Certificate Policy (CP) und Certificate Practice Statement (CPS) der Sub-CA der Thüga SmartService GmbH

Datum:	**24.05.2018**
Herausgegeben von:	**Thüga SmartService GmbH** **Zum Kugelfang 2** **95119 Naila** **Tel. 09282/9999-0** **info@smartservice.de**

Änderungshistorie

Autor/Bearbeiter	Stand	Version	Datum
Thüga SmartService GmbH	Freigabe	3.0	24.05.2018

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungen

Abkürzung	Begriff
ASP	Ansprechpartner
BSI	Bundesamt für Sicherheit und Informationstechnik
CA	Certification Authority
CLS	Controllable Local Systems
CN	Common Name
CP	Certificate Policy
CPS	Certificate Practice Statement
CRL	Certificate Revocation List (Zertifikatssperrliste)
EMT	Externer Marktteilnehmer
Enc	Encryption
GWA	Gateway Administrator
GWH	Gateway Hersteller
HAN	Home Area Network
ISO	International Organization of Standardization
ITU	International Telecommunication Union
LMN	Local Metrological Network
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PKI	Public Key Infrastructure
PP	Protection Profile
RA	Registration Authority
SMGW	Smart Meter Gateway
S/MIME	Secure/Multipurpose Internet Mail Extension
SM-PKI	Smart Metering Public Key Infrastructure
TLS	Transport Layer Security
TR	Technische Richtlinie
WAN	Wide Area Network
X.509	ITU-T-Standard für eine Public-Key-Infrastruktur

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 Systemarchitektur der SM-PKI ist in [TR-03109-4] spezifiziert. Das vorliegende Dokument beschreibt die Certificate Policy der Sub-CA der Thüga SmartService GmbH („**SmartServiceCA**“). Dieses Dokument dient zur Beschreibung der technischen, personellen und organisatorischen Anforderungen und deren Umsetzung und verweist bei den nicht spezifischen Punkten auf die SM-PKI Policy der Root-CA.

1.1 Überblick

Dieses Dokument richtet sich an alle Teilnehmer der SM-PKI, insbesondere die Zertifikatsnehmer (Endnutzer) der **SmartServiceCA** und ist in Anlehnung an die SM-PKI Policy der Root strukturiert und definiert. Die CP der **SmartServiceCA** unterwirft sich der SM-PKI Policy der Root-CA, die durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) betrieben wird, und berücksichtigt alle darin beschriebenen Anforderungen. Verantwortlich für die CP der **SmartServiceCA** ist die Thüga SmartService GmbH. Die Thüga SmartService GmbH behält sich vor, komplette Aufgaben oder Teilaufgaben von beauftragten Unternehmen ausführen zu lassen. In der Zertifizierung der **SmartServiceCA** nach [TR-03145-1] werden beauftragte Unternehmen berücksichtigt.

1.2 Name und Identifizierung des Dokuments

Titel	Certificate Policy und Certificate Practice Statement der Sub-CA der Thüga SmartService GmbH
Version	3.0
OID	1.3.6.1.4.1.45748.1.2.1.0

Tabelle 1: Identifizierung des Dokuments

Die aktuelle Version der CP kann unter https://www.smartservice.de/smartserviceca/cp/ heruntergeladen werden.

1.3 PKI-Teilnehmer

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

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

Tabelle 2: Übersicht der PKI-Teilnehmer

1.3.1 Zertifizierungsstellen

Die **SmartServiceCA** ist eine Sub-CA der SM-PKI, welche von der Root-CA zur Ausstellung von Zertifikaten autorisiert wird und Zertifikate für ihre Kunden ausstellt. Die folgende Grafik veranschaulicht die CA-Systeme der SM-PKI:

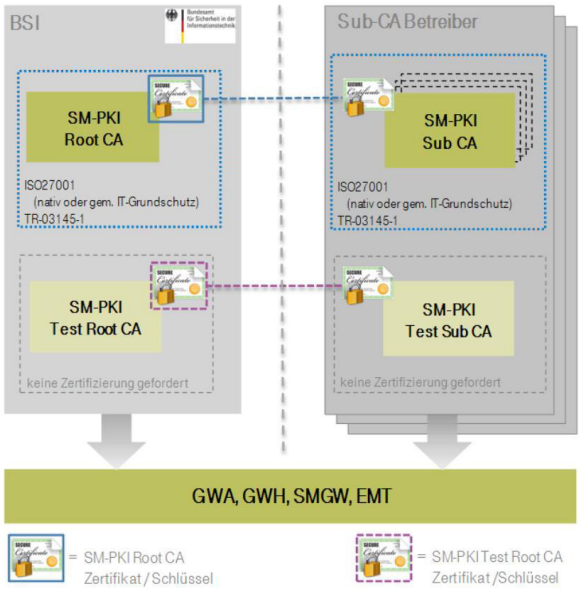

Abbildung 1: Schaubild der CA-Systeme der SM-PKI

Der Betreiber der **SmartServiceCA** als SM-PKI Sub-CA ist die Thüga SmartService GmbH. Neben dem Wirksystem der **SmartServiceCA** betreibt die Thüga SmartService GmbH auch die **SmartService-Test-CA.** Diese stellt für Testzwecke (z.B. Erst-Registrierung und zum Test systemkritischer Vorgänge, wie dem Wechsel des Vertrauensankers) die erforderlichen Funktionalitäten bereit.

Die technische Infrastruktur der **SmartService-Test-CA** entspricht der Wirkumgebung der **SmartServiceCA.** Beide Plattformen sind informationstechnisch voneinander getrennt. Die verwendeten Schlüssel sind in beiden Plattformen unterschiedlich. Die Anbindung an die jeweilige Root-CA ist in der o.a. Abbildung erläutert.

1.3.2 Registrierungsstelle der SmartServiceCA

Die **SmartServiceCA** verfügt über eine eigene Registrierungsstelle (registration authority (RA) der **SmartServiceCA**). Diese ist für die initialen Registrierungen sowie die Folgeanträge der Endnutzer zuständig.
Im Rahmen der initialen Registrierung wird eine zweifelsfreie Identifizierung des Antragstellers und die Authentifizierung der PKI-Rolle und der Identitätsdaten der ausführenden Personen festgestellt. Die Grundlage für die Prozesse der RA bildet dieses Dokument so wie die Vorgaben der Certificate Policy der Smart Metering PKI.

Für die beteiligten Parteien im Prozess des Zertifikatsmanagementflusses stellen die Registrierungsstelle zusammen mit der certification authority (CA), welche u.a. für die Ausgabe der Zertifikate zuständig ist, die wichtigsten Rollen dar. Die jeweiligen Stellen werden durch die RA Operatoren und die CA Operatoren der **SmartServiceCA** repräsentiert.

1.3.3 Zertifikatsnehmer

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

1.3.3.1 SMGW

Bei einem SMGW handelt es sich um eine technische Komponente, siehe [TR-03109-1], die von einer Sub-CA wie der **SmartServiceCA** mit Zertifikaten ausgestattet wird, welche für die Durchführung der definierten Prozesse und Kommunikationsverbindungen benötigt werden. Ein SMGW wird immer von einem GWA verwaltet.

1.3.3.2 Gateway-Administrator

Ein Gateway-Administrator (GWA) ist für die Verwaltung der ihm zugeordneten SMGWs verantwortlich. Die Aufgaben und Anforderungen an den GWA sind in [TR-03109-6] definiert.

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

1.3.3.3 Gateway-Hersteller

Ein Hersteller von Gateway-Komponenten (GWH) erhält von der **SmartServiceCA** Zertifikate, mit denen dieser insbesondere die Prozesse zur Beantragung und Verwaltung von Gütesiegelzertifikaten für SMGWs durchführen kann.

1.3.3.4 Externer Marktteilnehmer

Ein externer Marktteilnehmer (EMT) erhält von der **SmartServiceCA** Zertifikate, mit denen dieser insbesondere mit den SMGWs sicher kommunizieren kann. Überdies kann der Datenaustausch mit den anderen Teilnehmern der SM-PKI (z.B. einem GWA) abgesichert werden.

Ein EMT, welcher ein SMGW nutzt, um über dieses nachgelagerte Geräte (CLS) anzusprechen, wird als aktiver EMT bezeichnet. Die entsprechenden Anwendungsfälle zur Steuerung von CLS an der HAN-Schnittstelle durch einen EMT sind in der [TR-03109-1] definiert. Ein EMT, welcher keine nachgelagerten Geräte (CLS) anspricht bzw. steuert, sondern nur Daten empfängt, um auf Basis dieser Informationen die eigenen Geschäftsprozesse fortzuführen, wird als passiver EMT bezeichnet.

1.3.4 Zertifikatsnutzer

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

1.3.5 Andere Teilnehmer

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

1.4 Verwendung von Zertifikaten

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

1.4.1 Erlaubte Verwendung von Zertifikaten

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

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

Zertifikat der SmartServiceCA	**Signiert durch**	**Verwendungszweck**
C(Sub-CA)	Privater Schlüssel zu C(Root)	Der öffentliche Schlüssel aus dem Zertifikat wird zur Überprüfung der Signatur von nachgeordneten Zertifikaten benötigt, welche mit dem zum Zertifikat passenden privaten Schlüssel signiert wurden. Der zugehörige private Schlüssel wird für die Signatur von GWA, GWH, EMT, SMGW- sowie C_{TLS}(Sub-CA)-Zertifikaten und der Sperrliste der Sub-CA verwendet.
$C_{TLS,Root}$(Sub-CA)	Privater Schlüssel zu $C_{TLS\text{-}S}$(Root)	Diese Zertifikate werden beim Aufbau des TLS-Kommunikationskanals zwischen Sub-

		CA und der Root für das Zertifikatsmanagement eingesetzt.
C_{TLS}(Sub-CA)	Privater Schlüssel zu C(Sub-CA)	Diese Zertifikate werden beim Aufbau des TLS-Kommunikationskanals zwischen Sub-CA und anderen Systemen eingesetzt.

Tabelle 3: Zertifikate der SmartServiceCA

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

Zertifikate der Zertifikatsnehmer:

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

Tabelle 4: Zertifikate der Zertifikatsnehmer

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

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

Zertifikat eines Ansprechpartners	**Verwendungszweck**
$C_{S/MIME}$(ASP Root) $C_{S/MIME}$(ASP Sub-CA) $C_{S/MIME}$(ASP GWA) $C_{S/MIME}$(ASP GWH) $C_{S/MIME}$(ASP EMT)	Zertifikat für den privaten Schlüssel, der vom Ansprechpartner der Root, einer Sub-CA, eines GWA, eines GWH, eines EMT für die Signatur und Verschlüsselung der E-Mail-Kommunikation eingesetzt wird. Je nach Realisierung der ausstellenden CA KÖNNEN für die Signatur und die Verschlüsselung auch unterschiedliche Zertifikate eingesetzt werden. Es wird EMPFOHLEN, dass Zertifikate den Anforderungen der [TR-03116-4] entsprechen.

Tabelle 5: Kommunikationszertifikate der Ansprechpartner

1.4.2 Verbotene Verwendung von Zertifikaten

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

1.5 Administration der SmartServiceCA CP/CPS

Die für dieses Dokument verantwortliche Organisation ist die Thüga SmartService GmbH.

Organisation	Thüga SmartService GmbH
Adresse	Zum Kugelfang 2 95119 Naila
Telefon	09282/9999-0
Webseite	www.smartservice.de
E-Mail	ra@smartservice.de

Tabelle 6: Kontaktadresse CP/CPS SmartServiceCA

1.5.1 Pflege der SmartServiceCA CP/CPS

Jede aktualisierte Version dieses Dokumentes wird den Kunden der **SmartServiceCA** unverzüglich auf der folgenden Internetseite zur Verfügung gestellt:

https://www.smartservice.de/smartserviceca/cp/

Benannte Ansprechpartner eines Kunden werden per E-Mail über die aktualisierte Version informiert. Sollte innerhalb von zwei Wochen nach Benachrichtigung kein Widerspruch des Kunden erfolgen, gilt die neue Version als akzeptiert.

1.5.2 Zuständigkeit für das Dokument

Eigentümer und somit zuständig für die Erweiterung und/oder die nachträglichen Änderungen dieser **SmartServiceCA** CP/CPS ist ausschließlich die Thüga SmartService GmbH als Betreiber der **SmartServiceCA**.

1.5.3 Ansprechpartner/Kontaktperson

Siehe Tabelle 6.

1.5.4 Konformität zur CP SM-PKI

Das vorliegende Dokument ist Bestandteil der Betriebsdokumentation der **SmartServiceCA**. Die CP/CPS der **SmartServiceCA** wird im Rahmen der Registrierung durch die RA der SM-PKI Root auf Konformität zur [CP-SM-PKI] geprüft.

2 Verantwortlichkeit für Veröffentlichungen und Verzeichnisse

2.1 Verzeichnisse

Von der **SmartServiceCA** wird ein Verzeichnis gemäß [TR-03109-4] mit allen von der **SmartServiceCA** ausgestellten Zertifikaten bereitgestellt.

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

Die Informationen zum Verzeichnis und dem Sperrlistenverteilpunkt sind der Website der **SmartServiceCA** sowie den von der **SmartServiceCA** ausgestellten Zertifikaten zu entnehmen. Dieses wird laut 2.2.1 veröffentlicht.

2.2 Veröffentlichung von Informationen zur Zertifikatserstellung

2.2.1 Veröffentlichungen der SmartServiceCA

Die **SmartServiceCA** kann über die folgende Webseite der Thüga SmartService GmbH erreicht werden:

https://www.smartservice.de/smartserviceca

Diese Webseite beinhaltet u.a. Informationen über

- Kontaktdaten der **SmartServiceCA**
- Parameter zur Einrichtung eines Zugriffs auf die Sperrliste bzw. das LDAP-Verzeichnis
- CP/CPS der **SmartServiceCA**
- Beschreibung des Antragverfahrens
- Hinweise zur Teilnahme am Testsystem

2.3 Zeitpunkt und Häufigkeit der Veröffentlichungen

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

Sperrungen werden nach Durchführung durch eine Veröffentlichung in der jeweiligen Sperrliste in der **SmartServiceCA** als solche wirksam. Eine Aufnahme in die Sperrliste sowie deren Veröffentlichung erfolgt gemäß der in [CP SM-PKI] Abschnitt 4.8.3, Tabelle 10, festgelegten Zeiten.

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

2.4 Zugriffskontrollen auf Verzeichnisse

Der lesende Zugriff auf die LDAP-Verzeichnisdienste der **SmartServiceCA** wird auf die an der SM-PKI teilnehmenden Organisationen, wie die SM-PKI Root und Sub-CAs, GWA, GWH sowie EMTs beschränkt (ein SMGW verfügt über keine Schnittstelle zu den Verzeichnisdiensten, so dass diese Zertifikate für den Zugriff auch nicht freigeschaltet werden müssen). Dies wird über eine zertifikatsbasierte Authentisierung am jeweiligen Verzeichnisdienst mittels der TLS-Zertifikate der Zertifikatsnehmer gemäß den Anforderungen aus [TR-03116-3] sichergestellt.

Der Verzeichnisdienst der **SmartServiceCA** dient ausschließlich der Aktualisierung von angefragten Zertifikaten. Ein Massenabruf von Zertifikaten ist nicht gestattet. Der Verzeichnisdienst ist so konfiguriert, dass die Anzahl der zurückgegebenen Suchergebnisse auf 100 begrenzt ist/bei Bedarf entsprechend reglementiert wird.

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

3 Identifizierung und Authentifizierung

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

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

3.1 Regeln für die Namensgebung

Hinsichtlich des Namensschemas muss der Bezeichner (Common Name, CN) eines Zertifikats der **SmartServiceCA** dem Profil gemäß [CP-SM-PKI] Anhang A entsprechen.

3.1.1 Arten von Namen

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

3.1.2 Notwendigkeit für aussagefähige Namen

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

3.1.3 Anonymität oder Pseudoanonymität von Zertifikatsnehmern

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

3.1.4 Eindeutigkeit von Namen

Die Angaben der Zertifikatsinhaber werden gemäß den Anforderungen aus Abschnitt 3.1.1 in die Zertifikate der **SmartServiceCA** aufgenommen. Eine Namensgleichheit (gleicher CN bei unterschiedlichem Zertifikatsnehmer) wird durch die **SmartServiceCA** verhindert, entsprechend vergibt die **SmartServiceCA** einen CN nicht mehrfach. Sollten zwei oder mehr Zertifikatsnehmer der **SmartServiceCA** den gleichen CN besitzen wird dieser Konflikt gelöst. Es behält der Teilnehmer seinen CN, der zuerst sein initiales Zertifikat mit diesem CN von der **SmartServiceCA** erhalten hat. Der oder die anderen Zertifikatsnehmer lassen sich ein Zertifikat mit einem anderen CN ausstellen, um an der **SmartServiceCA** teilnehmen zu dürfen.

3.1.5 Anerkennung, Authentifizierung und die Rolle von Markennamen

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

3.2 Initiale Überprüfung zur Teilnahme an der 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.

3.2.1 Methoden zur Überprüfung bzgl. Besitz des privaten Schlüssels

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

Diese wird bei der Antragsprüfung durch Verifikation der inneren Signatur mit dem im Zertifikatsrequest enthaltenen zugehörigen öffentlichen Schlüssel durch die **SmartServiceCA** geprüft, wodurch sichergestellt wird, dass der Zertifikatsrequest vom Antragsteller kommt.

3.2.2 Authentifizierung von Organisationszugehörigkeiten

Die nachfolgenden Organisationen dürfen innerhalb der SM-PKI Zertifikatsanträge an die **SmartServiceCA** stellen: EMT, GWA und GWH.

Die grundsätzlichen Anforderungen für die Authentifizierung sind in [CP SM-PKI] Abschnitt 3.2.2 beschrieben. Weitergehende Anforderungen für den Prozess der Registrierung eines Teilnehmers sind in den „Geschäftsbedingungen der SmartServiceCA“ der Thüga SmartService GmbH dokumentiert.

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

3.2.3 Authentifizierung zur Identifizierung und Authentifizierung des Zertifikats-Antragstellers

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

3.2.4 Ungeprüfte Angaben zum Zertifikatsnehmer

Die Registrierungsstelle prüft beim EMT, GWA und GWH die Angaben zum Zertifikatsnehmer im Zertifikatsrequest gegen die eingereichten Unterlagen auf Korrektheit (siehe Abschnitt 3.2.2).

3.2.5 Prüfung der Berechtigung zur Antragstellung

Siehe Abschnitt 3.2.

3.2.6 Kriterien für den Einsatz interoperierender Systeme/Einheiten

Aktuell sind keine Kriterien definiert.

3.2.7 Aktualisierung/Anpassung der Zertifizierungsinformationen der Teilnehmer

Die für die Teilnehmer an der **SmartServiceCA** geforderten Zertifizierungen, wie sie in [CP SM-PKI] Abschnitt 8.1.2, Tabelle 15 beschrieben sind, unterliegen in der Regel einem jährlichen Überwachungszyklus, für das z.B. ein Audit positiv abgeschlossen werden muss.

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

Sollte der Teilnehmer die Zertifizierung nicht mehr erhalten, so wird das Zertifikat bzw. werden die Zertifikate aus der **SmartServiceCA,** wie in Kapitel 9 der „Geschäftsbedingungen der SmartServiceCA“ beschrieben, gesperrt. Informationen über relevante Änderungen, die beispielsweise

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

erfordern, muss der Zertifikatsnehmer unverzüglich inklusive der entsprechenden Informationen und besonders die Ergebnisse der Zertifizierung der **SmartServiceCA** zur Verfügung stellen. Die **SmartServiceCA** aktualisiert anschließend die entsprechenden Registrierungsdaten.

3.2.8 Aktualisierung/Anpassung der Registrierungsinformationen der Teilnehmer

Jeder Teilnehmer muss der Registrierungsstelle der **SmartServiceCA** unverzüglich eine Änderung bzgl. seiner Registrierungsdaten mitteilen.

Ergänzend wird die **SmartServiceCA** regelmäßig nach initialer Registrierung bei den Teilnehmern anfragen, ob Änderungen an den Registrierungsdaten vorliegen. Diese Anfrage erfolgt erstmals 12 Monate nach der initialen Registrierung via gesicherter Kommunikation via E-Mail (S/MIME) von der Registrierungsstelle der **SmartServiceCA** an die hinterlegten Ansprechpartner der Kunden. Anschließend wird die Anfrage in regelmäßigen Abständen von 12 Monaten durchgeführt.

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

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

Die grundsätzlichen Anforderungen für die Authentifizierung sind in [CP SM-PKI] Kapitel 3.3 beschrieben. Weitergehende Anforderungen für den Prozess der Identifizierung und Authentifizierung von Anträgen auf Schlüsselerneuerung bei einem routinemäßigen Folgeantrag sind in den „Geschäftsbedingungen der SmartServiceCA“ der Thüga SmartService GmbH dokumentiert.

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

3.4.1 Allgemein

Um einen nicht routinemäßigen Folgeantrag handelt es sich, wenn mindestens eine der folgenden Bedingungen erfüllt ist:

- Der Antragsteller besitzt kein gültiges TLS-Zertifikat für die Beantragung.
- Der Zertifikatsrequest ist nicht mit der gültigen Signatur des vorherigen Signaturschlüssels (äußere Signatur, [TR-03109-4] Abschnitt 3.4.1.1)

Die grundsätzlichen Anforderungen und Vorgehensweisen für die Authentifizierung sind in [CP SM-PKI] Kapitel 3.4 beschrieben. Weitergehende Anforderungen für den Prozess der Identifizierung und Authentifizierung von Anträgen auf Schlüsselerneuerung bei einem routinemäßigen Folgeauftrag sind in den „Geschäftsbedingungen der SmartServiceCA“ der Thüga SmartService GmbH dokumentiert.

3.4.2 Schlüsselerneuerung nach Sperrungen

Das weitere Vorgehen zur Identifizierung und Authentifizierung eines PKI-Teilnehmers der **SmartServiceCA** nach einer Sperrung ist davon abhängig, welche seiner Zertifikate von der Sperrung betroffen sind. Der PKI-Teilnehmer der **SmartServiceCA** stellt auf Basis der ihm zur Verfügung stehenden gültigen Zertifikate einen Folgeantrag gemäß Abschnitt 3.4.1, um seine gesperrten Zertifikate durch neue gültige Zertifikate zu ersetzen. Ein Endnutzer beantragt immer ein neues Zertifikatstripel, wenn eines seiner Zertifikate gesperrt wurde.

3.5 Identifizierung und Authentifizierung von Anträgen auf Sperrung

Die grundsätzlichen Anforderungen und Vorgehensweisen für die Identifizierung und Authentifizierung sind in [CP SM-PKI] Kapitel 3.5 beschrieben. Weitergehende Anforderungen für den Prozess der Identifizierung und Authentifizierung von Anträgen auf Sperrung sind in den „Geschäftsbedingungen der SmartServiceCA“ der Thüga SmartService GmbH dokumentiert.

3.6 Identifizierung und Authentifizierung von Anträgen auf Suspendierung

Die grundsätzlichen Anforderungen und Vorgehensweisen für die Identifizierung und Authentifizierung sind in [CP SM-PKI] Kapitel 3.6 beschrieben. Weitergehende Anforderungen für den Prozess der Identifizierung und Authentifizierung von Anträgen auf Suspendierung sind in den „Geschäftsbedingungen der SmartServiceCA“ der Thüga SmartService GmbH dokumentiert.

4 Betriebsanforderungen für den Zertifikatslebenszyklus

Die grundsätzlichen Anforderungen und Vorgehensweisen bei

- Zertifikatsbeantragung (initialer Antrag und Folgeantrag)
- Zertifikatsausstellung und -erneuerung
- Zertifizierung nach Schlüsselerneuerung
- Änderung/Sperrung von Zertifikaten
- Beendigung der Teilnahme sowie
- Hinterlegung und Wiederherstellung von Schlüsseln

sind in [CP SM-PKI] Kapitel 3.5 beschrieben. Weitergehende Anforderungen für den Betrieb von Zertifikaten, u.a. Bearbeitungszeiten und Pflichten des Zertifikatsnehmers, sind in den „Geschäftsbedingungen der SmartServiceCA“ der Thüga SmartService GmbH dokumentiert.

5 Organisatorische, betriebliche und physikalische Sicherheitsanforderungen

Die CP/CPS der **SmartServiceCA** spezifiziert technische und organisatorische Sicherheitsanforderungen an alle Teilnehmer an der **SmartServiceCA**, die im Kontext der SM-PKI relevant sind, um die Sicherheit der **SmartServiceCA** und der SM-PKI zu gewährleisten. Die Teilnehmer GWA/GWH und EMT müssen die Ziel- und Sicherheitsvorgaben aus der [CP-SM-PKI] Kapitel 5 beachten. Die Umsetzung der Sicherheitsanforderungen für diese Rollen sind im Folgenden nicht betrachtet.

5.1 Generelle Sicherheitsanforderungen

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

Der Betreiber der **SmartServiceCA**, die Thüga SmartService GmbH, hat eine Zertifizierung nach ISO27001 auf Basis von IT-Grundschutz.

5.1.1 Erforderliche Zertifizierungen der PKI-Teilnehmer

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

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

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

EMT: Ein passiver EMT erstellt ein Sicherheitskonzept, in dem die Anforderungen aus der **SmartServiceCA-**Policy berücksichtigt wurden. Gegenüber der **SmartServiceCA** bestätigt der EMT dieses im Rahmen des Registrierungsprozesses. Ein aktiver EMT (vgl. Abschnitt 1.3.3.4) hat eine ISO/IEC 27001-Zertifizierung vorgelegt bzw. nachgewiesen, dass ein nach ISO/IEC 27001 zertifizierter Dritter die Leistung für ihn erbringt. Möchte ein passiver EMT nachträglich auch die Aufgaben eines aktiven EMTs wahrnehmen oder möchte ein aktiver EMT nur noch als passiver EMT auftreten, so muss das Unternehmen dies der **SmartServiceCA** rechtzeitig und eigenverantwortlich mitteilen und die entsprechenden Prozesse (s. Abschnitt 3.2.2) durchlaufen werden.

- Die Aufgaben des aktiven EMT dürfen erst vom Antragsteller mit dem bestehenden Zertifikat ausgeübt werden, wenn die erfolgreiche Registrierung als aktiver EMT von der **SmartServiceCA** bestätigt wurde. Die Bestätigung erfolgt per signierter E-Mail an die registrierten Ansprechpartner.

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

Hier wird auf die Anforderungen aus der [CP SM-PKI] Abschnitt 5.1.2 verwiesen.

5.2 Erweiterte Sicherheitsanforderungen

5.2.1 Betriebsumgebung und Betriebsabläufe

Die Anforderungen an die Sicherheit der Betriebsumgebung und der Betriebsabläufe für die Endnutzer der **SmartServiceCA** entsprechen der Vorgaben aus der [CP SM-PKI] Abschnitt 5.2.1, sowie den spezifizierten Vorgaben für den GWA aus [TR-03109-6].

5.2.2 Verfahrensanweisungen

Für den Betrieb der **SmartServiceCA** werden die betreffenden Vorgaben aus [CP SM-PKI] Abschnitt 5.2.2 umgesetzt.

5.2.3 Personal

Der Betrieb der Sub-CA, GWH und EMT erfolgt durch angemessen geschultes und erfahrenes Personal. Die Anforderungen aus [CP SM-PKI] Abschnitt 5.2.3 sind erfüllt.

5.2.4 Monitoring

Die in [CP SM-PKI] Abschnitt 5.2.4 definierten Ereignisse werden erkannt und aufgezeichnet und dokumentiert.

5.2.5 Archivierung von Aufzeichnungen

Die **SmartServiceCA** verfügt über ein angemessenes Archivierungssystem. Die jeweiligen Zeiträume sind entsprechend [CP SM-PKI] Anhang B definiert. Die in [CP SM-PKI] Abschnitt 5.2.5 definierten Anforderungen bezüglich der Archivierung von Aufzeichnungen werden berücksichtigt.

5.2.6 Schlüsselwechsel einer Zertifizierungsstelle

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

- Geplanter Schlüsselwechsel: Im Fall eines planbaren Schlüsselwechsels werden die in der SM-PKI Policy beschriebenen Verfahren berücksichtigt und es sind entsprechende Prozesse vorhanden.
- Ungeplanter Schlüsselwechsel: Für den Fall, dass ein unvorhergesehener Schlüsselwechsel notwendig ist, werden die entsprechenden Verfahren im Notfallmanagement definiert.
- Sowohl ein geplanter als auch ein ungeplanter Schlüsselwechsel erfolgt gemäß dem Vier-Augen-Prinzip.

5.2.7 Auflösen einer Zertifizierungsstelle

Der Prozess einer Auflösung der **SmartServiceCA** entspricht den Vorgaben aus [CP SM-PKI] Abschnitt 5.2.7 und ist für die Sub-CA der Thüga SmartService GmbH in den „Geschäftsbedingungen der SmartServiceCA“ der Thüga SmartService GmbH definiert.

5.2.8 Aufbewahrung der privaten Schlüssel

Die Vorgaben an die Aufbewahrung der privaten Schlüssel werden durch die Umsetzung der in der [CP SM-PKI] Abschnitt 5.2.8 aufgeführten Anforderungen abgedeckt.

5.2.9 Behandlung von Vorfällen und Kompromittierung

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

- Bei einer Kompromittierung oder einem begründeten Verdacht auf Kompromittierung eines privaten Schlüssels wird das zugehörige Zertifikat unverzüglich gesperrt und es darf nicht wiederverwendet werden. Bei systemkritischen Zertifikaten wird die SM-PKI Root durch die SmartServiceCA informiert.
- Ein Fall von Kompromittierung sowie Verdachtsfälle wird durch den Schlüsselinhaber dokumentiert.
- Jeder Verdacht auf Kompromittierung oder Missbrauch des privaten Schlüssels muss aufgeklärt werden.
- Die Generierung neuer Schlüssel und Zertifikate wird überwacht und dokumentiert.

5.2.10 Meldepflichten

Bei Kompromittierung oder anderweitigen sicherheitsrelevanten Vorfällen wird eine Meldung aufbereitet und an die **SmartServiceCA** kommuniziert. Die Meldepflicht obliegt dem Zertifikatsnehmer. Bei der Kompromittierung eines GWA oder GWH wird zusätzlich die SM-PKI Root durch die **SmartServiceCA** informiert. Die meldepflichtigen Vorkommnisse sowie weitere Vorgaben aus [CP SM-PKI] Abschnitt 5.2.10 sind erfüllt.

5.3 Notfall-Management

Die Sub-CA, GWA, GWH und EMT gewährleisten, dass die Wiederherstellung des Normalbetriebs nach einer Störung oder nach einem Notfall innerhalb einer angemessenen Frist erfolgt. Die betreffenden Notfallszenarien sind in [CP SM-PKI] Abschnitt 5.3 dargelegt.

6 Technische Sicherheitsanforderungen

6.1 Erzeugung und Installation von Schlüsselpaaren

Jeder Zertifikatsnehmer generiert sein eigenes Schlüsselpaar. 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 **SmartServiceCA** und die teilnehmenden EMT, GWA und GWH stellen sicher, dass die Anforderungen an die Generierung von Schlüsselpaaren aus [CP SM-PKI] Abschnitt 6.1.1 erfüllt werden.

6.1.2 Lieferung privater Schlüssel

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

6.1.3 Lieferung öffentlicher Zertifikate

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

6.1.4 Schlüssellängen und kryptografische Algorithmen

Bezüglich Schlüssellängen und kryptografischer Algorithmen werden angemessene kryptografische Verfahren verwendet, welche zum jeweiligen Zeitpunkt der [TR-03116-3] entnommen werden. Der bei der Erzeugung und Nutzung von statischen und temporären Schlüssel innerhalb der **SmartServiceCA** verwendete Zufallsgenerator ist ebenfalls konform zu [TR-03116-3]. Bei statischen Schlüsseln wird ein Kryptografiemodul entsprechend Abschnitt 6.2 eingesetzt.

6.1.5 Festlegung der Parameter der Schlüssel und Qualitätskontrolle

Es werden die Anforderungen aus [CP SM-PKI] Abschnitt 6.1.5 umgesetzt.

6.1.6 Verwendungszweck der Schlüssel

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

6.2 Sicherung des privaten Schlüssels und Anforderungen an kryptografische Module

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

Für die **SmartService-Test-CA** werden Kryptografiemodule gemäß [CP SM-PKI] Anhang C1 eingesetzt.

6.2.1 Mehrpersonen-Zugriffssicherung zu privaten Schlüsseln

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

6.2.2 Ablage privater Schlüssel

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

6.2.3 Backup privater Schlüssel

Es werden die Anforderungen aus [CP SM-PKI] Abschnitt 6.2.3 eingehalten.

6.2.4 Archivierung privater Schlüssel

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

6.2.5 Transfer privater Schlüssel in oder aus kryptografischen Modulen

Der private Schlüssel kann zwischen kryptografischen Modulen transferiert werden.

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

6.2.6 Speicherung privater Schlüssel in kryptografischen Modulen

Die privaten Schlüssel der **SmartServiceCA** werden auf einem Kryptografiemodul gespeichert. Die einzige Ausnahme bilden die client- und serverseitigen TLS-Schlüssel bei der **SmartServiceCA**, welche zur TLS-Authentisierung an der Web-Service-Schnittstelle [TR-03116-3] und am Verzeichnisdienst verwendet werden. Die privaten Schlüssel der Testumgebung der **SmartServiceCA** werden von der Produktivumgebung getrennt.

6.2.7 Aktivierung privater Schlüssel

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

6.2.8 Deaktivierung privater Schlüssel

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

6.2.9 Zerstörung privater Schlüssel

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

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

Die Backups der Schlüssel werden ebenfalls berücksichtigt. Die Zerstörung der privaten Schlüssel erfolgt durch einen sicheren Lösch-Mechanismus im Kryptografiemodul. Die ENC-Schlüssel sind von dieser Anforderung ausgenommen. Diese dürfen nur noch für die Entschlüsselung abgelegter Daten genutzt werden, mit dem Ziel einer Umschlüsselung auf den aktuellen ENC-Schlüssel. Sollte der ENC-Schlüssel nicht mehr zur Umschlüsselung erforderlich sein, wird dieser zerstört.

6.2.10 Beurteilung kryptografischer Module

Es werden die Anforderungen aus [CP SM-PKI] Abschnitt 6.2.10 eingehalten.

6.3 Andere Aspekte des Managements von Schlüsselpaaren

6.3.1 Archivierung öffentlicher Schlüssel

Die Zertifikate aller Teilnehmer der **SmartServiceCA** werden inklusive der Statusdaten archiviert [CP SM-PKI, 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 werden die folgenden Zertifikate spätestens in dem hierzu angegebenen Intervall gewechselt.

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

Tabelle 7: Intervall Zertifikatswechsel bei der SmartServiceCA

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

6.4 Aktivierungsdaten

Die Aktivierungsdaten für die Kryptografiemodule werden sicher aufbewahrt.

6.5 Sicherheitsanforderungen für die Rechenanlagen

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

SmartServiceCA:

- *Netzwerkkontrolle*: es werden Maßnahmen umgesetzt, um das interne Netzwerk vom externen zu trennen und vor unbefugtem Zugriff zu schützen
- *Intrusion Detection Systeme (IDS)*: Der Einsatz von IDS im gesicherten Netzsegment wird berücksichtigt und die Log-Dateien des IDS werden regelmäßig kontrolliert.
- *System-Härtung*: Die CA-Server, die zur Erstellung von Zertifikaten verwendet werden, sind gehärtet. Dies umfasst die Konfiguration und Einstellung der verwendeten Hardware- und Softwarekomponenten.
- *System-Konfiguration*: Die Konfigurationsoptionen und -einstellungen einhalten nur die minimal benötigten Funktionalitäten für den Betrieb der CA.
- *Netzwerk-Separierung*: Die Netzwerke, in denen sich die CA-Server befinden, werden durch geeignete Maßnahmen geschützt.
- *Vertraulichkeit und Integrität*: Die CA schützt sensitive Daten vor unbefugtem Zugriff oder Veränderung
- *Logging und Audit-Trails*: Log-Dateien und Audit-Trails werden regelmäßig geprüft und automatisierte Benachrichtigungen weisen auf Abweichungen vom vorgesehenen Betrieb hin

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

Alle PKI-Teilnehmer:

- *Software-Updates*: Software-Updates werden bei sicherheitsrelevanten Änderungen schnellstmöglich eingespielt, andere Updates werden regelmäßig aktualisiert.
- Das System verfügt über eine angemessene Benutzerverwaltung.
- *Schutz vor Schadsoftware*: Die Integrität der System-Komponenten und Informationen wird gegen Viren, Schadsoftware sowie nicht zugelassene Programme geschützt.

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

6.6 Zeitstempel

Es gibt keine Anforderungen an Zeitstempel.

6.7 Validierungsmodell

Die Anforderungen an die Zertifikatsvalidierung, wie in [TR-03109-4] spezifiziert werden seitens der **SmartServiceCA** erfüllt.

7 Profile für Zertifikate und Sperrlisten

7.1 Profile für Zertifikate und Zertifikatsrequests

Die Profile für Zertifikate und die Zertifizierungsrequests sind entsprechend der Vorgaben aus [TR-03109-4] angelegt und umgesetzt. Das Namensschema zu den Zertifikaten ist laut [CP SM-PKI] Anhang A angelegt und umgesetzt.

Die Struktur der Sperrlisten und das Sperrmanagement (Veröffentlichung, Aktualisierung und Sperrlistenvalidierung) werden nach der jeweiligen aktuellen Fassung der [TR-03109-4] angelegt und umgesetzt.

7.1.1 Zugriffsrechte

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

7.1.2 Zertifikatserweiterung

Die Certificate Extensions werden in der jeweils aktuellen Fassung der [TR-03109-4] definiert und in der **SmartServiceCA** analog umgesetzt.

7.2 Profil für Sperrlisten (Certificate Revocation List (CRL))

Die Anforderungen an die Sperrlisten-Profile werden in der jeweils aktuellen Fassung der [TR-03109-4] definiert.

7.3 Profile für OCSP-Dienste

In der **SmartServiceCA** werden keine OCSP-Dienste eingesetzt.

8 Überprüfung und andere Bewertungen

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

8.1 Inhalte, Häufigkeit und Methodik

8.1.1 Testbetrieb

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

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

Tabelle 8: Testumgebungen der SmartServiceCA

8.1.2 Beantragung der Teilnahme an der SmartServiceCA

Folgende Anforderungen müssen bei Beantragung der Teilnahme an der SmartServiceCA erfüllt werden. Hierzu sind die in Abschnitt 8.1.1 aufgeführten Nachweise notwendig. Detaillierte Informationen sind neben Abschnitt 8.1.1 auch in Kapitel 5.1 definiert.

Antrag für Teilnahme als	Nachweis	Überprüfung der Nachweise	Wichtung
GWA	Zertifizierung entsprechend [TR-03109-6]	Zertifizierter [TR-03109-6] Auditor	Voraussetzung
	Signierte E-Mail der SmartServiceCA über erfolgreiche Tests	Prüfer der SmartServiceCA	Voraussetzung
GWH	CC-Zertifizierung [BSI-CC-PP-0073]	CC-Zertifizierungsverfahren	Voraussetzung
	Signierte E-Mail der SmartServiceCA über erfolgreiche Tests	Prüfer der SmartServiceCA	Voraussetzung
SMGW	CC-Zertifizierung [BSI-CC-PP-0073]	CC-Zertifizierungsverfahren	Voraussetzung
	Zertifizierung entsprechend [TR-03109-1]	Prüfstelle	Voraussetzung
Aktiver EMT	ISO 27001-Zertifizierung nativ ODER ISO 27001-Zertifizierung nach BSI Grundschutz	Zertifizierter ISO 27001 Lead Auditor ODER BSI-akkreditierter ISO 27001 Lead Auditor	Voraussetzung
	Signierte E-Mail der SmartServiceCA über erfolgreiche Tests	Prüfer der SmartServiceCA	Voraussetzung
Passiver EMT	Sicherheitskonzept	Sicherheitskonzept muss der Sub-CA nicht vorgelegt werden, kann im Schadensfall mit Bezug auf die Umsetzung herangezogen werden.	Voraussetzung

Tabelle 9: Anforderungen für die Teilnahme an der SmartServiceCA

8.1.3 Wirkbetrieb

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

Sollte eine Zertifizierung nicht mehr gültig sein, so muss dies der **SmartServiceCA** umgehend mitgeteilt werden (siehe Abschnitt 3.2.7).

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

8.2 Reaktionen auf identifizierte Vorfälle

Die Reaktionen auf identifizierte Vorfälle sind in Abschnitt 5.2.10 definiert.

9 Sonstige finanzielle und rechtliche Regeln

9.1 Preise

Die Preise für die Teilnahme an der **SmartServiceCA** sind in den individualvertraglichen Vereinbarungen zwischen der Thüga SmartService GmbH und seinen Kunden zu entnehmen.

9.2 Finanzielle Zuständigkeiten

Der Betreiber der **SmartServiceCA** ist die Thüga SmartService GmbH. Sie ist finanziell eigenständig und unabhängig.

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

Literaturverzeichnis

[BSI-CC-PP-0073]	BSI: Protection Profile for the Gateway of a Smart Metering System, 2014
[CP SM-PKI]	Certificate Policy der Smart Metering PKI
[ISO/IEC 27001]	Information technology — Security techniques — Information security management systems — Requirements
[Key Lifecyle Security Requirements]	BSI: Anforderungen an den Lebenszyklus von kryptographischem Schlüsselmaterial zum Einsatz in einer PKI
[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-03116-4]	BSI: Technische Richtlinie TR-03116-4, Kryptographische Vorgaben für Projekte der Bundesregierung, Teil 4 Kommunikationsverfahren in Anwendungen
[TR-03145-1]	BSI: Technische Richtlinie TR-03145-1, Secure CA operation, Part 1, Generic requirements for Trust Centers instantiating as Certifcation Authority (CA) in a Public-Key Infrastructure (PKI) with security level 'high'

24. 5. 2018

Datum

smartservice
Thüga SmartService GmbH
Zum Kugelfang 2 | 95119 Naila
www.smartservice.de
www.komdsl.de

Unterschrift Geschäftsführung