Certificate Policy der Sub-CA

COUNT+CARE Wissenswelt

Exported on 03/16/2018

Table of Contents

COUNT+CARE *Wissenswelt*

Certificate Policy der Sub-CA von COUNT+CARE GmbH & Co. KG

Vertraulichkeitsstufe: S0 / öffentlich 

1. Dokumenteninformationen

1.1 Bearbeitungsvermerk

	Name und Funktion	Version	Datum
Erstellt von:	L.Kominis	1.1.3	16.03.2018
Geprüft von:	A. Jorba	1.1.3	16.03.2018
Genehmigt von:	H. Mink, Head of CA	1.1.3	16.03.2018

1.2 Änderungshistorie

Datum	Bearbeiter	Version	Änderungsgrund / Änderungen
08.08.2017	L. Kominis	1.0	Initialdokument
27.02.2018	L.Kominis	1.1	Überprüfung und redaktionelle Anpassung auf SM-PKI Version 1.1.1
28.02.2018	L.Kominis	1.1.1	Anpassung bei URLs
09.03.2018	L. Kominis	1.1.2	Überarbeitung Hinweise Root CA
16.03.2018	L. Kominis	1.1.3	Finalisierung Hinweise Root CA

1.3 Klassifizierung

Die Certificate Policy der Sub-CA von COUNT+CARE GmbH & Co. KG ist unter S0 / öffentlich einzustufen, da sie jedem PKI-Teilnehmer zur Verfügung stehen muss.

1.4 Gleichstellungshinweis

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

2. Zweck, Anwendungsbereich und Benutzer

Die Certificate Policy der CC ist für die PKI Marktteilnehmer verpflichtend, die von der CC Sub-CA Zertifikate erhalten haben bzw. besitzen sowie für die CC Sub-CA selbst. Die CP ist für diese Zwecke auch auf der Internetseite der CC herunterladbar. Bei Aktualisierungen wird dies nach Freigabe ebenfalls auf die Internetseite gestellt.

3. Einleitung

Die volatile Stromerzeugung aus erneuerbaren Energien erfordert es, Netze, Erzeugung und Verbrauch effizient und intelligent miteinander zu verknüpfen. Zur Unterstützung dieses Ziels werden intelligente Messsysteme (Smart Metering Systems) eingesetzt.

Die zentrale Kommunikationseinheit des intelligenten Messsystems stellt das Smart Meter Gateway (SMGW) in den Haushalten der Letztverbraucher dar. Die Hauptaufgaben des SMGW bestehen 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 ist eine gegenseitige Authentisierung der Kommunikationspartner erforderlich. Die Kommunikation erfolgt dabei stets über einen verschlüsselten und integritätsgesicherten Kanal. Zudem werden Daten vom SMGW vor der Übertragung zur Integritätssicherung signiert und zur Gewährleistung des Datenschutzes für den Endempfänger verschlüsselt.

Damit die Authentizität und die Vertraulichkeit bei der Kommunikation der einzelnen Marktteilnehmer untereinander gesichert sind, wird eine Smart Metering Public Key Infrastruktur (SM-PKI) etabliert. Technisch wird der Authentizitätsnachweis der Schlüssel dabei über digitale X.509-Zertifikate aus der SM-PKI realisiert.

Die Systemarchitektur der SM-PKI ist in der [TR-03109-4] spezifiziert. Sie wird in die folgenden drei Hierarchiestufen unterteilt:

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

Die COUNT+CARE GmbH & Co hat sich dazu entschieden eine Sub-CA in der SM-PKI zu betreiben. Als Betreiber einer Sub-CA in der SM-PKI unterwirft sich die COUNT+CARE GmbH & Co. KG der Certificate Policy der SM-PKI.

Als Betreiber einer Sub-CA ist COUNT+CARE GmbH & Co. KG dazu verpflichtet, die folgende Certificate Policy für alle PKI-Teilnehmer zu veröffentlichen.

Die Certificate Policy von COUNT+CARE GmbH & Co. KG berücksichtigt die Anforderungen und Regelungen aus der Certificate Policy der SM-PKI Version 1.1.1 und dient dazu, die umgesetzten technischen, personellen und organisatorischen Sicherheitsanforderungen für die Ausstellung von Zertifikaten durch die CC Sub-CA in der SM-PKI zu beschreiben.

3.1 Überblick

Im Kapitel 4 werden die Verzeichnisdienste beschrieben. Neben der Darstellung der Verzeichnisse werden die veröffentlichten Informationen, die Häufigkeit der Veröffentlichungen sowie die eingesetzten Zugriffskontrollen beschrieben.

In Kapitel 5 werden Regeln zur Authentifizierung der einzelnen Teilnehmer beschrieben. Hierzu gehören neben Details zur erstmaligen Identifizierung auch detaillierte Vorgaben zur Schlüsselerneuerung.

Kapitel 6 beschreibt die Betriebsanforderungen für den Zertifikatslebenszyklus (Ausgabe, Sperrung, Ablauf). Kapitel 7 beschäftigt sich mit organisatorischen, betrieblichen und physikalischen Sicherheitsanforderungen für die Betriebsumgebungen der GWA und der EMT.

In Kapitel 8 werden technische Sicherheitsanforderungen wie die Erzeugung, die Lieferung, die Speicherung und das Management von Schlüsselpaaren definiert. Des Weiteren werden die Anforderungen an die einzusetzenden kryptographischen Module und Sicherheitsanforderungen für die Rechneranlagen spezifiziert.

Kapitel 9 beschreibt die Zertifikatsprofile für alle Teilnehmer der SM-PKI. In Kapitel 10 finden sich Bewertungsrichtlinien für die einzelnen Parteien, und das abschließende Kapitel 11 geht auf weitere rechtliche und finanzielle Regelungen ein.

3.2 Name und Identifizierung des Dokuments

Dieses Dokument ist die Certificate Policy (CP) und kann über die folgenden Informationen identifiziert werden.

Identifikator	Wert
Titel	Certificate Policy der Sub-CA von COUNT+CARE GmbH & Co. KG
Version	1.1.3
OID	1.3.6.1.4.1.47434.1.1.3
Organisation	IT Operations (C122)

Tabelle 1: Identifikation des Dokuments

Dieses Dokument kann unter https://www.countandcare.de/metering/Sub-CA bezogen werden.

3.3 PKI-Teilnehmer

In der nachfolgenden Tabelle werden die relevanten Rollen für die Sub-CA von COUNT+CARE GmbH & Co. KG aufgeführt:

Rollen	Zertifizierungsstelle	Registrierungsstelle	Zertifikatsnehmer	Zertifikatsnutzer
Sub-CA (COUNT+CARE GmbH & Co. KG)	X	X	X	X
Root-CA	X	X	X	X
GWH	X	X	X	X
GWA			X	X
EMT			X	X
SMGW			X	X

Tabelle 2: Relevanten Rollen für die Sub-CA von COUNT+CARE GmbH & Co. KG

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

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

3.3.1 Sub-CA von COUNT+CARE

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

COUNT+CARE GmbH & Co. KG betreibt dafür ein Wirksystem (Wirk-CA) und ein Testsystem (Test-CA) für Test- und Einarbeitungszwecke (z.B. bei der Erst-Registrierung und zum Test systemkritischer Vorgänge wie dem Wechsel des Vertrauensankers). Die Test-CA wird in einer separaten Test-PKI betrieben.

Funktional entspricht die technische Infrastruktur der Test-CA der Wirk-CA, die Systeme der Test-CA und Wirk-CA sind aber voneinander getrennt. Zudem werden in den beiden Systemen unterschiedliche Schlüssel verwendet.

3.3.2 Registrierungsstelle

In der Registrierungsstelle (Registration Authority, RA) wird vor der Ausstellung eines Zertifikats die zweifelsfreie Identifizierung des Antragstellers sowie die Authentifizierung der Rolle und der Identitätsdaten des Antragstellers durchgeführt.

3.3.3 Zertifikatsteilnehmer der Sub-CA

Die Sub-CA von COUNT+CARE GmbH & Co. KG stellt Zertifikate für die nachfolgend beschriebenen PKI-Teilnehmerrollen aus. Diese Rollen werden auch als Endnutzer oder Zertifikatsinhaber bezeichnet, da diese die ausgestellten Zertifikate ausschließlich zur Absicherung der Kommunikation verwenden und nicht zur Ausstellung von weiteren Zertifikaten.

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 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.

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

SMGW

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

Externe Marktteilnehmer

Ein externer Marktteilnehmer (EMT) erhält Zertifikate, mit denen dieser insbesondere mit den SMGWs 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 diesen nachgelagerten Geräten (Controllable Local Systems, CLS) anzusprechen, wird als **aktiver EMT** bezeichnet. 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. des zugehörigen Zertifikatsmanagements auch als Dienstleistung anbieten. Dieses Unternehmen würde somit das EMT-Frontend des Auftraggebers realisieren. Bei dem Aufbau einer solchen Systemstruktur MUSS darauf geachtet werden, dass die Übermittlung der Daten von dem Dienstleister zu dem Auftraggeber ein vergleichbares Sicherheitsniveau zu den in der [TR-03116-3] definierten Sicherheitsmechanismen einhält.

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

3.3.4 Zertifikatsnutzer

Zertifikatsnutzer im Sinne dieser Certificate Policy sind alle natürlichen und juristischen Personen bzw. technischen Komponenten, die Zertifikate aus der SM-PKI, ausgestellt von der Root-CA oder einer der Sub-CAs der SM-PKI, für die Erledigung von Geschäftsprozessen/Aufgaben verwenden.

3.4 Verwendung von Zertifikaten

Die erlaubte und verbotene Verwendung von Zertifikaten in der SM-PKI wird in der Certificate Policy der SM-PKI beschrieben (siehe [CP] Abschnitt 1.4). Es gibt keine weiteren Einschränkungen der Verwendung durch COUNT+CARE GmbH & Co. KG.

3.5 Administration der Certificate Policy

Die für dieses Dokument verantwortliche Organisation ist die COUNT+CARE GmbH & Co. KG und kann über folgende Adresse kontaktiert werden:

Organisation	COUNT+CARE GmbH & Co. KG
Abteilung	C122 IT Operations
Adresse	Landwehrstraße 55, 64293 Darmstadt
Telefon/Fax	+49 -06151-404-0
E-Mail-Adresse	RA_Operator@Countandcare.de
Webseite	https://www.countandcare.de/metering/sub-ca/

Tabelle 3: Kontaktadresse

3.5.1 Pflege der Certificate Policy

Jede aktualisierte Version der Certificate Policy wird den Anwendern unverzüglich über die Webseite (siehe 3.5) zur Verfügung gestellt.

4. Verantwortlichkeit für Veröffentlichungen und Verzeichnisse

4.1 Verzeichnisse

Ausgestellte und noch gültige Zertifikate der Sub-CA von COUNT+CARE GmbH & Co. KG werden in einem eigenständigen Verzeichnisdienst geführt. Die URL des Verzeichnisdienstes (LDAP) ist der o.g. Webseite zu entnehmen und entspricht den Vorgaben/Anforderungen der [TR-03109-4].

Außerdem werden die Sperrlisten auf dem LDAP veröffentlicht, der auf der o.g. Webseite benannt ist, in diesem sind alle gesperrten Zertifikate der Sub-CA von COUNT+CARE GmbH & Co. KG während ihres Gültigkeitszeitraums aufgeführt sind.

4.2 Veröffentlichung von Informationen zur Zertifikatserstellung

Die Sub-CA ist dazu verpflichtet, folgende Informationen über ihre Webseite zu veröffentlichen:

- Kontaktdaten für die Sub-CA
- Die aktuellen Zertifikate der Sub-CA inklusive der SHA256 Hashs. Das Format, in dem die Zertifikate und Hashs vorliegen, muss angegeben werden.
- Parameter zur Einrichtung eines Zugriffs auf die Sperrliste bzw. den Verzeichnisdienst
- Veröffentlichung dieser Certificate Policy der Sub-CA von COUNT+CARE GmbH & Co. KG

Darüber hinaus werden auf der Webseite noch folgende Informationen veröffentlicht:

- Formulare für Ansprechpartner hinzufügen oder sperren
- Formular für Antrag GWA oder EMT
- Formular für Antrag Sperrung Zertifikat
- Formular für Antrag Beendigung der Teilnahme GWA oder EMT

Die Adresse zur Webseite der Sub-CA findet sich im Abschnitt 3.5.

4.3 Zeitpunkt und Häufigkeit der Veröffentlichungen

Die Sperrliste wird aus Sicherheitsgründen täglich erzeugt, spätestens jedoch alle 4 Tage und hat eine Gültigkeit von 7 Tagen. Weitere Zeitpunkte und Häufigkeiten von Veröffentlichungen der Sub-CA von COUNT+CARE GmbH & Co. KG richten sich nach den Vorgaben der Certificate Policy der SM-PKI (siehe [CP] Abschnitt 2.3).

4.4 Zugriffskontrollen auf Verzeichnisse

Der lesende Zugriff auf den Verzeichnisdienst der Sub-CA von COUNT+CARE GmbH & Co. KG ist auf die Teilnehmer der SM-PKI beschränkt. Dies wird über eine zertifikatsbasierte Authentisierung am jeweiligen Verzeichnisdienst mittels der TLS-Zertifikate der Zertifikatsnehmer sichergestellt. Die Authentisierung ist gemäß den Anforderungen aus der [TR-03116-3] umgesetzt.

Der Verzeichnisdienst der Sub-CA von COUNT+CARE GmbH & Co. KG ist so konfiguriert, dass die Anzahl der zurückgegebenen Suchergebnisse begrenzt ist, um den Massenabruf von Zertifikaten zu verhindern. Es werden maximal 10 Zertifikate zurück geliefert.

Der lesende Zugriff auf die Sperrlisten der Sub-CA von COUNT+CARE GmbH & Co. KG erfolgt ohne Authentifikation und ohne Einschränkungen.

5. Identifizierung und Authentifizierung

Dieses Kapitel beschreibt die Prozeduren, um die Identität und die Berechtigung eines Antragstellers (**EMT, GWA,** oder **SMGW**) vor dem Ausstellen eines Zertifikats festzustellen. Zertifikatsrequests müssen konform zur [TR-03109-4] gestellt werden.

5.1 Regeln für Namensgebung

Für die Namensgebung werden die Regelungen aus der Certificate Policy der SM-PKI (siehe [CP], Abschnitt 3.1) angewendet.

5.2 Initiale Überprüfung zur Teilnahme an der SM-PKI

Dieser Abschnitt enthält Informationen über die Identifizierungs- und Authentifizierungsprozeduren für die Teilnahme an der SM-PKI. Für den initialen Zertifikatsantrag werden insbesondere die natürlichen Personen als Vertreter des Unternehmens sowie die Anforderung und Qualifikation des Unternehmens geprüft.

Bestandteil dieser Prozeduren sind auch die Prüfungen nach den Anforderungen aus Abschnitt 10 (bzw. [CP] Abschnitt 8.1).

5.2.1 Methoden zur Überprüfung bzgl. Besitz des pivaten Schlüssels

Für die Prüfung des Besitzes des privaten Schlüssels, muss ein Zertifikatsrequest gemäß [TR-03109-4] eine innere Signatur und den öffentlichen Schlüssel beinhalten.

Bei der Antragsprüfung wird durch die Verifikation der inneren Signatur mit dem dazugehörigen öffentlichen Schlüssel der Besitz des privaten Schlüssels durch die Sub-CA von COUNT+CARE GmbH & Co. KG geprüft.

5.2.2 Authentifizierung von Organisationszugehörigkeiten

Zur initialen Autorisierung als EMT oder GWA müssen die notwendigen Unterlagen und Daten für die Registrierung eingereicht werden. Die notwendigen Unterlagen und Daten sind der Certificate Policy der SM-PKI zu entnehmen (siehe [CP] Abschnitt 3.2.2). Bzgl. SMGWs stellt die CC Sub-CA ausschließlich SMGW-Wirkzertifikate aus.

5.2.3 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 GWA zu übermitteln sind.

5.2.4 Ungeprüfte Angaben zum Zertifikatsnehmer

Die Registrierungsstelle der Sub-CA von COUNT+CARE GmbH & Co. KG prüft die Korrektheit der Angaben zum Zertifikatsnehmer im Zertifikatsrequest gegenüber den eingereichten Unterlagen (siehe Abschnitt 5.2.2).

5.2.5 Aktualisierung / Anpassung der Zertifizierungsinformationen der Teilnehmer

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

Die Sub-CA von COUNT+CARE GmbH & Co. KG muss von dem Zertifikatsnehmer rechtzeitig vor Ablauf der eingereichten Zertifikatsunterlagen über die Ergebnisse der Auditierung informiert und soweit ausgestellt auch das entsprechende Zertifikat zur Verfügung gestellt bekommen.

Sollte der Teilnehmer die Zertifizierung nicht mehr erhalten, so MUSS die Sub-CA von COUNT+CARE GmbH & Co. KG das Zertifikat / die Zertifikate aus der SM-PKI sperren.

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 Sub-CA von COUNT+CARE GmbH & Co. KG zur Verfügung stellen.

Die Sub-CA von COUNT+CARE GmbH & Co. KG aktualisiert entsprechend die Registrierungsdaten des jeweiligen Teilnehmers.

5.2.6 Aktualisierung / Anpassung der Registrierungsinformationen der Teilnehmer

Jeder Zertifikatsnehmer MUSS der Sub-CA von COUNT+CARE GmbH & Co. KG unverzüglich mitteilen, falls sich Änderungen bzgl. seiner Registrierungsdaten ergeben (vgl. Abschnitt 6.7). Zusätzlich wird jährlich über die hinterlegten Ansprechpartner bei den Zertifikatsnehmern angefragt, ob Änderungen an den Registrierungsdaten vorliegen.

5.3 Identifizierung und Authentifizierung von Anträgen auf Schlüsselerneuerung

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

Folgeanträge müssen spätestens 4 Wochen vor Ablauf des vorherigen Zertifikats an die Sub-CA von COUNT+CARE GmbH & Co. KG gestellt werden. Bei einer Schlüsselerneuerung ist zu beachten, dass immer ein neuer Schlüssel erstellt werden MUSS.

Für die Behandlung von Folgeanträgen durch die Sub-CA von COUNT+CARE GmbH & Co. KG gelten die Regelungen aus der Certificate Policy der SM-PKI (siehe [CP] Abschnitt 3.3 und 3.4).

5.4 Identifizierung und Authentifizierung von Anträgen auf Sperrung oder Suspendierung

Die Sub-CA von COUNT+CARE GmbH & Co. KG bietet nur die in der Certificate Policy der SM-PKI geforderten Verfahren zur Sperrung und Suspendierung von Zertifikaten an (siehe [CP] Abschnitt 3.5 und 3.6).

6. 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.

Für die gesicherte personenbezogene Kommunikation ist der Einsatz von personenbezogenen CS/MIME(ASP)-Zertifikaten für alle beteiligten Parteien Voraussetzung. Relevante personenbezogene Kommunikation muss verschlüsselt und signiert erfolgen.

6.1 Zertifikatsantrag

6.1.1 Wer kann einen Zertifikatsantrag stellen?

Ein Zertifikatsrequest darf ausschließlich von einer Organisation gestellt werden. Befugte Organisationen sind GWA, EMT die sich gemäß Abschnitt 5.2 bei der Sub-CA von COUNT+CARE GmbH & Co. KG identifiziert haben.

Ein Endnutzer (nicht SMGW) KANN sofern erforderlich weitere Zertifikate bzw. Zertifikatstriple (siehe [TR-03109-4] für sich beantragen (z.B. für Lastmanagement oder Ausfallsicherheit). Die weiteren Zertifikate/ Zertifikatstriple werden eindeutig gemäß den Regelungen der Certificate Policy der SM-PKI (siehe [CP] Abschnitt 4.1.1) gekennzeichnet.

Der Zertifikatsrequest zu einem Folgeantrag (siehe Abschnitt 5.3) muss unter Nutzung der vorhandenen Zertifikate gestellt werden.

6.1.2 Beantragungsprozess und Zuständigkeiten

Für die Bearbeitung eines Zertifikatsantrags ist die Registration Authority (RA) der Sub-CA von COUNT+CARE GmbH & Co. KG verantwortlich.

6.2 Verarbeitung von initialen Zertifikatsanträgen

Die Prozesse zur „Durchführung der Identifizierung und Authentifizierung“ sowie zur „Annahme oder Ablehnung von initialen Zertifikatsanträgen“ erfolgen bei der Sub-CA von COUNT+CARE GmbH & Co. KG gemäß den Regelungen der Certificate Policy der SM-PKI (siehe [CP] Abschnitte 4.2.1 und 4.2.2).

6.2.1 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 für Endnutzer anzusehen. Die Ausgabe von Folgezertifikaten bzw. Ersatzzertifikaten nach der Sperrung von Zertifikaten können von den angegebenen Werten situationsabhängig abweichen.

Die Bearbeitung der Zertifikatsanträge gliedert sich in folgende Arbeitsschritte:

Arbeits schritt	Beschreibung des Arbeitsschrittes	Zeitrahmen
1	Start des Beantragungsprozesses durch den Endnutzer (GWA oder EMT)	-
2	Kontaktaufnahme zur Terminvereinbarung durch die Sub-CA von COUNT+CARE GmbH & Co. KG	3 Arbeitstage (Für Arbeitsschritt 3) wird ein Termin innerhalb der nachfolgenden 3 Arbeitstage ermöglicht)
3	Übergabe der Dokumente / Nachweise ggf. im Rahmen eines persönlichen Termins an die RA-Operatoren	-
4	Vorprüfung der Unterlagen und Rückmeldung an den Endnutzer über die RA-Operatoren	1 Kalenderwoche
5 (optional)	Nachlieferungsfrist für den Endnutzer	3 Kalenderwochen
6	Prüfung der Unterlagen durch die RA-Operatoren der COUNT+CARE GmbH & Co. KG inkl. Rückmeldung an den Endnutzer	1 Kalenderwoche
7	Ausstellung der Zertifikate für Endnutzer über die CA-Operatoren	2 Arbeitstage

Tabelle 4: Zeitablauf für die initale Ausgabe von Endnutzer-Zertifikaten

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.

6.2.2 Ausgabe von Zertifikaten

Die Ausgabe von Endnutzer-Folgezertifikaten erfolgt über die Web-Service-Schnittstelle. Ein Versand von Endnutzer- Folgezertifikaten per E-Mail an den Ansprechpartner ist grundsätzlich nicht vorgesehen. Bei technischen Problemen z.B. nicht Erreichbarkeit des Web-Services ist S/MIME jedoch zulässig.

Nur initiale Zertifikate werden per E-Mail an den Ansprechpartner gesendet inkl. eines durch das Sub-CA System zufällig generiertem Sperrpasswort. Mit Hilfe des Sperrpassworts können Zertifikate direkt durch RA-Operator gesperrt werden. Bei kritischen Fällen, wie bspw. Sperrung eines GWA oder falls keine Sperrpasswort bekannt ist, ist eine Kommunikation mit dem CA-Operator notwendig.

6.2.3 Benachrichtigung des Zertifikatsnehmers über die Ausgabe des Zertifikats

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

6.3 Annahme von Zertifikaten

Die Angaben der Endnutzer-Zertifikate müssen nach Erhalt durch den Ansprechpartner des Zertifikatsnehmers auf Korrektheit und Vollständigkeit geprüft werden.

Um ein Zertifikat zurückzuweisen, muss ein Ansprechpartner des Zertifikatsnehmers eine Nachricht an die Sub-CA von COUNT+CARE GmbH & Co. KG schicken. In der Nachricht ist der Grund für die Verweigerung der Annahme anzugeben. Bei fehlerhaften Zertifikaten sind die fehlerhaften bzw. unvollständigen Einträge zu benennen. Die zu verwendende Adresse lautet: CA_Operator@countandcare.de.

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

6.3.1 Veröffentlichung von Zertifikaten durch die CA

Alle ausgestellten Zertifikate werden direkt nach der Ausstellung im Verzeichnisdienst der Sub-CA von COUNT+CARE GmbH & Co. KG veröffentlicht.

6.4 Verwendung von Schlüsselpaar und Zertifikat

6.4.1 Verwendung des privaten Schlüssels und des Zertifikats durch den Zertifikatsnehmer

Zertifikate und die zugehörigen privaten Schlüssel müssen gemäß ihrem Verwendungszweck eingesetzt werden, vgl. [TR-03109-4].

6.4.2 Verwendung des öffentlichen Schlüssels und des Zertifikats durch Zertifikatsnutzer

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

6.5 Zertifikatserneuerung

Zertifikatserneuerung bedeutet das Ausstellen eines neuen Zertifikats für einen öffentlichen Schlüssel, der bereits zertifiziert wurde. Zertifikatserneuerungen dürfen gemäß den Vorgaben der Certificate Policy der SM-PKI nicht erfolgen und werden daher von der Sub-CA von COUNT+CARE GmbH & Co. KG nicht angeboten.

6.6 Zertifizierung nach Schlüsselerneuerung

Bei der Sub-CA von COUNT+CARE GmbH & Co. KG wird die Zertifizierung nach Schlüsselerneuerungen gemäß den Vorgaben der Certificate Policy der SM-PKI (siehe [CP] Abschnitt 4.6) durchgeführt.

Fehlermeldungen zu Zertifikaten sind der Sub-CA von COUNT+CARE GmbH & Co. KG über die in Abschnitt 6.3 genannten Schnittstelle mitzuteilen.

Alle ausgestellten Zertifikate werden direkt nach der Ausstellung im Verzeichnisdienst der Sub-CA von COUNT+CARE GmbH & Co. KG veröffentlicht.

6.7 Änderungen am Zertifikat

Änderungen an den Zertifikatsinhalten, abgesehen vom Schlüsselmaterial, sind nicht vorgesehen. Bei Änderungsbedarf, z.B. durch eine Umfirmierung eines Zertifikatsnehmers, MUSS ein neues initiales Zertifikat gemäß Kapitel 3.2 der [CP] beauftragt und das alte Zertifikat gesperrt werden.

6.8 Sperrung und Suspendierung von Zertifikaten

Die Initiierung der Sperrung oder der Suspendierung eines Wirkzertifikats kann durch Zertifikatsnehmer bei der Sub-CA von COUNT+CARE GmbH & Co. KG eingeleitet werden. Die Sperrberechtigung für SMGW-Zertifikate liegt außerdem beim GWA (vgl. [CP] Abschnitt 3.6).

Die Sperrung und Suspendierung von Wirkzertifikaten erfolgt gemäß den Regelungen der Certificate Policy der SM-PKI (siehe [CP] Abschnitt 3.6 und 4.8).

Wirkzertifikate von GWAs, EMTs und SMGWs können gesperrt werden; dies wird gemäß den Regelungen der Certificate Policy der SM-PKI (siehe [CP] Abschnitt 4.8.1) durchgeführt.

Wirkzertifikate für SMGWs können zusätzlich bis zu 30 Tage suspendiert werden. Auch dies wird gemäß den geltenden Regelungen der Certificate Policy der SM-PKI (siehe [CP] Abschnitt 4.8.2) durchgeführt. Suspendierte Zertifikate müssen von allen Teilnehmern als gesperrte Zertifikate behandelt werden.

Alle Sperrungen und Suspendierungen werden unverzüglich umgesetzt und über eine aktualisierte Sperrliste veröffentlicht. Zusätzlich wird die Sperrliste gemäß den Regelungen der Certificate Policy der SM-PKI (siehe [CP] Abschnitt 4.8.3) aktualisiert. Bei Sperrungen von "systemkritischen" Zertifikaten wie bspw. für einen GWA wird vorab die Einbindung bzw. Abstimmung mit der Root durch die Sub-CA initiiert.

Verfügbarkeit des Sperrdienstes:

Der Sperrdienst der Sub-CA ist entsprechend der Tabelle 10 [CP] täglich verfügbar. Bei einer Sperrung per Email an den Postkorb des RA-Operators (mit dem initial mitgeteilten Sperr-Passwort) oder CA-Operators (falls kein Passwort bekannt oder wenn es sich um einen systemkritische Zertifikatssperrung handelt) in der Zeit von 10:00 Uhr bis 15:00 Uhr wird eine unverzügliche Umsetzung sichergestellt.

6.9 Service zur Statusabfrage von Zertifikaten

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

6.10 Beendigung der Teilnahme

Die Beendigung der Teilnahme eines Zertifikatsnehmers an der SM-PKI kann gemäß den Regelungen der Certificate Policy der SM-PKI (siehe [CP] Abschnitt 4.10)

durchgeführt werden.

7. Organisatorische, betriebliche und physikalische Sicherheitsanforderungen

Für die Teilnahme an der SM-PKI sind in der Certificate Policy der SM-PKI (siehe [CP] Abschnitt 5) technische und organisatorische Sicherheitsanforderungen spezifiziert, die von an allen PKI-Teilnehmern entsprechend der Anforderungen für ihrer PKI-Rolle erfüllt werden müssen.

Darüber hinaus müssen Zertifikatsnehmer der Sub-CA von COUNT+CARE GmbH & Co. KG auch noch die weiteren Regelungen aus den folgenden Abschnitten berücksichtigen.

Die Einhaltung der Sicherheitsanforderungen ist Voraussetzung für die Ausstellung von Zertifikaten durch die Sub-CA von COUNT+CARE GmbH & Co. KG und wird durch die Prüfung geeigneter Nachweise sichergestellt.

7.1 Behandlung von Vorfällen und Kompromittierung

Bei der Kompromittierung (oder dem begründeten Verdacht) eines privaten Schlüssels muss das dazugehörige Zertifikat unverzüglich gesperrt werden. Die Sperrhotline der Sub-CA von COUNT+CARE GmbH & Co. KG kann wie folgt erreicht werden:

- RA_Operator@countandcare.de (falls initial mitgeteiltes Sperr-Passwort bekannt ist und es sich nicht um eine systemkritische Zertifikatssperrung handelt, z.B. EMT). Bitte senden Sie hierzu eine S/MIME mit einem entsprechenden Sperrgrund inkl. dem bekannten Initial erhaltenen Sperr-Passwort an diesen Postkorb.

- CA_Operator@countandcare.de (falls initiales Passwort nicht bekannt oder wenn es sich um eine systemkritische Zertifikatssperrung handelt, z.B. GWA). Bitte senden Sie hierzu eine S/MIME mit einem entsprechenden Sperrgrund an diesen Postkorb.

Hinweis: Das initial mitgeteilte Sperr-Passwort wurde dem PKI-Teilnehmer bei der Übermittlung des Erstzertifikats per S/MIME durch den RA-Operator mit gesendet.

7.2 Meldepflichten

Die Sub-CA von COUNT+CARE GmbH & Co. KG kommt ihren Meldepflichten über Veröffentlichungen auf der Webseite der Sub-CA (siehe Abschnitt 3.5) nach.

Auf der Webseite werden durch die Sub-CA von COUNT+CARE GmbH & Co. KG Meldungen zu folgenden Ereignissen veröffentlicht:

- Änderungen an der Certificate Policy der Sub-CA von COUNT+CARE GmbH & Co. KG
- Änderungen übergeordneten Regelungen wie der Certificate Policy der Smart Metering PKI, der [TR-03109-4] oder der [TR-03116-3]
- Ereignisse, die ggf. den Betrieb der Sub-CA einschränken oder gefährden können

7.3 Notfallmanagement

Die Sub-CA verfügt über etabliertes und dokumentiertes Notfallmanagement, dass unter ca_operator@countandcare.de kontaktiert werden kann.

Im Rahmen des Notfallmanagements sind Notfallorganisation, Benachrichtigungsketten und Ausweichstandorte (Rechenzentren und Büroflächen) definiert. Außerdem sind zu folgenden Szenarien konkrete Notfallpläne zur Behandlung vorhanden.

- Kompromittierung des privaten Schlüssels
- Entdeckte Schwachstellen in den verwendeten kryptografischen Verfahren
- Nichtverfügbarkeit von Sperrlisten als Nutzer
- Schwachstellen in genutzten sicherheitsrelevante Algorithmen
- Ungeplanter Schlüsselwechsel einer Zertifizierungsstellen
- Nichtverfügbarkeit von Sperrlisten als Bereitsteller
- Wiederherstellung von Daten, Schlüssel und Betriebsmittel, insbesondere Registrierungs-, Zertifizierungs-, und Sperrlisteninformationen
- Notfallpläne zur Reaktivierung der CA

Zusätzlich gibt es die allgemeineren Notfallpläne der IT.

In Rahmen der Notfallpläne sind Meldeketten, umgesetzte Vorbeugemaßnahmen sowie zu ergreifende Sofortmaßnahmen und Behebungsmaßnahmen dokumentiert. Auch durchzuführende Informationspflichten, z.B. an Kunden oder Behörden, sind dokumentiert.

8. Technische Sicherheitsanforderungen

Für die Teilnahme an der SM-PKI müssen die PKI-Teilnehmern auch die Technischen Sicherheitsanforderungen aus der Certificate Policy der SM-PKI (siehe [CP] Abschnitt 6) entsprechend der Anforderungen für ihrer PKI-Rolle erfüllen.

Darüber hinaus sind als Zertifikatsnehmer der Sub-CA von COUNT+CARE GmbH & Co. KG auch noch spezifischen Regelungen in den folgenden Abschnitten zu berücksichtigen.

Die Einhaltung der Sicherheitsanforderungen ist Voraussetzung für die Ausstellung von Zertifikaten durch die Sub-CA von COUNT+CARE GmbH & Co. KG und wird durch die Prüfung geeigneter Nachweise sichergestellt.

8.1.1 Lieferung öffentlicher Zertifikate

Von der Sub-CA von COUNT+CARE GmbH & Co. KG ausgestellte Zertifikate werden im Verzeichnisdienst abgelegt und sind somit für alle PKI-Teilnehmer zugänglich, Informationen zum Verzeichnisdienst finden sich im Kapitel 4.1.

8.1.2 Backup privater Schlüssel

EMTs, die Endbenutzerzertifikate von der Sub-CA von COUNT+CARE GmbH & Co. KG beziehen möchten, müssen Backups ihrer privaten Schlüssel gemäß den Vorgaben der Certificate Policy der SM-PKI für GWAs durchführen (siehe [CP] Abschnitt 6.2.3).

9. Profile für Zertifikate und Sperrlisten

Es gelten die Vorgaben und Regelungen der Certificate Policy der SM-PKI (siehe [CP] Abschnitt 7).

10. Überprüfung und andere Bewertungen

Überprüfungen und Bewertungen durch die Sub-CA von COUNT+CARE GmbH & Co. KG finden gemäß den Vorgaben der Certificate Policy der SM-PKI (siehe [CP] Abschnitt 8) statt.

11. Sonstige finanzielle und rechtliche Regelungen

11.1 Preise

Die Konditionen über das Servicemanagement der COUNT+CARE GmbH & Co KG über Servicemanagement-IT@countandcare.de erfragt werden.

11.2 Finanzielle Zuständigkeiten

Der Betreiber der CC Smart Metering Sub-CA ist die COUNT+CARE GmbH & Co KG. Sie ist finanziell eigenständig und unabhängig.

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

A Anhang

Die Anhänge A-D der Certificate Policy der SM-PKI sind umgesetzt (siehe [CP] Anhang A ff.)

B Literatur

[CP] BSI: Certificate Policy der Smart Metering PKI (Root-CA) Version 1.1.1

[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-03109-4] 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-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