Vertraulichkeitsstufe: Öffentlich (C1)

Stromnetz Hamburg

Certificate Policy der SNH-Metering-CA

Datum 02.11.2018

Stromnetz Hamburg GmbH

Bramfelder Chaussee 130

22177 Hamburg

pki.metering@fhh-infra.de

pki.metering.fhh-infra.de

Unser Netz für Ihre Energie

Änderungshistorie

Version	Datum	Historie
1.1	**05.05.2017**	**Version für Wirkbetrieb**
1.2	**22.06.2017**	**Einarbeitung Anmerkungen Root-CA, Abschnitte** 3.6 Suspendierung 4.8 Sperrung und Suspendierung von Zertifikaten
1.2	**30.08.2017**	**Version zur Veröffentlichung**
1.3	**19.10.2017**	**Anpassung Kapitel** Kap. 1.2 Ergänzung OID Wirk-PKI Kap. 1.1 Abs.3 Überblick Kap. 4.3 Annahme von Zertifikaten Kap. 4.7 Änderung von Zertifikaten Kap. 6.3.2 Allgemeine Gültigkeitszeitraum von Zertifikaten und Schlüsselpaaren Kap.10 Referenzdokumente
1.4	**27.10.2017**	**Anpassung Kapitel** Kap. 1.1 Klarstellung zur Regelung der Informationssicherheit in Lieferantenbeziehungen
1.5	**01.11.2017**	**Anpassung Kapitel 3.2.5** Verpflichtung Vertragskunde bei Zertifizierungsentzug
1.6	**23.11.2017**	**Anpassung Kapitel** Kap. 1.1 Klarstellung der Konformität zur SM-PKI Policy Kap. 4.8 Aktualisierung der Verweise in Sperrung und Suspendierung
1.6.1	**12.01.2018**	**Redaktionelle Änderungen**
1.6.2	**02.11.2018**	**Verweise aktualisiert**

Inhalt Seite

Abkürzungsverzeichnis

AGB	Allgemeine Geschäftsbedingungen
BSI	Bundesamt für Sicherheit in der Informationstechnik
CA	Certification Authority
CC	Common Criteria
CN	Common Name
CP	Certificate Policy
CPS	Certificate Practice Statement
CRL	Certificate Revocation List / Zertifikatssperrliste
CSIG	Certificate for Signature / Signaturzertifikat
CTLS	Certificate for TLS / TLS-Zertifikat
EMT	Externer Marktteilnehmer
GWA	Gateway – Administrator
GWH	Gateway – Hersteller
HSM	Hardware Sicherheitsmodul
ISMS	Information Security Management System
ISO	International Organization for Standardization
KEK	Key Encryption Key
LDAP	Lightweight Directory Access Protocol
OCSP	Online Certificate Status Protocol
PIN	Personal Identification Number
PKI	Public Key Infrastructure
RA	Registration Authority
SMGW	Smart Meter Gateway – Kommunikationseinheit eines intelligenten Messsystems
SM-PKI	Smart Metering Public Key Infrastructure
SNH	Stromnetz Hamburg GmbH
SSL	Secure Sockets Layer
Sub-CA	Sub Certification Authority
TLS	Transport Layer Security
TR	Technische Richtlinie

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. Zur Unterstützung dieses Ziels werden intelligente Messsysteme eingesetzt.

Zur Absicherung der Kommunikation ist eine gegenseitige Authentisierung der Kommunikationspartner erforderlich. Die Kommunikation erfolgt dabei stets über einen verschlüsselten und integritätsgesicherten Kanal. Damit die Authentizität und die Vertraulichkeit der Kommunikation der einzelnen Marktteilnehmer untereinander gesichert sind, wird eine Smart Metering Public Key Infrastruktur (SM-PKI) etabliert. Aus diesem Grund betreibt die Stromnetz Hamburg GmbH, im Folgenden SNH genannt, eine Sub-CA in der SM-PKI unterhalb der Root-CA. SNH erfüllt die Anforderungen aus der [CP-Root-CA] und der technischen Richtlinie [TR-03145-1] des BSI.

Die Sub-CA der SNH wird im Folgenden **SNH-Metering-CA** genannt.

1.1 Überblick

Dieses Dokument richtet sich an die Zertifikatsnehmer (Endnutzer) der SNH-Metering-CA und ist in Anlehnung an die SM-PKI Policy der Root CA [CP-Root-CA] strukturiert und definiert.

Diese Certificate Policy (CP) der SNH-Metering-CA unterwirft sich der SM-PKI Policy [CP-Root-CA] und beschreibt die Vorgaben der SNH-Metering-CA und deren Umsetzung.

Die Stromnetz Hamburg GmbH behält sich vor, Aufgaben oder Teilaufgaben von beauftragten Unternehmen ausführen zu lassen. Diese unterliegen den Regelungen zur Informationssicherheit in Lieferantenbeziehungen der Stromnetz Hamburg, welche bei den Zertifizierungen nach ISO2001/TR-03145 entsprechend berücksichtigt wurden.

Endnutzer der SNH-Metering-CA können nur jene Organisationen werden, welche vor der Ausstellung von Zertifikaten über einen Vertrag mit der Stromnetz Hamburg GmbH verfügen, nachfolgend auch als Vertragskunde bezeichnet. Die vertraglichen Verpflichtungen werden mit den Vertragskunden abgestimmt.

Im Vertrag mit dem Endnutzer wird zwischen der Teilnahme am Testbetrieb und am Wirkbetrieb der SNH-Metering-CA unterschieden. Jeder Endnutzer, der am Wirkbetrieb der SNH-Metering-CA teilnimmt, MUSS zuvor erfolgreich am Testbetrieb der SNH-Metering-CA teilgenommen haben.

Während die CP der SNH-Metering-CA die technischen, personellen und organisatorischen Sicherheitsanforderungen für die Ausstellung von GWA-, GWH-, EMT- und SMGW-Zertifikaten für Endnutzer beschreibt, ergeben sich Rechte und Pflichten allgemeinerer Art, die mit den Vertragskunden im Rahmen der Vertragsgestaltung geregelt werden.

1.2 Name und Identifizierung des Dokuments

Dieses Dokument ist die CP und kann über die folgenden Informationen identifiziert werden.

Tabelle 1 Identifikation des Dokuments

Identifikator	Wert
Titel	Certificate Policy der SNH-Metering-CA
Version	1.6.2
OID	1.3.6.1.4.1.48082.1.2 (Wirk-PKI) 1.3.6.1.4.1.48082.1.1 (Test-PKI)
Organisation	Stromnetz Hamburg GmbH

Das vorliegende Dokument kann bezogen werden unter https://pki.metering.fhh-infra.de.

Sollten sich Änderungen an dem vorliegenden Dokument ergeben wird eine neue Version erstellt und unter oben angegebener Adresse veröffentlicht.

Alle autorisierten Ansprechpartner werden per signierte E-Mail über Updates informiert. Die informierten Ansprechpartner sind dazu verpflichtet die Einhaltung der neuen Version zu bestätigen. Sollte nach der in der E-Mail angegebenen Frist keine Bestätigung über die Einhaltung von mindestens einem Ansprechpartner eines PKI-Teilnehmers bei der Stromnetz Hamburg GmbH eingehen, wird der Service für den jeweiligen PKI-Teilnehmer deaktiviert. Eine Aktivierung bei nachfolgendem Eingang der Bestätigung ist möglich.

1.3 PKI – Teilnehmer

Die Teilnehmer der SNH-Metering-CA müssen die Anforderungen aus der [CP-Root-CA] erfüllen. Aus diesem Grund wird auf die entsprechenden Kapitel der [CP-Root-CA] verwiesen.

1.3.1 Zertifizierungsstelle

Es gelten die Inhalte aus dem entsprechenden Kapitel der [CP-Root-CA].

1.3.2 Registrierungsstelle

Es gelten die Inhalte aus dem entsprechenden Kapitel der [CP-Root-CA].

1.3.3 Endnutzer der SNH-Metering-CA

Es gelten die Inhalte aus dem entsprechenden Kapitel der [CP-Root-CA].

1.3.4 Zertifikatsnutzer

Es gelten die Inhalte aus dem entsprechenden Kapitel [CP-Root-CA].

1.3.5 Andere Teilnehmer

Es gelten die Inhalte aus dem entsprechenden Kapitel der [CP-Root-CA].

1.4 Verwendung von Zertifikaten

Die erlaubte und verbotene Verwendung von Zertifikaten in der SM-PKI wird in [CP-Root-CA] beschrieben (siehe Abschnitt 1.4). Es gibt keine weiteren Einschränkungen der Verwendung durch die Stromnetz Hamburg GmbH.

1.5 Administration der Certificate Policy

Die für dieses Dokument verantwortliche Organisation ist die Stromnetz Hamburg GmbH und kann über folgende Adresse kontaktiert werden:

Tabelle 2: Kontaktdaten der CP der SNH-Metering-CA

Organisation	Stromnetz Hamburg GmbH
Abteilung	Metering Auftragssteuerung
Adresse	Bramfelder Chaussee 130, 22177 Hamburg
E-Mail Adresse	pki.metering@fhh-infra.de
Webseite	https://pki.metering.fhh-infra.de

1.6 Pflege der Certificate Policy

Jede aktualisierte Version dieser Certificate Policy der SNH-Metering-CA wird den Anwendern unverzüglich über die in Kapitel 1.5 angegebene Webseite zur Verfügung gestellt.

Auch jede Aktualisierung der [CP-Root-CA] hat Auswirkungen auf diese CP. Die aktuelle [CP-Root-CA] wird durch das BSI auf der jeweiligen Webseite veröffentlicht.

2 Verantwortlichkeit für Veröffentlichungen und Verzeichnisse

2.1 Verzeichnisse

Ausgestellte und noch gültige Zertifikate der SNH-Metering-CA werden in einem eigenständigen Lightweight Directory Access Protocol Verzeichnis (LDAP-Verzeichnis) geführt. Das LDAP-Verzeichnis für die Wirk-PKI ist unter ldap.metering.fhh-infra.de zu erreichen, für die Test-PKI ist ldap-ext.metering.fhh-infra.de vorgesehen.

Außerdem wird unter ldap.metering.fhh-infra.de bzw. ldap-ext.metering.fhh-infra.de die jeweilige Sperrliste veröffentlicht, in der alle gesperrten Zertifikate der SNH-Metering-CA während ihres Gültigkeitszeitraums aufgeführt sind.

2.2 Veröffentlichung von Informationen zur Zertifikatserstellung

Auf der Webseite der SNH-Metering-CA (siehe Abschnitt 1.5) sind die veröffentlichungspflichtigen Informationen gemäß [CP-Root-CA] aufgeführt.

2.3 Zeitpunkt und Häufigkeit der Veröffentlichungen

Zeitpunkt und Frequenz von Veröffentlichungen der SNH-Metering-CA richten sich nach den Vorgaben der [CP-Root-CA].

2.4 Zugriffskontrollen auf Verzeichnisse

Der lesende Zugriff auf das LDAP-Verzeichnis der SNH-Metering-CA ist über eine zertifikatsbasierte Authentisierung mittels TLS-Zertifikaten auf die Teilnehmer der SM-PKI beschränkt.

Der Verzeichnisdienst der Sub-CA der SNH ist so konfiguriert, dass die Anzahl der zurückgegebenen Suchergebnisse begrenzt ist, um den Massenabruf von Zertifikaten zu verhindern.

Der lesende Zugriff auf die Sperrlisten der SNH-Metering-CA erfolgt ohne Authentifikation und ohne Einschränkungen.

3 Identifizierung und Authentifizierung

Dieses Kapitel beschreibt die Prozeduren, um die Identität und die Berechtigungen eines Antragstellers (EMT, GWA, GWH oder SMGW) vor dem Ausstellen eines Zertifikats festzustellen. Zertifikatsrequests müssen konform zur [CP-Root-CA] gestellt werden.

3.1 Regeln für die Namensgebung

Für die Namensgebung werden die Regelungen aus Abschnitt 3.1 der [CP-Root-CA] angewendet.

3.2 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 8.1 der [CP-Root-CA].

3.2.1 Methoden zur Überprüfung bzgl. Besitz des privaten 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 SNH-Metering-CA geprüft.

3.2.2 Authentifizierung von Organisationszugehörigkeiten

Alle berechtigten Teilnehmer (EMT, GWA, SMGW und GWH) können Zertifikatsanträge bei der SNH-Metering-CA stellen.

Für alle Anträge EMT, GWA und GWH gilt:

1. Die Identität eines Antragstellers wird anhand seines Organisationsnamens und der im Antrag angegebenen Nummer des Unternehmensnachweises (i.d.R. des Handelsregisters) bestimmt.
2. Wenn ein zweiter Antrag von einem bereits registrierten Antragsteller eingeht, werden die Registrierungsdaten aus beiden Anträgen zusammengeführt.
3. Ein weiterer Antrag eines Antragsstellers zur selben Rolle (EMT, GWA, GWH) ist nur dann möglich, wenn
    a. Das Zertifikat zum vorangegangenen Antrag aufgegeben werden soll (z.B. durch Ablauf des Gültigkeitszeitraums oder durch Sperrung) und der weitere Antrag neue Registrierungsdaten erhält (z.B. ein anderer Common Name (CN)).
    b. Das Vorgängerzertifikat abgelaufen ist.
4. Ein weiterer Antrag eines Antragsstellers zu einer anderen Rolle ist möglich und erfordert ein eigenes Registrierungsverfahren.

Zur initialen Autorisierung als EMT, GWA, GWH oder SMGW müssen die notwendigen Unterlagen und Daten für die Registrierung eingereicht werden. Die notwendigen Unterlagen und Daten sind dem Abschnitt 3.2.2 der [CP-Root-CA] zu entnehmen.

3.2.3 Anforderungen zur Identifizierung und Authentifizierung des Zertifikats-Antragstellers

Zertifikatsrequests dürfen nicht von Einzelpersonen (natürliche Personen), sondern müssen 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 Überprüfte Angaben zum Endnutzer

Die Registrierungsstelle der SNH-Metering-CA prüft die Korrektheit der Angaben zum Endnutzer im Zertifikatsrequest gegenüber den eingereichten Unterlagen. Diese sind in dieser CP im Abschnitt 3.2.2 aufgeführt.

3.2.5 Aktualisierung / Anpassung der Registrierungsinformationen der Endnutzer

Jeder Teilnehmer an der SM-PKI muss der SNH-Metering-CA unverzüglich mitteilen, falls sich Änderungen bzgl. seiner Registrierungsdaten ergeben. Ergänzend fragt die SNH-Metering-CA jährlich über die Ansprechpartner des Vertragskunden an, ob Änderungen an den Registrierungsdaten vorliegen.

Zusätzlich verpflichtet sich der Vertragskunde beim Entzug der Zertifizierung die Mitarbeiter der SNH-Metering-CA rechtzeitig zu informieren.

3.3 Schlüsselerneuerung (Routinemäßiger Folgeantrag)

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

Für die Behandlung von routinemäßigen Folgeanträgen durch die SNH-Metering-CA gelten die Regelungen aus der [CP-Root-CA] (siehe Abschnitt 3.3).

Routinemäßige Folgeanträge müssen spätestens 4 Wochen vor Ablauf des vorherigen Zertifikats an die SNH-Metering-CA gestellt werden.

3.4 Schlüsselerneuerung (nicht routinemäßiger Folgeantrag)

Ein nicht routinemäßiger Folgeantrag liegt vor, wenn die Bedingungen aus der [CP-Root-CA] (Abschnitt 3.4.1) erfüllt sind. Entsprechend müssen die Maßnahmen aus diesem Abschnitt durchgeführt werden.

3.5 Sperrung

Die SNH-Metering-CA bietet nur die in [CP-Root-CA] (siehe Abschnitt 3.5) geforderten Verfahren zur Sperrung von Zertifikaten an; es werden keine zusätzlichen Verfahren zur Initiierung einer Sperrung unterstützt.

3.6 Suspendierung

Das Verfahren zur Suspendierung der Zertifikate eines SMGW kann der [CP-Root-CA] im Abschnitt 3.6 entnommen werden.

Für die SNH-Metering-CA ist eine Suspendierung von Zertifikaten derzeit nicht vorgesehen. Die Funktionalität wird entsprechend der vorgegebenen Umsetzungsfristen implementiert, spätestens jedoch bis zum 01.03.2018.

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 Zertifikatsanträge und
- Zertifikatsausstellung

Für die gesicherte personenbezogene Kommunikation ist der Einsatz von $C_{S/MIME}$(ASP)-Zertifikaten für alle beteiligten Parteien Voraussetzung. Relevante personenbezogene Kommunikation muss verschlüsselt und signiert erfolgen. E-Mails an zentrale Postfächer (ohne sicherheitskritischen Inhalt) können auch ohne Signatur und Verschlüsselung versendet werden.

4.1 Zertifikatsantrag

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

4.1.1 Wer kann einen Zertifikatsantrag stellen?

Ein Zertifikatsantrag darf ausschließlich von einer befugten Organisation (GWA, GWH oder EMT) gestellt werden, die sich gemäß Abschnitt 3.2.2 der [CP-Root-CA] identifiziert haben muss.

4.1.2 Beantragungsprozess und Zuständigkeiten

Für die Bearbeitung eines Zertifikatsantrags ist die Registration Authority (RA) der SNH-Metering-CA verantwortlich.

4.2 Verarbeitung von initialen Zertifikatsanträgen

Die Prozesse zur „Durchführung der Identifizierung und Authentifizierung“ sowie zur „Annahme oder Ablehnung von initialen Zertifikatsanträgen“ erfolgen bei der SNH-Metering-CA gemäß den Regelungen der [CP-Root-CA] (siehe Abschnitte 4.3.1 und 4.3.2).

4.2.1 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. Eine situationsbedingte Abweichung von den angegebenen Werten bei Ausgabe von Folge- bzw. Ersatzzertifikaten ist möglich.

Die Bearbeitung der Zertifikatsanträge gliedert sich in folgende Arbeitsschritte:

Tabelle 3: Zeitablauf für die initiale Ausgabe von Endnutzer Zertifikaten

Arbeitsschritt	Beschreibung	Zeitrahmen
1	Start des Beantragungsprozesses durch den Endnutzer (GWA, GWH oder EMT)	
2	Kontaktaufnahme zur Terminvereinbarung durch die SNH-Metering-CA	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	
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 SNH-Metering-CA inkl. Rückmeldung an den Endnutzer	1 Kalenderwoche
7	Ausstellung der Zertifikate für den Endnutzer	2 Arbeitstage

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 entsprechend verlängern.

4.2.2 Ausgabe von Zertifikaten

Die Ausgabe von Endnutzer-Zertifikaten erfolgt über die Web-Service-Schnittstelle. Ein Versand von Endnutzer-Zertifikaten per E-Mail an den Ansprechpartner der berechtigten Organisation ist nur bei der initialen Ausstellung von Zertifikaten vorgesehen.

4.2.3 Benachrichtigung des Endnutzers über die Ausgabe des Zertifikats

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

4.3 Annahme von Zertifikaten

Die Angaben der Endnutzer-Zertifikate müssen nach Erhalt durch den Ansprechpartner des Endnutzers auf Korrektheit und Vollständigkeit geprüft werden. Bei einem SMGW muss die Prüfung durch den GWA oder den GWH (automatisiert) z.B. bei Erhalt oder der Einbringung der Zertifikate erfolgen. Um ein Zertifikat zurückzuweisen, muss ein Ansprechpartner des Endnutzers eine Nachricht an den RA der SNH-Metering-CA senden (Kontaktadresse siehe Abschnitt 1.5). In der Nachricht ist der Grund für die Verweigerung der Annahme anzugeben. Bei fehlerhaften Zertifikaten sind die fehlerhaften bzw. unvollständigen Einträge zu benennen.

4.3.1 Veröffentlichung von Zertifikaten durch die CA

Alle ausgestellten Zertifikate werden direkt nach der Ausstellung im LDAP-Verzeichnisdienst der SNH-Metering-CA veröffentlicht.

4.4 Verwendung von Schlüsselpaar und Zertifikat

4.4.1 Verwendung des privaten Schlüssels und des Zertifikats durch den Endnutzer

Zertifikate und die zugehörigen privaten Schlüssel müssen gemäß ihrem Verwendungszweck eingesetzt werden, siehe [TR-03109-4]. Die Regelungen der Abschnitte 5.1 und 5.2 der [CP-Root-CA] sind anzuwenden.

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]. Es gilt insbesondere die Zertifikatsvalidierung.

4.5 Zertifikatserneuerung

Zertifikatserneuerung bedeutet das Ausstellen eines neuen Zertifikats für einen öffentlichen Schlüssel, der bereits identifiziert wurde.

Zertifikatserneuerungen dürfen gemäß den Vorgaben der [CP-Root-CA] nicht erfolgen und werden daher von der SNH-Metering-CA nicht angeboten. Fristen sind dem Abschnitt 3.3 dieser CP zu entnehmen.

4.6 Zertifizierung nach Schlüsselerneuerung

Bei der SNH-Metering-CA erfolgt die Zertifizierung nach Schlüsselerneuerung gemäß den Vorgaben im Abschnitt 4.6 der [CP-Root-CA].

4.7 Änderungen am Zertifikat

Änderungen an den Zertifikatsinhalten, abgesehen vom Schlüsselmaterial und den Seriennummern im SubjectDN, sind nicht vorgesehen. Bei Änderungsbedarf, z.B. durch eine Umfirmierung eines Endnutzers, muss ein neues initiales Zertifikat gemäß Abschnitt 3 dieser CP beauftragt und das alte Zertifikat gesperrt werden.

4.8 Sperrung und Suspendierung von Zertifikaten

Eine Suspendierung von Zertifikaten stellt einen Spezialfall der Sperrung dar. Suspendierte Zertifikate müssen in die Sperrliste aufgenommen und speziell gekennzeichnet werden, gemäß [TR-03109-4].

Bei suspendierten Zertifikaten kann die Sperrung innerhalb von 30 Tagen für die Beantragung von neuen Zertifikaten wieder zurückgenommen werden. Einmal suspendierte Zertifikate werden spätestens nach Ablauf dieser Frist endgültig gesperrt. Hierbei gelten die Vorgaben aus Abschnitt 4.8.2 der [CP-Root-CA].

Die Initiierung der Sperrung eines Zertifikats kann durch den Endnutzer bei der SNH-Metering-CA eingeleitet werden. Alle Sperrungen werden nach einer positiven inhaltlichen Prüfung unverzüglich umgesetzt, in die Sperrliste aufgenommen und gemäß den Vorgaben der [CP-Root-CA] veröffentlicht. Bei jedem Sperrvorgang prüft die SNH-Metering-CA die Sperranträge und bindet bei einem systemrelevanten Vorfall die Root-CA ein. Alle Teilnehmer müssen gemäß den Vorgaben der [CP-Root-CA] immer die aktuelle Sperrliste verwenden. In besonderen Fällen (Erstinbetriebnahme oder auf Aufforderung durch die SNH-Metering-CA) müssen neben den regelmäßigen Aktualisierungen auch neue Sperrlisten abgefragt werden. Ist die Sperrliste für einen Endnutzer nicht verfügbar, muss der registrierte Ansprechpartner unmittelbar Kontakt mit der SNH-Metering-CA aufnehmen. Dies gilt auch, falls gesperrte Zertifikate nach zwei Tagen nicht in die Sperrliste aufgenommen wurden.

4.9 Service zur Statusabfrage von Zertifikaten

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

4.10 Terminierung der Sub-CA

Bei der Auflösung der SNH-Metering-CA werden alle registrierten Teilnehmer durch die SNH-Metering-CA mindestens 14 Tage vor Terminierung schriftlich informiert. Die SNH-Metering-CA wird allen Teilnehmer eine Nachfolge CA vorschlagen. Nach Ablauf der Frist leitet die SNH-Metering-CA bei der Root-CA die Selbstsperrung ein. Hierbei kommen die Verfahren aus Abschnitt 5.2.7 dieser CP zur Anwendung.

5 Organisatorische, betriebliche und physikalische Sicherheitsanforderungen

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

5.1 Generelle Sicherheitsanforderungen

Die generellen Sicherheitsanforderungen an die PKI-Teilnehmer sind der [CP-Root-CA] (siehe Abschnitt 5.1) zu entnehmen. Diese bilden den Sicherheitsrahmen für die PKI-Teilnehmer.

5.1.1 Erforderliche Zertifizierungen der PKI-Teilnehmer

Es gelten die Vorschriften der [CP-Root-CA] aus Abschnitt 5.1.1.

5.1.2 Anforderungen an die Zertifizierung gemäß ISO/IEC 27001

Es gelten die Vorschriften der [CP-Root-CA] aus Abschnitt 5.1.2.

5.2 Erweiterte Sicherheitsanforderungen

5.2.1 Betriebsumgebung und Betriebsabläufe

Die Anforderungen an die Sicherheit der Betriebsumgebung und der Betriebsabläufe für die Endnutzer der SNH-Metering-CA entsprechen den Vorgaben aus der [CP-Root-CA], sowie den Anforderungen an den GWA aus [TR-03109-6].

5.2.2 Verfahrensanweisungen

Die Vorgaben aus der [CP-Root-CA] sind für alle Teilnehmer der SM-PKI relevant und müssen umgesetzt werden.

Für den Betrieb der GWA-Umgebung müssen zusätzlich alle Anforderungen aus [TR-03109-6] umgesetzt werden.

5.2.3 Personal

Es gelten die Anforderungen aus dem Abschnitt 5.2.3 der [CP-Root-CA].

5.2.4 Monitoring

Die Anforderungen aus der [CP-Root-CA] werden entsprechend umgesetzt.

5.2.5 Archivierung von Aufzeichnungen

Die SNH-Metering-CA verfügt über angemessene Archivierungsfunktionen. Die Zeiträume sind gemäß [CP-Root-CA] ausgestaltet.

5.2.6 Schlüsselwechsel einer Zertifizierungsstelle

Das Verfahren ist im Abschnitt 5.2.6 der [CP-Root-CA] beschrieben.

5.2.7 Auflösen einer Zertifizierungsstelle

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

- Übertragung der Aufgaben und Verpflichtungen: Die SNH hält ihre Aufgaben und Verpflichtungen für einen Übergangszeitraum aufrecht oder trägt Sorge dafür, dass diese bei einer endgültigen Auflösung, von einer Nachfolgeorganisation übernommen werden.
- Informationspflicht: Im Falle einer Auflösung informiert die SNH alle beteiligten Teilnehmer, sowie weitere Organisationen, mit denen Vereinbarungen bestehen, rechtzeitig vor der Kündigung der Dienstleistung. Insbesondere die Root-CA wird in den Auflösungsprozess eingebunden.
- Zerstörung von Schlüssel- und Zertifikatsinformationen: Nach Einstellung der Tätigkeit werden alle privaten Schlüssel einschließlich der Zertifikatsinformationen und

zugehörige Kundendaten zerstört. Alle ausgegebenen Zertifikate werden mit einer Frist von 14 Tagen widerrufen.

5.2.8 Aufbewahrung der privaten Schlüssel

Es gelten die Vorgaben aus Abschnitt 5.2.8 der [CP-Root-CA].

5.2.9 Behandlung von Vorfällen und Kompromittierung

Die Anforderungen aus [CP-Root-CA] (Abschnitt 5.2.9) werden erfüllt.

5.2.10 Meldepflichten

Es gelten die Vorgaben aus Abschnitt 5.2.10 [CP-Root-CA] und die Vorgaben aus Abschnitt 5.2.7 der CP der SNH-Metering-CA.

5.3 Notfall-Management

Es gelten die Vorgaben aus Abschnitt 5.3 [CP-Root-CA].

6 Technische Sicherheitsanforderungen

6.1 Erzeugung und Installation von Schlüsselpaaren

Jeder Endnutzer generiert sein eigenes Schlüsselpaar.

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 SNH-Metering-CA stellt sicher, dass die folgenden Anforderungen umgesetzt werden:

- Das Schlüsselpaar wird während der Schlüsselzeremonie im Vier-Augen-Prinzip unter Teilnahme des für den Schlüssel verantwortlichen Mitarbeiters generiert
- 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 aller Endnutzer in den HSM Modulen ist durch eine 2-Faktor-Authentisierung geschützt

6.1.2 Lieferung privater Schlüssel

Es erfolgt keine Lieferung von privaten Schlüsseln durch die SNH-Metering-CA.

6.1.3 Lieferung öffentlicher Zertifikate

Alle Zertifikate werden unmittelbar nach der Ausstellung in den LDAP-Verzeichnissen der SNH-Metering-CA veröffentlicht.

6.1.4 Schlüssellänge und kryptographische Algorithmen

Die SNH-Metering-CA hält sich bei der Erstellung von Zertifikaten an die Vorgaben der [TR-03116-3] für zu verwendende kryptographische Algorithmen und Schlüssellängen.

6.1.5 Festlegung der Parameter der Schlüssel und Qualitätskontrolle

Es gelten die Vorgaben aus der [CP-Root-CA] gemäß Abschnitt 6.1.5.

6.1.6 Verwendungszweck der Schlüssel

Der Verwendungszweck der Schlüssel wird eingehalten, siehe [CP-Root-CA] Abschnitte 1.4.1 und 1.4.2.

6.2 Anforderungen an kryptographische Module

Die Stromnetz Hamburg GmbH verwendet Hardware-Sicherheitsmodule (HSM) zur Generierung, Speicherung und Nutzung ihrer privaten Schlüssel zu ihren Zertifikaten aus der SM-PKI. Die Sicherheitsanforderungen an Kryptographiemodule zum Schutz der privaten Schlüssel zu den Zertifikaten der SM-PKI sind in Kapitel 6.2.10 beschrieben.

Weiterhin ist der sichere Umgang mit den privaten Schlüsseln sichergestellt. Die Anforderungen an den Lebenszyklus und die Einsatzumgebung aus [KeyLifecSec] – Security Level 2 werden eingehalten.

6.2.1 Mehrpersonen-Zugriffssicherung zu privaten Schlüsseln

Das Schlüsselmanagement der SNH-Metering-CA 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

Die Daten der privaten Schlüssel werden nach den Anforderungen aus Kapitel 5 der [CP-Root-CA] zur sicheren Handhabung und Lagerung von Schlüsselmaterial gespeichert.

6.2.3 Backup privater Schlüssel

Es gelten die Vorgaben aus der [CP-Root-CA] gemäß Abschnitt 6.2.3.

6.2.4 Archivierung privater Schlüssel

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

6.2.5 Transfer privater Schlüssel in oder aus kryptografischen Modulen

Es gelten die Vorgaben aus der [CP-Root-CA] gemäß Abschnitt 6.2.5.

6.2.6 Speicherung privater Schlüssel in kryptographischen Modulen

Es gelten die Vorgaben aus der [CP-Root-CA] gemäß Abschnitt 6.2.6.

6.2.7 Aktivierung privater Schlüssel

Die Aktivierung eines Schlüssels in einem HSM erfolgt unter Einhaltung des Vier-Augen-Prinzips.

6.2.8 Deaktivierung privater Schlüssel

Deaktivierte Schlüssel der SNH-Metering-CA werden nicht genutzt.

Gründe für einen deaktivierten Schlüssel können sein:

- Der Schlüssel ist für eine zukünftige Nutzung vorgesehen, die erst ab einem bestimmten Datum beginnt.
- Ein Schlüssel wird nicht mehr verwendet, da er durch einen Nachfolgeschlüssel ersetzt wurde.
- Ein Schlüssel wird aus weiteren Gründen für einen bestimmten Zeitraum nicht genutzt.

6.2.9 Zerstörung privater Schlüssel

Es gelten die Vorgaben aus der [CP-Root-CA] gemäß Abschnitt 6.2.9.

6.2.10 Beurteilung kryptographischer Module

Die in Kapitel 6.2 der [CP-Root-CA] definierten Sicherheitsanforderungen an Kryptographiemodule zum Schutz der privaten Schlüssel zu den Zertifikaten werden durch die SNH-Metering-CA erfüllt.

6.3 Andere Aspekte des Managements von Schlüsselpaaren

6.3.1 Archivierung öffentlicher Schlüssel

Ausgegebene Zertifikate werden in der Datenbank der SNH-Metering-CA inkl. der Statusdaten gespeichert. Diese unterliegt der Standard-Datensicherung.

6.3.2 Allgemeiner Gültigkeitszeitraum von Zertifikaten und Schlüsselpaaren

Die Laufzeit von Schlüsseln und Zertifikaten ist in der [TR-03109-4] Kapitel 3.2 geregelt.

Die folgende Tabelle gibt die Zertifikatslaufzeiten der übrigen Zertifikate verbindlich vor:

Tabelle 4: Laufzeiten von Zertifikaten in der SM-PKI

Zertifikat	Gültigkeitszeitraum
Root-CRL-Signer-Zertifikat	4 Jahre
Root-TLS-Signer-Zertifikat	4 Jahre
Sub-CA-Zertifikat	5 Jahre
TLS-Zertifikate der Root-CA und der Sub-CA	2 Jahre
Endnutzerzertifikat (TLS/Sign/Enc) Ausnahme GWA	2 Jahre
GWA-Zertifikat (TLS/Sign/Enc)	3 Jahre

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

Tabelle 5 Intervall Zertifikatswechsel der Root-CA / Sub-CA

Instanz	Zertifikat	Intervall
Root-CA	C_{CRL-S}(Root)	Alle 3 Jahre

	$C_{TLS\text{-}S}$(Root)	Alle 2 Jahre
Sub-CA	C(Sub-CA)	Alle 2 Jahre

Die maximalen Gültigkeiten sind jeweils in den Zertifikatstemplates der SNH-Metering-CA konfiguriert.

6.4 Aktivierungsdaten

Die Aktivierungsdaten (Admin Smart Cards) für die Verwaltung der Hardwaresicherheitsmodule werden sicher aufbewahrt.

6.5 Sicherheitsanforderungen für die Rechneranlagen

Die Rechneranlage für die SNH-Metering-CA erfüllt die Anforderungen an die eingesetzte IT-Infrastruktur gemäß Kapitel 6.5 der [CP-Root-CA].

6.6 Zeitstempel

Keine Anforderungen

6.7 Validierungsmodell

Die Anforderungen an die Zertifikatsvalidierung gemäß [TR-03109-4] sind erfüllt.

7 Profile für Zertifikate und Sperrlisten

7.1 Profile für Zertifikate und Zertifikatsrequests

Die Profile für Zertifikate, Zertifikatsrequests, Sperrlisten, sowie das Sperrmanagement gemäß [TR-03109-4] sind erfüllt.

Das Namensschema zu den Zertifikaten gemäß Anhang A der [CP-Root-CA] ist in Abschnitt 3.1 dieses Dokuments beschrieben.

7.1.1 Zugriffsrechte

Die erlaubte Funktion der Zertifikate wird mit der in [TR-03109-4] definierten Key-Usage-Extension angegeben.

7.1.2 Zertifikatserweiterung

Die Certificate Extensions gemäß [TR-03109-4] werden eingehalten.

7.2 Profile für Sperrlisten

Die Anforderungen an die Certification Revocation List (CRL) gemäß der [TR-03109-4] sind erfüllt.

7.3 Profile für OCSP Dienste

Es werden keine OCSP Dienste angeboten, siehe Abschnitt 4.9.

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 SNH-Metering-CA stellt eine Testumgebung zur Verfügung, welche die Antragsteller der SM-PKI zum Test der Funktionalitäten ihrer PKI-Infrastruktur und –Prozesse durchlaufen müssen, bevor diese Teilnehmer der PKI werden können.

Der Testbetrieb dient zur Erprobung der sicheren und erfolgreichen Teilnahme an der Wirk-PKI.

8.1.2 Wirkbetrieb

Die vorausgesetzten Nachweise / Zertifizierungen der Sub-CA werden im Wirkbetrieb auf Basis des Prüf-/Zertifizierungsschemas aufrechterhalten.

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 Preise für SNH-Metering-CA Dienstleistungen der Stromnetz Hamburg GmbH werden auf Anfrage mitgeteilt.

9.2 Finanzielle Zuständigkeiten

Die Stromnetz Hamburg GmbH als Betreiber der Sub-CA Instanz ist finanziell eigenständig und unabhängig.

10 Referenzdokumente

Referenz	Dokument
[CP-Root-CA]	Certificate Policy der Smart Metering-PKI, Version 1.1.1 09.08.2017 Link
[KeyLifecSec]	Key Lifecycle Security Requirements, Version 1.0.1, 29.11.2016 Link
[TR-03109-1]	Technische Richtlinie BSI TR-03109-1: Anforderungen an die Interoperabilität der Kommunikationseinheit eines intelligenten Messsystems - Version 1.0, 18.03.2013 Link
[TR-03109-4]	Technische Richtlinie BSI TR-03109-4: Smart Metering PKI- Public Key Infrastruktur für Smart Meter Gateway, Version 1.2.1, 09.08.2017 Link
[TR-03109-6]	Smart Meter Gateway Administration, Version 1.0, 26.11.2015 Link
[TR-03116-3]	Kryptographische Vorgaben für Projekte der Bundesregierung Teil 3: Intelligente Messsysteme, 23.04.2018 Link
[TR-03145-1]	Secure CA operation, Part 1, Version 1.1, 27.03.2017 Link