Certificate Policy der Schleupen Smart Metering Sub-CA

Veröffentlicht am: 18.02.2019

Herausgegeben von: Schleupen AG
Otto-Hahn-Str. 20
76275 Ettlingen

Tel. 07243_321-0

Manfred.Meinzer@schleupen.de

Titel	Certificate Policy der Schleupen Smart Metering Sub-CA		
Version	2.8	Ersetzt Version	2.6
OID	1.3.6.1.4.1.48941.341.1.28	Peter, Dr. Wenderoth Digital unterschrieben von Peter, Dr. Wenderoth Datum: 2019.02.12 17:46:53 +01'00'	
Gültig ab:	01.04.2019		

Tabelle 1: Identifikation des Dokuments

schleupen

Inhalt

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 sind, wird eine Smart Metering Public Key Infrastruktur (SM-PKI) etabliert. Technisch wird der Authentizitätsnachweis der Schlüssel dabei über digitale X.509-Zertifikate aus der SM-PKI realisiert.

Die grundsätzliche Systemarchitektur der SM-PKI ist in der [TR-03109-4] spezifiziert.

Das vorliegende Dokument beschreibt die Certificate Policy (CP) der Smart Meter Sub-CA der Schleupen AG, im Weiteren auch Schleupen SM-CP genannt.

Die Schleupen SM-CP dient dazu, die spezifischen Ausprägungen der technischen, personellen und organisatorischen Anforderungen zu beschreiben.

Bei den nicht spezifischen Punkten wird in dem Dokument auf die Vorgaben/Beschreibungen der SM-PKI Policy der Root CA verwiesen.

Die in diesem Dokument verwendeten Inhalte werden dem [RFC 2119] entsprechend mit folgenden deutschen Schlüsselworten beschrieben:

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

1.1 Überblick

Die Schleupen AG betreibt eine Sub-CA für die SM-PKI, die Schleupen Smart Metering Sub-CA. Die Sub-CA verfügt über ein ISMS-System, welches nach ISO/IEC 27001 zertifiziert ist, sowie über ein Zertifikat, das die Konformität zur TR-03145 bestätigt. Das Sicherheitskonzept berücksicht dabei auch die Einbindung von Dienstleistern, z.B. für das Housing der Hardware.

Die vorliegende Policy richtet sich an die Zertifikatsnehmer (Endnutzer) der Schleupen Smart Metering Sub-CA und ist in Anlehnung an die SM-PKI Policy der Root strukturiert und definiert.

Die CP der Schleupen Smart Metering Sub-CA unterwirft sich der SM-PKI Policy der Root, die durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) betrieben wird.
Sie erfüllt alle deren Anforderungen und konkretisiert in Einzelfällen die Umsetzung der Anforderungen, die die Policy der Root-CA an die Endnutzer stellt.

Verantwortlich für die Schleupen SM-CP ist die Schleupen AG.

Die Schleupen AG behält sich vor, komplette Aufgaben oder Teilaufgaben von beauftragten Unternehmen ausführen zu lassen.

1.2 Name und Identifizierung des Dokuments

S. Seite 1

1.3 PKI-Teilnehmer

Für die Schleupen Smart Metering Sub-CA gibt es keine spezifischen Ausprägungen zu den Inhalten dieses Kapitels. Somit verweisen wir auf das entsprechende Kapitel in der CP der Root-CA.

1.3.1 Zertifizierungsstellen

Es gelten die entsprechend Inhalte aus diesem Kapitel in der CP der Root-CA.

1.3.2 Registrierungsstellen

Es gelten die entsprechend Inhalte aus diesem Kapitel in der CP der Root-CA.

1.3.3 Zertifikatsnehmer

Es gelten die entsprechend Inhalte aus diesem Kapitel in der CP der Root-CA.

Die Schleupen Smart Metering Sub-CA stellt ausschließlich Zertifikate für die Instanzen GWA, SMGW und EMT aus, jedoch keine Gütesiegelzertifikate.

1.3.4 Zertifikatsnutzer

Es gelten die entsprechend Inhalte aus diesem Kapitel in der CP der Root-CA.

1.3.5 Andere Teilnehmer

Es gelten die entsprechend Inhalte aus diesem Kapitel in der CP der Root-CA.

1.4 Verwendung von Zertifikaten

Ergänzend zu dem entsprechenden Kapitel 1.4 ff. in der CP der Root-CA setzt die Schleupen Smart Metering Sub-CA für den Informationsaustausch mit den Ansprechpartnern neben der verschlüsselten und signierten Mail via S/MIME auch den DE-Mail-Dienst ein. Dabei ist die Schleupen Smart Metering Sub-CA kein De-Mail-Diensteanbieter. Kunden, die den DE-Mail-

Dienst nutzen möchten, müssen vorher bei einem akkreditierten Dienstanbieter ein DE-Mail-Konto einrichten.
Darüber hinaus gibt es für die Schleupen Smart Metering Sub-CA keine spezifischen Ausprägungen zu den Inhalten dieses Kapitels.

1.5 Administration der SM-PKI Policy

Die für dieses Dokument verantwortliche Organisation ist die Schleupen AG.

Die Schleupen AG kann über folgende Adresse kontaktiert werden:

Organisation	Schleupen AG
Bereich	Managed Services
Adresse	Otto-Hahn-Str. 20 76275 Ettlingen
Telephon	+49 (7243) 321-0
E-Mail (für den formalen Kommunikatsionsaustausch)	smgw-ra-operator@schleupen.de smgw-ra-operator@schleupen.de-mail.de
E-Mail (für den informellen Kommunikatsionsaustausch)	smgw-subca-info@schleupen.de
Webseite	https://www.schleupen.de

Tabelle 2: Kontaktadresse

Für den formalen Informationsaustausch werden ausschließlich signierte und verschlüsselte E-Mails akzeptiert.

1.5.1 Pflege der Schleupen SM-CP

Jede aktualisierte Version der Schleupen SM-CP wird unverzüglich über die angegebene Internetseite (siehe 2.2.2) zur Verfügung gestellt. Die Kunden der Schleupen Smart Metering Sub-CA werden per Mail an die genannten Kontaktpersonen auf eine neue Version hingewiesen. Erfolgt binnen 6 Wochen ab Veröffentlichung kein Widerspruch, gilt die neue Version der Policy als akzeptiert. Ein Widerspruch muss schriftlich, mindestens per Mail, von den Ansprechpartnern „smgwa-ra-operator" mitgeteilt werden. Nichtakzeptanz führt dazu, dass durch die Schleupen Smart Metering Sub-CA keine weiteren Zertifikate für den jeweiligen Kunden und dessen SMGW ausgestellt werden.

Jede Aktualisierung der SM-PKI Policy (Root CA) kann Auswirkungen auf diese CP haben. Die aktuelle CP der Root wird durch das BSI auf der Webseite

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03109/PKI_Certificate_Policy.html veröffentlicht.

1.5.2 Zuständigkeit für das Dokument

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

Zuständig für die Erweiterung und oder die nachträgliche Änderungen Schleupen SM-CP ist die Schleupen AG.

1.5.3 Ansprechpartner / Kontaktperson

Siehe Kapitel „Administration der SM-PKI Policy 1.5"

2 Verantwortlichkeit für Veröffentlichungen und Verzeichnisse

2.1 Verzeichnisse

Die von der Schleupen Smart Metering Sub-CA ausgestellten und noch gültigen Zertifikate können über das LDAP-Verzeichnis entnommen werden.

Alle von der Schleupen Smart Metering Sub-CA gesperrten Zertifikate werden während ihres Gültigkeitszeitraums in der Sperrliste aufgeführt.

2.2 Veröffentlichung von Informationen zur Zertifikatserstellung

2.2.1 Veröffentlichungen der Root-CA

Die Web-Seite der Root-CA mit den relevanten Veröffentlichungen kann über die Internetseite des BSI erreicht werden.

2.2.2 Veröffentlichungen der Sub-CA

Über die Web-Seite der Schleupen Smart Metering Sub-CA werden folgende Informationen veröffentlicht:

- CP der Schleupen Smart Metering Sub-CA
- Kontaktdaten der Schleupen Smart Metering Sub-CA
- Die aktuellen Zertifikate der Sub-CA inklusive der SHA256 Hashs.
- Parameter zur Einrichtung eines Zugriffs auf die Sperrliste bzw. das LDAP-Verzeichnis

Die Web-Seite kann über folgenden Link erreicht werden:
https://www.schleupen.de/energie-und-wasserwirtschaft/intelligenter-messstellenbetrieb/smart-meter-gateway-administration/sub-ca

2.3 Zeitpunkt und Häufigkeit der Veröffentlichungen

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

Sperrungen werden nach Durchführung durch eine Veröffentlichung in der jeweiligen Sperrliste in der Root-CA / Sub-CA als solche wirksam. Eine Aufnahme in die Sperrliste sowie deren Veröffentlichung erfolgt gemäß den in der [TR-03109-4] 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 ist auf die an der SM-PKI teilnehmenden Organisationen wie die Root-CA, die Sub-CA, die GWA, die GWH sowie EMTs beschränkt[1]. Dies wird über eine zertifikatsbasierte Authentisierung am jeweiligen Verzeichnisdienst mittels der TLS-Zertifikate der Zertifikatsnehmer sichergestellt.

Ein Verzeichnisdienst in der SM-PKI dient ausschließlich der Aktualisierung von angefragten Zertifikaten. Ein Massenabruf von Zertifikaten DARF NICHT erfolgen. Die Anzahl der zurückgegebenen Suchergebnisse im Verzeichnisdienst wird reglementiert.

Der lesende Zugriff auf die Sperrlisten der Schleupen Smart Metering Sub-CA ist ohne Authentifikation und ohne Einschränkungen möglich.

3 Identifizierung und Authentifizierung

Dieses Kapitel beschreibt die durchzuführenden Prozeduren, um die Identität und die Berechtigung eines Antragstellers (EMT, GWA 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

Für die Schleupen Smart Metering Sub-CA gibt es keine spezifischen Ausprägungen zu den Inhalten dieses Kapitels. Somit verweisen wir auf das entsprechende Kapitel in der CP der Root-CA.

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

3.2 Initiale Überprüfung zur Teilnahme an der PKI

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

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

3.2.1 Methoden zur Überprüfung bzgl. Besitz des privaten Schlüssels

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

Diese wird bei der Antragsprüfung durch Verifikation der inneren Signatur mit dem im Zertifikatsrequest enthaltenen zugehörigen öffentlichen Schlüssel durch die Schleupen Smart Metering Sub-CA geprüft werden. Dadurch wird sichergestellt, dass der Zertifikatsrequest vom Antragsteller kommt.

3.2.2 Authentifizierung von Organisationszugehörigkeiten

Die nachfolgenden Organisationen DÜRFEN innerhalb der SM-PKI Zertifikatsanträge an die Schleupen Smart Metering Sub-CA stellen: EMT und GWA (auch für SMGW).

Die grundsätzlichen Anforderungen sind in der CP der Root-CA beschrieben. Die spezielle Ausprägung des Prozesses zur Registrierung eines Teilnehmers sowie die Verpflichtung zur Einhaltung der Policy sind in den „Besonderen Vertragsbedingungen Sub-CA" dokumentiert.

Vor der Teilnahme an der Wirkumgebung MÜSSEN die Prozesse zum Zertifikatsmanagement (insbesondere Registrierung, Zertifikatsbeantragung, -erneuerung, -sperrung) mit der Test-Sub-CA erfolgreich durchgeführt und durch eine signierte Mail von der Schleupen Smart Metering Sub-CA bestätigt worden sein.

Die Nutzung des EMT-Zertifikats (aktiver oder passiver EMT) wird vom Antragssteller mit der Beantragung formal mitgeteilt. Die ausgestellten Zertifikate dürfen nur für den zuvor erklärten Nutzen eingesetzt werden. Möchte ein EMT die Nutzung ändern, so MUSS er dies rechtzeitig und eigenverantwortlich der Sub-CA mitteilen und dafür neue Zertifikate beantragen.

Aufgrund der adressierten Rollen sind die Kapitel 3.2.2.1 und 3.2.2.4 aus der CP der Root-CA nicht relevant.

3.2.3 Anforderungen zur Identifizierung und Authentifizierung des Zertifikats-Antragsstellers

Es gelten die entsprechend Inhalte aus diesem Kapitel in der CP der Root-CA.

3.2.4 Prüfung der Angaben zum Zertifikatsnehmer

Die Registrierungsstelle der Sub-CA prüft die Angaben zum Zertifikatsnehmer gegen die eingereichten Unterlagen auf Korrektheit.

3.2.5 Prüfung der Berechtigung des Antragsstellers

Es gelten die entsprechend Inhalte aus diesem Kapitel in der CP der Root-CA.

3.2.6 Kriterien für den Einsatz interoperierender Systeme/Einheiten

Aktuelle sind keine Kriterien definiert.

3.2.7 Aktualisierung/Anpassung der Zertifizierungsinformationen der Teilnehmer

Es gelten die entsprechend Inhalte aus diesem Kapitel in der CP der Root-CA.

3.2.8 Aktualisierung/Anpassung der Registrierungsinformationen der Teilnehmer

Es gelten die entsprechend Inhalte aus diesem Kapitel in der CP der Root-CA.

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

Die spezifischen Ausprägungen zu den Inhalten dieses Kapitels, insbesondere Bearbeitungs- und Vorlaufzeiten zur Beantragung von Zertifikaten sind in den „Besonderen Vertragsbedingungen Sub-CA" dokumentiert. Darüber hinaus verweisen wir auf das entsprechende Kapitel in der CP der Root-CA.

3.4 Identifizierung und Authentifizierung von Anträgen auf Schlüsselerneuerung (nicht routinemäßiger Folgeauftrag)

Die spezifischen Ausprägungen zu den Inhalten dieses Kapitels, insbesondere Bearbeitungs- und Vorlaufzeiten zur Beantragung von Zertifikaten sind in den „Besonderen Vertragsbedingungen Sub-CA" dokumentiert. Darüber hinaus verweisen wir auf das entsprechende Kapitel in der CP der Root-CA.

3.5 Identifizierung und Authentifizierung von Anträgen auf Sperrung

Die spezifischen Ausprägungen zu den Inhalten dieses Kapitels, insbesondere die spezielle Ausprägung des Prozesses zur „Sperrung durch Initiative des Zertifikatsinhabers" sind in den „Besonderen Vertragsbedingungen Sub-CA" dokumentiert. Darüber hinaus verweisen wir auf das entsprechende Kapitel in der CP der Root-CA.

Die Sperrung von GWA-Zertifikaten erfolgt nur in Abstimmung mit der Root-CA. Bei der Sperrungen von anderen Zertifikaten, die nach Ansicht der Schleupen SM Sub-CA systemrelevante Auswirkungen haben, wird vorab die Root-CA informiert.

3.6 Identifizierung und Authentifizierung von Anträgen auf Suspendierung

Es gelten die entsprechend Inhalte aus der CP der Root-CA.

Bei einer Suspendierung von SMGW-Zertifikatstripeln über den Web-Service MUSS der zuständige GWA umgehend eine signierte und verschlüsselte Mail mit der Begründung an den RA-Oparator der Sub-CA senden. Bleibt diese aus und erfolgt auch auf Nachfrage der Schleupen Smart Metering Sub-CA keine Rückmeldung, wird der Vorfall als Sicherheitsvorfall an die Root-CA gemeldet.

Die Suspendierung eines Zertifikatstripels wird zum 01.01.2018 unterstützt.

Sollte die Suspendierung nicht über den Web-Service erfolgen, muss der Ansprechpartner des Antragstellers eine signierte Mail an den RA-Oparator der Sub-CA mit folgenden Informationen senden:

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

Ein Zertifikat wird 30 Tage nach Eingang des Suspendierungsantrags immer gesperrt.

3.7 Anträge aufgrund von Namensänderungen

Bei Umfirmierung eines Zertifikatsnehmers (Änderung des Namens oder der Gesellschaftsform) MUSS grundsätzlich ein neuer initialer Zertifikatsrequest gestellt werden. Solange, wie der Prozess dauert, das neue Zertifikat auszurollen, sind beide Zertifikate gültig. Sobald das alte Zertifikat nicht mehr benötigt wird MUSS es gesperrt werden.

4 Betriebsanforderungen für den Zertifikatslebenszyklus

Die spezifischen Ausprägungen zu den Inhalten dieses Kapitels, insbesondere Bearbeitungszeiten und Pflichten des Subscribers sind in den „Besonderen Vertragsbedingungen Sub-CA" dokumentiert. Darüber hinaus verweisen wir auf das entsprechende Kapitel in der CP der Root-CA.

Die Schleupen Smart Metring Sub-CA verarbeitet Zertifikatsanträge zur Zertifikatserneuerung über die die Web-Service-Schnittstelle synchron.

Im Falle einer Zertifikats-Suspendierung eines SMGW MUSS der Sicherheitsvorfall an den RA-Operator (smgw-ra-operator@schleupen.de) gemeldet werden (s.a. Kap. 3.6).

5 Organisatorische, betriebliche und physikalische Sicherheitsanforderungen

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

Die Anforderungen der Root-CA an den Betrieb einer Sub-CA wurden umgesetzt.

Fokus der folgenden Kapitel sind die Anforderungen an die Endteilnehmer.

5.1 Generelle Sicherheitsanforderungen

Die generellen Sicherheitsanforderungen sind in der Policy der Root-CP beschrieben.

Dabei ist die Zertifizierung nach ISO 27001 zur Teilnahme an der Wirk-PKI für GWA und aktive EMT zwingend erforderlich, zur Teilnahme an der Test-PKI optional (GWH werden lt. Kap. 3.2.2 nicht berücksichtigt).

Eine ISO27001-Zertifizierung KANN nativ oder auf Basis von IT-Grundschutz vorgenommen werden.

5.1.1 Erforderliche Zertifizierungen der PKI-Teilnehmer

Die Schleupen Smart Metering Sub-CA verfügt über ein nach ISO/IEC 27001-2013 zertifiziertes ISMS sowie eine Zertifizierungen nach TR-03145.

Für die Schleupen Smart Metering Sub-CA gibt es keine zusätzlichen spezifischen Zertifizierungsanforderungen an die PKI-Teilnehmer. Es wird daher auf Vorgaben aus der Policy der Root-CA verwiesen.

5.1.2 Anforderungen an die Zertifizierung gemäß ISO 27001-Zertifizierung

Der Scope der Zertifikate (ISO/IEC27001 und TR-03145-1) der Schleupen Smart Metering Sub-CA umfasst alle Geschäftsprozesse und IT-Systeme für den Betrieb einer Sub-CA mit den Bereichen Registration Authority und Certification Authority.

Alle Anforderungen aus der CP der Root-CA sind umgesetzt.

Für die Schleupen Smart Metering Sub-CA gibt es keine zusätzlichen spezifischen Zertifizierungsanforderungen an die PKI-Teilnehmer. Es wird daher auf Vorgaben aus der Policy der Root-CA verwiesen.

5.2 Erweiterte Sicherheitsanforderungen

5.2.1 Betriebsumgebung und Betriebsabläufe

Die Anforderungen lt. CP der Root-CA hinsichtlich

- Objektschutz.
- Zutrittssicherheit.
- Geschäftsfortführung
- Informationsträger
- Notfall-Management und Wiederherstellung

werden duch die Schleupen Smart Metering Sub-CA umgesetzt.

Durch den Betrieb in einem hochwassergeschützen und nach ISO/IEC27001-zertifiziertem Tier 3 Rechenzentrum werden die Anforderungen an

- Brandschutz
- Strom
- Wasserschaden

erfüllt.

Die Anforderungenan an die Sicherheit der Betriebsumgebung und der Betriebsabläufe für die Endnutzer der Schleupen Smart Metering Sub-CA entsprechen der Vorgaben aus der Policy der Root-CA, sowie den spezifizierten Vorgaben für den GWA aus der TR-03109-6.

5.2.2 Verfahrensanweisungen

Die lt. CP der Root-CA notwendigen Verfahrensanweisungen hat die Schleupen Smart Metering Sub-CA umgesetzt.

Für den Betrieb der GWA-Umgebung und eines EMT MÜSSEN die Vorgaben aus der Policy der Root-CA umgesetzt werden.

5.2.3 Personal

Die lt. CP der Root-CA geforderten Dokumentationen und Anforderungen an das Personal sind durch die Schleupen Smart Metering sub-CA umgesetzt.

Der Betrieb der GWA- und EMT-Umgebung MUSS durch angemessen geschultes und erfahrenes Personal erfolgen.

Die Vorgaben aus der Policy der Root-CA MÜSSEN entsprechend umgesetzt werden.

5.2.4 Monitoring

Das Monitoring der Schleupen Smart Metering Sub-CA umfasst alle Vorgaben der Root-CA.

Die Vorgaben aus der Policy der Root-CA an die Endnutzer MÜSSEN durch diese entsprechend umgesetzt werden.

5.2.5 Archivierung von Aufzeichnungen

Die Schleupen Smart Metering Sub-CA verfügt über angemessene Archivierungsfunktionen, die den Anforderungen der Root-CA genügen. Die Zeiträume sind in Anhang B dokumentiert.

5.2.6 Schlüsselwechsel einer Zertifizierungsstelle

Die Prozesse für einen geplante und ungeplante Schlüsselwechsel der Schleupen Smart Metering Sub-CA sind dokumentiert und berücksichtigen das 4-Augen-Prinzip.

5.2.7 Auflösen einer Zertifizierungsstelle

Der Prozess einer Auflösung der Sub-CA entspricht den Vorgaben aus der Policy der Root-CA und ist für die Schleupen Smart Metering Sub-CA in dem Dokument „„Besondere Vertragsbedingungen Sub-CA““ definiert.

5.2.8 Aufbewahrung der privaten Schlüssel

Die Anforderungen lt. Policy der Root-CA werden durch die Schleupen Smart Metering Sub-CA umgesetzt.

Für die Endnutzer gelten die Vorgaben aus der Policy der Root-CA.

5.2.9 Behandlung von Vorfällen und Kompromittierung

Die Schleupen Smart Metering Sub-CA setzt die Anforderungen CP der Root-CA um. Bei der Sperrung systemkritischer Zertifikate wird die Root-CA eingebunden.

Für die Endnutzer gelten die Vorgaben aus der Policy der Root-CA.

5.2.10 Meldepflichten

Die Schleupen Smart Metering Sub-CA meldet Ereignisse gemäß der Policy der Root-CA an die Root-CA..

Für die Zertifikatsnutzer gelten die Vorgaben aus der Policy der Root-CA.

5.3 Notfall-Management

Die Anforderungen der Root-CA an das Notfallmanagement werden umgesetzt und sind als Teil des Betriebshandbuches der Schleupen Smart Metering Sub-CA dokumentiert.

Für alle Teilnehmer der SM-PKI gelten die Vorgaben aus der Policy der Root-CA.

6 Technische Sicherheitsanforderungen

Die Anforderungen der Root-CA an den Betrieb einer Sub-CA wurden umgesetzt und im Rahmen der Zertifizierungen nach ISO/IEC 27001 und TR-03145 überprüft. Fokus der folgenden Kapitel sind die Anforderungen an die Endteilnehmer.

6.1 Erzeugung und Installation von Schlüsselpaaren

Die Schleupen Smart Metering Sub-CA generiert ihre Schlüsselpaare selber. Sie erzeugt keine privaten Schlüssel für Antragsteller.

Jeder Zertifikatsnehmer MUSS sein eigenes Schlüsselpaar generieren.

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

6.1.1 Generierung von Schlüsselpaaren für die Zertifikate

Die Schleupen Smart Metering Sub-CA setzt die Anforderungen lt. CP der Root-CA um.

Für alle Endnutzer gelten die Vorgaben aus der Policy der Root-CA.

6.1.2 Lieferung privater Schlüssel

Die Erstellung der privaten Schlüssel erfolgt nicht durch die Sub-CA sondern durch die Zertifikatsnehmer der SM-PKI oder den von den Zertifikatsnehmern beauftragten Instanzen. Daher erfolgt keine Lieferung der privaten Schlüssel.

6.1.3 Lieferung öffentlicher Zertifikate

Alle Zertifikate werden nach Erzeugung umgehend in den jeweiligen Verzeichnissen der Schleupen Smart Metering Sub-CA abgelegt und sind somit für alle PKI-Teilnehmer zugänglich.

6.1.4 Schlüssellängen und kryptografische Algorithmen

Die Schleupen Smart Metering Sub-CA setzt die Anforderungen der Root-CA und der TR-03116-3 um.

Für alle Endnutzer gelten die Vorgaben aus der Policy der Root-CA.

6.1.5 Festlegung der Parameter der Schlüssel und Qualitätskontrolle

Die Schleupen Smart Metering Sub-CA setzt die Anforderungen lt. CP der Root-CA um.

Für alle Endnutzer gelten die Vorgaben aus der Policy der Root-CA.

6.1.6 Verwendungszweck der Schlüssel

Die Schleupen Smart Metering Sub-CA setzt ihre Schlüssel ausschließlich gemäß der Vorgaben der TR-03109-4 ein.

Die Schlüssel DÜRFEN ausschließlich für die in Kapitel 1.4.1 der Policy der Root-CA beschriebenen Verwendungszwecke eingesetzt werden. Der Verwendungszweck ist in der jeweils aktuellen Fassung der [TR-03109-4] konkretisiert.

6.2 Sicherung des privaten Schlüssels und Anforderungen an kryptografische Module

Es gelten die Vorgaben aus der Policy der Root-CA.

6.2.1 Mehrpersonen-Zugriffssicherung zu privaten Schlüsseln

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

Bei der Schleupen Smart Metering Sub-CA erfolgt das Schlüsselmanagement im Vier-Augen-Prinzip mit entsprechender Dokumentation und Protokollierung.

6.2.2 Ablage privater Schlüssel

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

Für die Schleupen Smart Metering Sub-CA ist dies sichergestellt.

6.2.3 Backup privater Schlüssel

Es gelten die Vorgaben aus der Policy der Root-CA.

Das Backup des privaten Schlüssels der Schleupen Smart Metering Sub-CA erfolgt als verschlüsselter Datencontainer.

6.2.4 Archivierung privater Schlüssel

Es wird keine Archivierung gesperrter oder abgelaufener privater Schlüssel durchgeführt. Diese privaten Schlüssel werden zerstört.

Dies gilt entsprechend für die privaten Schlüssel der Endnutzer.

6.2.5 Transfer privater Schlüssel in oder aus kryptografischen Modulen

Es gelten die Vorgaben aus der Policy der Root-CA.

Die Schleupen Smart Metering Sub-CA hält diese ein.

6.2.6 Speicherung privater Schlüssel in kryptografischen Modulen

Die Schleupen Smart Metering Sub-CA speichert ausschließlich ihre eigenen privaten Schlüssel und hält dabei die Vorgabe lt. CP der Root-CA ein. Die Schlüssel für die Test- und Wirkumgebung werden getrennt gespeichert.

Es gelten die Vorgaben aus der Policy der Root-CA.

6.2.7 Aktivierung privater Schlüssel

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

Diese Anforderung wird durch die Schleupen Smart Metering Sub-CA eingehalten.

6.2.8 Deaktivierung privater Schlüssel

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

Diese Anforderung wird durch die Schleupen Smart Metering Sub-CA eingehalten.

6.2.9 Zerstörung privater Schlüssel

Es gelten die Vorgaben aus der Policy der Root-CA.

Diese Anforderung wird durch die Schleupen Smart Metering Sub-CA eingehalten.

6.2.10 Beurteilung kryptografischer Module

Es gelten die Vorgaben aus der Policy der Root-CA.

Die Schleupen Smart Metering Sub-CA setzt ein Kryptografiemodule ein, für das der Hersteller eine Bestätigung erbracht hat, dass dieses den Anforderungen lt. CP der Root-CA entspricht..

6.3 Andere Aspekte des Managements von Schlüsselpaaren

6.3.1 Archivierung öffentlicher Schlüssel

Die Zertifikate aller Teilnehmer der Schleupen Smart Metering Sub-CA werden inklusive der Statusdaten archiviert (siehe Anhang B).

6.3.2 Gültigkeitszeitraum von Zertifikaten und Schlüsselpaaren

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

Instanz	Zertifikat	Intervall
Endnutzerzertifikat Ausnahme GWA	TLS/Sign/Enc	Alle 2 Jahre
GWA-Zertifikat	(TLS/Sign/Enc	Alle 3 Jahre

Tabelle 3: Intervall Zertifikatswechsel bei einer CA

Die Schleupen Smart Metering Sub-CA wechselt ihr Zertifikat alle 2 Jahre. Sobald sie über ein neues Zertifikat verfügt wird dieses zum Ausstellen neuer Zertifikate und der zugehörigen Sperrlisten verwendet werden.

6.4 Aktivierungsdaten

Die Aktivierungsdaten für die Kryptografiemodule werden sicher aufbewahrt.

6.5 Sicherheitsanforderungen für die Rechneranlagen

Die Anforderungen lt. CP der Root-CA an die Schleupen Smart Metering Sub-CA werden umgesetzt. Die Dateien der Audit-Trails werden nicht auf dem CA-Server, der für die Verwaltung von Zertifikaten genutzt wird, gespeichert.

Es gelten die Anforderungen an die entsprechenden Endnutzer aus der Policy der Root-CA.

6.6 Zeitstempel

Keine Anforderungen an Zeitstempel.

6.7 Validierungsmodell

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

Die Schleupen Smart Metering Sub-CA setzt diese um.

7 Profile für Zertifikate und Sperrlisten

Die folgenden Anforderungen werden durch die Schleupen Smart Metering Sub-CA umgesetzt.

7.1 Profile für Zertifikate und Zertifikatsrequests

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

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

7.1.1 Zugriffsrechte

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

7.1.2 Zertifikatserweiterung

Die Certificate Extensions werden in der jeweils aktuellen Fassung der [TR-3109-4] definiert.

7.2 Profile für Sperrlisten

Die Anforderungen an die Sperrlisten (Certification Revocation List, CRL)-Profile werden in der jeweils aktuellen Fassung der [TR-03109-4] definiert.

7.3 Profile für OCSP Dienste

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

8 Überprüfung und andere Bewertungen

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

8.1 Inhalte, Häufigkeit und Methodik

8.1.1 Testbetrieb

Die Schleupen Smart Metering Sub-CA stellt eine Testumgebung zur Verfügung.

Ziel und Zweck sind in der Policy der Root-CA beschrieben.

8.1.2 Beantragung Teilnahme an SM-PKI

Die Schleupen Smart Metering Sub-CA überprüft, ob die Antragsteller alle Anforderungend lt. CP der Root-CA einhalten..

8.1.3 Wirkbetrieb

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

Sollte eine Zertifizierung nicht mehr gültig sein, so MUSS dies der Schleupen Smart Metering Sub-CA mitgeteilt werden.

Wird eine neue Version dieser Policy veröffentlicht wird die Root-CA darüber per verschlüsselter und signierter Mail informiert.

8.2 Reaktionen auf identifizierte Vorfälle

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

9 Sonstige finanzielle und rechtliche Regelungen

9.1 Preise

Die Konditionen sind in dem Dokument „„Besondere Vertragsbedingungen Sub-CA"" der Schleupen Smart Metering Sub-CA beschrieben.

9.2 Finanzielle Zuständigkeiten

Der Betreiber der Schleupen Smart Metering Sub-CA ist die Schleupen AG. Sie ist finanziell eigenständig und unabhängig.

Die Geschäftsbeziehung wird über den Umfang der Auftragserteilung zwischen Auftraggeber und Auftragnehmer geregelt.

10 Anhang A – Namensschema

Es gelten die Vorgaben aus der Policy der Root-CA.

11 Anhang B – Archivierung

Es gelten die Vorgaben aus der Policy der Root-CA.

12 Anhang C – Defintionen

Es gelten die Vorgaben aus der Policy der Root-CA.

schleupen

13 Literaturverzeichnis

AIS 20	Anwendungshinweise und Interpretationen zum Schema AIS 20, Funktionalitätsklassen und Evaluationsmethodologie für determistische Zufallszahlengeneratoren Version 3, 2013
AIS 31	Anwendungshinweise und Interpretationen zum Schema AIS 20, Funktionalitätsklassen und Evaluationsmethodologie für physikalischer Zufallszahlengeneratoren Version 3, 2013
BSI CC-PP-0045	Protection Profile Cryptografic Modules, Security Level "Enhanced", Version 1.01, 2008
BSI-CC-PP-0073	Protection Profile for the Gateway of a Smart Metering System (Smart Meter Gateway PP), Version 1.3, 2014
BSI-CC-PP-0077	Protection Profile for the Security Module of a Smart Metering System, 2011
BSI CC-PP-0079	Protection Profile Cryptographic Modules, Security Level "Standard" Version 2.0.2, 2013
CEN/TC 224 EN 14169-1	Protection profiles for Secure signature creation device – Part 2: Device with key generation, 2009
DIN 43863-5	Herstellerübergreifende Identifikationsnummer für Messeinrichtungen (04/2012)
ISO 19005-1	Document management – Electronic document file format for longterm preservation – Part 1: User of PDF 1.4 (PDF/A-1)
ISO/IEC 27001	Information technology — Security techniques — Information security management systems — Requirements
MsysV (Entwurf)	Entwurf der Messsystensverordnung – Verordnung über technische Mindestanforderungen an den Einsatz von intelligenten Messsystemen
RFC 2119	Key words for use in RFCs to Indicate Requirements Levels
RFC 3647	Internet X.509 Public Key Infrastructure, Certificate Policy and Certification Practices Framework

TR-02102-1	BSI: Technische Richtlinie TR-02102-1, Kryptographische Verfahren: Empfehlungen und Schlüssellängen
TR-03109	BSI: Technische Richtlinie TR-03109, Technische Vorgaben für intelligente Messsysteme und deren sicheren Betrieb
TR-03109-1	BSI: Technische Richtlinie TR-03109-1, Anforderungen an die Interoperabilität der Kommunikationseinheit eines intelligenten Messsystems
TR-03109-2	BSI: Technische Richtlinie TR-03109-2, Smart Meter Gateway: Anforderungen an die Funktionalität und die Interoperabilität des Sicherheitsmoduls
TR-03109-4	BSI: Technische Richtlinie TR-03109-4, Smart Metering PKI – Public Key Infrastructure für Smart Meter Gateways
TR-03109-6	BSI: Technische Richtlinie TR-03109-6, Smart Meter Gateway Administration
TR-03116-3	BSI: Technische Richtlinie TR-03116-3, Kryptographische Vorgaben für Projekte der Bundesregierung, Teil 3 Intelligente Messsysteme
TR-03116-4	BSI: Technische Richtlinie TR-03116-4, Kryptographische Vorgaben für Projekte der Bundesregierung, Teil 4 Kommunikationsverfahren in Anwendungen
TR-03145	BSI: Technische Richtlinie TR-03145, Secure Certification Authority operation
TR-03145-1	BSI: Technische Richtlinie Secure CA operation, Part 1: Generic requirements for Trust Centers instantiating as Certification Authority (CA) in a Public-Key Infrastructure (PKI) with security level 'high', Version 1.0
Key Lifecycle Security Requirements	BSI: Anforderungen an den Lebenszyklus von kryptographischem Schlüsselmaterial zum Einsatz in einer PKI

Certificate Policy der Smart

Metering PKI BSI: Policy der Root CA

14 Stichwort- und Abkürzungsverzeichnis

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

Abkürzung	Begriff
PTG	hybride physikalische Zufallszahlgeneratoren (Funktionsklasse für Zufallsgeneratoren)
RA	Registration Authority
SHA	Secure Hash Algorithm
SigG	Signaturgesetz (Gesetz über Rahmenbedingungen für elektronische Signaturen)
SigV	Signaturverordnung (Verordnung zur elektronischen Signatur)
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

15 Mitgeltende Regelungen

Die Erstellung, Genehmigung und Veröffentlichung erfolgt verbindlich nach den Vorgaben „Lenkung von Dokumenten und Aufzeichnungen".

16 Versionshistorie

Version	Aktivität			Status: Entwurf / Review / Freigabe
	am	durch	Beschreibung	
V 0.1			Ersterstellung	Entwurf
V1.0.1	11.12.2015	MME	Freigabe	Freigabe
V1.0.2	06.05.2016	PWE	Tabelle 3 überarbeitet	Entwurf
V1.0.2	06.05.2016	MME	Freigabe	Freigabe
V.1.1.0	30.12.2016	MME	Anpassungen an Root CP Vers.1.1 eingearbeitet	Entwurf
V1.1.1	03.01.2017	PWE	Kommentiert	Entwurf
V1.1.2	03.01.2017	PWE/ MME	Anpassungen abgestimmt und eingearbeitet	Entwurf
V1.1.2	23.01.2017	MME/PWE	Fehlerkorrekturen, OID, Layout angepasst	Freigabe
V2.0	02.06.17	PWE	Erweiterung um Zertifikatssuspendierung	Freigabe
V2.0	02.06.17	MME	Freigabe	Freigabe
V2.1	08.08.17	PWE	Anpassungen lt. Kommentare Root-CA	Entwurf
V2.2	14.08.17	PWE	Anpasungen an Root-CP V1.1.1	Entwurf
V2.3	15.09.17	PWE	Erweiterung um CPS	Entwurf
V2.3	25.09.2017	MME	Freigabe	Freigabe
V2.4	19.10.17	PWE	Anpassungen lt. Kommentare Root-CA	Entwurf
V2.5	27.11.17	PWE	Anpassungen lt. Kommentare Root-CA und Ergänzung um DE-Mail-Verfahren.	Entwurf
V2.5	14.12.17	MME	Freigabe	Freigabe
V2.6	05.01.18	PWE	Neues Logo + Schriftart	Freigabe
V2.7	01.02.19	MME	Präzisierung in Kapitel 5 sowie Rechtschreibekorrektur in Kap. 5 und 6.1.2.	Review
V2.8	12.02.19	PWE	Anpassung Kap. 1.5.1: neu Policy: Widerspruchsfrist 6 Wochen	Freigabe