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

Digitale Division, Business Unit Energy

Version	07.00
Stand	10.06.2020
Status	freigegeben
Autor	Deutsche Telekom Security GmbH

Schutzklasse: öffentlich

Impressum

Herausgeber

Deutsche Telekom Security GmbH

Digitale Division, Business Unit Energy

Bonner Talweg 100
53113 Bonn

Dateiname	Dokumentennummer	Dokumentenbezeichnung
CP_CPS_EnergyCA_07.00_20200610_freigegeben.docx	1.3.6.1.4.1.7879.13.36	Certificate Policy (CP) & Certification Practice Statement (CPS)

Version	Stand	Status
07.00	10.06.2020	freigegeben

Autor	Inhaltlich geprüft von	Freigegeben von
AJ	ME	HH

Kurzinfo

In dem vorliegenden Dokument sind CP und CPS für die **EnergyCA** zusammengefasst.

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

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

Änderungshistorie

Version	Stand	Autor/Bearbeiter	Kommentar
2.0	Freigegeben	T-Systems Int. GmbH	Finales Dokument
2.1	Entwurf	AR	Formelle Prüfung/QS
3.0	Freigegeben	AR	nach Freigabe
3.1	Entwurf	AR	Anpassungen RA
3.2	Entwurf	AR	Formelle Prüfung/QS
4.0	freigegeben	AR	nach Freigabe
4.1	Entwurf	AR	Anpassung TR 1.1 (2016)
4.2	Entwurf	AR	Formelle Prüfung/QS
5.0	freigegeben	AR	nach Freigabe
5.9	Entwurf	AR	Neu: CP 1.1.1 / TR 1.2.1
5.9.1	Entwurf	AR	Formelle Prüfung/QS
6.0	freigegeben	AR	nach Freigabe
6.0.1	freigegeben	ME	Kleine formale Änderung in Deutsche Telekom Security GmbH
06.0.2	freigegeben	GK	Formelle Prüfung/QS
07.00	freigegeben	HH	Freigabe

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.

Deutsche Telekom Security GmbH – im Folgenden „T Security“ genannt - betreibt in diesem Kontext eine Sub-CA, die im folgenden als

EnergyCA

bezeichnet wird. Vor diesem Hintergrund entspricht die in diesem Dokument genannte Sub-CA der **EnergyCA**.

Das vorliegende Dokument stellt die Zertifizierungsrichtlinie (engl. Certificate Policy kurz CP) und die Erklärung zum Zertifizierungsbetrieb (engl. Certification Practice Statement, kurz CPS) der **EnergyCA** dar und beinhaltet Sicherheitsvorgaben sowie Beschreibungen technischer, organisatorischer und rechtlicher Aspekte.

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

1.1 Überblick

Das Dokument richtet sich an alle Teilnehmer der SM-PKI und insbesondere an Hersteller (GWH), Administratoren (GWA) und weitere Teilnehmer (EMT), die Zertifikate der **EnergyCA** nutzen oder benötigen.

Die Struktur des Dokumentes in folgenden Abschnitten orientiert sich am international anerkannten Standard (RFC3647). Damit wird der Vergleich mit anderen Public Key Infrastrukturen ermöglicht.

Die Verantwortlichkeit für die **EnergyCA** obliegt T Security. T Security behält sich vor, komplette Aufgaben oder Teilaufgaben von beauftragten Unternehmen ausführen zu lassen ohne diese explizit in diesem Dokument aufzuführen.

1.2 Name und Identifizierung des Dokuments

Dieses Dokument ist die Certificate Policy (CP) und das Certificate Practice Statement (CPS) der **EnergyCA** im Umfeld der deutschen Smart Metering PKI (SM-PKI-DE) und kann über die folgenden Informationen identifiziert werden.

Identifikator	Wert
Titel	CP & CPS EnergyCA
Version	07.00
OID	1.3.6.1.4.1.7879.13.36

Tabelle 1: OID CP/CPS EnergyCA

Dieses Dokument kann unter

https://www.telesec.de/de/energyca

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	Zertifizierungs-stelle	Registrierungs-stelle	Zertifikats-nehmer	Zertifikats-nutzer
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

1.3.1 Zertifizierungsstellen

Die **EnergyCA** ist eine Sub-CA der SM-PKI, welche von der Root-CA zur Ausstellung von Zertifikaten autorisiert wird und Zertifikate für ihre Kunden ausstellt.

Außerdem stellt die **EnergyCA** für sich selbst Zertifikate aus.

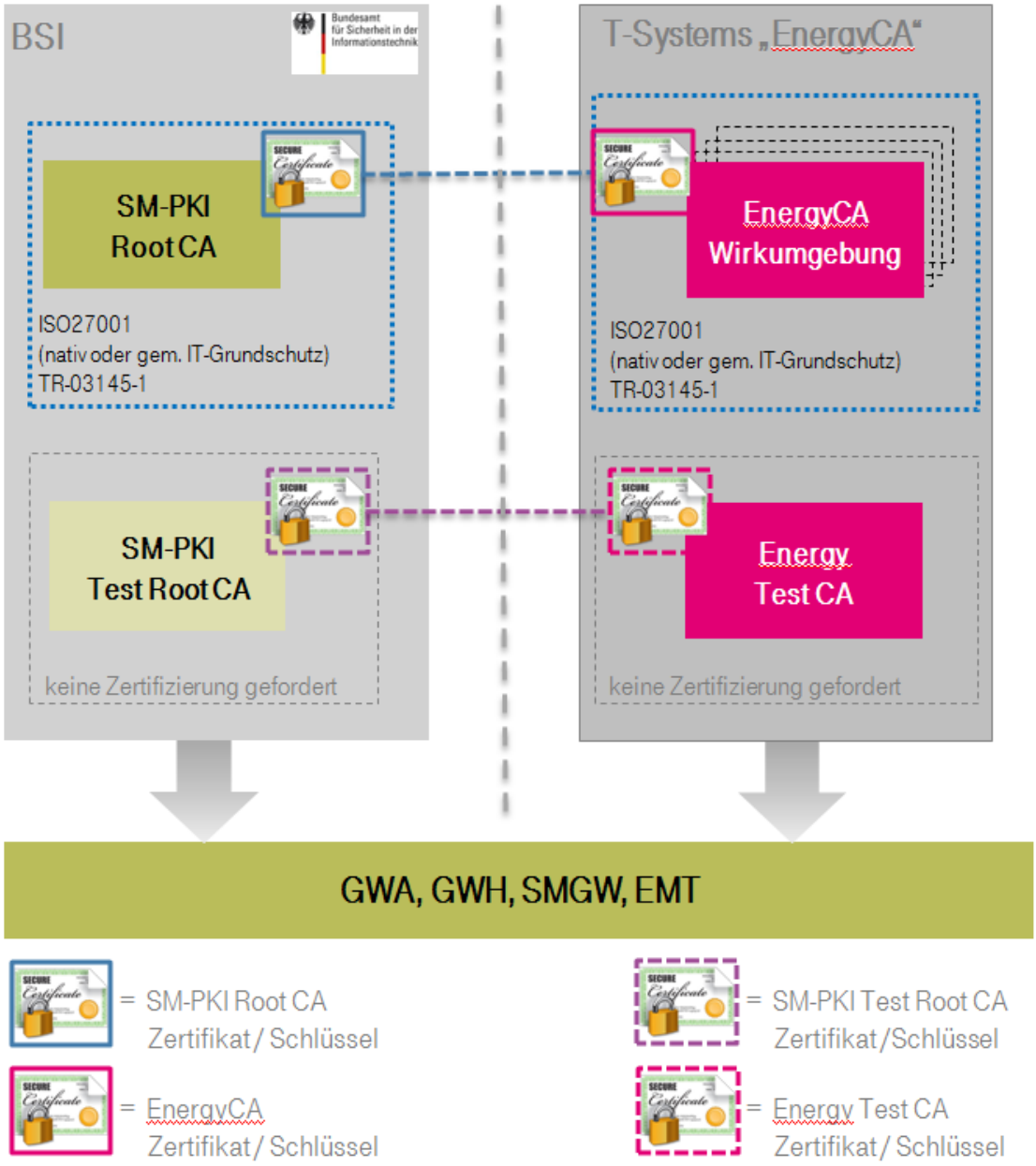

Abbildung 1-1: Schaubild der CA-Systeme der SM-PKI, hier: EnergyCA

Der Betreiber der **EnergyCA** als SM-PKI Sub-CA ist T Security.

Neben dem Wirksystem der **EnergyCA** betreibt T Security auch die **Energy Test CA.** Diese stellt für Testzwecke (z. B. Erst-Registrierung und zum Test systemkritischer Vorgänge, wie dem Wechsel des Vertrauensanker) die erforderlichen Funktionaltäten bereit.

Die technische Infrastruktur der **Energy Test CA** entspricht der Wirkumgebung der **EnergyCA.** Beide Plattformen sind informationstechnisch voneinander getrennt. Die verwendeten Schlüssel sind in beiden Plattformen unterschiedlich.

Die Anbindung an die jeweilige Root-CA ist in der o.a. Abbildung erläutert.

1.3.2 Registrierungsstelle der EnergyCA

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

Die Grundlage für die Prozesse der RA bildet diese Dokument so wie die Vorgaben der Certificate Policy der Smart Metering PKI.

1.3.3 Zertifikatsnehmer

Die nachfolgend beschriebenen PKI-Teilnehmer werden auch als Endnutzer oder Zertifikatsinhaber bezeichnet, da diese ihre Zertifikate nicht zur Ausstellung von Zertifikaten, sondern ausschließlich zur Absicherung der Kommunikation verwenden.

1.3.3.1 SMGW

Bei einem SMGW handelt es sich um eine technische Komponente (Kommunikationseinheit eines intelligenten Messsystems, siehe (TR-03109-1), die von der **EnergyCA** 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. Die Aufgaben und Anforderungen an den GWA sind in (TR-03109-6) definiert.

Ein Gateway-Administrator (GWA) erhält von der **EnergyCA** Zertifikate, mit denen dieser insbesondere die Beantragung und Verwaltung der Wirkzertifikate der SMGWs durchführen kann, die Administration der SMGWs durchführen kann und den Datenaustausch mit den anderen Teilnehmern der SM-PKI (z.B. EMT) absichern kann.

1.3.3.3 Gateway-Hersteller

Ein Hersteller von Gateway-Komponenten (GWH) erhält von der **EnergyCA** 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 der **EnergyCA** 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 erfolgen.

1.3.4 Zertifikatsnutzer

Zertifikatsnutzer im Sinne dieser **EnergyCA** Policy sind alle juristischen Personen bzw. technischen Komponenten, die Zertifikate aus der **EnergyCA** für die Erledigung von Geschäftsprozessen/Aufgaben verwenden.

1.3.5 Andere Teilnehmer

Teilnehmer (wie z.B. Endverbraucher), welche keine Verpflichtung im Rahmen dieser **EnergyCA** Policy eingegangen sind, sind nicht Bestandteil der **EnergyCA** Policy und werden daher nicht berücksichtigt.

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

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.

In den nachfolgenden Tabellen entspricht das C(Sub-CA) dem Sub-CA Zertifikat der **EnergyCA**.

EnergyCA:

Zertifikat der „EnergyCA“	**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- sowie 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 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 zwischen Sub-CA und anderen Systemen eingesetzt.

Tabelle 3: Zertifikate der EnergyCA

Das C_{TLS}(Sub-CA) Zertifikat wird seitens der **EnergyCA** für sich selbst ausgestellt. Der Prozess hierzu ist in der Betriebsdokumentation hinterlegt.

Zertifikate der Zertifikatsnehmer:

Zertifikat eines Zertifikats-nehmers	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 eines TLS-Kanals. 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 4: 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 **EnergyCA** bereitgestellt, die Anforderungen an diese Zertifikate sind in Tabelle 5 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 wird EMPFOHLEN, dass Zertifikate den Anforderungen der (TR-03116-4) entsprechen.

Tabelle 5: Kommunikationszertifikate der Ansprechpartner

1.4.2 Verbotene Verwendung von Zertifikaten

Die Zertifikate dürfen nur ausschließlich gemäß ihres Verwendungszwecks (siehe Abschnitt 1.4.1) eingesetzt werden.

1.5 Administration der EnergyCA CP/CPS

Die für dieses Dokument verantwortliche Organisation ist T Security.

Organisation	Deutsche Telekom Security GmbH
Abteilung	Digital Division, Business Unit Energy
Adresse	Bonner Talweg 100, 53113 Bonn
Fax	+49 391 58010 1697 (FAX)
E-Mail	EnergyCA_Kontakt@t-systems.com
Webseite	www.telesec.de/energyca

Tabelle 6: Kontaktadresse CP/CPS EnergyCA

1.5.1 Pflege der EnergyCA CP/CPS

Jede aktualisierte Version dieses Dokumentes wird den Kunden der **EnergyCA** unverzüglich über die angegebene Internetseite (siehe 1.5) zur Verfügung gestellt.

1.5.2 Zuständigkeit für das Dokument

Zuständig für die Erweiterung und oder die nachträgliche Änderungen dieser **EnergyCA** CP/CPS ist ausschließlich die Deutsche Telekom Security GmbH als Betreiber der **EnergyCA**.

1.5.3 Ansprechpartner / Kontaktperson

Siehe Tabelle 6: Kontaktadresse CP/CPS EnergyCA

1.5.4 Konformität zur CP SM-PKI

Das vorliegende Dokument ist Bestandteil der Betriebsdokumentation der **EnergyCA**.

2 Verantwortlichkeit für Veröffentlichungen und Verzeichnisse

2.1 Verzeichnisse

Von der **EnergyCA** wird ein Verzeichnis gemäß (TR-03109-4) mit allen von der **EnergyCA** ausgestellten Zertifikaten bereitgestellt.

Zusätzlich wird für den Verantwortungsbereich der **EnergyCA** eine Sperrliste erzeugt, in der alle gesperrten Zertifikate während ihres Gültigkeitszeitraums aufgeführt sind.

Die Informationen zum Verzeichnis und dem Sperrlistenverteilpunkt sind aus den Veröffentlichungen der **EnergyCA** (s. Kapitel 2.2.1) zu entnehmen.

2.2 Veröffentlichung von Informationen zur Zertifikatserstellung

2.2.1 Veröffentlichungen der EnergyCA

Die **EnergyCA** verfügt über eine eigene Web-Seite, welche die folgenden Informationen beinhaltet:

- Kontaktdaten der **EnergyCA**
- Die aktuellen Zertifikate der **EnergyCA** inklusive des SHA256 Hashs
- Parameter zur Einrichtung eines Zugriffs auf die Sperrliste bzw. das LDAP-Verzeichnis
- CP/CPS Dokument der **EnergyCA** (dieses Dokument)
    - wobei die CP/CPS der EnergyCA die (CP-SM-PKI) bestätigt
    - in der die für die Bereitstellung und Verwaltung notwendigen Prozesse beschrieben werden
    - in dem der für den Betrieb der **EnergyCA** verantwortliche Bereich (s. Tabelle 6)
- Beschreibung des Antragsverfahrens von Zertifikaten unterhalb der **EnergyCA**
- Formulare zur Beantragung von Zertifikaten
- Informationen zu den zu erstellenden jeweiligen Zertifikatsrequests
- Informationen zum Sperrprozess von Zertifikaten
- Formulare zur Sperrung von Zertifikaten / zur Übertragung der Sperrberechtigung
- Hinweise zur Teilnahme am Testsystem

2.3 Zeitpunkt und Häufigkeit der Veröffentlichungen

Alle Zertifikate der **EnergyCA** werden unmittelbar nach der Ausstellung im jeweiligen LDAP-Verzeichnis veröffentlicht.

Sperrungen oder Suspendierungen werden nach Durchführung durch eine Veröffentlichung in der jeweiligen Sperrliste in der **EnergyCA** als solche wirksam. Eine Aufnahme in die Sperrliste sowie deren Veröffentlichung erfolgt gemäß den in der (CP-SM-PKI) in Tabelle 11 festgelegten Zeiten.

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

2.4 Zugriffskontrollen auf Verzeichnisse

Der lesende Zugriff auf die LDAP-Verzeichnisdienste der **EnergyCA** wird auf die an der SM-PKI teilnehmenden Organisationen, wie die SM-PKI Root und Sub-CAs, GWA, GWH sowie EMTs beschränkt[1] Dies wird über eine zertifikatsbasierte Authentisierung am jeweiligen Verzeichnisdienst mittels der TLS-Zertifikate der Zertifikatsnehmer gemäß den Anforderungen aus (TR-03116-3) sichergestellt.

Der Verzeichnisdienst der **EnergyCA** dient ausschließlich der Aktualisierung von angefragten Zertifikaten. Ein Massenabruf von Zertifikaten ist nicht gestattet. Der Verzeichnisdienst ist so konfiguriert, dass die Anzahl der zurückgegebenen Suchergebnisse auf „100“ begrenzt ist.

Der lesende Zugriff auf die Sperrlisten der **EnergyCA** kann ohne Authentifikation und ohne Einschränkungen erfolgen.

[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 der **EnergyCA** *(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 **EnergyCA** dem Profil gemäß Anhang A der (CP-SM-PKI) entsprechen.

3.1.1 Arten von Namen

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

3.1.2 Notwendigkeit für aussagefähige Namen

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

3.1.3 Anonymität oder Pseudonymität von Zertifikatsnehmern

Über den Zertifikatsantrag besteht immer eine eindeutige Zuordnung zu einem Zertifikatsnehmer. Anonyme Zertifikatsnehmer sind in der **EnergyCA** nicht erlaubt. Pseudonyme werden nicht verwendet.

3.1.4 Eindeutigkeit von Namen

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

Eine Namensgleichheit (gleicher CN bei unterschiedlichem Zertifikatsnehmer) wird durch die **EnergyCA** verhindert, entsprechend vergibt die **EnergyCA** einen CN NICHT mehrfach.

Sollten zwei oder mehr Zertifikatsnehmer der **EnergyCA** den gleichen CN wünschen, wird dieser Konflikt gelöst. Es behält der Teilnehmer seinen CN, der zuerst sein initiales

Zertifikat mit diesem CN von der **EnergyCA** erhalten hat. Der oder die anderen Zertifikatsnehmer lassen sich ein Zertifikat mit einem anderem CN ausstellen, um an der **EnergyCA** teilnehmen zu dürfen.

3.1.5 Anerkennung, Authentifizierung und die Rolle von Markennamen

Die Übernahme von Firmennamen oder Markennamen in den CN erfolgt gemäß den Vorgaben aus Kapitel 3.1.1 auf Basis der Identität, die im Rahmen der initialen Überprüfung in das erste Zertifikat übernommen wurde.

3.2 Initiale Überprüfung zur Teilnahme an der EnergyCA als Teil der SM-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 der **EnergyCA**.

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

3.2.1 Methoden zur Überprüfung bzgl. Besitz des privaten Schlüssels

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

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

3.2.2 Authentifizierung von Organisationszugehörigkeiten

3.2.2.1 EMT

Zur Aufnahme eines neuen EMT in die **EnergyCA** wird das Unternehmen durch Registration Authority (RA) der **EnergyCA** authentifiziert.

Notwendige Unterlagen und Daten für die Registrierung sind:

- Antragsschreiben zur Ausgabe eines EMT-Zertifikats mit folgenden Daten bzw. beigefügten Informationen
  - Name der Firma bzw. der Institution
  - Anschrift des Unternehmens bzw. der Institution
  - Unternehmensnachweis (z.B. aktueller Auszug aus dem Handelsregister) oder Nachweis der Institution (durch ein entsprechendes Siegel der Institution)
  - Kontaktdaten der Ansprechpartner (unter Beachtung einer Vertreterregelung)
  - Bei der Beauftragung eines Dienstleisters für den Betrieb des EMT legt der Betreiber eine Bestätigung des Unternehmens vor, die den Dienstleister zur Beantragung und zum Betrieb für den EMT berechtigt.
  - Bestätigung der Geschäftsführung des Unternehmens bzw. der Leitung der Institution, in der der Vertreter des Unternehmens berechtigt wird, den Antrag für den EMT zu stellen und in der Sache dazu verbindliche Aussagen und Angaben zu machen. Persönliche/individuelle Zertifikate für die gesicherte E-Mail-Kommunikation der benannten Ansprechpartner ($C_{S/MIME}$(ASP EMT)) inklusive der zur Verifikation erforderlichen Zertifikatskette.
- Erklärung zur Nutzung des EMT-Zertifikats
  - Aus der Erklärung wird nachvollzogen, welche Funktionen und Aufgaben ein EMT wahrnehmen will. Es geht daraus insbesondere hervor, ob es sich um einen aktiven oder passiven EMT handelt.
- Erklärung zur Einhaltung der Sicherheitsvorgaben aus der EnergyCA Policy.
  - Der passive EMT reicht eine Erklärung zur Einhaltung der Sicherheitsvorgaben aus dieser **EnergyCA** Policy mit ein.
  - Der aktive EMT erbringt den Nachweis des sicheren Betriebs gemäß den Vorgaben zu den Anforderungen für die Teilnahme an der **EnergyCA** (s. Tabelle 16)
- Der Hashwert (SHA 256) des initialen Zertifikatsrequest-Pakets für das Signatur (C_{Sig}(EMT)), das Verschlüsselungs-(C_{Enc}(EMT)) und das TLS-Zertifikat (C_{TLS}(EMT)) des EMT (gemäß (TR-03109-4)) wird in gedruckter Form inklusive der Information zum Format der Darstellung mit der Bestätigung durch die Unterschrift des Bevollmächtigten vorgelegt. Der Hashwert wird dabei über die binär-codierte Request-Datei gebildet, welche das Zertifikatsrequest-Paket gemäß (TR-03109-4) enthält, und als base64-codierter Ausdruck in diesem Prozess verwendet.
- Bestätigung der erfolgreichen Test-Teilnahme
  - Vor der initialen Identifizierung und Authentifizierung ist die Registrierung, Zertifikatsbeantragung-, -erneuerung und -sperrung von EMT-Zertifikaten unterhalb der **Energy Test CA** (siehe Abschnitt 1.3.1) erfolgreich erprobt worden. Die erfolgreiche Teilnahme wird von einem Ansprechpartner der **Energy Test CA** per signierter E-Mail bestätigt.

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

3.2.2.2 GWA

Zur Aufnahme eines neuen GWA in die **EnergyCA** wird das Unternehmen authentifiziert und mindestens zwei bevollmächtigte Vertreter des GWA werden persönlich bei der Registration Authority (RA) der **EnergyCA** identifiziert und authentifiziert. Der Ortstermin wird durch die Ansprechpartner der **EnergyCA** aus Tabelle 7 koordiniert und abgestimmt.

Notwendige Unterlagen und Daten für die Registrierung sind:

- Antragsschreiben zur Ausgabe eines GWA-Zertifikats mit folgenden Daten bzw. beigefügten Informationen
  - Name der Firma bzw. der Institution
  - Anschrift des Unternehmens bzw. der Institution
  - Unternehmensnachweis (z.B. aktueller Auszug aus dem Handelsregister) oder Nachweis der Institution (durch ein entsprechendes Siegel der Institution)
  - Kontaktdaten der Ansprechpartner (unter Beachtung einer Vertreterregelung)
  - Bestätigung der Geschäftsführung des Unternehmens bzw. der Leitung der Institution, in der der Vertreter des Unternehmens berechtigt wird, den Antrag für den GWA zu stellen und in der Sache dazu verbindliche Aussagen und Angaben zu machen.
- Persönliche/individuelle Zertifikate für die gesicherte E-Mail-Kommunikation der benannten Ansprechpartner ($C_{S/MIME}$(ASP GWA)) inklusive der zur Verifikation erforderlichen Zertifikatskette
- Erklärung zur Einhaltung der Sicherheitsvorgaben aus dieser **EnergyCA** Policy
  - Nachweise über die Einhaltung der Vorgaben zu den Anforderungen für die Teilnahme an der **EnergyCA** (s. Tabelle 16)
- Bestätigung der erfolgreichen Testteilnahme
  - Vor der initialen Identifizierung und Authentifizierung ist die Registrierung, Zertifikatsbeantragung-, -erneuerung und -sperrung von GWA- und SMGW-Zertifikaten unterhalb der **Energy Test CA** (siehe Abschnitt 1.3.1) erfolgreich erprobt worden. Die erfolgreiche Teilnahme wird von einem Ansprechpartner der **Energy Test CA** per signierter E-Mail bestätigt.
- Der Hashwert (SHA 256) des initialen Zertifikatsrequest-Pakets für das Signatur- (C_{Sig}(GWA)), das Verschlüsselungs- (C_{Enc}(GWA)) und das TLS-Zertifikat (C_{TLS}(GWA)) des GWA (gemäß (TR-03109-4)) wird in gedruckter Form inklusive der Information zum Format der Darstellung mit der Bestätigung durch die Unterschrift des Bevollmächtigten vorgelegt. Der Hashwert wird dabei über die binär-codierte Request-Datei gebildet, welche das Zertifikatsrequest-Paket gemäß (TR-03109-4) enthält, und als base64-codierter Ausdruck in diesem Prozess verwendet. Die eigentlichen Zertifikatsrequests können zusätzlich im Rahmen dieses Termins als Dateien übergeben.
  - Es wird empfohlen die Zertifikatsrequests vorab der **EnergyCA** zuzusenden, so dass vor dem Termin eine Überprüfung auf Konformität erfolgen kann.

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

3.2.2.3 GWH

Zur Aufnahme eines neuen GWH in die **EnergyCA** wird das Unternehmen authentifiziert und mindestens zwei bevollmächtigte Vertreter des GWH persönlich bei der Registration Authority (RA) der **EnergyCA** identifiziert und authentifiziert. Der Ortstermin wird durch die Ansprechpartner der **EnergyCA** aus Tabelle 7 koordiniert und abgestimmt.

Notwendige Unterlagen und Daten für die Registrierung sind:

- Antragsschreiben zur Ausgabe eines GWH Zertifikats mit folgenden Daten bzw. beigefügten Informationen
  - Name der Firma bzw. der Institution
  - Anschrift des Unternehmens bzw. der Institution
  - Unternehmensnachweis (z.B. aktueller Auszug aus dem Handelsregister) oder Nachweis der Institution (durch ein entsprechendes Siegel der Institution)
  - Kontaktdaten der Ansprechpartner (unter Beachtung einer Vertreterregelung)
  - Bestätigung der Geschäftsführung des Unternehmens bzw. der Leitung der Institution, in der der Vertreter des Unternehmens berechtigt wird, den Antrag für den GWH zu stellen und in der Sache dazu verbindliche Aussagen und Angaben zu machen.
- Persönliche/individuelle Zertifikate für die gesicherte E-Mail-Kommunikation der benannten Ansprechpartner ($C_{S/MIME}$(ASP GWH)) inklusive der zur Verifikation erforderlichen Zertifikatskette
- Erklärung zur Einhaltung der Sicherheitsvorgaben aus dieser **EnergyCA** Policy
  - Zusätzlich wird durch den GWH der Nachweis über den sicheren Betrieb gemäß den Vorgaben zu den Anforderungen für die Teilnahme an der **EnergyCA** (s.Tabelle 16) vorlegt.
- Bestätigung der erfolgreichen Testteilnahme
  - Vor der initialen Identifizierung und Authentifizierung ist die Registrierung, Zertifikatsbeantragung-, -erneuerung und -sperrung von GWH und SMGW-Gütesiegelzertifikaten unterhalb der **Energy Test CA** (siehe Abschnitt 1.3.1) erfolgreich erprobt worden. Die erfolgreiche Teilnahme wird von einem Ansprechpartner der **Energy Test 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)) wird in gedruckter Form inklusive der Information zum Format der Darstellung mit der Bestätigung durch die Unterschrift des Bevollmächtigten vorgelegt. Der Hashwert wird dabei über die binär-codierte Request-Datei gebildet, welche das Zertifikatsrequest-Paket gemäß (TR-03109-4) enthält, und als base64-codierter Ausdruck in diesem

Prozess verwendet. Die eigentlichen Zertifikatsrequests KÖNNEN zusätzlich im Rahmen dieses Termins als Dateien übergeben werden.

- Es wird empfohlen die Zertifikatsrequests vorab der **EnergyCA** zuzusenden, so dass vor dem Termin eine Überprüfung auf Konformität erfolgen kann.

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

3.2.2.4 SMGW

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

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

Aufbringen der Gütesiegelzertifikate

Grundvoraussetzung für das Aufbringen von Gütesiegel-Zertifikaten ist, dass der GWH bei der **EnergyCA** registriert ist (siehe Abschnitt 3.2.2.3) und über gültige Zertifikate verfügt. Dabei werden die Anforderungen aus Tabelle 16 eingehalten.

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

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

Die von der **EnergyCA** 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 der **EnergyCA** registriert ist (siehe Abschnitt 3.2.2.2) und über gültige Zertifikate verfügt.

Bei den SMGWs sind die Gütesiegelzertifikate im Rahmen der Personalisierung nach der (TR-03109-1) beim erstmaligen Kontakt mit dem GWA durch Wirkzertifikate zu ersetzen.

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

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

3.2.3 Anforderungen zur Identifizierung und Authentifizierung des Zertifikats-Antragstellers

Ein Zertifikatsrequest darf nicht von einer Einzelperson (natürliche Person), sondern muss von einer Organisation (juristische Person) gestellt werden. Dies gilt insbesondere auch für die Zertifikatsrequests der SMGWs, die durch den GWH bzw. GWA zu übermitteln sind.

3.2.4 Ungeprüfte Angaben zum Zertifikatsnehmer

Die Registrierungsstelle prüft beim EMT, GWA und GWH die Angaben zum Zertifikatsnehmer im Zertifikatsrequest gegen die eingereichten Unterlagen auf Korrektheit (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 **EnergyCA** geforderten Zertifizierungen (s. Tabelle 16) in der Regel einem jährlichen Überwachungszyklus, für das z.B. ein Audit positiv abgeschlossen werden muss.

Die **EnergyCA** muss von dem Zertifikatsnehmer rechtzeitig vor Ablauf der eingereichten Zertifikatsunterlagen über die Ergebnisse der Auditierung informiert und soweit ausgestellt auch das entsprechende Zertifikat zur Verfügung gestellt bekommen.

Sollte der Teilnehmer die Zertifizierung nicht mehr erhalten, so wird das Zertifikat bzw. werden die Zertifikate aus der **EnergyCA** gesperrt.

Informationen über relevante Änderungen, die beispielsweise

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

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

Die **EnergyCA** aktualisiert anschließend die entsprechenden Registrierungsdaten.

3.2.8 Aktualisierung/Anpassung der Registrierungsinformationen der Teilnehmer

Jeder Teilnehmer muss der Registrierungsstelle der **EnergyCA** unverzüglich eine Änderung bzgl. seiner Registrierungsdaten mitteilen (vgl. hierzu Abschnitt 4.7).

Ergänzend wird die **EnergyCA** regelmäßig alle 12 Monate, erstmals 12 Monate nach der Registrierung bei den Teilnehmern anfragen, ob Änderungen an den Registrierungsdaten vorliegen. Diese Anfrage erfolgt durch gesicherte Kommunikation via E-Mail (S/MIME) von der RA der **EnergyCA** an die hinterlegten Ansprechpartner der Kunden.

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

Nach der initialen Zertifikatsausstellung erfolgen sogenannte Folgeanträge. Diese werden ebenso wie die initialen Zertifikatsanträge zweifelsfrei von der **EnergyCA** identifiziert und authentisiert.

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

Ein Zertifikatsinhaber ist dafür verantwortlich, rechtzeitig, d.h. vor dem Ablauf aller Zertifikate, neue Zertifikate zu beantragen (vgl. (TR-03116-4)). Dies gilt insbesondere für Zertifikate (Gütesiegelzertifikate und Wirkzertifikate) für SMGWs. Der Zeitpunkt ist so zu wählen, dass die neuen Zertifikate rechtzeitig in die Systeme eingebracht werden können, so dass der Betrieb ohne Beeinträchtigungen fortgeführt werden kann. Beim GWA, GWH und EMT kann es nach der Ausstellung des neuen Zertifikats zu einem temporären Betrieb mit mehreren gleichzeitig gültigen Zertifikaten kommen. Diese Phase dient dazu, allen relevanten Komponenten rechtzeitig das neue Zertifikat bekanntzumachen.

Der Antragsteller besitzt einen privaten Schlüssel des dem Betreiber zugeordneten TLS-Zertifikats, mit dem die Absicherung des Kommunikationskanals durchgeführt werden muss. Das Zertifikat zu diesem Schlüssel darf weder gesperrt noch abgelaufen sein. Der zu übermittelnde Zertifikatsrequest (unabhängig von dem Zertifikatstyp) bzw. das Zertifikatsrequest-Paket ist mit dem zuletzt gültigen Signaturschlüssel signiert worden, und das zugehörige Zertifikat ist noch gültig und nicht gesperrt

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

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

3.4.1 Allgemein

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

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

Entsprechend ist eine der beiden Absicherungen eines Folgeantrags nicht gegeben. Daher kann der zuvor beschriebene Regelprozess (routinemäßiger Folgeantrag) nicht

genutzt werden. Die weitere Vorgehensweise unterscheidet sich anhand der dem Antragsteller zu diesem Zeitpunkt noch zur Verfügung stehenden Sicherheitsmerkmale.

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

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

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

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

Zusätzlich wird ebenfalls über einen gesicherten Kanal (z.B. eine verschlüsselte und signierte E-Mail des benannten ASP des Zertifikatsnehmers) der Hashwert des Zertifikatspaketes zum Abgleich und zur Autorisation zugesendet. Die Hashwerte (SHA 256) werden dabei über die binär-codierte Request-Datei gebildet, welche das Zertifikatsrequest-Paket gemäß (TR-03109-4) enthält, und als base64-codierter Ausdruck in einer [ISO19005-1] konformen Datei versendet wird.

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

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

3.4.2 Schlüsselerneuerung nach Sperrung

Das weitere Vorgehen zur Identifizierung und Authentifizierung eines Teilnehmers der **EnergyCA** nach einer Sperrung ist davon abhängig, welche seiner Zertifikate von der

Sperrung betroffen sind. Der Teilnehmer der **EnergyCA** stellt auf Basis der ihm zur Verfügung stehenden gültigen Zertifikate einen Folgeantrag gemäß des vorangegangenen Unterkapitels, um seine gesperrten Zertifikate durch neue gültige Zertifikate zu ersetzen. Ein Endnutzer beantragt immer ein neues Zertifikatstripel.

3.5 Identifizierung und Authentifizierung von Anträgen auf Sperrung

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

- dem Zertifikatsinhaber
- der **EnergyCA**
- der Root CA

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

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

3.5.1 Initiative des Zertifikatsinhabers

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

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

Der benannte Ansprechpartner sendet in diesem Fall eine mittels seinem $C_{S/MIME}$ (ASP) signierte E-Mail an die **EnergyCA**. Diese prüft die Authentizität der Information, den Sperrwunsch laut Tabelle 10 auf Durchführbarkeit und Beteiligung der SM-PKI Root. Sperrungen von Zertifikaten mit systemrelevanter Bedeutung erfolgen in Abstimmung mit der SM-PKI Root.

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

Für die Sperrung von nicht systemrelevanten Zertifikaten bietet die **EnergyCA** im Kundenfrontend eine Sperrfunktion im „user-self-service“ (siehe Kapitel 4.8.1) an.

3.5.1.1 Verantwortlichkeit für die Sperrung eines SMGW

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

Voraussetzung für die Übertragung der technischen Verantwortlichkeit ist, dass der GWH den GWA, an den übertragen werden soll, bei der zugehörigen **EnergyCA** bekannt gemacht hat. Dieses erfolgt mittels eines Formulares, welches über den Download-Bereich (s. Tabelle 6: Kontaktadresse CP/CPS EnergyCA) bezogen werden kann. Das vom registrierten Ansprechpartner unterschriebene Formular ist elektronisch – mit den notwendigen Zertifikaten (laut Formular, z. B. C_{TLS} (GWA)…) – an die **EnergyCA** (s. Tabelle 7: Kontaktadresse EnergyCA Registration Authority (RA)) zu übermitteln. Dies muss über einen sicheren Kommunikationskanal erfolgen (z.B. signierte E-Mail). Die **EnergyCA** prüft die Angaben des GWH, indem ein sicherer Kanal (S/MIME) zum GWA aufgebaut wird. Das Ergebnis wird dem GWH mitgeteilt.

Ein GWA kann Gütesiegelzertifikate nur dann sperren, wenn seine technische Verantwortlichkeit für das betreffende SMGW in der **EnergyCA** registriert ist. Zur Durchführung dieser Registrierung kann der GWH die Webservice-Schnittstelle der **EnergyCA** nutzen, alternativ kann er einen entsprechend abgesicherten, etablierte Kommunikationskanal (z.B. signierte E-Mail) verwenden.

Falls der GWH die Webservice-Schnittstelle nutzen möchte, so erstellt einen Datensatz gemäß (TR-03109-4), in welchem er eines oder mehrere SMGWs und den dafür zuständigen GWA benennt. Diesen Datensatz signiert er mit dem privaten Schlüssel von C_{SIG}(GWH) und sendet ihn per Web-Service an die **EnergyCA**. Die Übertragung der technischen Verantwortlichkeit an den GWA ist mit sofortiger Wirkung gültig, sobald die **EnergyCA** den Datensatz erfolgreich verarbeitet hat.

Durch die Übertragung der technischen Verantwortlichkeit erhält der GWA die Berechtigung, die Gütesiegelzertifikate der betreffenden SMGWs zu sperren. Um Wirkzertifikate für das SMGW beantragen zu können, ist dieser Schritt nicht erforderlich.

Die Übertragung der technischen Verantwortlichkeit für SMGWs kann je SMGW nur einmalig vom zuständigen GWH initiiert werden.

Der GWA wird von der **EnergyCA** per signierter E-Mail an die zuvor benannten Ansprechpartner informiert, sobald die Übertragung der Verantwortlichkeit abgeschlossen wurde.

3.5.1.2 Sperrung eines SMGW

Die Sperrung eines SMGW-Zertifikats muss über die Web-Service-Schnittelle der EnergyCA als Paket (enthält Zertifikatstripel, siehe (TR-03109-4) beantragt werden. Die **EnergyCA** prüft bei der Bearbeitung von Sperranträgen für Gütesiegelzertifikate, ob der

Absender und Unterzeichner des Sperrantrags für die zu sperrenden Zertifikate technisch verantwortlich ist. Wurde die technische Verantwortlichkeit für Gütesiegelzertifikate an einen GWA übertragen, so ist dieser alleinig sperrberechtigt. In allen anderen Fällen ist diejenige Instanz sperrberechtigt, die die Zertifikate beantragt hat.

Im Ausnahmefall (z.B. Web-Service-Schnittstelle steht nicht zur Verfügung) kann die Sperrung auch über einen entsprechend abgesicherten, etablierten Kommunikationskanal (z.B. signierte E-Mail) erfolgen.

3.5.2 Initiative des Betreibers der Certificate Authority

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

- ein erkannter Verstoß gegen Betriebsauflagen (insbesondere gegen die Anforderungen für die Teilnahme an der **EnergyCA** (s. Tabelle 16),
- erkannte (erhebliche) Schwächen in der eingesetzten Kryptographie oder Kryptoimplementierung,
- Änderungen in den zentralen Vorgaben (z.B. der (TR-03109-4)),
- Änderung der Zertifikatsdaten (z.B. des Organisationsnamens),
- eine erkannte Schlüsselkompromittierung oder
- die Einstellung des Betriebs bzw. die Außerbetriebnahme der betroffenen Komponente.

Sperrungen von Zertifikaten mit systemrelevanter Bedeutung (das Sub-CA Zertifikat der **EnergyCA** selbst und GWA) erfolgen in Abstimmung mit der SM-PKI Root.

Die Zertifikate eines SMGW, GWH oder eines EMT können in der eigenen Verantwortung durch die **EnergyCA** gesperrt werden. Sollten nach Ansicht des Betreibers der **EnergyCA** Sperrungen dieser Zertifikate systemrelevante Auswirkungen haben, so informiert die **EnergyCA** die Root vorab.

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

3.6 Identifizierung und Authentifizierung von Anträgen auf Suspendierung

Die Suspendierung der Wirk-Zertifikate eines SMGW MUSS vom zugehörigen GWA durchgeführt werden.

Bei einer Suspendierung müssen dafür folgende Informationen an die **EnergyCA** übermittelt werden:

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

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

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

4 Betriebsanforderungen für den Zertifikatslebenszyklus

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

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

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

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

4.1 Zertifikatsantrag

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

4.1.1 Wer kann einen Zertifikatsantrag stellen?

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

Ein Endnutzer (nicht SMGW) kann sofern erforderlich, weitere Zertifikate bzw. Zertifikatstripel siehe (TR-03109-4) für sich beantragen (z.B. für Lastmanagement oder Ausfallsicherheit).

Der Zertifikatsrequest muss als Folgeantrag (siehe Kapitel 3.3) unter Nutzung der vorhandenen Zertifikate bei der **EnergyCA** gestellt werden.

Die weiteren Zertifikate/Zertifikatstripel müssen eindeutig gekennzeichnet werden (siehe Anhang A der (CP-SM-PKI)). Die Eindeutigkeit von Zertifikaten erfolgt aus der Kombination von Common Name, der Sequenznummer im Subject-DN, der Seriennummer des Zertifikats und dem Issuer-DN (Herausgeber/CA).

4.1.2 Beantragungsprozess und Zuständigkeiten

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

Die Kontaktadresse zur Koordinierung lautet wie folgt:

Adresse	Deutsche Telekom Security GmbH
	Trust Center Notary
Strasse	Querstraße 1-9
PLZ und Ort	04103 Leipzig
E-Mail	tc.notary.leipzig@t-systems.com

Tabelle 7: Kontaktadresse EnergyCA Registration Authority (RA)

4.2 Verarbeitung von initialen Zertifikatsanträgen

4.2.1 Durchführung der Identifizierung und Authentifizierung

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

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

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

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

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

4.2.2 Annahme oder Ablehnung von initialen Zertifikatsanträgen

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

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

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

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

4.2.3 Fristen für die Bearbeitung von Zertifikatsanträgen

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

4.2.3.1 Ausgabe von initialen Endnutzer-Zertifikaten

Die Bearbeitung der Zertifikatsanträge gliedert sich in folgende Arbeitsschritte:

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

Tabelle 8: Zeitablauf für die initiale Ausgabe von Endnutzer-Zertifikaten (GWA,GWH, EMT)

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

4.2.4 Ausgabe von Zertifikaten

Die Ausgabe von SMGW-Zertifikaten erfolgt ausschließlich über die Web-Service-Schnittstelle.

Bei Endnutzer-Zertifikaten erfolgt, abgesehen von den initialen Zertifikaten, die Ausgabe über die Web-Service-Schnittstelle (EMT Folgezertifikate können auch über die anderen definierten Schnittstellen ausgegeben werden).

Die initialen Zertifikate werden immer, Folgezertifikate alternativ per E-Mail an den Ansprechpartner gesendet. Der Versand per E-Mail kann unverschlüsselt erfolgen.

4.2.5 Benachrichtigung des Zertifikatsnehmers über die Ausgabe des Zertifikats

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

4.3 Annahme von Zertifikaten

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

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

Die **EnergyCA** stellt eine Funktionsmailbox (FMB, E-Mail) für Fehlermeldungen zur Verfügung. Diese ist in Tabelle 9 aufgeführt.

E-Mail Support	Energyca_support@t-systems.com

Tabelle 9: Kommunikationsschnittstelle (E-Mail) der EnergyCA

4.3.1 Veröffentlichung von Zertifikaten durch die CA

Alle ausgestellten Zertifikate werden direkt nach deren Ausstellung im Verzeichnisdienst der **EnergyCA** veröffentlicht.

4.4 Verwendung von Schlüsselpaar und Zertifikat

4.4.1 Verwendung des privaten Schlüssels und des Zertifikats durch den Zertifikatsnehmer

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

4.4.2 Verwendung des öffentlichen Schlüssels und des Zertifikats durch Zertifikatsnutzer

Die Verwendung des öffentlichen Schlüssels und des Zertifikats erfolgt gemäß (TR-03109-4).

4.5 Zertifikatserneuerung

Zertifikatserneuerungen, d. h. das Ausstellen eines neuen Zertifikats für einen öffentlichen Schlüssel, der bereits zertifiziert wurde, sind bei der **EnergyCA** nicht erlaubt.

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

4.6.3 Bearbeitung von Zertifikatsanträgen für Schlüsselerneuerungen

Es gibt zwei unterschiedliche Arten der Folgeanträge:

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

Folgeanträge über eine automatisierte Schnittstelle (synchroner Betrieb)

Hier wird über eine gesicherte TLS Verbindung (siehe (TR-03116-3)) ein Zertifikatsrequest gemäß (TR-03109-4) an die **EnergyCA** gesendet.

Die **EnergyCA** beantwortet diesen Zertifikatsrequest synchron, so dass die beantragten Zertifikate unmittelbar in der Response enthalten sind. Eine zeitverzögerte Zustellung

(asynchroner Betrieb) der Zertifikate per Webservice wird seitens der **EnergyCA** nicht unterstützt.

Folgeanträge über eine abgesicherte E-Mail Kommunikation

Bei einem Folgeantrag wird der Zertifikatsrequest gemäß (TR-03109-4) vom benannten Ansprechpartner des Zertifikatsnehmers an die **EnergyCA** in einer verschlüsselten und signierten E-Mail gesendet.

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

4.6.4 Benachrichtigung des Zertifikatsnehmers über die Ausgabe eines Nachfolgezertifikats

Der Beantragende wird durch die Zustellung des Nachfolgezertifikats seitens der **EnergyCA** informiert.

Die sonstigen Teilnehmer der **EnergyCA** werden grundsätzlich nicht individuell über die Ausgabe von Zertifikaten zur Schlüsselerneuerung informiert. Eine Benachrichtigung erfolgt nur über die Veröffentlichung im Verzeichnisdienst (siehe Abschnitt 4.6.7).

4.6.5 Verhalten für die Annahme von Zertifikaten für Schlüsselerneuerungen

Bei den GWA/GWH/EMT-Zertifikaten muss der Ansprechpartner des Zertifikatsnehmers nach Erhalt die Angaben im Zertifikat auf Korrektheit und Vollständigkeit prüfen. Um ein Zertifikat zurückzuweisen, schickt der Ansprechpartner des Zertifikatsnehmers eine Nachricht an die **EnergyCA**. In einer solchen Nachricht ist der Grund für die Verweigerung der Annahme anzugeben. Bei fehlerhaften Zertifikaten sind, soweit möglich, die fehlerhaften bzw. unvollständigen Einträge zu benennen.

Bei einem SMGW kann diese Prüfung durch den GWH oder den GWA automatisiert z.B. bei dem Erhalt oder der Einbringung der Zertifikate erfolgen. Die **EnergyCA** stellt eine Kommunikationsschnittstelle für Fehlermeldungen bereit. (vgl Kapitel 4.3 bzw. Tabelle 9)

4.6.6 Veröffentlichung von Zertifikaten für Schlüsselerneuerungen durch die EnergyCA

Alle ausgestellten Zertifikate werden unmittelbar nach der Ausstellung in dem Verzeichnisdienst der **EnergyCA** veröffentlicht.

4.6.7 Benachrichtigung anderer PKI-Teilnehmer über die Ausgabe eines Nachfolgezertifikats

Alle ausgestellten Zertifikate werden direkt nach der Ausstellung in dem Verzeichnisdienst der **EnergyCA** veröffentlicht.

4.7 Änderungen am Zertifikat / der Ansprechpartner

Änderungen an den Zertifikatsinhalten sind nicht vorgesehen. Sollte sich Änderungsbedarf ergeben, z.B. durch eine Umfirmierung eines Zertifikatsnehmers (d.h. die Änderung des Firmennamens oder der Gesellschaftsform), wird ein neues initiales Zertifikat gemäß Abschnitt 3.2 bei der **EnergyCA** beauftragt. Das alte Zertifikat wird seitens der **EnergyCA** umgehend gesperrt.

Änderungen der bei der Registrierung an der **EnergyCA** hinterlegten Ansprechpartner sind der **EnergyCA** zeitnah anzuzeigen. Diese Meldung muss in einer signierten und verschlüsselten E-Mail (S/MIME) an die RA der **EnergyCA** laut Tabelle 7 erfolgen. Diese E-Mail muss das entsprechende ausgefüllte Formular inkl. der Unterschrift der zeichnungsberechtigten Person (Geschäftsführer o. ä. laut HRA) enthalten.

Die RA der **EnergyCA** prüft den Änderungswunsch. Hat sich im Vergleich zur Erstregistrierung die unterschriftsberechtige Person (Geschäftsführer o. ä.) geändert bzw. weicht hiervon ab, ist ein neuer Handelsregisterauszug mit den neuen Angaben vorzulegen. Fehlt diese Anlage, wird der Änderungswunsch abgelehnt und der Antragsteller hierüber informiert.

Das Formular zur Änderung der Ansprechpartner kann im Downloadbereich auf der Webseite laut Kapitel 1.5 bezogen werden.

4.8 Sperrung und Suspendierung von Zertifikaten

Die Initiierung der Sperrung eines Zertifikats kann durch den Zertifikatsnehmer, die **EnergyCA** 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

Die Sperrung der nicht systemrelevanten Zertifikate können vom Zertifikatsnehmer direkt über das „Kunden-Frontend“ der **EnergyCA** umgesetzt werden.

Für die Sperre ist eine erfolgreiche Anmeldung am Frontend mit Kunden (TLS) Zertifikat in der Rolle „Kunde“ Voraussetzung. Dieses Zertifikat stammt nicht aus der SM-PKI. Es wird im Rahmen der Erstregistrierung für den Kunden explizit durch T Security erstellt und über einen sicheren Kanal (S/MIME) an den Kunden übermittelt.

Nach Auswahl des Menüpunktes „Zertifikate sperren“ kann der zuständige Ansprechpartner die Zertifikat laut nachfolgender Tabelle sperren:

Rolle	Eigenes Zertifikat	SMGW Wirkzertifikat	SMGW Gütesiegelzertifikat
GWA	Nicht im Kunden-Frontend möglich.[2]	X	Nicht im Kunden-Frontend möglich.[3]
GWH	X		X
EMT	X		

Tabelle 10: Zertifikats Sperr Matrix der EnergyCA im Kundenfrontend

Alternativ – bzw. für die systemrelevante Sperrung des GWA Zertifikates - ist der Sperrwunsch via S/MIME von einem der registrierten Ansprechpartner über die Kommunikationsschnittstelle der Registration Authority (RA) der **EnergyCA** nach Tabelle 7 möglich.

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

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

Alle Anträge zum zu sperrenden Zertifikat müssen folgende Angaben beinhalten:

- SerialNumber (drei HexWerte des Zertifikatstripel)
- DN
    - Common Name (CN)
    - Organisation O
    - Organisation Unit OU
    - Country C
    - Serial Number
- Zertifikatstyp (GWA/GWH/EMT/SMGW Güte- oder Wirkzertifikat)
- Sperrgrund, insbesondere
    - Änderung an den Zertifikatsdaten
    - Schlüsselkompromittierung

[2] Das GWA Zertifikat unterliegt aufgrund der Systemrelevanz einer Beteiligung der SM-PKI Root CA.

[3] Das Gütesiegelzertifikat ist standardmäßig dem GWH zugeordnet. Eine Sperre ist mit dem entsprechenden Nachweis des GWH über S/MIME oder Telefon möglich. Der Nachweis des Besitzüberganges erfolgt in schriftlicher Form an die RA der **EnergyCA** (s. Kapitel3.5.1)

    - Einstellung des Betriebes
    - Sonstiges
- Sperrzeitpunkt

Die **EnergyCA** prüft die Anträge zur Sperrung auf Inhalt und systemrelevanter Bedeutung und führt diese anschließend im Vier-Augen-Prinzip seitens der RA durch.

Bei einer negativen Prüfung wird der Antragsteller über das Ergebnis der Prüfung per S/MIME informiert.

Eine Sperrung kann nicht zurückgenommen werden. Eine Ausnahme stellt der Spezialfall Suspendierung dar (siehe Abschnitt 4.8.2).

Alle Sperrungen innerhalb der **EnergyCA** werden unverzüglich umgesetzt und in die neue Sperrlisten aufgenommen. 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 der **EnergyCA** müssen gemäß (TR-03109-4) immer die aktuelle Sperrliste verwenden. In besonderen Fällen (Erstinbetriebnahme oder auf Aufforderung einer CA-Instanz) müssen neben den regelmäßigen Aktualisierungen die Sperrlisten auch anlassbezogen abgefragt werden.

4.8.2 Sperrung und Suspendierung von SMGW Zertifikaten

Bei SMGW-Wirkzertifikaten (nicht jedoch bei SMGW-Gütesiegelzertifikaten) kann alternativ zu einer Sperrung auch eine Suspendierung 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 vorübergehend wieder zurückgenommen werden, um neue Zertifikate zu erhalten und somit wieder in den Wirkbetrieb aufgenommen zu werden.

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

Initiiert der Zertifikatsnehmer eine Suspendierung, so muss er dies an einen Ansprechpartner der **EnergyCA** mittels signierter E-Mail als Sicherheitsvorfall melden (siehe auch Kapitel 5.2.10). Hierbei muss der Grund für die Suspendierung genannt werden. Die **EnergyCA** dokumentiert diese Begründung. Dies gilt auch für Suspendierungen, welche über die Webservice-Schnittstelle in Auftrag gegeben wurden. Wird seitens des Zertifikatsnehmers der Grund für die Suspendierung des SMGW-Wirkzertifikates nicht innerhalb von 7 Kalendertagen an die **EnergyCA** übermittelt, wird dieser an seine Informationspflicht gegenüber der **EnergyCA** informiert. Sollte ab dem Zeitpunkt der Erinnerung innerhalb von 3 Arbeitstagen keine Begründung für die Suspendierung via S/MIME eingehen, wird dieser Umstand als Sicherheitsvorfall an die SM-PKI Root nach Kapitel 5.2.10 kommuniziert.

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

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

Im Positivfall (SMGW ist weiterhin vertrauenswürdig) KANN der GWA innerhalb der in Kapitel 4.8.2.1 definierten Frist die Suspendierung zurücknehmen, um anschließend mittels Zertifikatsrequest neue Zertifikate für das SMGW beantragen zu können. Dabei werden die suspendierten Zertifikate für die Neubeantragung temporär von der Sperrliste entfernt. Die Rücknahme der Suspendierung erfolgt, ebenso wie die Suspendierung, durch den GWA über die von der **EnergyCA** angebotene Schnittstelle (Webservice, alternativ durch per S/MIME verschlüsselte und signierte E-Mail). Anschließend MUSS der GWA sicherstellen, dass die -vorübergehend wieder gültigen- SMGW-Zertifikate ausschließlich für die Neubeantragung verwendet werden. Sobald die neuen Zertifikate auf dem SMGW installiert sind, MUSS der GWA die alten Zertifikate endgültig sperren lassen, so dass diese wieder in die Sperrliste eingetragen werden.

Die **EnergyCA** prüft in diesem Fall

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

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

Dieser Zusatzschritt wird bei den SMGW vorgenommen, um ggf. einen zum Zeitpunkt des Auftretens nicht nachweisbaren Verdacht des Verlusts der Vertrauenswürdigkeit des SMGW-Zertifikats innerhalb eines angemessenen Zeitraums untersuchen zu können.

Suspendierte Zertifikate MÜSSEN von allen Teilnehmern der **EnergyCA** als gesperrte Zertifikate behandelt werden.

4.8.2.1 Maximale Dauer einer Suspendierung

Die maximale Dauer einer Suspendierung beträgt 30 Tage.

Unabhängig von der Klärung der Vertrauenswürdigkeit des SMGW durch den GWA, unabhängig von einer eventuellen Rücknahme der Suspendierung und unabhängig von der Beantragung neuer SMGW-Zertifikate wird die **EnergyCA** einmal suspendierte SMGW-Zertifikate nach Ablauf dieses Zeitraums endgültig sperren, sofern der GWA dies nicht zwischenzeitlich selbst veranlasst hat (Kennzeichnung in der Sperrliste als „suspendiert“ entfällt).

Wurde ein SMGW, dessen Zertifikate suspendiert worden sind, bis zum Fristablauf nicht mit neuen Zertifikaten versorgt, so dürfen keine neuen Zertifikate für dieses SMGW mehr ausgestellt werden.

4.8.3 Aktualisierungs- und Prüfzeiten bei Sperrung

In der folgenden Tabelle sind die minimal erforderlichen Aktualisierungs- und Prüfungszeiten der Sperrlisten für die einzelnen **EnergyCA** 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 **EnergyCA** wie in Tabelle 11 definiert erreichbar ist.

Nach Eintreffen eines Antrags für eine Sperrung wird dieser von der **EnergyCA** unverzüglich geprüft. Ist der Antrag valide wird dieser zeitlich, wie in Tabelle 11 definiert, umgesetzt.

Die Gültigkeit einer Sperrliste darf max. 3 Tage länger sein, als das in Tabelle 11 definierte Aktualisierungsintervall.

Sollte eine Sperrliste nicht verfügbar bzw. abrufbar sein, wird ersatzweise mit der zuletzt bekannten Sperrliste weitergeprüft. Die **EnergyCA** wird hierüber unverzüglich informiert (über Kontaktadresse laut Tabelle 7). Diese stellt dann auf anderem Wege eine aktuelle Sperrliste zur Verfügung. Steht nach 3 Tagen immer noch keine aktualisierte Sperrliste zur Verfügung, wird die Root-CA informiert.

PKI-Teilnehmer	**Regelmäßige Aktualisierung der Sperrliste**	**Erreichbarkeit für Sperrungen**	**Anlassbezogene Aktualisierung der Sperrliste**	**Abruf der Sperrliste**	**Prüfung der Zertifikate auf Sperrung**
EnergyCA	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 11: Zeitliche Anforderungen bei Sperrungen

4.9 Service zur Statusabfrage von Zertifikaten

Für die **EnergyCA** ist kein OCSP-Dienst vorgesehen. Statusabfragen hinsichtlich einer Sperrung können über die entsprechende CRL erfolgen (siehe (TR-03109-4)).

4.10 Beendigung der Teilnahme

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

Die Beendigung gliedert sich in drei Schritte:

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

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

4.11 Hinterlegung und Wiederherstellung von Schlüsseln

EnergyCA Teilnehmer können eine Schlüsselhinterlegung (z.B. für die Katastrophenfallvorsorge) gemäß den definierten Sicherheitsanforderungen durchführen. Der Prozess für die **EnergyCA** ist in der Betriebsdokumentation beschrieben.

5 Organisatorische, betriebliche und physikalische Sicherheitsanforderungen

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

Die Teilnehmer GWA/GWH und EMT müssen die Ziel- und Sicherheitsvorgaben aus der (CP-SM-PKI) beachten. Die Sicherheitsanforderungen an diese Rollen sind im Folgenden nicht betrachtet.

5.1 Generelle Sicherheitsanforderungen

In diesem Abschnitt werden generelle Sicherheitsanforderungen an die **EnergyCA** definiert. Diese bauen auf den Vorgaben der SM PKI auf und ergänzen diese gegebenenfalls.

T Security besitzt eine gültige ISO27001-Zertifizierung und erfüllt die aufgelisteten Sicherheitsanforderungen.

T Security als Betreiber der **EnergyCA** hat zusätzlich eine Zertifizierung nach ISO 27001 auf Basis von IT-Grundschutz. Diese ISO27001-Zertifizierung umfasst alle Geschäftsprozesse und IT-Systeme des Registrierungs- und Zertifizierungsbetriebs der **EnergyCA**. Es wurde hierbei von einem hohen Schutzbedarf ausgegangen.

5.1.1 Erforderliche Zertifizierungen der PKI-Teilnehmer

EnergyCA: Die Zertifizierung nach (ISO/IEC 27001) auf Basis IT-Grundschutz sowie eine Zertifizierung nach (TR-03145) ist vorhanden und wurde nachgewiesen.

GWA: Ein GWA muss alle Anforderungen gemäß (TR-03109-6) erfüllen und das entsprechende Zertifikat nachgewiesen.

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.

EMT: Ein passiver EMT erstellt ein Sicherheitskonzept, in dem die Anforderungen aus der **EnergyCA** -Policy berücksichtigt wurden. Gegenüber der **EnergyCA** bestätigt der EMT dieses im Rahmen des Registrierungsprozesses. Ein aktiver EMT (vgl. Abschnitt 1.3.3.4) hat eine ISO/IEC 27001-Zertifizierung vorgelegt bzw. nachgewiesen, dass ein nach ISO/IEC 27001 zertifizierter Dritter die Leistung für ihn erbringt.

Möchte ein passiver EMT nachträglich auch die Aufgaben eines aktiven EMTs wahrnehmen oder möchte ein aktiver EMT nur noch als passiver EMT auftreten, so muss das

Unternehmen dies der **EnergyCA** rechtzeitig und eigenverantwortlich mitteilen und die entsprechenden Prozesse (s. Kapitel 3.2.2.1) durchlaufen werden.

- Die Aufgaben des aktiven EMT dürfen erst vom Antragsteller mit dem bestehenden Zertifikat ausgeübt werden, wenn die erfolgreiche Registrierung als aktiver EMT von der **EnergyCA** bestätigt wurde. Die Bestätigung erfolgt per signierter E-Mail an den registrierten Ansprechpartner.
- Die zusätzlichen Auflagen für den Betrieb des aktiven EMT fallen erst weg, wenn der Rollenwechsel von der **EnergyCA** bestätigt wurde. Die Bestätigung erfolgt per signierter E-Mail an den registrierten Ansprechpartner.

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

Die Zertifizierung gemäß (ISO/IEC 27001) auf Basis IT-Grundschutz umfasst bei der **EnergyCA** alle Geschäftsprozesse und IT-Systeme des Registrierungs- und Zertifizierungsbetriebs der betreffenden PKI-Infrastruktur. Hierbei wird von einem hohen Schutzbedarf ausgegangen.

Bei einem aktiven EMT muss eine entsprechende 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) auf Basis IT-Grundschutz die Überprüfung beinhalten, dass alle Anforderungen aus der (TR-03109-4) und aus der (CP-SM-PKI) eingehalten werden. Das Ergebnis wird im Auditbericht dokumentiert werden, damit es bei Bedarf vorgelegt werden kann.

Fach- oder Administrationsprozesse, die per Remote-Management realisiert sind, werden per 2-Faktor-Authentisierung abgesichert. Das Remote-Management wird im Sicherheitskonzept behandelt und wurde als Bestandteil der Zertifizierung gemäß (ISO/IEC 27001) überprüft. Zugehörige WAN-Verbindungen sind vom Sicherheitsniveau vergleichbar mit den WAN-Verbindungen gemäß (TR-03109-6).

Bei den Systemen der **Energy Test CA** (siehe Abschnitt 1.3.1) ist keine Zertifizierung entsprechend (ISO/IEC 27001) erforderlich (siehe (CP-SM-PKI) Anhang C.1).

5.2 Erweiterte Sicherheitsanforderungen

5.2.1 Betriebsumgebung und Betriebsabläufe

Nachfolgend werden die Umsetzungen der Anforderungen an eine sichere Betriebsumgebung und an sichere Betriebsabläufe für **EnergyCA** definiert. Entsprechende Anforderungen an den GWA sind in (TR-03109-6) spezifiziert.

- **Objektschutz:** Die betrieblichen Prozesse werden vor Störung geschützt.

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

Die **EnergyCA** erfüllt weiterhin folgende Anforderungen:

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

5.2.2 Verfahrensanweisungen

Für den Betrieb der **EnergyCA** wurden folgende Verfahrensanweisungen umgesetzt:

- **Einhaltung von Verpflichtungen:** Basierend auf den verschiedenen Aufgaben halten die Mitarbeiter die Pflichten entsprechend ihren Rollen bei ihren Tätigkeiten ein.
- **Vertreterreglung:** Für jede definierte Rolle wurde ein Vertreter ernannt.
- **Verantwortungsbereiche:** Die Verantwortungsbereiche der Mitarbeiter wurden klar definiert. Für die Verantwortungsbereiche sind klare Rollen definiert.
- **Vier-Augen-Prinzip:** Kritische Vorgänge erfolgen nach dem Vier-Augen-Prinzip (siehe Definition in der (CP-SM-PKI) Anhang C). Zudem wird das Vier-Augen-Prinzip an jeder möglichen Stelle technisch umgesetzt. Es wird immer dokumentiert, welche Personen einen kritischen Vorgang durchgeführt haben.
- **Beschränkung der Anzahl Mitarbeiter:** Die Anzahl der Personen, die sicherheitsrelevante oder kritische Funktionen durchführen, ist auf die unbedingt notwendige Anzahl begrenzt.
- **Eskalationsmanagement:** Es wurde ein gut definiertes und eindeutiges Eskalationsmanagement umgesetzt.

5.2.3 Personal

Der Betrieb der **EnergyCA** wird durch angemessen geschultes und erfahrenes Personal erfolgen. Insbesondere sind folgende Anforderungen erfüllt:

- **Rollen und Verantwortungen:** Die Rollen und Verantwortlichkeiten sind gemäß (TR-03145) für den sicheren CA-Betrieb umgesetzt. In Bezug auf kritische Aufgaben/Funktionen bezüglich des Schlüssel- und Zertifikatsmanagement-Lebenszyklus wurden die Verantwortlichkeiten klar definiert und für den Betrieb der **EnergyCA** als Trust-Center Lösung festgelegt.
- **Rollenbeschreibungen:** Für temporäres und permanentes Personal wurden Rollenbeschreibungen definiert, welche Aufgabentrennung, Mindestberechtigungen, Sicherheitsprüfungen, Verpflichtung zu Mitarbeiter- und Sensibilisierungsschulungen enthalten.
- **Einhaltung der ISMS-Anforderungen:** Das Personal führt administrative und betriebliche Verfahren und Prozesse im Einklang mit dem Standard (ISO/IEC 27001) durch.

Für den Betrieb der **EnergyCA** gilt darüber hinaus:

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

5.2.4 Monitoring

Folgende Ereignisse werden erkannt und aufgezeichnet bzw. dokumentiert:

EnergyCA:

- Die aus der (ISO/IEC 27001) für den Betrieb, Prozesse und Infrastruktur relevanten Kontrollen
- Schlüsselmanagement (siehe Definition in (CP-SM-PKI)Anhang C) auf dem Kryptografiemodul
- Nutzung des privaten Schlüssels der **EnergyCA**, 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 sind in der Zertifizierung nach (ISO/IEC 27001) nachgewiesen worden (siehe (CP-SM-PKI) Anhang B).
- Es wurde sichergestellt, dass unautorisierter oder unbeabsichtigter Gebrauch von PKI-relevanten Systemen erkannt wird.
- Regelmäßige Prüfung der Überwachungsmaßnahmen durch externe Auditoren.
- Remote-Anbindung über WAN
    - Mehrfach ungültige Login-Versuche über die WAN-Schnittstelle

5.2.5 Archivierung von Aufzeichnungen

Die Systeme der **EnergyCA** verfügen über angemessene Archivierungsfunktionen. Die Zeiträume werden analog zu Anhang B der (CP-SM-PKI) umgesetzt. Details zur Archivierung ist der Betriebsdokumentation der **EnergyCA** zu entnehmen. Folgende Anforderungen werden berücksichtigt:

EnergyCA:

- Archivierung der öffentlichen Schlüssel: Die **EnergyCA** stellt sicher, dass die relevanten Informationen zu den öffentlichen Schlüsseln des Zertifikates archiviert werden.
- Eindeutige Zuordnung von Zertifikaten: Die Beteiligten der **EnergyCA** sind in der Lage, die jeweiligen Zertifikate eindeutig den registrierten Benutzern zuzuordnen.
- Verfügbarkeit: Mit Hilfe einer angemessenen Archivierung klar definierter Daten der verbreiteten öffentlichen Zertifikatsschlüssel wird nach einer vollständigen Wiederherstellung die Verfügbarkeit der Dienste gewährleistet.
- Datenbanken: Die Aktualität, Integrität und Vertraulichkeit der Datenbanken der **EnergyCA** sind gewährleistet, 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, sind klar definiert.
- Die zu archivierenden Informationen für öffentliche Schlüssel enthalten:
    - Registrierungsinformationen
    - Essentielle CA-Ereignisse (z.B. Generierung von Zertifikaten)
    - Schlüsselverwaltung
    - Zertifizierungsereignisse
- Für jedes Ereignis wird der Zeitpunkt der Archivierung präzise festgelegt.

Die wesentlichen Ereignisse, die archiviert werden, umfassen insbesondere:

- Zertifikatserstellung
- Erneuerung und Aktualisierung der öffentlichen Zertifikats-Schlüssel
- Incident- oder Notfall-Management bezüglich Zertifikats-relevanter Vorfälle.

5.2.6 Schlüsselwechsel

Der Schlüsselwechsel der **EnergyCA** kann einerseits geplant und andererseits ungeplant erfolgen:

- *Geplanter Schlüsselwechsel***:** Im Fall eines planbaren Schlüsselwechsels werden die Verfahren gemäß der (CP-SM-PKI) berücksichtigt und entsprechend der vorhandenen Prozesse abgearbeitet. Eine Information über den geplanten Wechsel erfolgt via E-Mail an die registrierten Ansprechpartner und auf der Webseite.

- *Ungeplanter Schlüsselwechsel:* Für den Fall, dass ein unvorhergesehener Schlüsselwechsel notwendig ist, sind entsprechende Verfahren im Notfallmanagement definiert.

Sowohl ein geplanter als auch ein ungeplanter Schlüsselwechsel der **EnergyCA** erfolgt gemäß dem **Vier-Augen-Prinzip.**

5.2.7 Auflösen der Zertifizierungsstelle

Wenn die **EnergyCA** aufgelöst wird, werden alle von ihr ausgestellten Zertifikate gesperrt. Folgende Anforderungen werden dabei erfüllt

- Abstimmung über die geplante Auflösung der **EnergyCA** mit der SM-PKI Root.
- *Übertragung der Aufgaben und Verpflichtungen***:** Im Falle der Auflösung der **EnergyCA** werden deren Aufgaben und Verpflichtungen für eine Übergangszeit aufrechterhalten oder bei einer endgültigen Auflösung von einer Nachfolgeorganisation übernommen. Dies umfasst die Bereitstellung des Sperrdienstes und von Sperrinformationen für die Restlaufzeit der ausgegebenen Zertifikate.
- *Informationspflicht:* die **EnergyCA** wird 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 werden alle privaten Schlüssel einschließlich Zertifikatsinformationen und zugehörige Kundendaten zerstört.

5.2.8 Aufbewahrung der privaten Schlüssel

Folgende Anforderungen an die private Schlüsselaufbewahrung werden umgesetzt:

- *Kryptografiemodule*: Die Schlüssel werden in vertrauenswürdigen Kryptografiemodulen gespeichert (siehe Abschnitt 6.2). Im Backup-Konzept ist hinterlegt, dass die privaten Schlüssel der **EnergyCA** außerhalb des Sicherheitsmodules mit dem gleichen Schutzniveau, wie bei der Schlüsselerstellung aufbewahrt werden.

Die **EnergyCA** stellt sicher, dass folgende Anforderungen umgesetzt werden.

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

- *Gehärtete IT-Systeme*: Es ist sichergestellt, dass die Anforderungen an gehärtete IT-Systeme und -Netzwerke sowie an die physische Sicherheit eingehalten werden. Die Basis für umgesetzte Maßnahmen ist ESARIS.

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 werden und darf nicht wiederverwendet werden. Bei systemkritischen Zertifikaten ist die SM-Root zu beteiligen.
- Ein Fall von Kompromittierung sowie Verdachtsfälle müssen durch den Schlüsselinhaber dokumentiert werden.
- Jeder Verdacht auf Kompromittierung oder Missbrauch des privaten Schlüssels muss aufgeklärt werden.
- Die Generierung neuer Schlüssel und Zertifikate muss überwacht und dokumentiert.

5.2.10 Meldepflichten

Bei Kompromittierung oder anderweitigen sicherheitsrelevanten Vorfällen muss eine Meldung aufbereitet und an die **EnergyCA** kommuniziert. Die Meldepflicht obliegt dem Zertifikatsnehmer. Bei der Kompromittierung eines GWA oder GWH muss zusätzlich die SM-PKI Root durch die **EnergyCA** informiert werden.

Folgende Vorkommnisse sind Beispiele für eine Meldepflicht:

- Kompromittierung des privaten Schlüsselmaterials
- Verstoß gegen relevante Betriebsauflagen
- 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?

Ein EMT der **EnergyCA** 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 **EnergyCA** gewährleistet, 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

Details zur Umsetzung sind in der Betriebsdokumentation zur **EnergyCA** und in der TrustCenter Notfall-Management Dokumentation beschrieben.

Insbesondere gelten folgende Anforderungen, welche erfüllt werden:

- *Notfallmanagement***:** Die **EnergyCA** reagiert rechtzeitig angemessen auf Störungen oder Notfälle, um Schäden zu minimieren und den Geschäftsbetrieb zu gewährleisten.
- *Maßnahmenplanung:* Die **EnergyCA** ist mit angemessenen Maßnahmen für den Fall vorzubereiten, 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 **EnergyCA**-Teilnehmer sollten entsprechende Maßnahmen zur Minimierung von Risiken und Schäden anwenden.
- *Vermeidung von Vorfällen:* Alle **EnergyCA**-Teilnehmer müssen angemessene Maßnahmen vorbereiten sowie die Ursachen von Vorfällen ermitteln, um diese in Zukunft zu vermeiden.
- *Notfallpläne:* Die **EnergyCA** hat entsprechende Pläne vorbereitet, um die Geschäftsprozesse nach einem Notfall wiederherzustellen.
- *Backups:* Die **EnergyCA** führt Backups von privaten und öffentlichen Schlüsseln, ausgestellten Zertifikaten und Sperrinformationen durch.
- *Vorgehen nach einer Störung***:** Nach einer schweren Störung stellen alle **EnergyCA**-Teilnehmer sicher, dass die entstandene Sicherheitslücke geschlossen werden.

6 Technische Sicherheitsanforderungen

6.1 Erzeugung und Installation von Schlüsselpaaren

Jeder Zertifikatsnehmer muss individuelles Schlüsselmaterial generieren. Eine Mehrfachverwendung ist nicht gestattet.

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 **EnergyCA** und die teilnehmenden EMT, GWA und GWH stellen sicher, dass folgende Anforderungen umgesetzt werden:

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

6.1.2 Lieferung privater Schlüssel

Die Erstellung der privaten Schlüssel erfolgt dezentral durch die Zertifikatsnehmer der **EnergyCA**. Daher erfolgt keine Lieferung der privaten Schlüssel.

6.1.3 Lieferung öffentlicher Zertifikate

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

6.1.4 Schlüssellängen und kryptografische Algorithmen

Bezüglich Schlüssellängen und kryptografischer Algorithmen werden angemessene kryptografische Verfahren verwendet. Die zum jeweiligen Zeitpunkt konkret zu verwendenden kryptografischen Algorithmen und Schlüssellängen werden der (TR-03116-3) entnommen.

Bei der Erzeugung und Nutzung von statischen und temporären Schlüsseln innerhalb der **EnergyCA** wird ein Zufallsgenerator verwendet, der konform zu den Anforderungen aus (TR-03116-3) ist. Des Weiteren wird bei statischen Schlüsseln ein Kryptografiemodul gemäß Abschnitt 6.2 eingesetzt.

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 halten angemessene Maßnahmen zur sicheren Handhabung und Lagerung von Schlüsselmaterial ein.
- *Defektes Krypto-Modul (KM):* Im Falle eines defekten KM ist sichergestellt, 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 ist sichergestellt, 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 ist sichergestellt, dass der private Schlüssel nicht unverschlüsselt oder unberechtigt aus dem Schlüsselspeicher exportiert werden kann. Es werden angemessene Maßnahmen zur sicheren Handhabung und Lagerung von Schlüsselmaterial eingehalten. Die zum jeweiligen Zeitpunkt konkret zu verwendenden kryptografischen Algorithmen und Schlüssellängen entsprechen den jeweils aktuellen Empfehlungen aus (TR-02102-1).
- 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 **EnergyCA** Policy. Die verwendeten Testschlüssel werden ausschließlich für den Testbetrieb erzeugt und werden nicht im Wirkbetrieb des SM-PKI Umfeldes eingesetzt.

6.1.6 Verwendungszweck der Schlüssel

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

6.2 Sicherung des privaten Schlüssels und Anforderungen an kryptografische Module

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

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

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

6.2.1 Mehrpersonen-Zugriffssicherung zu privaten Schlüsseln

Das Schlüsselmanagement bei **EnergyCA** wird im Vier-Augen-Prinzip, unter entsprechender Dokumentation und Protokollierung insbesondere der Rollen und eindeutiger Identifikation der teilnehmenden Personen, durchgeführt.

6.2.2 Ablage privater Schlüssel

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

6.2.3 Backup privater Schlüssel

Die **EnergyCA** stellt sicher, dass Maßnahmen zum sicheren Backup der eigenen privaten Schlüssel umgesetzt werden. Insbesondere werden folgende Anforderungen eingehalten:

Die Vorgaben aus Kapitel 6.2.5 *Transfer* privater Schlüssel in oder aus kryptografischen Modulen werden eingehalten.

Bestandteil des ISMS nach ISO 27001: Die technischen Maßnahmen zum Backup privater Schlüssel wurden in der Auditierung nach (ISO/IEC 27001) berücksichtigt.

Sichere Schlüssel-Backups: Die Durchführung von sicheren Backups der privaten Schlüssel sind nach den Vorgaben zur sicheren Handhabung und Lagerung von Schlüsselmaterial durchgeführt.

Durchführung des Schlüssel-Backups: Das Schlüssel-Backup wird während der Schlüsselzeremonie gemäß dem Vier-Augen-Prinzip unter Teilnahme des für den Schlüssel

verantwortlichen Mitarbeiters durchgeführt. Automatisierte Prozesse zur Übertragung der Schlüssel auf ein weiteres HSM (z.B. für ein Cold-Standby-Backup) werden genutzt.

Schlüsselspeicherung: Es wird sichergestellt, dass die Backup-Daten des öffentlichen Schlüssels nach den Vorgaben zur sicheren Handhabung und Lagerung von Schlüsselmaterial gespeichert werden.

Zugriff auf Backup-Daten: Es ist sichergestellt, dass nur vertrauenswürdige Mitarbeiter Zugriff auf die Schlüsselspeicher- und Backup-Daten haben.

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 ist auf das Betriebspersonal beschränkt.
  - Die Wiederherstellung des Dateicontainers ist technisch ausschließlich im Vier-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 ist auf das Betriebspersonal beschränkt.

6.2.4 Archivierung privater Schlüssel

Bei der **EnergyCA** erfolgt keine Archivierung gesperrter oder abgelaufener privater Schlüssel. Diese privaten Schlüssel werden unter Beachtung der Einschränkungen aus Kapitel 6.2.9 zerstört.

6.2.5 Transfer privater Schlüssel in oder aus kryptografischen Modulen

Der private Schlüssel KANN zwischen kryptografischen Modulen transferiert werden.

- Es werden nur Kryptografiemodule verwendet werden, welche die Anforderungen aus Abschnitt 6.2 erfüllen.
- Der private Schlüssel wird hierbei verschlüsselt und integritätsgesichert transferiert. Die Ver-/Entschlüsselung erfolgt in den Kryptografiemodulen.
- Der KEK zur Ver-/Entschlüsselung des privaten Schlüssels wird vertraulich und integritätsgesichert ausgetauscht.
- Bei der Durchführung eines manuellen Transfers wird das Vier-Augen-Prinzip eingehalten.

6.2.6 Speicherung privater Schlüssel in kryptografischen Modulen

- Grundsätzlich werden die privaten Schlüssel der **EnergyCA** auf einem Kryptografiemodul gespeichert.
    - Die einzige Ausnahme bilden die client- und serverseitigen TLS-Schlüssel der **EnergyCA**, die zur TLS-Authentisierung an der Web-Service-Schnittelle (siehe (TR-03116-3) und am Verzeichnisdienst verwendet werden.
- Die privaten Schlüssel der **EnergyCA** - Testumgebung werden von der Produktivumgebung getrennt.

6.2.7 Aktivierung privater Schlüssel

Die Aktivierung eines Schlüssels in einem Kryptografiemodul erfolgt nach dem Vier-Augen-Prinzip.

6.2.8 Deaktivierung privater Schlüssel

Im deaktivierten Zustand der Schlüssel ist technisch sichergestellt, dass diese nicht mehr genutzt werden können.

6.2.9 Zerstörung privater Schlüssel

Die privaten Schlüssel der **EnergyCA** werden in folgenden Fällen sicher und unwiederherstellbar zerstört:

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

Die Backups der Schlüssel werden ebenfalls berücksichtigt.

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

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

6.2.10 Beurteilung kryptografischer Module

Geltungsbereich: Alle PKI-Teilnehmer (Ausnahme SMGW)

Innerhalb der **EnergyCA** werden verschiedene Produktklassen von Kryptografiemodulen eingesetzt, z.B. Hardware-Sicherheitsmodule (HSM), Chipkarten und Secure Elements (vgl. Kategorien der Schutzprofile in (KeyLifeSec)).

Die SMGWs bzw. der Betrieb von SMGWs ist von den Anforderungen aus (KeyLifeSec) ausgenommen.

Sicherheitsanforderungen

Um ein Kryptografiemodul in der **EnergyCA** einsetzen zu können, wird dieses konform zu den Anforderungen an Kryptografiemodule aus (KeyLifeSec) – Security Level 2 [4] sein. Ergänzend zu (KeyLifeSec) kann für GWA, GWH und EMT auch ein Kryptografiemodul eingesetzt werden, das nach (BSI-CC-PP-0095) zertifiziert ist.

Hinsichtlich der Anforderungen an den Zufallsgenerator des Kryptografiemodules gelten die Anforderung aus (TR-03116-3).

Diese Anforderungen werden im Wirkbetrieb umgesetzt.

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 werden die Anforderungen aus der (CP-SM-PKI) speziell hinsichtlich des Key-Lifecycle im ISMS berücksichtigt.

[4] 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	EnergyCA
Anforderung an die Betriebsumgebung	Siehe Tabelle 16	Siehe Tabelle 16	Siehe Tabelle 16	Siehe Tabelle 16	Siehe Tabelle 16
Nachweise	Erforderlichkeit				
Sicher Zufallszahlengenerator gemäß (TR-03116-3)	MUSS	MUSS	MUSS	MUSS	MUSS
Tamper-Schutz gegen Attack Potential "moderate"	SOLLTE	SOLLTE	SOLLTE	SOLLTE	SOLLTE
Seitenkanalresistenz gegen Attack Potential "moderate"	SOLLTE	SOLLTE	SOLLTE	SOLLTE	SOLLTE

Tabelle 12: Übergangsregelungen Anforderungen HSM (zertifizierte und nicht Einsatzumgebung)

Nicht Zertifizierte Einsatzumgebung					
	EMT Pa_{ssiv}	EMT aktiv	GWH	GWA	EnergyCA
Nachweise	Erforderlichkeit				
Sicher Zufallszahlengenerator gemäß (TR-03116-3) Prüfanforderungen (AIS 20) und (AIS 31)	MUSS	*Entfällt*	*Entfällt*	*Entfällt*	*Entfällt*
Tamper-Schutz gegen Attack Potential "moderate"	MUSS	*Entfällt*	*Entfällt*	*Entfällt*	*Entfällt*
Seitenkanalresistenz gegen Attack Potential "moderate"	MUSS	*Entfällt*	*Entfällt*	*Entfällt*	*Entfällt*

Tabelle 13: Übergangsregelungen Anforderungen HSM (nicht zertifizierte Einsatzumgebung)

Die in der Tabelle dargestellten Nachweise für eine Übergangslösung wurden jeweils durch eine durch das BSI für Common Criteria-Evaluierungen anerkannte Prüfstelle erbracht. Die Prüfstelle hat in den letzten 5 Jahren mindestens die Prüfung eines Zufallszahlengenerators gemäß [AIS 20]/[AIS 31] im Rahmen eines CC-Zertifizierungsverfahrens erfolgreich abgeschlossen. 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.

Die **EnergyCA** besitzt für seine Kryptografiemodule 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 wurde durch den Auditor bei dem Audit der Einsatzumgebung geprüft, sofern eine Auditierung der Einsatzumgebung erforderlich war (siehe Siehe Tabelle 16).

6.3 Andere Aspekte des Managements von Schlüsselpaaren

6.3.1 Archivierung öffentlicher Schlüssel

Die Zertifikate eines Teilnehmers der **EnergyCA** werden inklusive der Statusdaten archiviert.

6.3.2 Gültigkeitszeitraum von Zertifikaten und Schlüsselpaaren

Der Gültigkeitszeitraum von Zertifikaten und Schlüsseln wird in (TR-03109-4) definiert.

Unabhängig vom Gültigkeitszeitraum werden die folgenden Zertifikate spätestens in dem hierzu angegebenen Intervall gewechselt.

Instanz	Zertifikat	Intervall
Sub-CA	C(EnergyCA)	Alle 2 Jahre

Tabelle 14: Intervall Zertifikatswechsel bei der EnergyCA

Sobald die **EnergyCA** über ein neues Zertifikat verfügt, wird dieses zum Ausstellen neuer Zertifikate und der zugehörigen Sperrlisten verwendet.

6.4 Aktivierungsdaten

Die Aktivierungsdaten für die Kryptografiemodule werden sicher aufbewahrt.

6.5 Sicherheitsanforderungen für die Rechneranlagen

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

EnergyCA**: Netzwerkkontrolle:** Es werden entsprechende Maßnahmen umgesetzt, um das interne Netzwerk vom externen zu trennen und vor unbefugtem Zugriff zu schützen.

EnergyCA**: Intrusion Detection Systeme (IDS):** Der Einsatz von Intrusion-Detection-Systemen (IDS) im gesicherten Netzsegment werden berücksichtigt. Die Log-Dateien des IDS werden regelmäßig kontrolliert.

***EnergyCA**: System-Härtung:* Die CA-Server, die zur Erstellung von Zertifikaten verwendet werden, wurden gehärtet. Dies umfasst die Konfiguration und Einstellung der verwendeten Hardware- und Software-Komponenten.

EnergyCA**: System-Konfiguration:** Die Konfigurationsoptionen und -einstellungen enthalten nur die minimal benötigten Funktionalitäten für den CA Betrieb.

***EnergyCA**: Netzwerk-Separierung:* Die Netzwerke, in denen sich die CA-Server befinden, werden durch geeignete Maßnahmen geschützt.

Alle PKI-Teilnehmer: Software-Updates: Software-Updates werden bei sicherheitsrelevanten Änderungen schnellstmöglich eingespielt werden, andere Updates werden regelmäßig aktualisiert werden.

EnergyCA: Vertraulichkeit und Integrität: Die CA schützt sensitive Daten vor unbefugtem Zugriff oder Veränderung.

EnergyCA: Logging und Audit-Trails: Log-Dateien und Audit-Trails werden regelmäßig geprüft, und automatisierte Benachrichtigungen weisen auf Abweichung vom vorgesehenen Betrieb hin.

***EnergyCA**:* Speicherort von Log-Dateien: Die Dateien der Audit-Trails werden nicht auf dem CA-Server, der für die Verwaltung von Zertifikaten verwendet wird, gespeichert. Der Speicherort für Log-Dateien KANN temporär der CA-Server sein. Die Log-Dateien werden dann regelmäßig auf einen anderen Speicherort ausgelagert.

Details sind der Betriebsdokumentation zu entnehmen.

Alle PKI-Teilnehmer: Das System verfügt über eine angemessene Benutzerverwaltung.

***EnergyCA**: Systemfunktionen:* Die CA begrenzt den Zugriff auf die benötigten Systemfunktionen und Hilfsprogramme.

*Alle **EnergyCA**-Teilnehmer:* Schutz vor Schadsoftware: Die Integrität der System-Komponenten und Informationen müssen 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

Es gibt keine Anforderungen an Zeitstempel.

6.7 Validierungsmodell

Die Anforderungen an die Zertifikatsvalidierung, wie in der (TR-03109-4) spezifiziert werden seitens der **EnergyCA** erfüllt.

7 Profile für Zertifikate und Sperrlisten

7.1 Profile für Zertifikate und Zertifikatsrequests

Die Profile für Zertifikate und die Zertifizierungsrequests sind entsprechend der Vorgaben aus der (TR-03109-4) angelegt und umgesetzt.

Das Namensschema zu den Zertifikaten ist laut Anhang A der (CP-SM-PKI) angelegt und umgesetzt.

Die Struktur der Sperrlisten, das Sperrmanagement (Veröffentlichung, Aktualisierung und Sperrlistenvalidierung) werde nach der jeweils aktuellen Fassung der (TR-03109-4) angelegt und umgesetzt.

7.1.1 Zugriffsrechte

Die erlaubte Funktion der Zertifikate wird über die Key-Usage-Extension definiert (siehe (TR-03109-4)) und in der **EnergyCA** analog umgesetzt.

7.1.2 Zertifikatserweiterung

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

7.2 Profil für Sperrlisten

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

7.3 Profil für OCSP Dienste

In der **EnergyCA** werden keine OCSP Dienste eingesetzt.

8 Überprüfung und andere Bewertungen

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

8.1 Inhalte, Häufigkeit und Methodik

8.1.1 Testbetrieb

Die **EnergyCA** stellt eine Testumgebung zur Verfügung, welche die Antragsteller der **EnergyCA** zum Test der Funktionalitäten ihrer PKI-Infrastruktur und -Prozesse durchlaufen müssen, bevor diese Teilnehmer der **EnergyCA** werden (s. Kapitel 3.2)

Testumgebung bereitgestellt durch	**Nutzer**	**Zweck**	**Ergebnis**
EnergyCA	GWA	Nachweis der vollständigen und korrekten Funktion der Zertifikatsantragsstellung und Zertifikatsannahme sowie von Sperrungen. Basis: Web-Service-Schnittstelle	Nach erfolgreichem Abschluss der Tests erfolgt die Bestätigung der erfolgreichen bestandenen Tests durch einen Prüfer der EnergyCA per signierter E-Mail.
	GWH	Nachweis der vollständigen und korrekten Funktion der Zertifikatsantragsstellung und Zertifikatsannahme sowie von Sperrungen. Basis: Web-Service-Schnittstelle	Nach erfolgreichem Abschluss der Tests erfolgt die Bestätigung der erfolgreichen bestandenen Tests durch einen Prüfer der EnergyCA per signierter E-Mail.
	EMT	Nachweis der korrekten Funktion der Zertifikatsantragsstellung und Zertifikatsannahme sowie von Sperrungen.	Nach erfolgreicher Prüfung erfolgt die Bestätigung per signierter E-Mail von einem Prüfer der EnergyCA

Tabelle 15: Testumgebung der EnergyCA

8.1.2 Beantragung Teilnahme an der EnergyCA

Folgende Anforderungen müssen bei Beantragung der Teilnahme an der **EnergyCA** erfüllt werden. Hierzu sind dazu die in Kapitel 8.1.1 aufgeführten Nachweise notwendig.

Detaillierte Informationen sind in den Kapiteln 5.1 und 8.1.1 definiert.

Antrag für Teilnahme als	Nachweis	Überprüfung der Nachweise	Wichtung
GWA	Zertifizierung entsprechend (TR-03109-6)	Zertifizierter (TR-03109-6) Auditor	Voraussetzung
	Signierte E-Mail der Energy Test CA über erfolgreiche Tests	Prüfer der EnergyCA	Voraussetzung
GWH	CC-Zertifizierung (BSI-CC-PP-0073)	CC-Zertifizierungsverfahren	Voraussetzung
	Signierte E-Mail der Energy Test CA über erfolgreiche Tests	Prüfer der EnergyCA	
SMGW	CC-Zertifizierung entsprechend (BSI-CC-PP-0073)	CC-Zertifizierungsverfahren	Voraussetzung
	Zertifizierung entsprechend (TR-03109-1)	Prüfstelle	
Aktiver EMT	oder ISO27001-Zertifizierung nativ	Zertifizierter ISO27001 Lead Auditor	Voraussetzung
	oder ISO27001-Zertifizierung nach BSI Grundschutz	BSI-akkreditierter ISO27001 Lead Auditor	
	signierte E-Mail der Energy Test CA über erfolgreiche Tests	Prüfer der EnergyCA	
Passiver EMT	Sicherheitskonzept	Sicherheitskonzept und Umsetzung der Maßnahmen kann im Schadensfall mit Bezug auf die Umsetzung herangezogen werden.	Voraussetzung
	signierte E-Mail der EnergyCA über erfolgreiche Tests	Prüfer der EnergyCA	

Tabelle 16: Anforderungen für die Teilnahme an der EnergyCA

8.1.3 Wirkbetrieb

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

Sollte eine Zertifizierung nicht mehr gültig sein, so muss dies der **EnergyCA** umgehend mitgeteilt werden.

Bei einer Änderung und Veröffentlichung der **EnergyCA** CP/CPS wird die SM-PKI Root per verschlüsselter und signierter Email hierüber informiert.

8.2 Reaktion 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

Die Preise für die Teilnahme an der **EnergyCA** sind in den jeweiligen Preislisten der individualvertraglichen Vereinbarungen zwischen T Security und den Endkunden zu entnehmen.

Die Preisliste erhält der Kunde als Anlage zu seinem Angebot seitens T Security.

9.2 Finanzielle Zuständigkeiten

Der Angebotswunsch zur Teilnahme und Fragen zu den finanziellen Konditionen und Zuständigkeiten sind über folgende Schnittstelle an T Security zu richten.

E-Mail-Kontakt	EnergyCA_Kontakt@t-systems.com

Tabelle 17: Adresse für vertriebliche / kommerzielle Anfragen der EnergyCA

10 Stichwort- und Abkürzungsverzeichnis

Abkürzung	Begriff
ASP	Ansprechpartner (des Unternehmens)
BSI	Bundesamt für Sicherheit in der Informationstechnik
CA	Certificate Authority
CC	Common Criteria
CLS	controllable local systems
CN	Common Name
CP	Certificate Policy
CPS	Certificate Practise Statement
CRL	Certificate Revocation List (Zertifikatssperrliste)
EMT	Externe Marktteilnehmer
ENC	Encryption / Verschlüsselung
ESARIS	Enterprise Security Architecture for reliable ICT Services
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
OCSP	Online Certificate Status Protocol
PIN	Personal Identifikation Number
PKI	Public Key Infrastructure
PP	Protection Profile
RA	Registration Authority
SHA	Secure Hash Algorithm
SMGW	Smart Meter Gateway
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

11 Literaturverzeichnis

AIS 20. (2013). *Anwendungshinweise und Interpretationen zum Schema AIS 20, Funkionalitätsklassen und Evaluationsmethodologie für determistische Zufallszahlengeneratoren Version 3.* BSI.

AIS 31. (2013). *Anwendungshinweise und Interpretationen zum Schema AIS 20, Funkionalitätsklassen und Evaluationsmethodologie für physikalischer Zufallszahlengeneratoren Version 3.* BSI.

BSI-CC-PP-0073. (2014). *Protection Profile für the Gateway of a Smart Metering System (Smart Meter Gateway PP), Version 1.3.* Bonn: BSI.

BSI-CC-PP-0095. (2017). *Protection Profile for the Security Module of a Smart Meter Mini-HSM (Mini-HSM Security Moduel PP), Version 1.0.* Bonn: BSI.

CP-SM-PKI. (2017). *Certificate Policy der Smart Metering PKI Version 1.1.1 (09.08.2017).* Bonn: BSI.

ISO/IEC 27001. (2015). *IT-Sicherheitsverfahren – Informationssicherheits-Managementsysteme – Anforderungen.* DIN.

KeyLifeSec. (kein Datum). *Key Lifecycle Security Requirements Version 1.0.* BSI.

RFC3647. (2003). *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework.*

RFC5280. (2008). *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.* https://www.ietf.org/rfc/rfc5280.txt.

TR-02102-1. (kein Datum). *Kryptographische Verfahren: Empfehlungen und Schlüssellängen.* Bonn: BSI.

TR-03109. (2015). *Technische Vorgaben für intelligente Messsysteme und deren sicherer Betrieb.* Bonn: BSI.

TR-03109-1. (2013). *Anforderungen an die Interoperabilität der Kommunikationseinheit eines intelligenten Messsystems.* Bonn: BSI.

TR-03109-4. (2017). *Technische Richtlinie - Public Key Infrastruktur für Smart Meter Gateways Version 1.2.1 (09.08.2017).* Bonn: BSI.

TR-03109-4. (2017). *Technische Richtlinie - Public Key Infrastruktur für Smart Meter Gateways Version 1.2.1 (09.08.2017).* Bonn: BSI.

TR-03109-6. (2015). *Smart Meter Gateway Administration.* Bonn: BSI.

TR-03116-3. (2016). *Kryptographische Vorgaben für Projekte der Bundesregierung; Teil 3: Intelligente Messsysteme.* Bonn: BSI.

TR-03116-4. (2016). *Kryptographische Vorgaben für Projekte der Bundesregierung; Teil 4: Kommunikationsverfahren in Anwendungen.* Bonn: BSI.

TR-03145. (2016). *Secure Certification Authority operation.* Bonn: BSI.