolgen.

Der Betreiber einer Sub-CA KANN zusätzliche Verfahren zur Initiierung einer Sperrung anbieten, sofern dieser über eine authentisierte und integre Kommunikationsschnittstelle verfügt. Diese optionalen Verfahren MÜSSEN in der Certificate Policy der Sub-CA beschrieben werden.

3.5.2 Initiative des Betreibers der Certificate Authority

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

- ein erkannter Verstoß gegen Betriebsauflagen (insbesondere gegen die Anforderungen für die Teilnahme an der SM-PKI (s. Tabelle 15)),
- 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 (Sub-CA und GWA) MÜSSEN in Abstimmung mit der Root erfolgen.

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

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

3.6 Identifizierung und Authentifizierung von Anträgen auf Suspendierung

Die Suspendierung der Zertifikate eines SMGW MUSS vom zugehörigen GWA bzw. durch den GWH (nur Gütesiegelzertifikate) durchgeführt werden.

Bei einer Suspendierung MÜSSEN dafür folgende Informationen an die Sub-CA übermittelt werden:

- Zertifikatstyp
- Ausstellende Sub-CA bzw. Root-CA
- Zertifikatsnummer (Der Wert des Felds “SerialNumber“ des Zertifikats, siehe [TR-03109-4])
- Grund für die Suspendierung

Die Suspendierung MUSS über die Web-Service-Schnittelle der Sub-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 MUSS über die Sperrliste der CA veröffentlicht werden. Der Zertifikatsinhaber (GWA) MUSS über den abgeschlossenen Sperrprozess informiert werden.

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

4.1 Zertifikatsantrag

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

4.1.1 Wer kann einen Zertifikatsantrag stellen?

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

Ein Endnutzer (nicht SMGW) KANN sofern erforderlich weitere Zertifikate bzw. Zertifikatstriple (siehe [TR-03109-4] für sich beantragen (z.B. für Lastmanagement oder Ausfallsicherheit).

Der Zertifikatsrequest MUSS als Folgeantrag (siehe Abschnitt 3.3) unter Nutzung der vorhandenen Zertifikate bei der Root-CA oder einer Sub-CA gestellt werden.

Die weiteren Zertifikate/Zertifikatstriple MÜSSEN eindeutig gekennzeichnet werden (siehe A). 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 jeweiligen CA verantwortlich.

4.2 Verarbeitung von initialen Zertifikatsanträgen

4.2.1 Durchführung der Identifizierung und Authentifizierung

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

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

Sollte einer der benannten und identifizierten Mitarbeiter ausscheiden, MUSS sich mindestens ein neuer Vertreter im Rahmen eines persönlichen Termins (vergleichbar dem im Abschnitt 3.2 beschriebenen Prozess)

bei der CA identifizieren lassen. Die Benennung des neuen Vertreters bzw. der neuen Vertreter sowie die Information über das Ausscheiden des bisherigen Vertreters MUSS von einem der benannten Ansprechpartner des Teilnehmers bestätigt werden.

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

Bei allen Prozessen zur Beantragung, Ausgabe und Verwaltung der Zertifikate MUSS bei der SM-PKI hinsichtlich der eingesetzten Kryptografie immer die aktuelle Version der [TR-03116-3] bei der Nutzung des Webservices bzw. SOLLTE die [TR-03116-4] zu der Absicherung der E-Mail-Kommunikation via S/MIME berücksichtigt werden.

4.2.2 Annahme oder Ablehnung von initialen Zertifikatsanträgen

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

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

Durch die RA MÜSSEN 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 werden.

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

4.2.3 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 Sub-CA Zertifikaten

Die Bearbeitung der Zertifikatsanträge gliedert sich in folgende Arbeitsschritte:

Arbeitsschritt	Beschreibung des Arbeitsschrittes	Zeitrahmen
1	Start des Beantragungsprozesses durch den Sub-CA Betreiber	-
2	Kontaktaufnahme zur Terminvereinbarung durch die Root-CA	1 Kalenderwoche (Der Root-Betreiber soll dabei einen Termin (für Arbeitsschritt 3) innerhalb der nachfolgenden 2 Kalenderwochen ermöglichen)
3	Übergabe der Dokumente / Nachweise im Rahmen eines persönlichen Termins	-
4	Vorprüfung der Unterlagen und Rückmeldung an den Sub-CA Betreiber	1 Kalenderwoche
5 (optional)	Nachlieferungsfrist für den Sub-CA Betreiber	3 Kalenderwochen
6	Prüfung der Unterlagen durch die Root-CA inkl. Rückmeldung an den Sub-CA Betreiber	2 Kalenderwochen
7	Ausstellung der Zertifikate für die Sub-CA	3 Arbeitstage

Tabelle 8: Zeitablauf für die initiale Ausgabe von Sub-CA Zertifikaten

Für die Einhaltung der hier definierten Zeiträume ist eine fristgerechte und fachliche Lieferung / Mitwirkung des Sub-CA Betreibers Voraussetzung. Sollten sich die Lieferungen / Zuarbeiten der Sub-CAs verzögern, können sich die Zeiten verlängern.

Grundsätzlich sind die in Tabelle 8 angegebenen Zeitrahmen als Obergrenze anzusehen.

4.2.3.2 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 Sub-CA	3 Arbeitstage (Der Sub-CA Betreiber soll dabei einen Termin (für Arbeitsschritt 3) innerhalb der nachfolgenden 3 Arbeitstage ermöglichen)
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 Sub-CA inkl. Rückmeldung an den Endnutzer	1 Kalenderwoche
7	Ausstellung der Zertifikate für Endnutzer	2 Arbeitstage

Tabelle 9: 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.

Die hier angegeben Werte sind als Richtwerte anzusehen, die von den Sub-CA-Betreibern in der jeweiligen Sub-CA-Policy konkretisiert werden MÜSSEN.

4.2.4 Ausgabe von Zertifikaten

Die Ausgabe von SMGW-Zertifikaten MUSS über die Web-Service-Schnittstelle erfolgen.

Bei Endnutzer-Zertifikaten SOLLTE, abgesehen von den initialen Zertifikaten für die Endnutzer, die Ausgabe über die Web-Service-Schnittstelle erfolgen. Die hier angegeben Zeitwerte sind als Richtwerte anzusehen, die von den Sub-CA-Betreibern in der jeweiligen Certificate Policy der Sub-CA konkretisiert werden MÜSSEN.

Die initialen Zertifikate MÜSSEN, Folgezertifikate KÖNNEN per E-Mail an den Ansprechpartner gesendet werden. Der Versand per E-Mail KANN unverschlüsselt erfolgen.

4.2.5 Benachrichtigung des Zertifikatsnehmers über die Ausgabe des Zertifikats

Der Ansprechpartner SOLLTE nach der Ausstellung eines initialen Zertifikats per E-Mail informiert werden.

4.3 Annahme von Zertifikaten

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

Bei einem SMGW kann diese Prüfung durch den GWH oder den GWA automatisiert z.B. bei dem Erhalt oder der Einbringung der Zertifikate erfolgen.

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

4.3.1 Veröffentlichung von Zertifikaten durch die CA

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

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 MÜSSEN gemäß ihrem Verwendungszweck eingesetzt werden, vgl. [TR-03109-4].

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

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

4.6 Zertifizierung nach Schlüsselerneuerung

4.6.1 Bedingungen der Zertifizierung nach Schlüsselerneuerungen

Es gelten die Anforderungen aus Kapitel 3.3.

4.6.2 Wer darf Zertifikate für Schlüsselerneuerungen beantragen?

Jeder PKI-Teilnehmer MUSS darauf achten, rechtzeitig vor Ablauf der Zertifikatslaufzeit ein neues Schlüsselpaar zu generieren und ein Zertifikat zu beantragen. Für ein SMGW MUSS dies vom zuständigen GWA durchgeführt werden.

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 (synchron bzw. asynchron)

Hier wird über eine gesicherte TLS-Verbindung (siehe [TR-03116-3]) ein Zertifikatsrequest gemäß [TR--03109-4]an die jeweils zuständige CA gesendet.

Folgeanträge über eine abgesicherte E-Mail Kommunikation

Bei einem Folgeantrag über die E-Mail-Schnittstelle wird der Zertifikatsrequest gemäß [TR-03109-4] vom benannten Ansprechpartner des Zertifikatsnehmers an die jeweilige 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 direkt ausgestellt. Bei einem nicht routinemäßigen Folgeantrag MUSS wie in Abschnitt 3.4 beschrieben verfahren werden.

4.6.4 Benachrichtigung des Zertifikatsnehmers über die Ausgabe eines Nachfolgezertifikats

Der Beantragende wird durch die Zustellung des Nachfolgezertifikats informiert.

Die sonstigen Teilnehmer der PKI 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, MUSS der Ansprechpartner des Zertifikatsnehmers eine Nachricht an die CA schicken. In einer solchen Nachricht ist der Grund für die Verweigerung der Annahme anzugeben. Bei fehlerhaften Zertifikaten sind, soweit möglich, die fehlerhaften bzw. unvollständigen Einträge zu benennen.

Bei einem SMGW kann diese Prüfung durch den GWH oder den GWA automatisiert z.B. bei dem Erhalt oder der Einbringung der Zertifikate erfolgen. Der Sub-CA Betreiber MUSS eine Kommunikationsschnittstelle für Fehlermeldungen bereitstellen. Die entsprechende Kommunikationsschnittstelle MUSS von der Sub-CA in der Sub-CA CP definiert werden.

4.6.6 Veröffentlichung von Zertifikaten für Schlüsselerneuerungen durch die CA

Alle ausgestellten Zertifikate MÜSSEN unmittelbar nach der Ausstellung in dem Verzeichnisdienst der jeweiligen CA veröffentlicht werden.

4.6.7 Benachrichtigung anderer PKI-Teilnehmer über die Ausgabe eines Nachfolgezertifikats

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

4.7 Änderungen am Zertifikat

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

4.8 Sperrung und Suspendierung von Zertifikaten

Die Initiierung der Sperrung eines Zertifikats kann durch den Zertifikatsnehmer, die für das Zertifikat zuständige CA und die Root eingeleitet werden. Die Sperrberechtigung für SMGW-Zertifikate liegt außerdem beim GWA bzw. vor der Übergabe beim GWH (vgl. Abschnitt 3.6).

4.8.1 Sperrung

Alle Zertifikate werden über die von der Root- bzw. Sub-CA bereitgestellten Schnittstellen/Prozesse gesperrt. Eine Sperrung kann nicht zurückgenommen werden. Eine Ausnahme stellt der Spezialfall Suspendierung dar (siehe Abschnitt 4.8.2).

Alle Sperrungen MÜSSEN unverzüglich umgesetzt und in die neue Sperrlisten aufgenommen werden. Die Veröffentlichung erfolgt gemäß den Vorgaben der [TR-03109-4].

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 MÜSSEN gemäß den Vorgaben aus [TR-03109-4] immer die aktuelle Sperrliste verwenden. In besonderen Fällen (Erstinbetriebnahme oder auf Aufforderung einer CA-Instanz) MÜSSEN neben den regelmäßigen Aktualisierungen auch neue Sperrlisten abgefragt werden.

4.8.2 Sperrung und Suspendierung von SMGW-Zertifikaten

Bei einem SMGW kann alternativ zu einer Sperrung auch eine Suspendierung der Zertifikate erfolgen (vgl. Abschnitt 3.6). 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 wieder zurückgenommen werden.

Eine Sperrung MUSS gemäß den Vorgaben im Kapitel 4.8.1 verarbeitet werden, und wird z.B. bei der Außerbetriebnahme des SMGW durchgeführt.

Eine Suspendierung eines SMGW-Zertifikats 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 des definierten Zeitraums mittels Zertifikatsrequest für das SMGW neue Zertifikate beantragen. Dabei werden die suspendierten Zertifikate für die Neubeantragung temporär von der Sperrliste entfernt. Diese Desuspendierung erfolgt, ebenso wie die Suspendierung, durch den GWA über die von der jeweiligen Sub-CA angebotenen Schnittstelle (Webservice, alternativ durch per S/MIME verschlüsselte und signierte E-Mail). Dabei MUSS der GWA sicherstellen, dass die Zertifikate des SMGW nur für die Neubeantragung genutzt werden. Nachdem das SMGW neue Zertifikate erhalten hat, MÜSSEN die alten Zertifikate als gesperrt in die Sperrliste eingetragen werden.

Die Sub-CA MUSS 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

prüfen.

Sind die Bedingungen erfüllt, werden die neuen Zertifikate erstellt und durch den GWA in das SMGW eingebracht. 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 Teilnehmer als gesperrte Zertifikate behandelt werden.

Erfolgt innerhalb eines vorgegebenen Zeitraums (siehe [TR-03109-4]) keine Klärung der vertrauenswürdigen Verwendung des SMGW durch den GWA, so MUSS der Status spätestens nach Ablauf dieser Frist automatisch von „Suspendiert“ auf „Gesperrt“ geändert werden (Kennzeichnung in der Sperrliste als suspendiert entfällt). Entsprechend DÜRFEN KEINE neuen Zertifikate für das SMGW mehr ausgestellt werden.

4.8.3 Aktualisierungs- und Prüfungszeiten bei Sperrungen

In der folgenden Tabelle sind die minimal erforderlichen Aktualisierungs- und Prüfungszeiten der Sperrlisten für die einzelnen PKI-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 CA wie in Tabelle 10 definiert erreichbar ist.

Nach Eintreffen eines Antrags für eine Sperrung MUSS dieser von der zugehörigen CA unverzüglich geprüft werden. Ist der Antrag valide MUSS dieser zeitlich, wie in Tabelle 10 definiert, umgesetzt werden.

Die Gültigkeit einer Sperrliste darf max. 3 Tage länger sein, als das in Tabelle 10 definierte Aktualisierungsintervall.

Sollte eine Sperrliste nicht verfügbar bzw. abrufbar sein, MUSS ersatzweise mit der zuletzt bekannten Sperrliste weitergeprüft werden. Die für die Sperrliste verantwortliche CA MUSS hierüber unverzüglich informiert werden (über Kontaktadresse in der CP der jeweiligen CA). Diese MUSS dann auf anderem Wege eine aktuelle Sperrliste zur Verfügung stellen. Steht nach 3 Tagen immer noch keine aktualisierte Sperrliste zur Verfügung, MUSS die Sub-CA die Root-CA informieren. Den Zertifikaten der entsprechenden CA kann in diesem Fall nicht vertraut werden.

PKI-Teilnehmer		**Regelmäßige Aktualisierung der Sperrliste**	**Erreichbarkeit für Sperrungen**	**Anlassbezogene Aktualisierung der Sperrliste**	**Abruf der Sperrliste**	**Prüfung der Zertifikate auf Sperrung**
Root-CA	Root-CA-CRL	Innerhalb von 30 Tagen	Täglich	Unverzüglich	Entfällt (Keine übergeordnete Sperrliste)	Entfällt (Keine übergeordnete Sperrliste)
	Root-TLS-CRL	Innerhalb von 7 Tagen				
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 10: Zeitliche Anforderungen bei Sperrungen

4.9 Service zur Statusabfrage von Zertifikaten

Für die SM-PKI ist kein OCSP-Dienst vorgesehen. Statusabfragen hinsichtlich einer Sperrung oder Suspendierung können über die entsprechende CRL erfolgen (siehe [TR-03109-4]).

4.10 Beendigung der Teilnahme

Die Beendigung der Teilnahme eines Zertifikatsnehmers kann durch diesen selbst oder die zugehörige 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 muss hierbei durch den Zertifikatsinhaber jedes Unternehmen (EMT, GWH und GWA) informiert werden, 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 MUSS eine entsprechende Abstimmung zwischen den Beteiligten bezüglich des dazu notwendigen Zeitrahmens erfolgen. Ausgenommen hiervon ist die Sperrung von Zertifikaten aufgrund von Gefahren für den sicheren Betrieb der SM-PKI).

– Sperrung aller Zertifikate des Zertifikatsnehmers sowie entsprechende Kennzeichnung der bekannten $C_{S/MIME}$(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 MÜSSEN die Zertifikate des SMGW gesperrt werden. Die Sperrung MUSS der zugehörigen CA über deren Webservice-Schnittelle mitgeteilt werden (siehe [TR-03109-4]).

4.11 Hinterlegung und Wiederherstellung von Schlüsseln

Für die Root-CA MUSS eine Hinterlegung für die Schlüssel und Zertifikate durchgeführt werden.

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

5 Organisatorische, betriebliche und physikalische Sicherheitsanforderungen

Die SM-PKI Policy spezifiziert technische und organisatorische Sicherheitsanforderungen an alle PKI-Teilnehmer, die im Kontext der PKI relevant sind, um die Sicherheit der PKI zu gewährleisten.

5.1 Generelle Sicherheitsanforderungen

In diesem Abschnitt werden die generellen Sicherheitsanforderungen an die PKI-Teilnehmer definiert. Diese bilden den Sicherheitsrahmen für die PKI-Teilnehmer. Hierauf aufbauend werden in dieser SM-PKI Policy erweiterte Sicherheitsanforderungen definiert.

Für die Einhaltung der generellen Sicherheitsanforderungen ist die Zertifizierung nach [ISO/IEC 27001] relevant. Eine ISO27001-Zertifizierung KANN nativ [ISO/IEC 27001] oder auf Basis von IT-Grundschutz (gemäß BSI-Standard 100-2) vorgenommen werden.

5.1.1 Erforderliche Zertifizierungen der PKI-Teilnehmer

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

Root-CA: Die Root-CA bildet den Vertrauensanker der SM-PKI. Die Zertifizierung nach [ISO/IEC 27001] und nach [TR-03145-1] MUSS vorhanden sein.

Sub-CA: Die Zertifizierung nach [ISO/IEC 27001] sowie eine Zertifizierung nach [TR-03145-1] MUSS vorhanden sein und nachgewiesen werden.

GWH: Ein Gateway-Hersteller benötigt ein Common-Criteria-Zertifikat auf Basis von [BSI-CC-PP-0073] für sein Produkt, um die Sicherheit seiner Produktionsumgebung nachzuweisen. Für die SM-PKI ist diese Produktionsumgebung insbesondere relevant, da dort die initialen Schlüssel und Zertifikate (inkl. Gütesiegelzertifikate) auf das SMGW aufgebracht werden.

GWA: Ein GWA MUSS alle Anforderungen gemäß [TR-03109-6] erfüllen und das entsprechende Zertifikat nachweisen.

SMGW: Ein SMGW MUSS über ein Common-Criteria-Zertifikat auf Basis von [BSI-CC-PP-0073] verfügen.

Der Zeitpunkt zur Nachweispflicht hinsichtlich der Interoperabilität gemäß [TR-03109-1] wird durch das BSI festgelegt werden und im Ausschuss Gateway-Standardisierung bekannt gemacht. Ein Nachweis zur Interoperabilität gemäß [TR-03109-1] MUSS ab diesem Zeitpunkt für ein SMGW vorhanden sein. Dieser Nachweis MUSS dem GWA vorgelegt werden.

EMT: Ein passiver EMT MUSS ein Sicherheitskonzept erstellen, in dem die Anforderungen aus dieser SM-PKI Policy berücksichtigt werden. Ein aktiver EMT (siehe Abschnitt 1.3.3.4) MUSS eine Zertifizierung gemäß [ISO/IEC 27001] vorweisen bzw. nachweisen, dass ein nach [ISO/IEC 27001] zertifizierter Dritter die Leistung für ihn erbringt. Bei einem Wechsel der Rollen zwischen aktiven und passiven EMT MUSS dieses der Sub-CA angezeigt und die entsprechenden Prozesse (s. Kapitel 3.2.2.2) durchlaufen werden.

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

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

Bei einem aktiven EMT MUSS eine ensprechende Zertifizierung alle für die PKI relevanten Geschäftsprozesse und IT-Systeme (insbesondere hinsichtlich Beantragung, Empfang und Nutzung von Schlüsseln und Zertifikaten) umfassen.

Allgemein MUSS die Zertifizierung nach [ISO/IEC 27001] die Überprüfung beinhalten, dass alle Anforderungen aus [TR-03109-4] und aus dieser SM-PKI Policy eingehalten werden. Das Ergebnis MUSS im Auditbericht dokumentiert werden, damit es bei Bedarf vorgelegt werden kann.

Werden Fach- oder Administrationsprozesse per Remote-Management realisiert MUSS dieses per 2-Faktor-Authentisierung abgesichert werden. Das Remote-Management MUSS im Sicherheitskonzept behandelt werden und MUSS als Bestandteil der Zertifizierung gemäß [ISO/IEC 27001] überprüft werden. Zugehörige WAN-Verbindungen MÜSSEN vom Sicherheitsniveau vergleichbar mit den WAN-Verbindungen gemäß [TR-03109-6] sein.

Bei den Systemen einer Test-CA (siehe Abschnitt 1.3.1) ist keine Zertifizierung entsprechend [ISO/IEC 27001] erforderlich (siehe Anhang C.1).

5.2 Erweiterte Sicherheitsanforderungen

5.2.1 Betriebsumgebung und Betriebsabläufe:

Nachfolgend werden die Anforderungen an eine sichere Betriebsumgebung und an sichere Betriebsabläufe für Root-CA, Sub-CA, GWH und EMT definiert. Entsprechende Anforderungen an den GWA sind in [TR-03109-6] spezifiziert.

- **Objektschutz:** Die betrieblichen Prozesse MÜSSEN vor Störung geschützt werden.
- **Zutrittssicherheit:** Es MÜSSEN Vorkehrungen zur Sicherung des Zutritts vor Unbefugten zu den jeweiligen Betriebsräumen getroffen werden.
- **Geschäftsfortführung:** Die Wiederaufnahme der Betriebsabläufe sowie die Wiederherstellung der notwendigen Ressourcen (Personal, Technologie, Standort, Information) MÜSSEN nach einer Unterbrechung unverzüglich erfolgen.
- **Informationsträger:** Bei der Verarbeitung und Aufbewahrung von Informationen in IT-Systemen MUSS der Schutz vor unautorisiertem oder unbeabsichtigtem Gebrauch gewährleistet werden. Wenn nicht mehr benötigt, MUSS der Informationsträger sicher und unwiederherstellbar zerstört werden.

Für die CAs gelten überdies die folgenden Anforderungen:

- **Brandschutz:** Es MÜSSEN bei den CAs Maßnahmen getroffen werden, die der Entstehung eines Brandes und der Ausbreitung von Feuer vorbeugen sowie wirksame Löscharbeiten ermöglichen.
- **Strom:** Eine gesicherte Stromversorgung einschließlich Redundanzkonzept für Strom SOLLTE bei den CAs gewährleistet werden.
- **Wasserschaden:** Die IT-Infrastruktur SOLLTE bei CAs gegen das Eintreten eines Wasserschadens geschützt werden.
- **Notfall-Management und Wiederherstellung:** Die CAs MÜSSEN ihre Systeme durch Backup-Mechanismen sichern, um die Wiederherstellung des Betriebs nach einer Störung oder einem Notfall zu ermöglichen. Nur vertrauenswürdiges Betriebspersonal SOLLTE Backup- und Wiederherstellungsprozesse durchführen.

5.2.2 Verfahrensanweisungen

Für den Betrieb der Root-CA, Sub-CA, GWH und eines aktiven EMT MÜSSEN folgende Verfahrensanweisungen umgesetzt werden:

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

Ein passiver EMT MUSS folgende der oben aufgeführten Verfahrensanweisungen umsetzen:

- **Einhaltung von Verpflichtungen**
- **Beschränkung der Anzahl Mitarbeiter**
- **Eskalationsmanagement**

Der Betrieb eines GWA wird nicht innerhalb dieses Dokuments beschrieben, da dieser entsprechend [TR--03109-6]erfolgen MUSS.

5.2.3 Personal

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

- **Rollen und Verantwortungen:** Die Rollen und Verantwortlichkeiten sind gemäß der Anforderungen in Kapitel 5.2.2 zu dokumentieren. In Bezug auf kritische Aufgaben/Funktionen bezüglich des Schlüssel- und Zertifikatsmanagement-Lebenszyklus MÜSSEN die Verantwortlichkeiten klar definiert werden.
- **Rollenbeschreibungen:** Für temporäres und permanentes Personal MÜSSEN Rollenbeschreibungen definiert werden, welche Aufgabentrennung, Mindestberechtigungen, Sicherheitsprüfungen,Verpflichtung zu Mitarbeiter- und Sensibilisierungsschulungen enthalten.
- **Einhaltung der ISMS-Anforderungen:** Das Personal MUSS administrative und betriebliche Verfahren und Prozesse im Einklang mit dem Standard ISO 27001 durchführen.

Für den Betrieb einer CA gilt darüber hinaus:

- **Qualifiziertes Personal:** Die CA MUSS Personal beschäftigen, welches über die erforderlichen Fachkenntnisse, Erfahrung und Qualifikation für das Aufgabenfeld und die angebotenen Dienste verfügt.
- **Sicherheitsüberprüfung:** Die CA MUSS sicherstellen, dass an kritischen und sicherheitsrelevanten Prozessen beteiligte Personen bezüglich der persönlichen Eignung geprüft und die Prüfung dokumentiert wurde.

Die Regelungen zum Personal eines GWA werden nicht innerhalb dieses Dokuments beschrieben, da diese in der [TR-03109-6] enthalten sind.

5.2.4 Monitoring

Folgende Ereignisse MÜSSEN erkannt und aufgezeichnet bzw. dokumentiert werden:

Root-CA und Sub-CA:

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

GWA:

– Durchführung der Überwachungsmaßnahmen gemäß [TR-03109-6]
– Schlüsselmanagement auf dem Kryptografiemodul
– Direkter Zugriff auf das SecMod des SMGWS (External Authentication am SecMod)

GWH:

– Schlüsselmanagement auf dem Kryptografiemodul
– Zertifikatsanträge von SMGWs für Gütesiegel-Zertifikate

EMT:

– Schlüsselmanagement auf dem Kryptografiemodul
– EMT aktiv: Ansprechen und Steuern von Geräten über ein SMGW

5.2.5 Archivierung von Aufzeichnungen

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

Root-CA und Sub-CA:

– **Archivierung der öffentlichen Schlüssel:** Die Beteiligten MÜSSEN sicherstellen, dass die relevanten Informationen zu den öffentlichen Schlüsseln des Zertifikates archiviert werden.
– **Eindeutige Zuordnung von Zertifikaten:** Die Beteiligten MÜSSEN in der Lage sein, die jeweiligen Zertifikate eindeutig den registrierten Benutzern zuzuordnen.
– **Verfügbarkeit:** Mit Hilfe einer angemessenen Archivierung klar definierter Daten der verbreiteten öffentlichen Zertifikatsschlüssel MUSS nach einer vollständigen Wiederherstellung die Verfügbarkeit der Dienste gewährleistet werden.
– **Datenbanken:** Die Aktualität, Integrität und Vertraulichkeit der Datenbanken MÜSSEN gewährleistet sein, insbesondere bezüglich der Konsistenz der Datenbanken zur Verbreitung von Zertifikaten und der Datenbank zur Nutzer-Registrierung.
– **Definition der zu archivierenden Informationen:** Die Informationen, welche für das Tracking und die Wiederherstellung von öffentlichen Schlüsseln benötigt werden, MÜSSEN klar definiert werden.

– **Die zu archivierenden Informationen für öffentliche Schlüssel MÜSSEN enthalten**:
  - Registrierungsinformationen
  - Essentielle CA-Ereignisse (z.B. Generierung von Zertifikaten)
  - Schlüsselverwaltung
  - Zertifizierungsereignisse
  - Für jedes Ereignis MUSS der Zeitpunkt der Archivierung präzise festgelegt werden.
– **Zu archivierende Ereignisse:** Die wesentlichen Ereignisse, die archiviert werden, umfassen:
  - Zertifikatserstellung
  - Erneuerung und Aktualisierung der öffentlichen Zertifikats-Schlüssel
  - Incident- oder Notfall-Management bezüglich Zertifikats-relevanter Vorfälle.
– **Verlorene Schlüssel / Zertifikate:** Daten von verbreiteten Schlüsseln / Zertifikaten DÜRFEN NICHT wiederhergestellt werden. Es MÜSSEN neue Schlüssel / Zertifikate beantragt werden.

Ein GWA MUSS folgende der oben aufgeführten Verfahrensanweisungen umsetzen:

– **Zu archivierende Ereignisse im Kontext Kommunikation mit der Sub-CA:**
  - Zertifikatsbeantragung
  - Incident- oder Notfall-Management bezüglich Zertifikats-relevanter Vorfälle.

Ein EMT MUSS folgende der oben aufgeführten Verfahrensanweisungen umsetzen:

– **Archivierung der öffentlichen Schlüssel**
– **Definition zu archivierender Informationen**
– **Zu archivierende Ereignisse**
  - Zertifikatsbeantragung
  - Incident- oder Notfall-Management bezüglich Zertifikats-relevanter Vorfälle.

5.2.6 Schlüsselwechsel einer Zertifizierungsstelle

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

– **Geplanter Schlüsselwechsel:** Im Fall eines planbaren Schlüsselwechsels einer Zertifizierungsstelle MÜSSEN die in Kapitel 5.2.7 beschriebenen Verfahren berücksichtigt werden und entsprechende Prozesse vorhanden sein.
– **Ungeplanter Schlüsselwechsel:** Für den Fall, dass ein unvorhergesehener Schlüsselwechsel einer Zertifizierungsstelle notwendig ist, MÜSSEN entsprechende Verfahren im Notfallmanagement definiert werden.
– Sowohl ein geplanter als auch ein ungeplanter Schlüsselwechsel einer Zertifizierungsstelle MUSS gemäß dem **Vier-Augen-Prinzip** erfolgen.

5.2.7 Auflösen einer Zertifizierungsstelle

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

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

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

5.2.8 Aufbewahrung der privaten Schlüssel

Alle Teilnehmer der SM-PKI MÜSSEN folgende Anforderung umsetzen:

– **Kryptografiemodule:** Die Schlüssel MÜSSEN in vertrauenswürdigen Kryptografiemodulen gespeichert werden (siehe Abschnitt 6.2). Wenn private Schlüssel der Root-CA, Sub-CA, GWA und ggf. von Teilnehmern außerhalb des Sicherheitsmoduls (z.B. als Backup) aufbewahrt werden, MÜSSEN diese mit dem gleichen Schutzniveau, wie bei der Schlüsselerstellung verarbeitet werden.

Die Root-CA, Sub-CA, GWH und EMT MÜSSEN sicherstellen, dass folgende Anforderungen umgesetzt werden (die diesbezüglichen Anforderungen an die GWA sind Teil von [TR-03109-6]):

– **Schutz der Speichermedien:** Die Speichermedien MÜSSEN gegen nicht autorisierte Nutzung, Schäden durch Personen und weitere Bedrohungen (z.B. Feuer) gesichert werden (siehe auch 5.2.1).
– **Schlüsselaufbewahrung:** Die Speichermedien MÜSSEN sich in einem physisch und logisch hoch gesicherten Bereich befinden. Der Zutritt MUSS auf eine klar definierte Anzahl von Personen eingeschränkt werden.
– **Vertrauenswürdiges Personal:** Der private Schlüssel DARF NUR durch vertrauenswürdiges Personal erzeugt, gespeichert und für Signaturen verwendet werden.
– **Abfallbeseitigung:** Es MUSS sichergestellt werden, dass Abfälle nicht unberechtigt genutzt und vertrauliche Informationen veröffentlicht werden können.
– **Gehärtete IT-Systeme :** Es MUSS sichergestellt werden, dass die Anforderungen an gehärtete IT-Systeme und -Netzwerke sowie an die physische Sicherheit eingehalten werden. Eine Basis für umzusetzende Maßnahmen kann aus dem BSI-Grundschutzkatalog entnommen werden.

5.2.9 Behandlung von Vorfällen und Kompromittierung

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

– Bei einer Kompromittierung oder einem begründeten Verdacht auf Kompromittierung eines privaten Schlüssels MUSS das zugehörige Zertifikat unverzüglich gesperrt und DARF NICHT wiederverwendet werden.
– Ein Fall von Kompromittierung sowie Verdachtsfälle MÜSSEN durch den Schlüsselinhaber dokumentiert werden.
– Jeder Verdacht auf Kompromittierung oder Missbrauch des privaten Schlüssels ist aufzuklären.
– Die Generierung neuer Schlüssel und Zertifikate MUSS überwacht und dokumentiert werden.

5.2.10 Meldepflichten

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

Root:

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

- Änderungen dieser SM-PKI Policy, an der [TR-03109-4] oder an der [TR-03116-3]

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

EMT:

Ein EMT MUSS dem zugehörigen GWA mitteilen, wenn

- dieser Anomalien bei den von einem SMGW empfangen Daten feststellt, die auf eine Fehlfunktion oder Kompromittierung hindeuten könnten, oder
- dieser (wiederholt) unberechtigte Kommunikationsversuche von einem oder mehreren gesperrten SMGWs feststellt.

5.3 Notfall-Management

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

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

Insbesondere gelten folgende Anforderungen, welche erfüllt werden MÜSSEN:

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

6 Technische Sicherheitsanforderungen

6.1 Erzeugung und Installation von Schlüsselpaaren

Jeder Zertifikatsnehmer MUSS sein eigenes Schlüsselpaar generieren.

Die technischen Anforderungen an die Erzeugung, Verwendung und Gültigkeit von Schlüsseln werden in [TR-03109-4] beschrieben.

6.1.1 Generierung von Schlüsselpaaren für die Zertifikate

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

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

Der EMT MUSS nur folgende der oben aufgeführten Anforderungen bei der Generierung von Schlüsselpaaren umsetzen:

- **Generierung eines Schlüsselpaars**

6.1.2 Lieferung privater Schlüssel

Die Erstellung der privaten Schlüssel erfolgt dezentral durch die Zertifikatsnehmer der SM-PKI. Daher erfolgt keine Lieferung der privaten Schlüssel.

6.1.3 Lieferung öffentlicher Zertifikate

Alle Zertifikate werden in den jeweiligen Verzeichnissen der ausstellenden CAs abgelegt und sind somit für alle PKI-Teilnehmer zugänglich.

6.1.4 Schlüssellängen und kryptografische Algorithmen

Schlüssellängen und kryptografische Algorithmen der Schlüsselpaare MÜSSEN angemessene kryptografische Verfahren einhalten. Die zum jeweiligen Zeitpunkt konkret zu verwendenden kryptografischen Algorithmen und Schlüssellängen MÜSSEN der [TR-03116-3] entnommen werden.

Bei der Erzeugung und Nutzung von statischen und temporären Schlüsseln im Rahmen der SM-PKI MUSS ein Zufallsgenerator verwendet werden, der konform zu den Anforderungen aus [TR-03116-3] ist. Des Weiteren MUSS bei statischen Schlüsseln ein Kryptografiemodul gemäß Abschnitt 6.2 eingesetzt werden.

6.1.5 Festlegung der Parameter der Schlüssel und Qualitätskontrolle

- **Sichere Handhabung und Lagerung von Schlüsselmaterial:** Software- und Hardware-Komponenten zur Erzeugung, Handhabung und Lagerung der privaten Schlüssel MÜSSEN angemessene Maßnahmen zur sicheren Handhabung und Lagerung von Schlüsselmaterial einhalten.
- **Defektes Krypto-Modul (KM):** Im Falle eines defekten KM ist sicherzustellen, dass das Schlüssel-Backup sicher und im Vier-Augen-Prinzip in ein neues KM nach angemessenen Maßnahmen zur sicheren Handhabung und Lagerung von Schlüsselmaterial importiert wird.
- **Schutz vor Angriff auf den privaten Schlüssel:** Es MUSS sichergestellt werden, dass der private Schlüssel nicht von einem Angreifer für kryptografische Operationen missbraucht werden kann und dass angemessene Maßnahmen (siehe Abschnitt 6.2.3. bis 6.2.6) zur sicheren Handhabung und Lagerung von Schlüsselmaterial und gehärteten IT-Systemen und -Netzwerken eingehalten werden.
- **Unverschlüsselter / unberechtigter Export des privaten Schlüssels:** Es MUSS sichergestellt werden, dass der private Schlüssel nicht unverschlüsselt oder unberechtigt aus dem Schlüsselspeicher exportiert werden kann. Es MÜSSEN angemessene Maßnahmen zur sicheren Handhabung und Lagerung von Schlüsselmaterial eingehalten werden. Die zum jeweiligen Zeitpunkt konkret zu verwendenden kryptografischen Algorithmen und Schlüssellängen MÜSSEN den jeweils aktuellen Empfehlungen aus [TR-02102-1] entsprechen.
- Die Testteilnahme erfolgt auf Basis von **Testschlüsseln (Test-PKI**, siehe Abschnitt 1.3.1) unter Einhaltung der Anforderungen an den Wirkbetrieb aus [TR-03109-4] und dieser SM-PKI Policy. Die verwendeten Testschlüssel werden ausschließlich für den Testbetrieb erzeugt und DÜRFEN NICHT im Wirkbetrieb des SM-PKI Umfeldes eingesetzt werden.

6.1.6 Verwendungszweck der Schlüssel

Die Schlüssel DÜRFEN ausschließlich für die in Kapitel 1.4.1 beschrieben Verwendungszwecke eingesetzt werden. 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 SM-PKI MÜSSEN Kryptografiemodule zur Generierung, Speicherung und Nutzung ihrer privaten Schlüssel zu ihren Zertifikaten aus der SM-PKI verwenden. Die Sicherheitsanforderungen an Kryptografiemodule zum Schutz der privaten Schlüssel zu den Zertifikaten der SM-PKI werden in Kapitel 6.2.10 definiert.

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

Die in diesem Kapitel definierten Anforderungen ergänzen die Anforderungen aus [KeyLifecSec]. Dabei gelten vorrangig die Vorgaben aus der CP.

Die Anforderung an Kryptografiemodule für den Einsatz in der Test-PKI ist in C.1 definiert.

6.2.1 Mehrpersonen-Zugriffssicherung zu privaten Schlüsseln

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

6.2.2 Ablage privater Schlüssel

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

6.2.3 Backup privater Schlüssel

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

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

Es wird EMPFOHLEN, dass der EMT und der GWH ein Backup durchführen. Sobald ein Backup durchgeführt wird, SOLLTEN die vorstehenden Anforderungen eingehalten werden.

Der private Schlüssel KANN als Backup wie folgt exportiert werden:

- Verschlüsselter Dateicontainer:
  - Datenstruktur, die den geheimen Schlüssel enthält und mit einem KEK (Key Encryption Key) verschlüsselt ist (Für die Verschlüsselung sind jeweils die aktuellen Empfehlungen aus [TR-02102-1] einzuhalten).
  - Die Nutzung des Dateicontainers erfordert den Import in ein Kryptografiemodul, das die Anforderungen aus Kapitel 6.2 erfüllt.
  - Der Zugriff auf den verschlüsselten Dateicontainer MUSS auf das Betriebspersonal beschränkt sein.
  - Die Wiederherstellung des Dateicontainers ist technisch ausschließlich im 4-Augen-Prinzip möglich.
- Backup Kryptografiemodul:
  - Der private Schlüssel wird verschlüsselt direkt in das Backup-Kryptografiemodul transferiert (siehe Abschnitt 6.2.5).
  - Der Zugang zum Backup-Kryprografiemodul MUSS auf das Betriebspersonal beschränkt sein.

6.2.4 Archivierung privater Schlüssel

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

6.2.5 Transfer privater Schlüssel in oder aus kryptografischen Modulen

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

6.2.6 Speicherung privater Schlüssel in kryptografischen Modulen

- Grundsätzlich MÜSSEN die privaten Schlüssel eines PKI-Teilnehmers auf einem Kryptografiemodul gespeichert werden.
  - Die einzige Ausnahme bilden die client- und serverseitigen TLS-Schlüssel bei Sub-CA und Root-CA, die bei der Root-CA und den Sub-CAs zur TLS-Authentisierung an der Web-Service-Schnittelle (siehe [TR-03116-3]) und am Verzeichnisdienst verwendet werden. Hier SOLLTE ein Kryptografiemodul eingesetzt werden.
- Auf einem HSM DÜRFEN private Schlüssel von PKI-Teilnehmern derselben PKI-Rolle[2] gespeichert werden (Bsp.: es dürfen mehrere CA-Schlüssel auf demselben HSM gespeichert werden). Diese MÜSSEN aber in getrennten Sicherheitsdomänen (Trennung auf Anwendungsebene) verwaltet werden. Entsprechend MÜSSEN diese im HSM logisch getrennt sein.
- Auf einem HSM DÜRFEN KEINE privaten Schlüssel von verschiedenen PKI-Rollen gespeichert werden. Es darf entsprechend keine Vermischung von Schlüsseln von unterschiedlichen PKI-Rollen auf einem HSM erfolgen (Bsp.: es dürfen keine CA- und GWA-Schlüssel auf dem selben HSM gespeichert werden).
- Die privaten Schlüssel der PKI-Teilnehmer aus einer Testumgebung MÜSSEN von der Produktivumgebung getrennt werden.

6.2.7 Aktivierung privater Schlüssel

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

6.2.8 Deaktivierung privater Schlüssel

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

6.2.9 Zerstörung privater Schlüssel

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

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

2 Passiver EMT und aktiver EMT gehören beide zur PKI-Rolle EMT. Entsprechend können passive und aktive EMT-Schlüssel auf demselben HSM gespeichert werden.

Die Backups der Schlüssel MÜSSEN ebenfalls berücksichtigt werden.

Die Zerstörung der privaten Schlüssel MUSS durch einen sicheren Lösch-Mechanismus im Kryptografiemodul (falls vorhanden) oder durch die unwiederherstellbare mechanische Zerstörung erfolgen. Für diesen Prozess gelten die Anforderungen aus [KeyLifecSec].

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, MUSS dieser ebenfalls zerstört werden.

6.2.10 Beurteilung kryptografischer Module

Geltungsbereich: Alle PKI-Teilnehmer (Ausnahme SMGW)

Innerhalb der PKI können verschiedene Produktklassen von Kryptografiemodulen eingesetzt werden, z.B. Hardware-Sicherheitsmodule (HSM), Chipkarten und Secure Elements (vgl. Kategorien der Schutzprofile in [KeyLifecSec]). Die SMGWs bzw. der Betrieb von SMGWs ist ausgenommen von den Anforderungen aus [KeyLifecSec]

Sicherheitsanforderungen

Um ein Kryptografiemodul in der SM-PKI einsetzen zu können, MUSS dieses konform zu den Anforderungen an Kryptografiemodule aus [KeyLifecSec] – Security Level 2[3] sein. Hinsichtlich der Anforderungen an den Zufallsgenerator des Kryptografiemodules gelten die Anforderung aus [TR-03116-3].

Übergangsregelung

Die für ein Kryptografiemodul in Security Level 2 geforderte Zertifizierung KANN bis auf Widerruf alternativ durch die in der folgenden Tabelle aufgeführten Nachweise erfüllt werden.

Bzgl. der Anforderungen wird insbesondere zwischen einer zertifizierten und einer nicht zertifizierten Einsatzumgebung unterschieden.

Bei einer zertifizieren Einsatzumgebung MÜSSEN die Anforderungen aus der SM-PKI Policy speziell hinsichtlich des Key-Lifecycle im ISMS berücksichtigt werden.

3 Informativ: Derzeit erstellt das BSI basierend auf BSI-CC-PP-0077 und zugehöriger TR ein adaptiertes PP für den serverseitigen Einsatz des Sicherheitsmoduls, welches auf dem Sicherheitsniveau Security Level 2 in die CP aufgenommen werden soll.

Zertifizierte Einsatzumgebung						
	EMT passiv	**EMT aktiv**	**GWH**	**GWA**	**Sub-CA**	**Root**
Anforderung am die Betriebsumgebung	Siehe Tabelle 15	Siehe Tabelle 15	Siehe Tabelle 15	Siehe Tabelle 15	Siehe Tabelle 15	Siehe Tabelle 15
Nachweise	Erforderlichkeit					
Sicher Zufallszahlen-generator gemäß [TR-03116-3].	MUSS	MUSS	MUSS	MUSS	MUSS	MUSS
Tamper-Schutz gegen Attack Potential "moderate"	SOLLTE	SOLLTE	SOLLTE	SOLLTE	SOLLTE	MUSS
Seitenkanalresistenz gegen Attack Potential "moderate"	SOLLTE	SOLLTE	SOLLTE	SOLLTE	SOLLTE	MUSS

Tabelle 11: Übergangsregelungen Anforderungen HSM (zertifizierte Einsatzumgebung)

Nicht zertifizierte Einsatzumgebung						
	EMT passiv	**EMT aktiv**	**GWH**	**GWA**	**Sub-CA**	**Root**
Nachweise	Erforderlichkeit					
Sicher Zufallszahlen-generator gemäß [TR-03116-3].	MUSS	*Entfällt*	*Entfällt*	*Entfällt*	*Entfällt*	*Entfällt*
Tamper-Schutz gegen Attack Potential "moderate"	MUSS	*Entfällt*	*Entfällt*	*Entfällt*	*Entfällt*	*Entfällt*
Seitenkanalresistenz gegen Attack Potential "moderate"	MUSS	*Entfällt*	*Entfällt*	*Entfällt*	*Entfällt*	*Entfällt*

Tabelle 12: Übergangsregelungen Anforderungen HSM (nicht zertifizierte Einsatzumgebung)

Die in der Tabelle dargestellten Nachweise für eine Übergangslösung MÜSSEN jeweils durch eine durch das BSI für Common Criteria-Evaluierungen anerkannte Prüfstelle erbracht werden. Die Prüfstelle MUSS in den letzten 5 Jahren mindestens die Prüfung eines Zufallszahlengenerators gemäß [AIS 20]/[AIS 31] im Rahmen eines CC-Zertifizierungsverfahrens erfolgreich abgeschlossen haben. Die Prüfungen werden eigenverantwortlich durch die Prüfstelle durchgeführt. Dabei kann die Prüfstelle für die Nachweise auch Ergebnisse heranziehen, die auf CC-Zertifizierungen des Kryptografiemoduls basieren, die nicht auf Grundlage eines Schutzprofils aus [KeyLifecSec] - Security Level 2 durchgeführt wurden.

Der PKI-Teilnehmer benötigt für sein Kryptografiemodul eine Bestätigung bzw. eine Sicherheitsaussage des Herstellers, dass diese Nachweise durch eine entsprechende Prüfstelle erbracht wurden.

Das Vorhandensein der Bestätigung zu dem vom PKI-Teilnehmer eingesetzten Kryptografiemodul MUSS durch den Auditor bei dem Audit der Einsatzumgebung geprüft werden, sofern eine Auditierung der Einsatzumgebung erforderlich ist (siehe Tabelle 15).

SMGW

Bei einem SMGW MUSS ein Kryptografiemodul eingesetzt werden, das nach [BSI-CC-PP-0077] zertifiziert ist.

6.3 Andere Aspekte des Managements von Schlüsselpaaren

6.3.1 Archivierung öffentlicher Schlüssel

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

6.3.2 Gültigkeitszeitraum 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.

Instanz	Zertifikat	Intervall
Root-CA	C(Root)	Alle 3 Jahre
	$C_{CRL\text{-}S}$(Root)	Alle 3 Jahre
	$C_{TLS\text{-}S}$(Root)	Alle 2 Jahre
Sub-CA	C(Sub-CA)	Alle 2 Jahre

Tabelle 13: Intervall Zertifikatswechsel bei einer CA

Sobald eine CA über ein neues Zertifikat verfügt, MUSS dieses zum Ausstellen neuer Zertifikate und der zugehörigen Sperrlisten verwendet werden.

6.4 Aktivierungsdaten

Die Aktivierungsdaten für die Kryptografiemodule MÜSSEN sicher aufbewahrt werden.

6.5 Sicherheitsanforderungen für die Rechneranlagen

Nachfolgend werden die Anforderung an die Rechneranlagen definiert, die von den jeweiligen PKI-Teilnehmern umgesetzt werden MÜSSEN:

- **Root-CA, Sub-CA, GWH, EMT: Netzwerkkontrolle:** Es MÜSSEN entsprechende Maßnahmen umgesetzt werden, um das interne Netzwerk vom externen zu trennen und vor unbefugtem Zugriff zu schützen.
- **Root-CA, Sub-CA, aktive EMT: Intrusion Detection Systeme (IDS):** Der Einsatz von Intrusion-Detection-Systemen (IDS) im gesicherten Netzsegment MUSS berücksichtigt werden. Die Log-Dateien des IDS MÜSSEN regelmäßig kontrolliert werden.
- **Root-CA, Sub-CA: System-Härtung:** Die CA-Server, die zur Erstellung von Zertifikaten verwendet werden, MÜSSEN gehärtet werden. Dies umfasst die Konfiguration und Einstellung der verwendeten Hardware- und Software-Komponenten.
- **Root-CA, Sub-CA: System-Konfiguration:** Die Konfigurationsoptionen und -einstellungen DÜRFEN nur die minimal benötigten Funktionalitäten für den CA Betrieb enthalten.
- **Root-CA, Sub-CA: Netzwerk-Separierung:** Die Netzwerke, in denen sich die CA-Server befinden, MÜSSEN durch geeignete Maßnahmen geschützt werden.
- **Alle PKI-Teilnehmer: Software-Updates:** Software-Updates MÜSSEN bei sicherheitsrelevanten Änderungen schnellstmöglich eingespielt werden, andere Updates SOLLTEN regelmäßig aktualisiert werden.

- **Root-CA, Sub-CA: Vertraulichkeit und Integrität:** Die CA MUSS sensitive Daten vor unbefugtem Zugriff oder Veränderung schützen.
- **Root-CA, Sub-CA, GWH und EMT: Logging und Audit-Trails:** Log-Dateien und Audit-Trails MÜSSEN regelmäßig geprüft werden, und automatisierte Benachrichtigungen MÜSSEN auf Abweichung vom vorgesehenen Betrieb hinweisen.
- **Root-CA, Sub-CA: Speicherort von Log-Dateien:** Die Dateien der Audit-Trails SOLLEN NICHT auf dem CA-Server, der für die Verwaltung von Zertifikaten verwendet wird, gespeichert werden. Der Speicherort für Log-Dateien KANN temporär der CA-Server sein. Die Log-Dateien MÜSSEN dann regelmäßig auf einen anderen Speicherort ausgelagert werden.
- **Alle PKI-Teilnehmer:** Das System MUSS über eine angemessene Benutzerverwaltung verfügen.
- **Root-CA, Sub-CA: Systemfunktionen:** Die CA MUSS den Zugriff auf die benötigten Systemfunktionen und Hilfsprogramme begrenzen.
- **Alle PKI-Teilnehmer: Schutz vor Schadsoftware:** Die Integrität der System-Komponenten und Informationen MUSS gegen Viren, Schadsoftware sowie nicht zugelassene Programme geschützt werden.

Die spezifischen Anforderungen an die Rechneranlagen eines GWA sind Teil von [TR-03109-6].

6.6 Zeitstempel

Keine Anforderungen an Zeitstempel.

6.7 Validierungsmodell

Die Anforderungen an die Zertifikatsvalidierung werden in [TR-03109-4] spezifiziert.

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 dieser SM-PKI Policy 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.

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.

7.3 Profile für OCSP Dienste

In der SM-PKI werden keine OCSP-Dienste eingesetzt.

8 Überprüfung und andere Bewertungen

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

8.1 Inhalte, Häufigkeit und Methodik

8.1.1 Testbetrieb

Die Root-CA und die Sub-CAs stellen Testumgebungen zur Verfügung (siehe Kapitel 1.3.1 und C), welche die Antragsteller der SM-PKI zum Test der Funktionalitäten ihrer PKI-Infrastruktur und -Prozesse durchlaufen MÜSSEN, bevor diese Teilnehmer der PKI werden (siehe Kapitel 3.2).

Testumgebung bereitgestellt durch	Nutzer	Zweck	Ergebnis
Root-CA	Sub-CA	Nachweis der vollständigen und korrekten Funktion der Zertifikatsantragsstellung und Zertifikatsannahme. Basis: Web-Service-Schnittstelle	Nach erfolgreichem Abschluss der Tests erfolgt die signierte Bestätigung der erfolgreichen bestandenen Tests durch einen Prüfer der Root-CA
Sub-CA	GWA	Nachweis der vollständigen und korrekten Funktion der Zertifikatsantragsstellung und Zertifikatsannahme. Basis: Web-Service-Schnittstelle	Nach erfolgreichem Abschluss der Tests erfolgt die signierte Bestätigung der erfolgreichen bestandenen Tests durch einen Prüfer der Sub-CA
	GWH	Nachweis der vollständigen und korrekten Funktion der Zertifikatsantragsstellung und Zertifikatsannahme. Basis: Web-Service-Schnittstelle	Nach erfolgreichem Abschluss der Tests erfolgt die signierte Bestätigung der erfolgreichen bestandenen Tests durch einen Prüfer der Sub-CA
	EMT	Nachweis der Konformität des Zertifikatsrequests	Nach erfolgreicher Prüfung erfolgt die signierte Bestätigung per E-Mail von einem Prüfer der Sub-CA

Tabelle 14: Testumgebungen

8.1.2 Beantragung Teilnahme an SM-PKI

Folgende Anforderungen MÜSSEN bei Beantragung der Teilnahme an der SM-PKI erfüllt werden. Teilweise sind dazu vorab die in Kapitel 8.1.1 aufgeführten Nachweise zu erbringen. Detaillierte Informationen sind in Punkt 5.1 definiert.

Antrag für Teilnahme als	Nachweis		Überprüfung der Nachweise	Wichtung
Sub-CA	oder	ISO27001-Zertifizierung nativ der Sub-CA	Zertifizierter ISO27001 Lead Auditor	Voraussetzung
		ISO27001-Zertifizierung nach BSI Grundschutz der Sub-CA	BSI-akkreditierter ISO27001 Lead Auditor	
	Signierte E-Mail der Root-CA über erfolgreiche Tests		Prüfer der Root-CA	
	Zertifizierung nach [TR-03145-1]		Zertifizierter [TR-03145-1] Auditor	
GWA	Zertifizierung entsprechend [TR-03109-6]		Zertifizierter [TR-03109-6] Auditor	Voraussetzung
	Signierte E-Mail der Sub-CA über erfolgreiche Tests		Prüfer der Sub-CA	Voraussetzung
GWH	CC-Zertifizierung entsprechend [BSI-CC-PP-0073]		CC-Zertifizierungsverfahren	Voraussetzung
	Signierte E-Mail der Sub-CA über erfolgreiche Tests		Prüfer der Sub-CA	
SMGW	CC-Zertifizierung entsprechend [BSI-CC-PP-0073]		CC-Zertifizierungsverfahren	Voraussetzung
	Zertifizierung entsprechend [TR3109-1]		Prüfstelle	
Aktiver EMT	oder	ISO27001-Zertifizierung nativ	Zertifizierter ISO27001 Lead Auditor	Voraussetzung
		ISO27001-Zertifizierung nach BSI Grundschutz	BSI-akkreditierter ISO27001 Lead Auditor	
	signierte E-Mail der Sub-CA über erfolgreiche Tests		Prüfer der Sub-CA	
Passiver EMT	Sicherheitskonzept		Sicherheitskonzept und Umsetzung der Maßnahmen kann im Schadensfall herangezogen werden.	Voraussetzung

Tabelle 15: Anforderungen für die Teilnahme an der SM-PKI

8.1.3 Wirkbetrieb

Die vorausgesetzten Nachweise/Zertifizierungen (siehe Kapitel 8.1.2) MÜSSEN im Wirkbetrieb auf Basis des jeweiligen Prüf-/Zertifizierungsschemas aufrechterhalten werden.

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

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

8.2 Reaktionen auf identifizierte Vorfälle

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

9 Sonstige finanzielle und rechtliche Regelungen

9.1 Preise

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

9.2 Finanzielle Zuständigkeiten

Die Root-CA obliegt der finanziellen Zuständigkeit des BSI und damit den entsprechenden Regelungen der Bundesverwaltung.

Die Betreiber von Sub-CA-Instanzen sind finanziell eigenständig und unabhängig.

A Namensschema

Die Common Names (CN) der verschiedenen SM-PKI Teilnehmer MÜSSEN folgendem Schema entsprechen:

‘<org>.<function>[.<extension>]‘

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

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

Tabelle 16 beschreibt die Bestandteile der CN für die Teilnehmer der SM-PKI:

Namensteil	Bedeutung	Länge, Kodierung, Ausnahmen
<org>	Kürzel der Identität/Organisation	Länge max. 48 Zeichen, erstes Zeichen muss ein Buchstabe oder eine Ziffer sein.
<function>	Funktionskennzeichnung innerhalb der SM-PKI	Länge max. 4 Zeichen. Feste Werte: CA, EMT, GWA, GWH oder SMGW.
<extension>	Erweiterung, zusätzliche Informationen	Länge max. 10 Zeichen. Optional, z.B. für leichteres Auffinden in Listen. Zwingend vorgegebene Werte bei CA´s gemäß Tabelle 18 (Root-CA) und 22 (Sub-CA).

Tabelle 16: Namensschema (Kodierung Common Name)

Grundsätzliche Festlegungen:

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

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

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

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

sein.

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

Root-CA: „SM-Root“

SMGW: Herstellerübergreifende Identifikationsnummer entsprechend [DIN 43863-5] und Codierung gemäß [TR-03109-1].

Die Zertifikate der Wirkumgebung haben das in den folgenden Tabellen angegebene Namensschema[4].

A.1 Root-CA

Die Zertifikate der Root-CA haben folgendes Namensschema:

C(Root) und Link-C(Root)

Attribut Typ	Kürzel	Vorgabe	Wert	Erläuterung
common name	CN	mandatory	„SM-Root.CA“	Name der Root-CA
organisation	O	mandatory	„SM-PKI-DE“	Name der PKI
organisational unit	OU	optional	„<Organisationseinheit>“	Name der Organisationseinheit
country	C	mandatory	„DE“	Ländercode
serial number	SERIAL NUMBER	mandatory	„<SN>“	Sequenznummer der Zertifikats im Bereich von 1 bis 2^{31}-1. Diese wird bei jedem neuen Zertifikat um den Wert 1 hochgezählt.

Tabelle 17: Namensschema Zertifikat C(Root) und Link-C(Root)

$C_{CRL\text{-}S}$(Root)

Attribut Typ	Kürzel	Vorgabe	Wert	Erläuterung
common name	CN	mandatory	„SM-Root.CA.CRL-S“	Kennzeichnung als CRL-Signer
organisation	O	mandatory	„SM-PKI-DE“	Name der PKI
organisational unit	OU	optional	„<Organisationseinheit>“	Name der Organisationseinheit
country	C	mandatory	„DE“	Ländercode

Tabelle 18: Namensschema Zertifikat $C_{CRL\text{-}S}$(Root)

$C_{TLS\text{-}S}$(Root)

Attribut Typ	Kürzel	Vorgabe	Wert	Erläuterung
common name	CN	mandatory	„SM-Root.CA.TLS-S“	Kennzeichnung als TLS-Signer
organisation	O	mandatory	„SM-PKI-DE“	Name der PKI
organisational unit	OU	optional	„<Organisationseinheit>“	Name der Organisationseinheit
country	C	mandatory	„DE“	Ländercode

4 Die Informationen für die Test-PKI können C.2.6 entnommen, und MÜSSEN bei der Beantragung, Ausgabe und Verwaltung der Zertifikate beachtet werden.

Attribut Typ	Kürzel	Vorgabe	Wert	Erläuterung
serial number	SERIAL NUMBER	mandatory	„<SN>“	Sequenznummer der Zertifikats im Bereich von 1 bis 2^{31}-1. Diese wird bei jedem neuen Zertifikat um den Wert 1 hochgezählt.

Tabelle 19: Namensschema Zertifikat $C_{TLS\text{-}S}$(Root)

C_{TLS}(Root)

Attribut Typ	Kürzel	Vorgabe	Wert	Erläuterung
common name	CN	mandatory	„SM-Root.CA.TLS“	Kennzeichnung als TLS-Zertifikat der Root
organisation	O	mandatory	„SM-PKI-DE“	Name der PKI
organisational unit	OU	optional	„<Organisationseinheit>“	Name der Organisationseinheit
country	C	mandatory	„DE“	Ländercode
serial number	SERIAL NUMBER	mandatory	„<SN>“	Sequenznummer der Zertifikats im Bereich von 1 bis 2^{31}-1. Diese wird bei jedem neuen Zertifikat um den Wert 1 hochgezählt.

Tabelle 20: Namensschema Zertifikat C_{TLS}(Root)

A.2 Sub-CA

Sub-CAs haben folgendes Namensschema:

Attribut Typ	Kürzel	Vorgabe	Wert	Erläuterung
common name	CN	mandatory	„<org>.CA“	Eindeutiger Name der Sub-CA.
organisation	O	mandatory	„SM-PKI-DE“	Name der PKI
organisational unit	OU	optional	„<Organisationseinheit>“	Name der Organisationseinheit
country	C	mandatory	<LC>	Zwei Zeichen Ländercode gemäß [ISO 3116 ALPHA-2]
serial number	SERIAL NUMBER	mandatory	„<SN>“	Sequenznummer der Zertifikats im Bereich von 1 bis 2^{31}-1. Diese wird bei jedem neuen Zertifikat um den Wert 1 hochgezählt.
street	street	optional	„<Straße>“	Straße der Sub-CA
postal code	postal code	optional	„<PLZ>“	Postleitzahl der Sub-CA
locality	L	optional	„<Ortsname>“	Ortsname des Sub-CA-Inhaberstandortes
state	ST	optional	„<Bundesland>“	Bundesland des Sub-CA-Inhaberstandortes

Tabelle 21: Namensschema der Sub-CA-Zertifikate

Bei den TLS-Zertifikaten der Sub-CA MUSS der common name, wie in folgenden Tabelle definiert ergänzt werden. Die Unterscheidung, ob das Zertifikat von der Root oder der Sub-CA selbst ausgestellt wurde, erfolgt über den Issuer-DN im Zertifikat.

Zertifikat	Wert	Erläuterung
$C_{TLS,Root}$(Sub-CA)	„<org>.CA.TLS“	Kennzeichnung als TLS-Zertifikat der Sub-CA
C_{TLS}(Sub-CA)	„<org>.CA.TLS“	Kennzeichnung als TLS-Zertifikat der Sub-CA

Tabelle 22: Erweiterung Common Name: TLS-Zertifikate Sub-CA

A.3 EMT

EMT haben folgendes Namensschema:

Attribut Typ	Kürzel	Vorgabe	Wert	Erläuterung
common name	CN	mandatory	„<org>.EMT[.<extension>]“	Eindeutiger Name der Organisation
organisation	O	mandatory	„SM-PKI-DE“	Name der PKI
organisational unit	OU	optional	„<Organisationseinheit>“	Name der Organisationseinheit
country	C	mandatory	<LC>	Zwei Zeichen Ländercode gemäß [ISO 3116 ALPHA-2]
serial number	SERIAL NUMBER	mandatory	„<SN>“	Sequenznummer der Zertifikats im Bereich von 1 bis 2^{31}-1. Diese wird bei jedem neuen Zertifikat um den Wert 1 hochgezählt.
street	street	optional	„<Straße>“	Straße des Zertifikatsinhabers
postal code	postal code	optional	„<PLZ>“	Postleitzahl des Zertifikatsinhabers
locality	L	optional	„<Ortsname>“	Ortsname des Zertifikatsinhabers
state	ST	optional	„<Bundesland>“	Bundesland des Zertifikatsinhabers

Tabelle 23: Namensschema der EMT-Zertifikate

A.4 GWA

Für GWAs gilt folgendes Namensschema:

Attribut Typ	Kürzel	Vorgabe	Wert	Erläuterung
common name	CN	mandatory	„<org>.GWA[.<extension>]“	Eindeutiger Name des GWA.
organisation	O	mandatory	„SM-PKI-DE“	Name der PKI
organisational unit	OU	optional	„<Organisationseinheit>“	Name der Organisationseinheit
country	C	mandatory	<LC>	Zwei Zeichen Ländercode gemäß [ISO 3116 ALPHA-2]

Attribut Typ	Kürzel	Vorgabe	Wert	Erläuterung
serial number	SERIAL NUMBER	mandatory	„<SN>“	Sequenznummer der Zertifikats im Bereich von 1 bis 2^{31}-1. Diese wird bei jedem neuen Zertifikat um den Wert 1 hochgezählt.
street	street	optional	„<Straße>“	Straße des Zertifikatsinhabers
postal code	postal code	optional	„<PLZ>“	Postleitzahl des Zertifikatsinhabers
locality	L	optional	„<Ortsname>“	Ortsname des Zertifikatsinhabers
state	ST	optional	„<Bundesland>“	Bundesland des Zertifikatsinhabers

Tabelle 24: Namensschema der GWA-Zertifikate

A.5 GWH

GWHs haben folgendes Namensschema:

Attribut Typ	Kürzel	Vorgabe	Wert	Erläuterung
common name	CN	mandatory	„<org>.GWH[.<extension>]“	Eindeutiger Name des GWH.
organisation	O	mandatory	„SM-PKI-DE“	Name der PKI
organisational unit	OU	optional	„<Organisationseinheit>“	Name der Organisationseinheit
country	C	mandatory	<LC>	Zwei Zeichen Ländercode gemäß [ISO 3116 ALPHA-2]
serial number	SERIAL NUMBER	mandatory	„<SN>“	Sequenznummer der Zertifikats im Bereich von 1 bis 2^{31}-1. Diese wird bei jedem neuen Zertifikat um den Wert 1 hochgezählt.
street	street	optional	„<Straße>“	Straße des Zertifikatsinhabers
postal code	postal code	optional	„<PLZ>“	Postleitzahl des Zertifikatsinhabers
locality	L	optional	„<Ortsname>“	Ortsname des Zertifikatsinhabers
state	ST	optional	„<Bundesland>“	Bundesland des Zertifikatsinhabers

Tabelle 25: Namensschema der GWH-Zertifikate

A.6 SMGW

Bei SMGWs wird zwischen Gütesiegel- und Wirkzertifikaten unterschieden.

SMGW Wirkzertifikate

Das Namensschema für Wirkzertifikate lautet wie folgt:

Attribut Typ	Kürzel	Vorgabe	Wert	Erläuterung
common name	CN	mandatory	„<org>.SMGW[.<extension>]“	<org>=Herstellerübergreifende Identifikationsnummer für Messeinrichtungen
organisation	O	mandatory	„SM-PKI-DE“	Name der PKI
organisational unit	OU	mandatory	„<Organisationseinheit>“	Name des zuständigen GWA
country	C	mandatory	<LC>	Zwei Zeichen Ländercode gemäß [ISO 3116 ALPHA-2]
serial number	SERIAL NUMBER	mandatory	„<SN>“	Sequenznummer der Zertifikats im Bereich von 1 bis 2^{31}-1 und startet bei 1. Diese wird bei jedem neuen Zertifikat um den Wert 1 hochgezählt.

Tabelle 26: Namensschema der SMGW-Zertifikate im Wirkbetrieb

SMGW Gütesiegelzertifikate

Das Namensschema für Gütesiegelzertifikate ist das folgende:

Attribut Typ	Kürzel	Vorgabe	Wert	Erläuterung
common name	CN	mandatory	„<org>.SMGW[.<extension>]“	<org>=Herstellerübergreifende Identifikationsnummer für Messeinrichtungen
organisation	O	mandatory	„SM-PKI-DE“	Name der PKI
organisational unit	OU	optional	„<Organisationseinheit>“	Name des SMGW-Herstellers
country	C	mandatory	<LC>	Zwei Zeichen Ländercode gemäß [ISO 3116 ALPHA-2]
serial number	SERIAL NUMBER	mandatory	„0“	Sequenznummer der Zertifikats, im Gütesiegelzertifikat mit 0 belegt

Tabelle 27: Namensschema der SMGW-Gütesiegelzertifikate

A.7 Alternativnamen

Die Zertifikatserweiterungen (extensions) SubjectAltNames und IssuerAltName MÜSSEN gemäß der folgenden Tabellen (Tabelle 28 und 29) genutzt werden.

A.7.1 SubjectAltNames

Die Belegung der Extension SubjectAltNames (Extension-ID (OID): 2.5.29.17) ist wie folgt:

Zertifikat	Rfc822Name	dNSName	uniformResourceIdentifier
C(Root)	eine Kontakt E-Mail-Adresse	Entfällt	Zugehörige Webseite
$C_{CRL\text{-}S}$(Root)		Entfällt	
$C_{TLS\text{-}S}$(Root)		Entfällt	

Zertifikat	Rfc822Name	dNSName	uniformResourceIdentifier
C_{TLS}(Root)		Domain Name (TLS-Server-Zertifikat)	
$C_{TLS,Root}$(Sub-CA)			
C(Sub-CA)		Entfällt	
C_{TLS}(Sub-CA)		Domain Name (TLS-Server-Zertifikat)	Optional: Zugehörige Webseite
C(GWA) - C_{Enc}(GWA) - C_{Sig}(GWA) - C_{TLS}(GWA)		Domain Name (ausschließlich bei einem TLS-Server-Zertifikat, siehe nachfolgende Anforderungen)	
C(GWH) - C_{Enc}(GWH) - C_{Sig}(GWH) - C_{TLS}(GWH)			
C(EMT) - C_{Enc}(EMT) - C_{Sig}(EMT) - C_{TLS}(EMT)			

Tabelle 28: Belegung Extension SubjectAltNames für CAs und Endnutzer

Bei einem TLS-Server-Zertifikat, welches über die Extension ExtendedKeyUsage mit dem Wert TLS-Web-Server-Authentifikation (1.3.6.1.5.5.7.3.1) gemäß [TR-03109-4] verfügt, MUSS der zugehörige Domain Name in der Extension SubjectAltNames angegeben werden.

Falls notwendig, ist es möglich mehrere Domain Name aufzunehmen, mit einer Obergrenze von 20 Einträgen.

Zertifikate DÜRFEN KEINE Wildcards im SubjectAltName enthalten.

A.7.2 IssuerAltName

Die Belegung der Extension IssuerAltName (Extension-ID (OID): 2.5.29.18) ist wie folgt:

Zertifikat	Inhalt
C(Root)	Entsprechend der Extension SubjectAltNames in C(Root) (s. Tabelle 28)
C_{CRL-S}(Root)	
$C_{TLS-S(}$Root)	
C(Sub-CA)	
C_{TLS}(Root)	Entsprechend der Extension SubjectAltNames in C_{TLS-S}(Root) (s. Tabelle 28)
$C_{TLS,Root}$(Sub-CA)	
C_{TLS}(Sub-CA)	Entsprechend der Extension SubjectAltNames in C(Sub-CA) (s. Tabelle 28)
C(GWA) - C_{Enc}(GWA) - C_{Sig}(GWA) - C_{TLS}(GWA)	
C(GWH)	

Zertifikat	Inhalt
- C_{Enc}(GWH) - C_{Sig}(GWH) - C_{TLS}(GWH)	
C(EMT) - C_{Enc}(EMT) - C_{Sig}(EMT) - C_{TLS}(EMT)	
C(SMGW) - C_{Enc}(SMGW) - C_{Sig}(SMGW) - C_{TLS}(SMGW)	

Tabelle 29: Belegung Extension IssuerAltName für CAs und Endnutzer

B Archivierung

Die folgende Tabelle gibt die Archivierungszeiträume für die unterschiedlichen Zertifikate der SM-PKI Teilnehmer wieder. Die Speicherung bzw. auch die Bereitstellung der Zertifikate KANN in dem LDAP-Verzeichnis der Sub-CA erfolgen, wobei die anderen Teilnehmer von der eigenverantwortlichen Speicherung der Zertifikate nicht befreit werden.

Teilnehmer	Archivierungsort	Zertifikatstyp	Archivierungsdauer
Root-CA	Zertifikatsspeicher	C(Root)	Zertifikatslaufzeit + 10 ½ Jahre
		LinkC(Root)	
		C_{CLR-S}(Root)	
		C_{TLS-S}(Root)	
		C_{TLS}(Root)	
Sub-CA	Zertifikatsspeicher	C(Sub-CA)	Zertifikatslaufzeit + 10 ½ Jahre
		C_{TLS}(Sub-CA)	
EMT	Zertifikatsspeicher	C_{TLS}(EMT)	Zertifikatslaufzeit + 2 ½ Jahre
		C_{Enc}(EMT)	
		C_{Sig}(EMT)	
GWA	Zertifikatsspeicher	C_{TLS}(GWA)	Zertifikatslaufzeit + 2 ½ Jahre
		C_{Enc}(GWA)	
		C_{Sig}(GWA)	
GWH	Zertifikatsspeicher	C_{TLS}(GWH)	Zertifikatslaufzeit + 2 ½ Jahre
		C_{Enc}(GWH)	
		C_{Sig}(GWH)	
SMGW	Zertifikatsspeicher	C_{TLS}(SMGW)	Zertifikatslaufzeit + 2 ½ Jahre
		C_{Enc}(SMGW)	
		C_{Sig}(SMGW)	
ASP Root, ASP Sub-CA, ASP GWA, ASP GWH, ASP EMT	Zertifikatsspeicher	$C_{S/MIME}$(ASP Root) $C_{S/MIME}$(ASP Sub-CA) $C_{S/MIME}$(ASP GWA) $C_{S/MIME}$(ASP GWH) $C_{S/MIME}$(ASP EMT)	Zertifikatslaufzeit + 2 ½ Jahre

Tabelle 30: Archivierung öffentlicher Schlüssel

C Test-PKI

C.1 Test-PKI Sicherheitsanforderungen

Im Folgenden werden die Sicherheitsanforderungen an die Teilnehmer der SM-Test-PKI definiert.

Alle Teilnehmer (Ausnahme SMGW)

Alle Teilnehmer der SM-Test-PKI MÜSSEN ihre Schlüssel in Kryptografiemodulen generieren, speichern und nutzen.

Um ein Kryptografiemodul in der SM-Test-PKI einsetzen zu können, MUSS dieses mindestens konform zu den Anforderungen an Kryptografiemodule aus [KeyLifecSec] – Security Level 1 sein. Es wird EMPFOHLEN, dass ein Teilnehmer in der Test-PKI ein Kryptografiemodul verwendet, welches baugleich zu seinem in der SM-PKI verwendeten Modell ist. Dies ermöglicht sicherheitskritische Abläufe möglichst nahe an der Wirkbetriebsumgebung zu testen. Die Kryptografiemodule MÜSSEN in einer sicheren Betriebsumgebung betrieben werden, für die ein Sicherheitskonzept besteht.

Sollte der Teilnehmer über eine zertifizierte Betriebsumgebung verfügen wird EMPFOHLEN das Kryptografiemodul für die SM-Test-PKI in das ISMS zu integrieren.

Auf einem Kryptografiemodul das konform zu den Anforderungen aus Kapitel 6.2.10 ist, dürfen in der Test-PKI auch Schlüssel von Teilnehmern unterschiedlicher PKI-Rollen in folgender Kombination gespeichert werden:

– Root und Sub-CA

– Alle Endnutzer

SMGW

Es wird EMPFOHLEN ausschließlich SMGWs einzusetzen, die über eine Common-Criteria-Zertifizierung gemäß [BSI-CC-PP-0073] verfügen.

Das SMGW MUSS ein Sicherheitsmodul verwenden, welches einen sicheren Zufallsgenerator gemäß [TR--03116-3]besitzen MUSS und funktional konform zu [TR-03109-2] sein SOLLTE.

C.2 Test-PKI Root und Sub-CA Anforderungen

C.2.1 Allgemein

In diesem Abschnitt werden die von dem Wirkbetrieb abweichenden Anforderungen und Regelungen für die Root und die Sub-CAs der Test-PKI (SM-Test-PKI) definiert.

Grundsätzlich soll der Betrieb der Test-PKI analog nach den Vorgaben für die Wirkumgebung erfolgen, um das Testen unter funktionalen Echtbedingungen zu ermöglichen. In den nachfolgenden Abschnitten werden einige Vereinfachungen gegenüber dem Wirkbetrieb definiert.

C.2.2 Identifizierung und Authentifizierung

Eine Sub-CA der Test-PKI MUSS sich bei der Root der Test-PKI registrieren. Die zugehörigen Formulare werden auf der Web-Seite der Root zur Verfügung gestellt. Dabei MUSS die Einhaltung dieser SM-PKI Policy gegenüber der Root von der Sub-CA bestätigt werden.

Die Vorlage von Erklärungen, Nachweisen, Zertifizierungen, einer Certificate-Policy und die persönliche Identifizierung von Ansprechpartnern im Rahmen der initialen Überprüfung zur Teilnahme an der Test-PKI ist nicht erforderlich.

C.2.3 Verzeichnisdienste

Jede CA der Test-PKI MUSS die von ihr ausgestellten Zertifikate in einem Verzeichnis mit dem DN der Form 'dc=Certificates, dc=SM-Test-PKI-DE' veröffentlichen.Der Zugriff auf den Verzeichnisdienst SOLLTE analog zur Wirkbetrieb auf die Teilnehmer der SM-PKI beschränkt werden.

C.2.4 Technische Sicherheitsanforderungen

Bei dem Betrieb der Testumgebung sind die Vorgaben zum 4-Augen-Prinzip und zur Speicherung der Schlüssel unterschiedlicher Rollen auf einem HSM nicht zwingend einzuhalten (siehe dazu auch C.1).

C.2.5 Überprüfung und andere Bewertungen

Die Testumgebungen sind für die nach 8.1.1 geforderten Funktionalitätstests erforderlich, für die Teilnahme eines Endnutzers werden keine Anforderungen an Zertifizierungen oder andere vorhergehende Prüfungen definiert.

Eine Meldepflicht für Sicherheitsvorfälle existiert für die Testumgebungen nicht.

C.2.6 Namensschema

Die Vorgaben für das Namensschema entsprechen denen der Wirkbetriebsumgebung. Eine Ausnahme stellt die Belegung des Attributs organisation (O) im subjectDN der Zertifikate dar.

In der folgenden Tabelle ist diese Abweichung gegenüber der Wirkbetriebsumgebung beschrieben:

Attribut Typ	Kürzel	Vorgabe	Wert	Erläuterung
organisation	O	mandatory	„SM-Test-PKI-DE“	Name der PKI (hier: Test-PKI)

Tabelle 31: SM-Test-PKI - Abweichung Namensschema von der SM-PKI

C.2.7 Archivierung

Die Verpflichtung zur Archivierung der Zertifikate über den Zeitraum der Zertifikatslaufzeit entfällt.

D Definitionen

Begriff	Beschreibung
Ansprechpartner	Der Ansprechpartner (auch ASP oder Vertreter genannt) ist im Rahmen der operativen Tätigkeit der Vertreter des Unternehmens in Richtung der CA-Instanz und darf in dessen Namen die Entscheidungen treffen bzw. die Anträge autorisieren.
Antragsteller	Der Antragsteller im Sinne dieses Dokumentes ist das Unternehmen, welches die Zertifikate für den Betrieb einer Sub-CA, eines GWH, eines GWA oder eines EMT bei der zuständigen CA-Instanz anfordert.
Gütesiegel-Zertifikat	siehe [TR-03109-4]
Vier-Augen-Prinzip	Parallele Gegenkontrolle durch eine zweite Person bei der Durchführung eines Vorgangs. Die eindeutige Identifikation und Rolle der teilnehmenden Mitarbeiter MUSS protokolliert werden. Das Vier-Augen-Prinzip KANN organisatorisch so umgesetzt werden, dass bei diesem Prozess zwei unterschiedliche Personen beteiligt sein MÜSSEN, die nicht zeitgleich gemeinsam am gleichen Ort agieren MÜSSEN.
Schlüsselmanagement	Verwaltung von Schlüsseln (insbesondere Erzeugung, Speicherung und Löschung bzw. Zerstörung von Schlüsseln)
Hinterlegung von Schlüsseln	Sichere Verwahrung einer Kopie eines Schlüssels an einem Zweitort.
Zerstörung von Schlüsseln	Zerstörung des Schlüssels durch einen sicheren Löschmechanismus im Kryptografiemodul. Dieser wird i.d.R. durch ein Überschreiben mit einem vorgegebenen Wert oder durch das interne dauerhafte Sperren aller Zugriffe auf den Schlüssel realisiert. Verfügt das Kryptografiemodul nicht über einen entsprechen Löschmechanismus, muss eine unwiederherstellbare mechanische Zerstörung erfolgen.
PKI-Rolle	Die PKI-Rolle beschreibt die Funktionsklasse eines PKI-Teilnehmers in der SM-PKI. Folgende PKI-Rollen sind in der SM-PKI vorhanden: GWA, GWH, EMT, Sub-CA, SMGW und Root-CA. Ein PKI-Teilnehmer ist eine Instanz seiner PKI-Rolle.
Wirkzertifikat	siehe [TR-03109-4]
Sequenznummer	SERIAL NUMBER des Distinguished Name, siehe Anhang A
Serialnumber	serialNumber Feld des Zertifikats, siehe TR-03109-4

Tabelle 32: Definitionen

Literaturverzeichnis

Literaturverzeichnis

AIS 20	BSI: Anwendungshinweise und Interpretationen zum Schema AIS 20, Funktionalitätsklassen und Evaluationsmethodologie für determistische Zufallszahlengeneratoren Version 3, 2013
AIS 31	BSI: Anwendungshinweise und Interpretationen zum Schema AIS 20, Funktionalitätsklassen und Evaluationsmethodologie für physikalischer Zufallszahlengeneratoren Version 3, 2013
BSI-CC-PP-0073	BSI: Protection Profile for the Gateway of a Smart Metering System (Smart Meter Gateway PP), Version 1.3, 2014
BSI-CC-PP-0077	BSI: Protection Profile for the Security Module of a Smart Meter Gateway (Security Module PP),
DIN 43863-5	DIN: Herstellerübergreifende Identifikationsnummer für Messeinrichtungen, 2012
GDEW	: Gesetz zur Digitalisierung der Energiewende, 2016
ISO 19005-1	ISO/IEC: Document management – Electronic document file format for longterm preservation – Part 1: User of PDF 1.4 (PDF/A-1),
ISO 3116 ALPHA-2	ISO: Codes for countries and their subdivisions, ALPHA-2 coding,
ISO/IEC 27001	ISO/IEC: Information technology — Security techniques — Information security management systems — Requirements,
KeyLifecSec	BSI: Key Lifecycle Security Requirements Version 1.0,
RFC 2119	IETF: Key words for use in RFCs to Indicate Requirements Levels,
RFC 3647	IETF: Internet X.509 Public Key Infrastructure, Certificate Policy and Certification Practices Framework,
TR-02102-1	BSI: Technische Richtlinie Kryptographische Verfahren: Empfehlungen und Schlüssellängen,
TR-03109-1	BSI: Anforderungen an die Interoperabilität der Kommunikationseinheit eines intelligenten Messsystems, 2013
TR-03109-2	BSI: Smart Meter Gateway – Anforderungen an die Funktionalität und Interoperabilität des Sicherheitsmoduls, 2013
TR-03109-4	BSI: Technische Richtlinie TR-03109-4, Smart Metering PKI – Public Key Infrastructure für Smart Meter Gateways,
TR-03109-6	BSI: Smart Meter Gateway Administration, 2015
TR-03116-3	BSI: eCard-Projekte der Bundesregierung - Kryptographische Vorgaben für die Infrastruktur von intelligenten Messsystemen,
TR-03116-4	BSI: Technische Richtlinie TR-03116-4, Kryptographische Vorgaben für Projekte der Bundesregierung, Teil 4 Kommunikationsverfahren in Anwendungen,
TR-03145-1	BSI: Technische Richtlinie Secure CA operation, Part 1: Generic requirements for Trust Centers instantiating as Certification Authority (CA) in a Public-Key Infrastructure (PKI) with security level 'high', Version 1.0,

Stichwort- und Abkürzungsverzeichnis

Abkürzung	Begriff
ASP	Ansprechpartner (des Unternehmens)
BSI	Bundesamt für Sicherheit in der Informationstechnik
CA	Certificate Authority
CC	Common Criteria
CER	Canonical Encoding Rules (Format zur Zertifikatscodierung)
CLS	controllable local systems
CN	Common Name
CP	Certificate Policy
CPS	Certificate Practise Statement
CRL	Certificate Revocation List (Zertifikatssperrliste)
DRG	(Funktionsklasse für Zufallsgeneratoren)
DN	Distinguished Name
EMT	Externe Marktteilnehmer
ENC	Encryption / Verschlüsselung
GWA	Gateway Administrator
GWH	Gateway Hersteller
HAN	Home Area Network (Heimnetz)
HSM	Hardware Sicherheitsmodul
ISMS	Information Security Management System
ISO	International Organization of Standardization
KEK	Key Encyption Key
KM	Krypto Modul
LDAP	Lightweight Directory Access Protocol
LMN	Lokales metrologisches Netzwerk
NTG	hybride deterministische Zufallszahlgeneratoren (Funktionsklasse für Zufallsgeneratoren)
OCSP	Online Certificate Status Protocol
PIN	Personal Identifikation Number
PKI	Public Key Infrastructure
PP	Protection Profile
PTG	hybride physikalische Zufallszahlgeneratoren (Funktionsklasse für Zufallsgeneratoren)
RA	Registration Authority
SHA	Secure Hash Algorithm
SMGW	Smart Meter Gateway

Abkürzung	Begriff
S/MIME	Secure/Multipurpose Mail Extension
SM-PKI	Smart Metering – Public Key Infrastructure
TLS	Transport Layer Security (Protokoll zur Verschlüsselung einer Datenübertragung)
TR	Technische Richtlinie
WAN	Wide Area Network (Weitverkehrsnetz)
X.509	ITU-T-Standard für eine Public-Key-Infrastruktur