GWAdriga

Certificate Policy GWADRIGA SMART ENERGY CA

Inhalt

Tabellenverzeichnis

Abbildungsverzeichnis

0. Dokumentenlenkung

0.1. Bearbeitungsvermerk

	Name	Datum	Unterschrift / Signatur
Erstellt:	Axel Pätzold	28.04.2017	gez. Pätzold
Geprüft:	Bernd Ganß,	03.09.2023	gez. Ganß
	Micha Elies	03.09.2023	gez. Elies
Freigegeben:	GF GWADRIGA	04.09.2023	gez. Sobótka
Verteiler:	Mitarbeiter		

0.2. Änderungs-Historie

Version	Datum	Beschreibung der Änderung	Autor
0.1	16.06.2015	Erstellung Vorlage	Bernd Ganß
1.0	28.04.2017	Initiale Version	Axel Pätzold
1.0.3	22.06.2017	Überarbeitung gemäß Anmerkungen nach Vorprüfung durch die Root-CA und Überarbeitung hinsichtlich der Root-Policy vom 9.12.2016	Axel Pätzold
1.0.4	28.06.2017	Überarbeitung gemäß Anmerkungen nach Prüfung durch die Root-CA	Axel Pätzold
1.0.5	03.07.2017	Überarbeitung gemäß weiterer Anmerkungen nach Prüfung durch die Root-CA	Axel Pätzold
1.0.6	05.07.2017	Version zur abschließenden Vorlage bei der Root-CA	Axel Pätzold
1.0.7	02.08.2017	Ergänzung/Korrektur der Angaben zur Dokumentenlenkung, Aktualisierung der Versionsnummer, insbesondere in Ab-	Axel Pätzold

Version	Datum	Beschreibung der Änderung	Autor
		schnitt 1.2.	
1.0.8	25.09.2017	Korrektur der Webadressen für PKI und Test-PKI Korrektur der Sperrlistenadressen	Axel Pätzold
1.1.0	07.05.2018	Überarbeitung hinsichtlich der Root-Policy Version 1.1.1 vom 9.08.2017	Axel Pätzold
1.1.1	30.06.2019	Überarbeitung zur Detaillierung einzelner Punkte sowie Aktualisierung der mitgeltenden Dokumente	Axel Pätzold
1.1.2	15.07.2023	Überarbeitung zur Detaillierung einzelner Punkte sowie Aktualisierung der mitgeltenden Dokumente	Axel Pätzold

0.3. 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 physischer oder psychischer Fähigkeiten, oder eine sonstige Wertung vorzunehmen.

1. Einleitung

Intelligente Zähler für Strom und Gas – sogenannte „Smart Meter“ – werden in Zukunft die beiden Themen Energiewirtschaft und IT-Sicherheit eng verbinden: Denn während die Verbraucher ihre Strom- und Gaszähler heute noch einmal pro Jahr selbst ablesen, werden in naher Zukunft intelligente Zähler diese Aufgabe übernehmen.

Damit jedoch die intelligenten Zähler ihre Arbeit leisten können, ist eine vertrauenswürdige und sichere Kommunikation zum Schutz der dabei anfallenden Daten wie Verbrauch oder Lebensgewohnheiten notwendig, vgl. §28 Messstellenbetriebsgesetz [MsbG].

Die vertrauenswürdige und sichere Kommunikation in der Smart Metering Infrastruktur basiert technisch auf einer Public Key Infrastruktur (PKI), der Smart Metering PKI (SM-PKI). Das Bundesamt für Sicherheit in der Informationstechnik (BSI) ist für den Betrieb der Smart Metering Root Certificate Authority (SM-Root-CA) verantwortlich, welche die Wurzelinstanz (Root) der SM-PKI bildet. Für die sichere Kommunikation der Teilnehmer der Smart Metering Infrastruktur werden Zertifikate eingesetzt, welche von unterschiedlichen kommerziellen Anbietern unterhalb der im Auftrag des BSI betriebenen SM-Root-CA ausgestellt werden. Außerdem wird die sogenannte Marktkommunikation im Energiemarkt, geregelt durch Festlegungen der Bundesnetzagentur, durch die SM-PKI abgesichert.

Für den Eigentümer GWAdriga GmbH & Co. KG wird eine Sub-CA unterhalb der SM-Root-CA betrieben, die zur Zertifizierung von Endnutzerschlüsseln dient. Diese wird im Fremdbetrieb von Eviden Germany GmbH - im Folgenden Betreiber genannt - konform zur übergeordneten SM-Root-CA geführt und wird im folgenden Text:

GWAdriga Smart Energy CA

genannt.

Die GWAdriga Smart Energy CA bietet für die Teilnehmer folgende Leistungen an:

- Registrierung und Verwaltung von Endnutzern GWA, GWH und EMT
- Ausstellen und Sperren von Endnutzer-Zertifikaten GWA, GWH, EMT und SMGW
- Bereitstellen der Webservice-Schnittstelle
- Bereitstellen von Verzeichnissen und der Sperrliste

Das vorliegende Dokument beschreibt die Certificate Policy (CP) der GWAdriga Smart Energy CA, im Weiteren auch SM-GWAdriga Policy genannt. Die SM-GWAdriga Policy beschreibt die technischen, personellen und organisatorischen Sicherheitsanforderungen für die Ausstellung von Zertifikaten in der GWAdriga Smart Energy CA.

Die SM-GWAdriga Policy ist konform zur [SM-PKI-Policy]. In der SM-GWAdriga Policy werden GWAdriga Smart Energy CA spezifische Festlegungen bzw. Konkretisierungen der [SM-PKI-Policy] vorgenommen (vgl. Abschnitt 1.1.2).

In einer ersten Version der SM-GWAdriga Policy sind in diesem Dokument auch CPS-Anteile enthalten.

1.1. Überblick

Dieses Dokument richtet sich an Endnutzer der GWAdriga Smart Energy CA.

Endnutzer der GWAdriga Smart Energy CA kann nur werden, wer vor der Ausstellung von Zertifikaten über einen Vertrag mit dem Eigentümer der Sub-CA verfügt – im Weiteren auch als Vertragskunde bezeichnet.

Im Vertrag mit dem Endnutzer wird zwischen der Teilnahme am Testbetrieb und am Wirkbetrieb der GWAdriga Smart Energy CA unterschieden. Jeder Endnutzer bzw. sein Dienstleister, der am Wirkbetrieb der GWAdriga Smart Energy CA teilnimmt, MUSS zuvor am Testbetrieb der GWAdriga Smart Energy CA teilgenommen haben, vgl. Abschnitt 8.1.1. Informationen zum Testbetrieb können auch der Webseite:

https://www.gwadriga.de/pki/test-pki/

entnommen werden.

Das vorliegende Dokument definiert die Pflichten und Verpflichtungen der GWAdriga Smart Energy CA und ihrer Kunden im Rahmen der technischen, personellen und organisatorischen Sicherheitsanforderungen für die Ausstellung von GWA-, GWH-, EMT- und SMGW-Zertifikaten für Endnutzer.

1.1.1. Überblick über den Aufbau des vorliegenden Dokuments

Nach der Einleitung (Kapitel 1) werden in Kapitel 2 die Verzeichnisdienste beschrieben. Hierunter fallen, neben der Darstellung der Verzeichnisse, Details dazu, welche Informationen veröffentlicht werden, die Häufigkeit der Veröffentlichung sowie Zugriffskontrollen auf diese Komponenten.

In Kapitel 3 werden Regeln zur Authentifizierung der einzelnen Teilnehmer beschrieben. Hierzu gehören neben Details zur erstmaligen Identifizierung auch detaillierte Vorgaben zur Schlüsselerneuerung.

Kapitel 4 enthält die Betriebsanforderungen für den Zertifikatslebenszyklus (Ausgabe, Sperrung, Ablauf) sowie den Sonderfall der Außerbetriebnahme der vorliegenden Sub-CA.

Kapitel 5 beschäftigt sich mit organisatorischen, betrieblichen und physikalischen Sicherheitsanforderungen für die Betriebsumgebungen Sub-CA, GWA, GWH und der EMT. Dabei wird u. a. auf Verfahrensanweisungen, Anforderungen an das Personal, Überwachungsanforderungen, die Organisation von Schlüsselwechseln, die Aufbewahrung von Schlüsseln, das Notfall-Management, die Behandlung von Sicherheitsvorfällen sowie Anforderungen an Maßnahmen bei einer Kompromittierung des Schlüsselmaterials eingegangen.

In Kapitel 6 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 7 beschreibt die Zertifikatsprofile für alle Teilnehmer der GWAdriga Smart Energy CA.

In Kapitel 8 finden sich Bewertungsrichtlinien für die einzelnen Parteien, und das abschließende Kapitel 9 geht auf weitere rechtliche und finanzielle Regelungen ein.

1.1.2. Abdeckung der [SM-PKI-Policy] der Smart Metering Root-CA

Die Gliederung des vorliegenden Dokuments SM-GWAdriga Policy (Policy der GWAdriga Smart Energy CA) entspricht der Gliederung der [SM-PKI-Policy].

In der SM-GWAdriga Policy werden GWAdriga Smart Energy CA spezifische Festlegungen bzw. Konkretisierungen der [SM-PKI-Policy] vorgenommen.

1.2. Name und Identifizierung des Dokuments

Dieses Dokument ist die Certificate Policy (CP) der GWAdriga Smart Energy CA und kann über die folgenden Informationen identifiziert werden.

Identifikator	Wert
Titel	Certificate Policy GWAdriga Smart Energy CA
Version	1.1.2
OID	1.3.6.1.4.1.49814.1.2.1.1

Tabelle 1 OID der GWAdriga Smart Energy CA

Das vorliegende Dokument kann bezogen werden unter https://www.gwadriga.de/pki.

Im Antrag auf Teilnahme als Endnutzer an der GWAdriga Smart Energy CA bestätigt der Antragsteller u. a. die Einhaltung der vorliegenden Policy. Liegt die Bestätigung nicht vor, ist die Registrierung nicht erfolgreich.

Sobald sich Änderungen an dem vorliegenden Dokument ergeben, weil sich Prozesse oder Strukturen der CA verändert haben, wird eine neue Version des Dokuments erstellt und wie oben angegeben veröffentlicht.

Alle autorisierten Ansprechpartner werden per signierter E-Mail über ein Update informiert. Die in der Mail zum Update angegebene neue Version gilt von den so informierten Ansprechpartnern als angenommen, sofern nicht innerhalb von 14 Tagen widersprochen wird. Ein Widerspruch muss schriftlich an die in Abschnitt 1.3.2 aufgeführte E-Mail-Adresse des Teilnehmerservices erfolgen.

1.3. PKI-Teilnehmer

Nachfolgend werden Zertifizierungsstellen, Registrierungsstellen, Zertifikatsnehmer und Zertifikatsnutzer aufgeführt. Alle die vorliegende Sub-CA betreffenden Teilnehmerrollen werden mit „S“ angegeben, die Teilnehmerrollen der übergeordneten Root-CA mit „B“ für BSI und PKI-Teilnehmer für die GWAdriga Smart Energy CA Zertifikate ausstellt mit „X“.

Instanz	Zertifizierungs-stelle	Registrierungs stelle	Zertifikatsnehmer	Zertifikatsnutzer
Root-CA	B	B	B	S/B/X
Sub-CA	S	S	S/B	S/B/X
GWA			X	S/B/X
GWH			X	S/B/X
EMT			X	S/B/X
SMGW			X	S/B/X

Tabelle 2 PKI-Teilnehmerrollen relevant für GWAdriga Smart Energy CA

Für den Betrieb der GWAdriga Smart Energy CA wird die Trennung von Instanzen gemäß [SM-PKI-Policy] eingehalten, vgl. auch Abschnitt 6.2.6.

1.3.1. Zertifizierungsstellen

1.3.1.1. Root-CA

Die Root-CA ist die oberste Zertifizierungsinstanz der nationalen Smart Metering PKI, wird vom BSI betrieben und stellt zwei der drei Sub-CA-Zertifikate für die GWAdriga Smart Energy CA aus:

- ein Zertifikat zum Signieren und
- ein TLS-Zertifikat für die TLS-Kommunikation zwischen Sub-CA und Root-CA.

1.3.1.2. Sub-CA

Eine Sub-CA ist eine Zertifizierungsinstanz der zweiten Ebene der Smart Metering PKI. Sie stellt die Zertifikate für die PKI-Teilnehmer EMT, GWA, GWH und SMGW aus.

Die vorliegende GWAdriga Smart Energy CA Policy definiert alle Regelungen für den Betrieb als Sub-CA unterhalb der nationalen Smart Metering Root-CA:

- unter Einhaltung aller Anforderungen der Root-CA,
- als GWAdriga-eigene Zertifizierungsstelle (**Fremdbetrieb durch den Betreiber für GWAdriga** - wie in Abschnitt 1 ausgeführt -),
- es werden Endnutzer-Zertifikate für verschiedene Vertragskunden ausgestellt und
- die Endnutzerzertifikate werden mit dem Zertifikat einer Sub-CA-Instanz signiert, die am CN erkennbar ist.

Zur TLS-Kommunikation zwischen Sub-CA und den PKI-Teilnehmern stellt die GWAdriga Smart Energy CA für sich selbst ein TLS-Zertifikat aus.

Die Rollen bzw. Technische Komponenten innerhalb der Zertifizierungsstelle, die in diesem Dokument angesprochen werden sind:

Rolle/Technische Komponente	Kürzel	Aufgabe
Zertifizierer (Rolle)	-	Erfüllung aller Aufgaben, um per S/MIME-Kommunikation eingegangene Zertifikatsrequests der Zertifizierung zuzuführen und die Zertifizierungsergebnisse (Zertifikate oder Fehlermeldungen) an den Antragsteller zurück zu geben.
Webservice (Techn. Komponente)	-	Bereitstellung der Webservice-Schnittstelle u. a. für die automatisierte Verarbeitung von Zertifikatsrequest-Paketen, Weitergabe des Pakets nach Eingangsprüfung an das CA-System
CA-System (Techn. Komponente)	-	Durchführung der Zertifizierung, Durchführung der Sperrung
Keymanager (Rolle)	-	Rolle zur Administration der HSMs der Zertifizierungsstelle

Tabelle 3 Rollen bzw. Technische Komponenten innerhalb der Zertifizierungsstelle relevant für SM-GWAdriga Policy

Über die hier aufgeführten Rollen hinaus gibt es weitere Rollen, die im Rollenkonzept [Betr_Roko] spezifiziert sind.

Für den Testbetrieb stellt GWAdriga Smart Energy CA eine zugehörige Test-CA bereit, vgl. Abschnitte 1.1 und Anhang Testbetrieb.

1.3.2. Registrierungsstellen

Die GWAdriga Smart Energy CA verfügt über eine Registrierungsstelle, um

- die initialen Registrierungen durchzuführen sowie
- die Wiederholungsanträge der Endnutzer zu bearbeiten – sofern sie per E-Mail eingehen.

Die Registrierung besteht aus:

- der zweifelsfreien Identifizierung des Antragstellers,
- der Authentifizierung der PKI-Rolle und
- der Authentifizierung der Identitätsdaten der ausführenden Personen für den Antragsteller (im folgenden Ansprechpartner genannt).

Bei Nutzung des Webservices für Wiederholungsanträge und bei Smart Meter Gateways (SMGW) auch für initiale Anträge erfolgt die Registrierung automatisiert. Dies ist möglich, da die Kommunikation zum Webservice TLS-gesichert durchgeführt wird, so dass der Antragsteller authentisch ist. Ferner besitzen per Webservice eingehende Request-Pakete eine äußere Signatur durch den Antragsteller.

Die einzelnen Rollen innerhalb der Registrierungsstelle:

Rolle	Kürzel	Aufgabe
Registrierungsstelle	RA	übergeordnete Bezeichnung für TS und RG
Teilnehmerservice	TS	Single Point of Contact für die Zertifikatsnehmer, Funktions-Postfach: pki@gwadriga.de, gibt die eingegangenen Mails in die Registrierung
Registrator	RG	Interne Rolle zur Bearbeitung der Anträge
Leiter GWAdriga Smart Energy CA	(L-SGC)	Eskalationsstufe

Tabelle 4 Rollen der GWAdriga Smart Energy CA

1.3.3. Zertifikatsnehmer

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

SMGW technische Komponente (Kommunikationseinheit eines intelligenten Messsystems, siehe [TR-03109-1]), die von der GWAdriga Smart Energy CA mit Zertifikaten ausgestattet wird, welche für die Durchführung der definierten Prozesse und Kommunikationsverbindungen benötigt werden. Auf ein SMGW wird vom Hersteller (GWH, s. unten) ein Gütesiegelzertifikat aufgebracht. Zur Inbetriebnahme wird ein SMGW immer von einem GWA verwaltet. Der GWA bringt dazu ein Wirkzertifikat auf.

Anmerkung: Beide Zertifikate (Gütesiegel- und Wirkzertifikat) können von unterschiedlichen Sub-CAen ausgegeben sein.

GWA ein Gateway-Administrator 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 einer Sub-CA Zertifikate, mit denen er

- die Beantragung und Verwaltung der Wirkzertifikate der SMGWs durchführen,
- die Administration der SMGWs durchführen und
- den Datenaustausch mit den anderen Teilnehmern der SM-PKI (z. B. EMT) absichern kann.

GWH: Ein Hersteller von Gateway-Komponenten erhält von einer oder mehreren Sub-CA der SM-PKI Zertifikate, mit denen er insbesondere die Prozesse zur Beantragung und Verwaltung von Gütesiegelzertifikaten für SMGWs durchführen kann.

EMT: Ein externer Marktteilnehmer (EMT) erhält von einer Sub-CA der SM-PKI Zertifikate, mit denen er insbesondere mit den SMGWs sicher kommunizieren kann. Überdies

kann der Datenaustausch mit den anderen Teilnehmern der SM-PKI (z. B. einem GWA) abgesichert werden. Die Teilnehmer der Marktkommunikation sind EMT.

Aktiver EMT — Ein aktiver EMT nutzt ein SMGW, um über dieses nachgelagerte Geräte (Controllable Local Systems, CLS) anzusprechen. Die entsprechenden Anwendungsfälle zur Steuerung von CLS an der HAN-Schnittstelle durch einen EMT sind in der [TR-03109-1] definiert.

1.3.4. Zertifikatsnutzer

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

1.3.5. Andere Teilnehmer

Endverbraucher sind weder Teilnehmer dieser Policy noch der übergeordneten SM-PKI Policy, da sie keine Verpflichtungen hinsichtlich beider Policies eingehen.

Die Begriffe „Antragsteller“, „Vertreter“ und „Dienstleister“ werden im Glossar erläutert.

1.4. Verwendung von Zertifikaten

1.4.1. Erlaubte Verwendung von Zertifikaten

Die Zertifikate der PKI-Teilnehmer werden

- zur Authentisierung,
- zur Verschlüsselung und
- zur Erstellung von elektronischen Signaturen

eingesetzt werden.

Die nachfolgenden Tabellen zeigen die Zertifikate, die für die GWAdriga Smart Energy CA relevant sind:

- Zertifikate, die die Sub-CA einsetzt -> vgl. Tabelle 5
- Zertifikate, die die Sub-CA ausstellt -> vgl. Tabelle 6

Zertifikate der Sub-CA	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,

Zertifikate der Sub-CA	Signiert durch	Verwendungszweck
		GWH, EMT, SMGW- sowie CTLS(Sub-CA)-Zertifikaten verwendet. Zusätzlich wird der zugehörige private Schlüssel auch für die Signatur des Sub-CA-CRL eingesetzt, vgl. [TR-03109-4]#Abschnitt 2.2.2
CTLS, Root(Sub-CA)	Privater Schlüssel zu CTLS-S(Root)	Diese Zertifikate werden beim Aufbau des TLS-Kommunikationskanals zwischen Sub-CA und der Root für das Zertifikatsmanagement eingesetzt.
CTLS(Sub-CA)	Privater Schlüssel zu C(Sub-CA)	Diese Zertifikate werden beim Aufbau des TLS-Kommunikationskanals zwischen Sub-CA und anderen Systemen eingesetzt.

Tabelle 5 Verwendete Zertifikate der GWAdriga Smart Energy CA

Zertifikate ausgestellt durch die Sub-CA	Signiert durch	Verwendungszweck
CTLS(Sub-CA)	Privater Schlüssel zu C(Sub-CA)	Diese Zertifikate werden beim Aufbau des TLS-Kommunikationskanals zwischen Sub-CA und anderen Systemen eingesetzt.
CTLS(EMT) CTLS(GWA) CTLS(GWH) CTLS(SMGW)	Privater Schlüssel zu C(Sub-CA)	Zertifikat des entsprechenden Endnutzers zur Authentisierung beim Kommunikationspartner und zum Aufbau einer TLS- Verbindung (vgl. [TR-03116-3]). Das Zertifikat CTLS(GWA) wird zudem auch für die Authentifikation am Sicherheitsmodul des SMGW verwendet.
CEnc(EMT) CEnc(GWA) CEnc(GWH) CEnc(SMGW)	Privater Schlüssel zu C(Sub-CA)	Zertifikat zur Verschlüsselung von Inhaltsdaten für den entsprechenden Endnutzer. EMT-Zertifikate, deren Extension mit MAK beginnt, werden für die Datenübertragung in der Marktkommunikation (vgl. [TR-03116-3] Abschnitt 9) verwendet.
CSig(EMT) CSig(GWA) CSig(GWH) CSig(SMGW)	Privater Schlüssel zu C(Sub-CA)	Zertifikat zur Verifikation von Inhaltsdatensignaturen des entsprechenden Endnutzers. EMT-Zertifikate, deren Extension mit MAK beginnt, werden für die Datenübertragung in der Marktkommunikation (vgl. [TR-03116-3] Abschnitt 9) verwendet.

Tabelle 6 Von GWAdriga Smart Energy CA ausgestellte Zertifikate und deren Verwendungszweck

Die nachfolgende Abbildung enthält alle zuvor aufgeführten Zertifikate und zeigt grafisch die Zusammenhänge hinsichtlich der Signierung der einzelnen Zertifikate auf. Der grüne Rahmen kennzeichnet

die von der Sub-CA GWAdriga Smart Energy CA ausgestellten Zertifikate, vgl. **Tabelle 6**, Spalte „Signiert durch“:

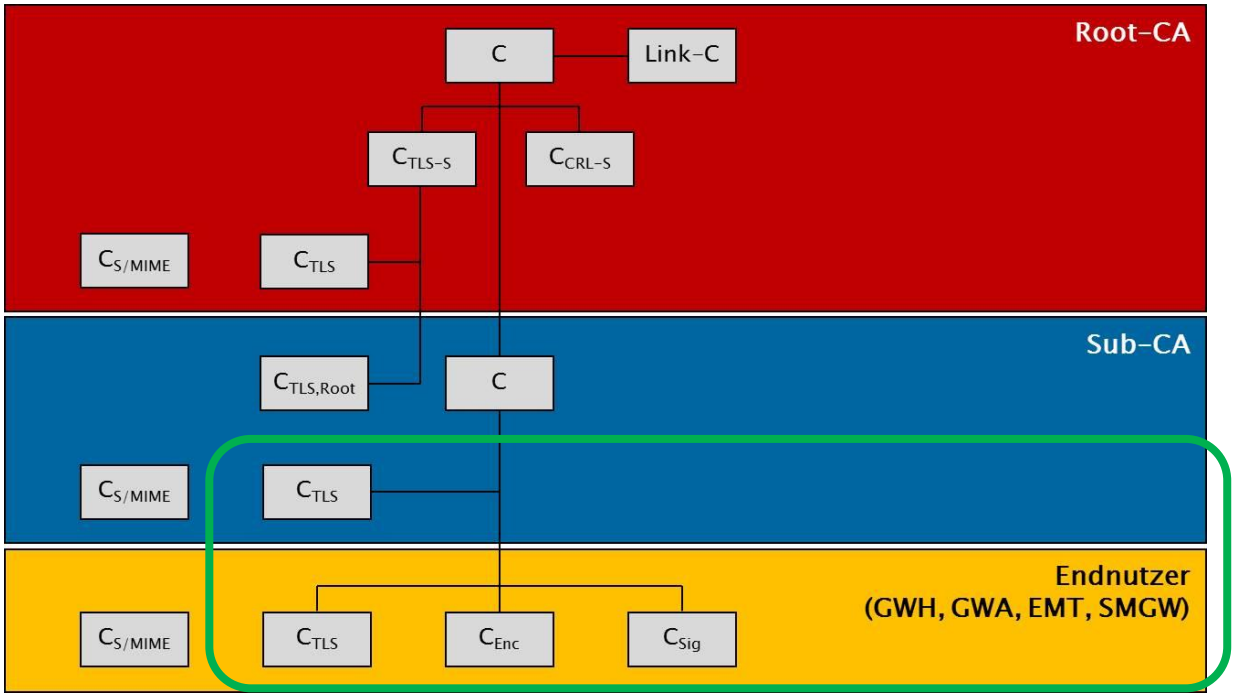

Abbildung 1 Smart Metering Zertifikate, die die GWAdriga Smart Energy CA ausstellt

1.4.2. Verbotene Verwendung von Zertifikaten

Alle Verwendungszwecke der oben aufgeführten Zertifikate, die in **Tabelle 6**, Spalte „Verwendungszweck“ enthalten sind, sind erlaubt. Andere Verwendungszwecke sind nicht zulässig.

1.5. Administration der GWAdriga Smart Energy CA Policy

Die für dieses Dokument verantwortliche Organisation ist GWAdriga GmbH & Co. KG:

Firma/Organisation:	GWAdriga GmbH & Co. KG
Abteilung:	PKI Services
Adresse:	Kurfürstendamm 33 10719 Berlin
Fax:	+49 030 95 999 09-12
E-Mail:	pki@gwadriga.de
Webseite:	https://www.gwadriga.de/pki

Tabelle 7 Administration Policy

1.5.1. Pflege der GWAdriga Smart Energy CA Policy

Nach jeder Aktualisierung wird dieses Dokument unter der o.a. Webseite abgelegt.

1.5.2. Zuständigkeit für das Dokument

Siehe Abschnitt 1.5.

1.5.3. Ansprechpartner /Kontaktperson

Siehe Abschnitt 1.5, Zeile „Fax und E-Mail-Adresse“.

1.5.4. Zuständiger für die Anerkennung eines CPS

Siehe Abschnitt 1.5, Zeile „Abteilung“. Ein CPS ist Bestandteil der Betriebsdokumentation.

1.5.5. CPS-Aufnahmeverfahren

Ein CPS für die GWAdriga Smart Energy CA Policy muss alle Anforderungen dieses Dokumentes umsetzen.

2. Verantwortlichkeit für Veröffentlichungen und Verzeichnisse

2.1. Verzeichnisse

Von der GWAdriga Smart Energy CA werden folgende Verzeichnisse geführt:

- ein LDAP-Verzeichnis mit allen von der jeweiligen CA ausgestellten und noch gültigen Zertifikaten (eingeschränkt verfügbar)
- eine auf den Verantwortungsbereich beschränkte Sperrliste, in der alle gesperrten Zertifikate während ihres Gültigkeitszeitraums aufgeführt sind (öffentlich verfügbar)

2.2. Veröffentlichung von Informationen zur Zertifikatserstellung

2.2.1. Veröffentlichungen der Sub-CA

Die Sub-CA GWAdriga Smart Energy CA stellt eine Webseite zur Verfügung, die alle geforderten Informationen bereitstellt:

- Kontaktdaten der Sub-CA, u.a.
    - alle Daten der Ansprechpartner des Sub-CA-Betreibers, die zum Senden eines Sperrauftrags benötigt werden, vgl. Abschnitt 3.5.1.
- Die aktuellen Zertifikate der Sub-CA inklusive der SHA256Hashs. Das Format, in dem die Zertifikate und Hash vorliegen, wird angegeben.
- Parameter zur Einrichtung eines Zugriffs auf die Sperrliste bzw. das LDAP-Verzeichnis
- Das vorliegende Dokument, die Certificate Policy der Sub-CA GWAdriga Smart Energy CA, die die folgenden Mindestanforderungen erfüllt:
    - Die CP bestätigt die Einhaltung der Policy der Root-CA [SM-PKI-Policy].

- Die CP beschreibt die für die Bereitstellung und Verwaltung der Zertifikate notwendigen Prozesse.
- Die CP benennt die für den Betrieb verantwortlichen Bereiche / Ansprechpartner.

Die folgenden weiteren Informationen werden bereitgestellt:

- Beschreibung des Antragsverfahrens von Zertifikaten unterhalb der GWAdriga Smart Energy CA
- Formulare zur Beantragung von Zertifikaten
- Informationen zu den zu erstellenden jeweiligen Zertifikatsrequests(-Paketen)
- Informationen zum Sperrprozess sowie Formular zum Sperren von Zertifikaten
- Hinweise zur Teilnahme am Testbetrieb
- FAQ zu „Verwandte Zertifikate“
- LDIF-Datei zur Bereitstellung von EMT-MAK-Zertifikaten gemäß ChangeLog der Root-CA

2.3. Zeitpunkt und Häufigkeit der Veröffentlichungen

Die Veröffentlichungen der GWAdriga Smart Energy CA werden wie folgt aktualisiert:

- LDAP-Verzeichnis:
  unmittelbar nach der Ausstellung eines Zertifikats
- Sperrliste:
  - Eintrag einer Sperrung oder Suspendierung innerhalb der in [TR-03109-4] festgelegten Zeiten
  - Ist ein gesperrtes Zertifikat abgelaufen, wird es aus der Sperrliste ausgetragen

2.4. Zugriffskontrollen auf Verzeichnisse

Zugriffskontrollen auf das LDAP-Verzeichnis umfassen folgende Punkte:

- Es wird ausschließlich lesender Zugriff gewährt.
- Der Zugriff ist beschränkt auf alle an der SM-PKI teilnehmenden Organisationen wie die Root-CA, die Sub-CAen, die GWAs, die GWHs und EMTs.
- Der Zugriff wird über eine zertifikatsbasierte Authentisierung mittels der TLS-Zertifikate der Zertifikatsnehmer gewährt.

3. Identifizierung und Authentifizierung

Dieser Abschnitt beschreibt alle Prozessschritte der GWAdriga Smart Energy CA, um die Identität und die Berechtigung eines Antragstellers (und späteren Zertifikatsnehmers) der verschiedenen Endnutzer-Zertifikate (**EMT, GWA, GWH** oder **SMGW)** vor dem Ausstellen eines Zertifikats festzustellen.

Die Profile der Zertifikatsrequests der einzelnen Zertifikatsnehmer sind konform zu [TR-03109-4].

Zum Ausstellen des eigenen Sub-CA-Zertifikats CTLS(Sub-CA) erfolgt keine Identifizierung und Authentifizierung. In den Abschnitten 3.1 und 4.2.3.1 wird das für sich selbst auszustellende Zertifikat der Vollständigkeit halber aufgeführt. Ab Abschnitt 3.2 bis 4.1.1 und 4.3 bis einschließlich Abschnitt 4.7 werden ausschließlich Regelungen für die PKI-Teilnehmer unterhalb der GWAdriga Smart Energy CA beschrieben.

3.1. Regeln für die Namensgebung

Die Common Name (CN) der verschiedenen SM-PKI Teilnehmer entsprechen dem folgenden Schema:

‘<org>.<function>[.<extension>]‘

Zertifikatstyp	Attribut (Kürzel)	Wert	Erläuterung
C(Sub-CA)	common name (CN)	„<org>.CA“	Eindeutiger Name der Sub-CA
CTLS,Root(Sub-CA)	common name (CN)	„<org>.CA.TLS“	Kennzeichnung als TLS-Zertifikat der Sub-CA
CTLS(Sub-CA)	common name (CN)	„<org>.CA.TLS“	Kennzeichnung als TLS-Zertifikat der Sub-CA
CTLS(EMT) CTLS(GWA) CTLS(GWH) CTLS(SMGW)	common name (CN)	<org>.EMT[.<extension>] <org>.GWA[.<extension>] <org>.GWH[.<extension>] <org>.SMGW[.<extension>]	Der CN eines Endnutzer-Teilnehmers wird für alle drei Zertifikatstypen verwendet, wg. der Unterscheidung siehe nächste Tabelle
CEnc(EMT) CEnc(GWA) CEnc(GWH) CEnc(SMGW)	common name (CN)	<org>.EMT[.<extension>] <org>.GWA[.<extension>] <org>.GWH[.<extension>] <org>.SMGW[.<extension>]	
CSig(EMT) CSig(GWA) CSig(GWH) CSig(SMGW)	common name (CN)	<org>.EMT[.<extension>] <org>.GWA[.<extension>] <org>.GWH[.<extension>] <org>.SMGW[.<extension>]	

Tabelle 8 Common Name der PKI-Teilnehmer

Für Zertifikate der Marktkommunikation sind die ersten 3 Zeichen der <extension> des Attributes commonName (CN) fest vorgegeben: „MAK“. Die weiteren 7 Zeichen sind frei wählbar im Rahmen der verfügbaren Zeichen.

3.1.1. Arten von Namen

Die Inhalte für die Identifikation des Zertifikatsinhabers (Subject) bzw. des Zertifikatsherausgebers (Issuer) der verschiedenen von GWAdriga Smart Energy CA ausgestellten Zertifikate sind wie folgt spezifiziert:

Zertifikats-typ	Subject-CN	Issuer-CN	KeyUsage	KeyUsage Octet-String
CTLS(Sub-CA)	<org>.CA.TLS	GWAdriga-SmartEnergy.CA	DigitalSignature	80
CTLS(EMT) CTLS(GWA) CTLS(GWH) CTLS(SMGW)	<org>.EMT[.<extension>] <org>.GWA[.<extension>] <org>.GWH[.<extension>] <org>.SMGW[.<extension>]	GWAdriga-SmartEnergy.CA	DigitalSignature	80
CEnc(EMT) CEnc(GWA) CEnc(GWH) CEnc(SMGW)	<org>.EMT[.<extension>] <org>.GWA[.<extension>] <org>.GWH[.<extension>] <org>.SMGW[.<extension>]	GWAdriga-SmartEnergy.CA	KeyEnciphermen t, KeyAgreement	28
CSig(EMT) CSig(GWA) CSig(GWH) CSig(SMGW)	<org>.EMT[.<extension>] <org>.GWA[.<extension>] <org>.GWH[.<extension>] <org>.SMGW[.<extension>]	GWAdriga-SmartEnergy.CA	DigitalSignature	80

Tabelle 9 Weitere Bestandteile des Zertifikatsprofils der PKI-Teilnehmer

Für die Endnutzer-Zertifikatstypen (für Rollen SMGW, GWA, GWH und EMT) erfolgt die Unterscheidung nicht über das Feld Subject, sondern über die Extension KeyUsage. Wenn ein TLS-Zertifikat beantragt wird, muss außerdem die Extension ExtendedKeyUsage vorhanden sein, ansonsten darf die Extension nicht vorhanden sein.

In EMT-Zertifikaten für die Marktkommunikation muss verpflichtend

- in das Attribut organisationalUnit (OU) die Marktpartner-ID des Teilnehmers der Marktkommunikation eingetragen werden und
- in der Extension SubjectAltName die URI des zugehörigen AS4-Webservice angegeben werden.

3.1.2. Notwendigkeit für aussagefähige Namen

Die Angaben der Zertifikatsinhaber aus Abschnitt 3.1.1 werden in die Zertifikate aufgenommen.

3.1.3. Anonymität oder Pseudonymität von Zertifikatsnehmern

Anonymität oder Pseudonymität von Zertifikatsnehmern sind nicht erlaubt.

3.1.4. Eindeutigkeit von Namen

Ein bereits vergebener CN unterhalb ein und derselben CA kann nicht für einen zweiten Zertifikatsnehmer verwendet werden. Der Zertifikatsnehmer wird informiert, die Angabe eines neuen CNs ist erforderlich, ein neuer Request ist einzureichen.

Für CNs unterhalb verschiedener Sub-CAs, z. B. bei Erneuerung der CA-Zertifikate besteht diese Forderung nach Eindeutigkeit nicht.

3.1.5. Anerkennung, Authentifizierung und die Rolle von Markennamen

Ein Firmenname, vgl. Angaben <org> im Subject-CN, wird auf Basis der Identität eines Zertifikatsnehmers im Zertifikat verwendet. Die initiale Überprüfung des CNs zur Übernahme in das erste Zertifikat erfolgt wie in Abschnitt 3.2.2 beschrieben:

- für EMT-Zertifikate: Abschnitt 3.2.2.1,
- für GWA-Zertifikate: Abschnitt 3.2.2.2,
- für GWH-Zertifikate: Abschnitt 3.2.2.3 und
- für SMGW-Zertifikate: Abschnitt 3.2.2.4.

3.2. Initiale Überprüfung zur Teilnahme an der PKI

Dieser Abschnitt beschreibt den formalen Prozess zur Beantragung der Registrierung einschließlich der verwendeten Schnittstellen und ggf. der öffentlich zur Verfügung stehenden Informationen zum Beantragungsprozess.

3.2.1. Methoden zur Überprüfung bzgl. Besitz des privaten Schlüssels

Für ein Endnutzer-Zertifikat erstellt der Antragsteller unmittelbar vor der Beantragung ein Schlüsselpaar; der private Schlüssel wird zur Erstellung eines Zertifikatsrequests verwendet.

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

Diese wird bei der Antragsprüfung durch Verifikation der inneren Signatur gegen den im Zertifikatsrequest enthaltenen zugehörigen öffentlichen Schlüssel durch die GWAdriga Smart Energy CA geprüft, um festzustellen, ob der Antragsteller im Besitz des privaten Schlüssels ist.

3.2.2. Authentifizierung von Organisationszugehörigkeiten

Authentifiziert werden können Personen, nicht aber technische Komponenten.

Bei der Authentifizierung ist zwischen

- der Authentifikation einer Organisation (eines Unternehmens oder Instituts) als juristische Person und
- der Authentifikation von Ansprechpartnern der Organisation als natürliche Person

zu unterscheiden.

Für alle Anträge EMT, GWA und GWH gilt:

- Die Identität eines Antragstellers wird bestimmt anhand seines Organisationsnamens und der im Antrag angegebenen Nummer des Organisationsnachweises (i.R. des Handelsregisters).
- Wenn ein zweiter Antrag von einem bereits registrierten Antragsteller eingeht, dann werden die Registrierungsdaten zu beiden Anträgen verbunden.
- Ein weiterer Antrag eines Antragstellers zur gleichen Rolle EMT, GWA, GWH ist nur dann möglich, wenn
    - das Zertifikat zum Vorgängerantrag aufgegeben werden soll (entweder durch zeitnahes Erreichen des Gültigkeitsendes oder durch Sperrung) und der weitere Antrag neue Registrierungsdaten enthält (z. B. ein anderer CN),
    - das Vorgängerzertifikat abgelaufen ist.
- Ein weiterer Antrag eines Antragstellers zu einer anderen Rolle EMT, GWA, GWH ist möglich und erfordert ein eigenes Registrierungsverfahren.

3.2.2.1. EMT

Wenn ein externer Marktteilnehmer (EMT) einen Antrag auf Registrierung stellt, führt die GWAdriga Smart Energy CA

- eine Authentifikation des Unternehmens

durch.

Vor der Registrierung:

- Formular für Antragschreiben herunterladen/ausfüllen per Webpage, vgl. Link dazu in Abschnitt 1.5

Voraussetzungen, notwendige Unterlagen und Daten für die Registrierung sind:

- Der Antragsteller ist Vertragskunde, vgl. 1.1,
- Antragschreiben zur Ausgabe eines EMT-Zertifikats mit folgenden Daten bzw. beigefügten Bestätigungen
    - Name der Firma bzw. der Institution
    - Anschrift des Unternehmens bzw. der Institution

- Unternehmensnachweis (z. B. aktueller Auszug aus dem Handelsregister) oder Nachweis der Institution (durch ein entsprechendes Siegel der Institution)
- Kontaktdaten der Ansprechpartner (unter Beachtung einer Vertreterregelung)
- Bei der Beauftragung eines Dienstleisters für den Betrieb des EMT MUSS der Betreiber eine Bestätigung des Unternehmens vorlegen, die den Dienstleister zur Beantragung und zum Betrieb für den EMT berechtigt.
- Bestätigung der Geschäftsführung des Unternehmens bzw. der Leitung der Institution, in der der Vertreter des Betreibers berechtigt wird, den Antrag für den EMT zu stellen und in der Sache dazu verbindliche Aussagen und Angaben zu machen.
- Bestätigung, dass die Sicherheitsvorgaben an einen EMT eingehalten werden, und dass eine entsprechende Erklärung und die dafür erforderlichen Nachweise beigefügt sind.
- Bestätigung, dass die Nutzungsbedingungen der GWAdriga Smart Energy CA und die SM-GWAdriga Policy eingehalten werden.
- Der Antragsteller verpflichtet sich, Änderungen an allen Daten im Antrag (z. B. den Wechsel eines Ansprechpartners) zeitnah mitzuteilen. Zu diesen Daten gehören auch die vorgelegten Nachweise: Sollte eine Zertifizierung nicht mehr gültig sein, so verpflichtet sich der EMT dies mitzuteilen.

- Persönliche/individuelle Zertifikate für die gesicherte E-Mail-Kommunikation der benannten Ansprechpartner (CS/MIME(EMT)) inklusive der zur Verifikation erforderlichen Zertifikatskette.
- Erklärung zur Nutzung des EMT-Zertifikats
  - Aus der Erklärung MUSS nachvollzogen werden können, welche Funktionen und Aufgaben ein EMT wahrnehmen will. Es MUSS daraus insbesondere hervorgehen, ob es sich um einen aktiven oder passiven EMT handelt. Aus der Erklärung muss hervorgehen, ob es sich um einen Teilnehmer der Marktkommunikation handelt.
  - Ein EMT verpflichtet sich bei einem Wechsel von passivem zu aktivem EMT oder umgekehrt, die GWAdriga Smart Energy CA rechtzeitig zu informieren und die erforderlichen Unterlagen für die neue EMT-Rolle vorzulegen, vgl. nächster Abschnitt.
  - Ein EMT verpflichtet sich bei einem Wechsel von passivem zu aktivem EMT die Aufgabe des aktiven EMTs erst dann auszuüben, wenn der Antrag auf Wechsel zum aktiven EMT von GWAdriga Smart Energy CA per signierter E-Mail bestätigt wurde.
  - Zum Abschluss des Rollenwechsels MÜSSEN bestehende Zertifikate gesperrt werden. Für die Wahrnehmung der neuen Rolle als passiver oder aktiver EMT MUSS ein neues initiales Zertifikat beantragt und ausgestellt werden. Dies erfolgt wie zuvor per signierter/verschlüsselter Mail von einem autorisierten Ansprechpartner mit einem CSR.

- Wenn eine Sub-CA einen aktiven EMT positiv geprüft hat, wird dies dokumentiert und dem aktiven EMT in Form eines elektronisch signierten Nachweises zur Verfügung gestellt.

- Teilnehmer der Marktkommunikation MÜSSEN vor der Beantragung von EMT-Zertifikaten mit der Extension MAK und der Marktpartner-ID im OU-Attribut eine Zuteilungsurkunde einreichen, die eine autorisierte Nutzung der Marktpartner-ID bescheinigt. Die Zuteilungsurkunde kann je nach Anwendungsgebiet von verschiedenen Betreibern der Codenummernverzeichnisse (z.B: „BDEW Energie Codes GmbH“ für die Sparte Strom und DVGW Service und Consult GmbH für die Sparte Gas) ausgestellt werde. GWAdriga Smart Energy CA gleicht die Angaben der Zuteilungsurkunde mit den öffentlich verfügbaren Informationen der jeweiligen Codenummernverzeichnisse ab. Wenn eine Organisation über mehr als eine Zuteilungsurkunde verfügt, können alle Zuteilungsurkunden bei der Beantragung des ersten EMT-Zertifikatetripels angegeben werden. Pro Zertifikatetripel kann jedoch nur jeweils eine Marktpartner-ID eingetragen wer-den.
- Erklärung zur Einhaltung der Sicherheitsvorgaben aus der SM-PKI Policy
  - Der EMT MUSS eine Erklärung zur Einhaltung der Sicherheitsvorgaben aus der SM-PKI Policy mit einreichen.
  - Ein passiver EMT MUSS ein Sicherheitskonzept erstellen und umsetzen, in dem die Anforderungen aus der SM-PKI Policy berücksichtigt werden, vgl. Abschnitt 5.1.1.
  - Ein aktiver EMT (siehe Abschnitt 1.3.3) MUSS eine ISO 27001-Zertifizierung vorweisen bzw. nachweisen, dass ein nach ISO 27001 zertifizierter Dritter die Leistung für ihn erbringt, vgl. Abschnitt 5.1.1.
  - Der EMT MUSS den Nachweis des sicheren Betriebs gemäß den Vorgaben zu den Anforderungen für die Teilnahme an der SM-PKI erbringen:
    - Der EMT fügt dem Antrag zum Wirkbetrieb die Bestätigung zur erfolgreichen Teilnahme am Testbetrieb bei.
- Bestätigung der erfolgreichen Testteilnahme
  - Vor der initialen Identifizierung und Authentifizierung MUSS die Zertifikatsausstellung und -sperrung von EMT-Zertifikaten unterhalb der zur GWAdriga Smart Energy CA zugehörigen Test-Sub-CA (siehe Abschnitt 1.3.1) der Test-PKI entweder vom Antragsteller oder seinem Dienstleister erfolgreich erprobt worden sein. Die erfolgreiche Teilnahme wird von einem Ansprechpartner der Test-Sub-CA per signierter E-Mail bestätigt.
- Der Hashwert (SHA 256) des initialen Zertifikatsrequest-Pakets für das Signatur- (CSig(EMT)), das Verschlüsselungs- (CEnc(EMT)) und das TLS-Zertifikat (CTLS(EMT)) des EMT (gemäß [TR-

03109-4]) MUSS in gedruckter Form inklusive der Information zum Format der Darstellung mit der Bestätigung durch die Unterschrift des Bevollmächtigten zugesendet werden. Der Hashwert wird dabei über die binär-codierte Request-Datei gebildet, welche das Zertifikatsrequest-Paket gemäß [TR-03109-4] enthält, und als base64-codierter Ausdruck in diesem Prozess verwendet.

  - Im Wirkbetrieb wird empfohlen, das Zertifikatsrequest-Paket der GWAdriga Smart Energy CA vorab zuzusenden.

3.2.2.2. GWA

Wenn ein neuer Gateway-Administrator (GWA) einen Antrag auf Registrierung stellt, führt die GWAdriga Smart Energy CA:

- eine Authentifikation des Unternehmens und
- eine persönliche Identifikation und Authentifikation (anhand der Antragsdaten, der S/MIME-Kommunikation und mit zusätzlichem Präsenztermin) von mindestens zwei bevollmächtigten Vertretern des GWAs

durch.

Vor der Registrierung:

- Formular für Antragschreiben herunterladen/ausfüllen per Webpage, vgl. Link dazu in Abschnitt 1.5

Voraussetzungen, notwendige Unterlagen und Daten für die Registrierung sind:

- Der Antragsteller ist Vertragskunde, vgl. 1.1,
- Antragschreiben zur Ausgabe eines GWA-Zertifikats mit folgenden Daten bzw. beigefügten Bestätigungen
  - Name der Firma bzw. der Institution;
  - Anschrift des Unternehmens bzw. der Institution;
  - Unternehmensnachweis (z. B. aktueller Auszug aus dem Handelsregister) oder Nachweis der Institution (durch ein entsprechendes Siegel der Institution);
  - Kontaktdaten der Ansprechpartner des Unternehmens (unter Beachtung einer Vertreterregelung)
  - Sollte ein Dienstleister für den Betrieb eines GWA beauftragt werden, MUSS zusätzlich zu den genannten Unterlagen eine schriftliche Bestätigung durch den Auftraggeber (hier: Antragsteller) mit Benennung der autorisierten Ansprechpartner des Dienstleisters für den Betrieb als GWA vorgelegt werden.
    Der GWA-Dienstleister 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.
    - Bestätigung der Geschäftsführung des Unternehmens bzw. der Leitung der Institution, in der der Vertreter des Betreibers berechtigt wird, den Antrag für den GWA zu stellen und in der Sache dazu verbindliche Aussagen und Angaben zu machen;
    - Bestätigung, dass die Sicherheitsvorgaben an einen GWA eingehalten werden, und dass eine entsprechende Erklärung und die dafür erforderlichen Nachweise beigefügt sind.
    - Bestätigung, dass die Nutzungsbedingungen der GWAdriga Smart Energy CA und die SM-GWAdriga Policy eingehalten werden;
    - Der Antragsteller verpflichtet sich, Änderungen an allen Daten (z. B. den Wechsel eines Ansprechpartners) im Antrag, zeitnah mitzuteilen. Zu diesen Daten gehören auch die vorgelegten Nachweise: Sollte eine Zertifizierung nicht mehr gültig sein, so verpflichtet sich der GWA dies mitzuteilen.
- Persönliche/individuelle Zertifikate für die gesicherte E-Mail-Kommunikation der benannten Ansprechpartner (CS/MIME(GWA)) inklusive der zur Verifikation erforderlichen Zertifikatskette
- Erklärung zur Einhaltung der Sicherheitsvorgaben aus der SM-PKI Policy
    - Ein GWA MUSS alle Anforderungen gemäß [TR-03109-6] erfüllen und das entsprechende Zertifikat nachweisen, vgl. Abschnitt 5.1.1.
      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.
    - Nachweise über die Einhaltung der Vorgaben zu den Anforderungen für die Teilnahme an der SM-PKI:
        - Der GWA bestätigt, dass ausschließlich SMGW-Zertifikate für SMGWs beantragt werden, die über
            - eine Zertifizierung entsprechend [TR-03109-1] und
            - eine CC-Zertifizierung entsprechend [BSI-CC-PP-0073]

          verfügen.
        - Der GWA fügt dem Antrag zum Wirkbetrieb die Bestätigung zur erfolgreichen Teilnahme am Testbetrieb bei.
- Erklärung zur Nutzung des GWA-Zertifikats
    - Aus der Erklärung MUSS nachvollzogen werden können, welche Funktionen und Aufgaben der GWA beabsichtigt wahrzunehmen. Die Nutzung der GWA-Zertifikate für Funktionen und Aufgaben der Rolle EMT ist nicht zulässig. In diesem Fall ist ein weiterer Antrag für die EMT-Rolle zu stellen, vgl. 3.2.2.1.

- Bestätigung der erfolgreichen Testteilnahme
    - Vor der initialen Identifizierung und Authentifizierung MUSS die Zertifikatsausstellung und -sperrung von GWA- und SMGW-Zertifikaten unterhalb der zur GWAdriga Smart Energy CA zugehörigen Test Sub-CA der Test-PKI erprobt worden sein. Die erfolgreiche Teilnahme wird von einem Ansprechpartner der Test-Sub-CA per signierter E-Mail bestätigt.
- Der Hashwert (SHA 256) des initialen Zertifikatsrequest-Pakets für das Signatur- (CSig(GWA)), das Verschlüsselungs- (CEnc(GWA)) und das TLS-Zertifikat (CTLS(GWA)) des GWA (gemäß [TR-03109-4]) MUSS in gedruckter Form inklusive der Information zum Format der Darstellung mit der Bestätigung durch die Unterschrift des Bevollmächtigten vorgelegt werden. Der Hashwert wird dabei über die binär-codierte Request-Datei gebildet, welche das Zertifikatsrequest-Paket gemäß [TR-03109-4] enthält, und als base64-codierter Ausdruck in diesem Prozess verwendet.
    - Im Wirkbetrieb wird empfohlen, das Zertifikatsrequest-Paket der GWAdriga Smart Energy CA vorab zuzusenden.

3.2.2.3. GWH

Wenn ein neuer Gateway-Hersteller (GWH) einen Antrag auf Registrierung stellt, führt die GWAdriga Smart Energy CA:

- eine Authentifikation des Unternehmens und
- eine persönliche Identifikation und Authentifikation (anhand der Antragsdaten, der S/MIME-Kommunikation und mit zusätzlichem Präsenztermin) von mindestens zwei bevollmächtigten Vertretern des GWHs

durch.

Vor der Registrierung:

- Formular für Antragschreiben herunterladen/ausfüllen per Webpage, vgl. Link dazu in Abschnitt 1.5

Voraussetzungen, notwendige Unterlagen und Daten für die Registrierung sind:

- Der Antragsteller ist Vertragskunde, vgl. 1.1,
- Antragschreiben zur Ausgabe eines GWH-Zertifikats mit folgenden Daten bzw. beigefügten Bestätigungen
    - Name der Firma bzw. der Institution
    - Anschrift des Unternehmens bzw. der Institution

- Unternehmensnachweis (z. B. aktueller Auszug aus dem Handelsregister) oder Nachweis der Institution (durch ein entsprechendes Siegel der Institution)
- Kontaktdaten der Ansprechpartner (unter Beachtung einer Vertreterregelung)
- Sollte ein Dienstleister für den Betrieb eines GWH beauftragt werden, MUSS zusätzlich zu den genannten Unterlagen eine schriftliche Bestätigung durch den Auftraggeber (hier: Antragsteller) mit Benennung der autorisierten Ansprechpartner des Dienstleisters für den Betrieb als GWH vorgelegt werden.
- Bestätigung der Geschäftsführung des Unternehmens bzw. der Leitung der Institution, in der der Vertreter des Betreibers berechtigt wird, den Antrag für den GWH zu stellen und in der Sache dazu verbindliche Aussagen und Angaben zu machen.
- Bestätigung, dass die Sicherheitsvorgaben an einen GWH eingehalten werden, und dass die dafür erforderlichen Nachweise beigefügt sind.
- Bestätigung, dass die Nutzungsbedingungen der GWAdriga Smart Energy CA und die SM-GWAdriga Policy eingehalten werden
- Der Antragsteller verpflichtet sich, Änderungen an allen Daten (z. B. den Wechsel eines Ansprechpartners) im Antrag, zeitnah mitzuteilen. Zu diesen Daten gehören auch die vorgelegten Nachweise: Sollte eine Zertifizierung nicht mehr gültig sein, so verpflichtet sich der GWH dies mitzuteilen.

- Persönliche/individuelle Zertifikate für die gesicherte E-Mail-Kommunikation der benannten Ansprechpartner (CS/MIME(GWH)) inklusive der zur Verifikation erforderlichen Zertifikatskette
- Erklärung zur Einhaltung der Sicherheitsvorgaben aus der SM-PKI Policy:
  - Ein Gateway-Hersteller benötigt ein Common-Criteria-Zertifikat auf Basis von [BSI-CC-PP-0073] für sein Produkt, um die Sicherheit seiner Produktionsumgebung nachzuweisen, vgl. Abschnitt 5.1.1. Für die SM-PKI ist diese Produktionsumgebung insbesondere relevant, da dort die initialen Schlüssel und Zertifikate (inkl. Gütesiegelzertifikate) auf das SMGW aufgebracht werden.
  - Zusätzlich muss durch den GWH der Nachweis über den sicheren Betrieb gemäß den Vorgaben zu den Anforderungen für die Teilnahme an der SM-PKI vorlegt werden:
    - Der GWH bestätigt, dass ausschließlich SMGW-Zertifikate für SMGWs beantragt werden, die über
      - eine Zertifizierung entsprechend [TR-03109-1] und
      - eine CC-Zertifizierung entsprechend [BSI-CC-PP-0073]

      verfügen.
    - Der GWH fügt dem Antrag zum Wirkbetrieb die Bestätigung zur erfolgreichen Teilnahme am Testbetrieb bei.

- Bestätigung der erfolgreichen Testteilnahme
    - Vor der initialen Identifizierung und Authentifizierung MUSS die Zertifikatsausstellung und -sperrung von GWH- und SMGW-Gütesiegelzertifikaten unterhalb der zur GWAdriga Smart Energy CA zugehörigen Test-Sub-CA (siehe Abschnitt 1.3.1) der Test-PKI erfolgreich erprobt worden sein. Die erfolgreiche Teilnahme wird von einem Ansprechpartner der Test-Sub-CA per signierter E-Mail bestätigt.
- Der Hashwert (SHA 256) des initialen Zertifikatsrequest-Pakets für das Signatur- (CSig(GWH)), das Verschlüsselungs- (CEnc(GWH)) und das TLS-Zertifikat (CTLS(GWH)) des GWH (gemäß [TR-03109-4]) MUSS in gedruckter Form inklusive der Information zum Format der Darstellung mit der Bestätigung durch die Unterschrift des Bevollmächtigten vorgelegt werden. Der Hashwert wird dabei über die binär-codierte Request-Datei gebildet, welche das Zertifikatsrequest-Paket gemäß [TR-03109-4] enthält, und als base64-codierter Ausdruck in diesem Prozess verwendet. Die eigentlichen Zertifikatsrequests KÖNNEN zusätzlich im Rahmen dieses Termins als Dateien übergeben werden.
    - Im Wirkbetrieb soll das Zertifikatsrequest-Paket der GWAdriga Smart Energy CA vorab zugesendet werden, so dass vor dem Termin eine Überprüfung auf Konformität erfolgen kann.

3.2.2.4. SMGW

SMGW (Gütesiegelzertifikate) – Antragsteller GWH

Voraussetzungen:

1. **Antragsteller ist registriert:**
   der beantragende Gateway-Hersteller (GWH) ist selbst bereits registriert und verfügt über seine gültigen Zertifikate, vgl. Abschnitt 3.2.2.3.
2. **Durch GWH signiertes Zertifikatsrequest-Paket ist erzeugt:**
   Der GWH MUSS das Sicherheitsmodul im SMGW so ansteuern, dass darin die drei Schlüsselpaare für die Gütesiegelzertifikate generiert werden. Das SMGW erzeugt daraus zusammen mit den eigenen Identifikationsdaten je Schlüsselpaar einen Zertifikatsrequest. Der GWH exportiert die drei Requests und bildet mit weiteren relevanten Daten daraus einen gemeinsamen Datensatz (Zertifikatsrequest-Paket, siehe [TR-03109-4]). Das Zertifikatsrequest-Paket wird mit dem CSig(GWH) signiert (Autorisierungssignatur, vgl. [TR-03109-4]).

Vorgehensweise der Sub-CA zur Erzeugung der Gütesiegelzertifikate:

Das signierte Zertifikatsrequest-Paket geht über die per TLS-Kanal gesicherte Webservice-Schnittstelle der GWAdriga Smart Energy CA ein.

Das Zertifikatsrequest-Paket wird geprüft (siehe [TR-03109-4]). Es werden Zertifikate für das SMGW ausgestellt.

Die Zertifikate werden von der GWAdriga Smart Energy CA erzeugt und über die Webservice-Schnittstelle an den GWH übertragen.

Nachbedingung zum Einbringen der Gütesiegelzertifikate ins SMGW:

Die von der Sub-CA produzierten Gütesiegelzertifikate werden von dem GWH geprüft und in das SMGW eingebracht.

SMGW (Wirkzertifikate)

Voraussetzungen:

1. **Antragsteller ist registriert:**
   der beantragende Gateway-Administrator (GWA) ist selbst bereits registriert und verfügt über seine gültigen Zertifikate, vgl. Abschnitt 3.2.2.2.
2. **Durch GWA signiertes Zertifikatsrequest-Pakets für Wirkzertifikate ist erzeugt:**
   Bei den SMGWs sind die Gütesiegelzertifikate im Rahmen der Personalisierung nach der [TR-03109-1] beim erstmaligen Kontakt mit dem GWA durch Wirkzertifikate zu ersetzen. Zum Austausch der Gütesiegelzertifikate durch Wirkzertifikate kommuniziert das SMGW mit dem GWA:
   - Aufbau einer sicheren TLS-Verbindung, vgl. [TR-03116-3]) zwischen SMGW und GWA unter Zuhilfenahme der aufgebrachten TLS-Gütesiegelzertifikate.
   - Generierung neuer SMGW-Schlüsselpaare für TLS, Signatur und Verschlüsselung durch das Sicherheitsmodul des SMGW.
   - Generierung der Zertifikatsrequests durch das SMGW gemäß [TR-03109-4]. Die Zertifikatsrequests MÜSSEN mit einer äußeren Signatur (siehe [TR-03109-4]) versehen sein, um die Authentizität des SMGW nachzuweisen.
   - Senden der Zertifikatsrequests an den GWA.
   - Der GWA prüft die Zertifikatsrequests. Neben der syntaktischen Prüfung des Requests MÜSSEN auch die Gütesiegelzertifikate auf Gültigkeit geprüft werden. Nur wenn beide Prüfungen ein positives Ergebnis haben, DÜRFEN für dieses SMGW Wirkzertifikate beantragt werden.
   - Der GWA erzeugt aus den drei Zertifikatsrequests und weiteren relevanten Daten ein Zertifikatsrequest-Paket (siehe [TR-03109-4]), welches dann mit dem CSig(GWA) signiert wird (Autorisierungssignatur, siehe [TR-03109-4]). Durch diese Signatur autorisiert der GWA die Beantragung.

Vorgehensweise der Sub-CA zur Erzeugung der Wirkzertifikate:

Das signierte Zertifikatsrequest-Paket geht über die per TLS-Verbindung gesicherte Webservice-Schnittstelle der GWAdriga Smart Energy CA ein.

Die Authentizität des Zertifikatsrequest-Pakets wird geprüft (siehe [TR-03109-4]). Es werden ausschließlich Wirkzertifikate für authentische SMGWs ausgestellt werden, deren Beantragung durch den zugehörigen GWA autorisiert wurde.

Die Wirkzertifikate werden von der GWAdriga Smart Energy CA erzeugt und über die Webservice-Schnittstelle an den GWA übertragen.

Nachbedingung zum Einbringen der Wirkzertifikate ins SMGW:

Der GWA prüft die Wirkzertifikate und installiert diese auf dem SMGW (vgl. [TR-03109-4]).

3.2.3. Anforderungen zur Identifizierung und Authentifizierung des Zertifikats-Antragstellers

Zertifikatsrequests werden ausschließlich von einer Organisation (juristische Person) gestellt – nicht von Einzelpersonen (natürliche Person), vgl. insbesondere für die Zertifikatsrequests der SMGWs, Abschnitt 3.2.2.

Natürliche Personen handeln stellvertretend für die Organisationen, wenn sie dazu autorisiert sind, vgl. auch Abschnitt 4.1.1.

3.2.4. Ungeprüfte Angaben zum Zertifikatsnehmer

Die Registrierungsstelle prüft alle Angaben im initialen Zertifikatsrequest-Paket GWH, GWA oder EMT zum Zertifikatsnehmer je nach Rolle gegen die eingereichten Unterlagen auf Korrektheit und Vollständigkeit hinsichtlich der Anforderungen wie in Abschnitt 3.2.2 je Rolle spezifiziert.

3.2.5. Prüfung der Berechtigung zur Antragstellung

Die Berechtigung zur Antragstellung für Organisationen und deren Mitarbeiter wird wie folgt geprüft:

<u>Zertifikatsrequests GWA/GWH/EMT betreffend:</u>

Beim ersten Zertifikatsrequest wird die Organisation registriert. Sie ist erst nach erfolgreicher Registrierung berechtigt ein Zertifikat zu erhalten.

Bedingungen für die Registrierung sind:

- Unternehmensnachweis (z. B. aktueller Auszug aus dem Handelsregister) oder Nachweis der Institution (durch ein entsprechendes Siegel der Institution)
- Kontaktdaten der Ansprechpartner (unter Beachtung einer Vertreterregelung)
- Bestätigung der Geschäftsführung des Unternehmens bzw. der Leitung der Institution, in der der Vertreter des Betreibers berechtigt wird, den Antrag für die Rolle zu stellen und in der Sache dazu verbindliche Aussagen und Angaben zu machen.

Vgl. 3.2.2.1, 3.2.2.2, 3.2.2.3 für weitere rollenspezifische Bedingungen

Für jedes weitere Zertifikat kann die Kommunikation per Webservice-Schnittstelle erfolgen (Berechtigung wird mittels ausgegebenem TLS-Zertifikat und der äußeren Signatur des Zertifikatsrequest-Pakets geprüft. Falls vorhanden wird ebenfalls die Autorisierungssignatur geprüft).

Bei jedem weiteren Zertifikat einer bereits registrierten Organisation kann es sich nur um ein Folgezertifikat für einenden bereits registrierten CN oder um einen CN handeln, der sich nur in der Extension unterscheidet. Sofern die Extension neu ist, handelt es sich um verwandte Zertifikate. Dazu wird auf unserer Webseite ein FAQ veröffentlicht. Ist der Anteil für die Organisationsbezeichnung im CN (erster Teil des CN vor der Rollenbezeichnung) zu ändern, dann ist eine erneute Registrierung erforderlich, vgl. 3.2.2.

Die in 3.2.2 ff. geforderte Bestätigung der Vertretungsberechtigten einer Organisation MUSS schriftlich erfolgen. Die Bestätigung KANN auch in elektronischer Form erfolgen, wenn die Bestätigung von den Vertretungsberechtigten der Organisation qualifiziert elektronisch signiert wird.

Zertifikatsrequests SMGW betreffend:

Auch beim ersten Zertifikatsrequest wird ausschließlich per Webservice-Schnittstelle kommuniziert, welche eine zertifikatsbasierte Autorisierung (mit TLS-Zertifikat sowie Autorisierungssignatur GWH) beinhaltet.

3.2.6. Kriterien für den Einsatz interoperierender Systeme/Einheiten

Keine.

3.2.7. Aktualisierung/Anpassung der Zertifizierungsinformationen der Teilnehmer

Die PKI-Teilnehmer EMT, GWA und GWH unterhalb der GWAdriga Smart Energy CA reichen mit dem Antrag auf Registrierung auch die geforderten Nachweise für Zertifizierungen ein, die in Abschnitt 8.1.2.2 je Teilnehmer aufgeführt sind. Alle Informationen zu den Nachweisen werden in den Registrierungsdaten der GWAdriga Smart Energy CA hinterlegt.

GWAdriga Smart Energy CA hat mit Beantragung des Wirkbetriebs die geforderten Nachweise bei der Root-CA vorgelegt und unterzieht sich einem jährlichen Überwachungsaudit zum Erhalt der Zertifizierungen.

Sofern diese Zertifizierungen einem regelmäßigen Überwachungszyklus unterliegen, muss der Teilnehmer rechtzeitig vor Ablauf der Nachweise bei jedem Audit und jeder Re-Zertifizierung die Ergebnisse der jeweils zertifikatsausgebenden Stelle bekannt geben.

Darüber hinaus muss jeder Teilnehmer seiner zertifikatsausgebenden Stelle Informationen zu relevanten Änderungen mitteilen, die eine Erst-, Rezertifizierung bzw. eine Sperrung von Zertifikaten erfordern, insbesondere:

- bei Wechsel eines passiven EMTs zu aktivem EMT
- bei Wechsel des IT-Betriebsstandorts oder
- Wegfall einer Marktpartner-ID.

3.2.8. Aktualisierung/Anpassung der Registrierungsinformationen der Teilnehmer

Die PKI-Teilnehmer EMT, GWA und GWH teilen der GWAdriga Smart Energy CA mit, wenn sich Änderungen an den Informationen ergeben, die im Registrierungsantrag angegeben wurden. Insbesondere müssen mitgeteilt werden:

- Änderungen zu erforderlichen Zertifizierungen, vgl. Abschnitt 3.2.7,
- Daten, die Bestandteil des Zertifikats sind, z.B. der Name der Organisation, vgl. Abschnitt 3.2.7, und
- Änderungen zu den Ansprechpartnern, vgl. Abschnitt 4.1.1.

In gleicher Weise teilt GWAdriga Smart Energy CA der Root-CA mit, wenn sich Änderungen an den Informationen ergeben, die im Registrierungsantrag angegeben waren.

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

Ein routinemäßiger Folgeantrag für ein Folgezertifikat wird in der Regel per Webservice gestellt. Dazu ist es erforderlich, dass das Folgerequest-Paket rechtzeitig vor Ablauf des Zertifikatstripels gestellt wird, damit das jeweils erforderliche TLS-Zertifikat zur Identifizierung und Authentisierung des Antragstellers am Webservice verwendet wird.

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

3.4.1. Allgemein

Wenn die Voraussetzungen zur Absicherung der Kommunikation mit dem Webservice zum Einreichen eines Folgerequest-Pakets fehlen:

- Kein gültiges TLS-Zertifikat und/oder
- Keine oder ungültige äußere Signatur

sind die Vorgehensweisen wie bei der initialen Identifizierung und Authentifizierung erforderlich vgl. Abschnitt 3.2.

Folgezertifikate können nicht routine-mäßig per E-Mail beauftragt werden:

- Als verschlüsselte und signierte Mail eines autorisierten Ansprechpartners
- Mit Zertifikatsrequests-Paket:
    - mit äußerer Signatur sofern das Vorgängerzertifikat anwendbar ist oder
    - ohne äußere Signatur: Zusätzlich wird ebenfalls über einen gesicherten Kanal (z.B. eine verschlüsselte und signierte E-Mail des benannten ASP des Zertifikatsnehmers) der Hashwert des Zertifikats-Pakets zum Abgleich und zur Autorisation zugesendet. Die Hashwerte (SHA 256) werden dabei über die binär-codierte Request-Datei gebildet, welche das Zertifikatsrequest-Paket gemäß [TR-03109-4] enthält, und als base64-codierter Ausdruck in einer [ISO19005-1] (PDF/A-Standard) konformen Datei versendet wird.

3.4.2. Identifizierung und Authentifizierung zur Schlüsselerneuerung nach Sperrungen

Nach der Sperrung eines Zertifikats wird bei den Endnutzer-Zertifikaten zwischen

EMT-/GWA- und GWH-Zertifikaten und SMGW-Zertifikaten unterschieden:

3.4.2.1. EMT-/GWA- und GWH-Zertifikate

Endnutzer können zeitgleich mehrere Zertifikate (Zertifikatstripel) besitzen (mindestens direkt nach Einreichen von Folgerequests und Ausstellen neuer Zertifikate). Eine Sperrung hat zu diesem Zeitpunkt keine Neuregistrierung zur Folge, da gültige Zertifikate vorhanden sind. Wenn ein Endnutzer aber ein neues Zertifikatstripel beantragt, nachdem alle Zertifikate gesperrt wurden, sind die Vorgehensweisen wie bei der initialen Identifizierung und Authentifizierung erforderlich vgl. Abschnitt 3.2.

3.4.2.2. SMGW-Zertifikate

Es wird ein neues Zertifikat nach den Regelungen der Folgezertifikate ausgestellt, sofern ein noch gültiges Zertifikat vorliegt, z. B. ein Gütesiegelzertifikat. Liegt kein gültiges Zertifikat für ein SMGW vor, kann auch kein Folgerequest gestellt werden.

Anmerkung:

Mit jedem noch gültigen (d.h. nicht abgelaufenen und nicht gesperrten) SMGW-Zertifikat kann ein Folgerequest gestellt werden – selbst dann, wenn eines der Zertifikate in der Kette der Folgezertifikate schon gesperrt ist.

3.5. Identifizierung und Authentifizierung von Anträgen auf Sperrung

Der vorliegende Abschnitt beschreibt nur das Stellen eines Antrags auf Sperrung:

- wer ergreift die Initiative,
- welche Gründe kann welcher Antragsteller angeben,
- wie wird der Antragsteller identifiziert und authentifiziert.

Die Durchführung der Sperrung selbst und insbesondere die Abstimmung mit der Root-CA bei Sperrung systemkritischer Zertifikate ist in Abschnitt 4.8 beschrieben.

Die Sperrung eines Zertifikats wird initiiert durch:

- den Zertifikatsinhaber:
    - Für EMT-/GWA-/GWH-Zertifikate durch die jeweilige Organisation vertreten durch einen berechtigten Ansprechpartner (und damit: geprüft ist, dass der jeweilige Ansprechpartner von der Organisation autorisiert wurde und über ein S/MIME-Zertifikat verfügt), der eine verschlüsselte und signierte Mail mit einem Sperrantrag einsendet
    - Für SMGW-Zertifikate (in der Regel per Webservice)
        - SMGW-Gütesiegelzertifikate: durch den GWH bzw. nach Besitzübergang des SMGWs auf den GWA durch den GWA
        - SMGW-Wirkzertifikate: durch den GWA
- den Betreiber der ausstellenden CA:
    - die übergeordnete Root-CA kann GWAdriga Smart Energy CA-Zertifikate sperren
    - GWAdriga Smart Energy CA kann die von ihr ausgestellten Endnutzer-Zertifikate sperren

Folgende Informationen werden übermittelt:

- Zertifikatstyp
- Ausstellende Sub-CA (IssuerDN des zu sperrenden Zertifikats) bzw. Root-CA
- Zertifikatsnummer (Der Wert des Felds “SerialNumber“ des Zertifikats, siehe [TR-03109-4])
- Sperrgrund (für Sub-CA, GWA, GWH, EMT zwingend, für SMGW optional),
  vgl. dazu auch Abschnitt 4.8,
- Optional, nur wenn der genaue Zeitpunkt bekannt ist: Zeitpunkt, ab dem das Zertifikat als unsicher/gesperrt einzustufen ist.

Sperrung von SMGWs

Die Sperrung von SMGW-Zertifikaten MUSS über die Webservice-Schnittstelle erfolgen.

Ausnahmen:

- die Webservice-Schnittstelle steht nicht zur Verfügung,

3.5.1. Initiative des Zertifikatsinhabers

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

- eine Änderung der Zertifikatsdaten,
- die bisherigen Informationen zum Zertifikat stellen sich als inkorrekt heraus,
- eine Schlüsselkompromittierung (privater Schlüssel eines Endnutzer-Zertifikats ist kompromittiert),
- ein anderes Security-Incident auf den IT Systemen des Zertifikatsnehmers ist aufgetreten oder
- die Einstellung des Betriebs.

Der berechtigte Ansprechpartner sendet in diesem Fall

- entweder eine mittels CS/MIME (ASP) signierte E-Mail - möglichst unter Verwendung des Formulars zur Sperrung, das auf der in Abschnitt 1.5 angeführten Webseite verfügbar ist - an den Betreiber der CA
- oder als Besitzer eines SMGW-Zertifikats – zum Besitz eines SMGW-Zertifikats vgl. die Ausführungen in Abschnitt 3.5.1 - einen Sperrauftrag per Webservice des Betreibers der CA.

Die Ansprechpartner des Betreibers der CA sind aus der Webseite der GWAdriga Smart Energy CA ersichtlich (inkl. E-Mail-Adresse und S/MIME-Zertifikat), vgl. Abschnitt 2.2.1. Dieser prüft die Authentizität der Information und sperrt das Zertifikat.

3.5.1.1. Verantwortlichkeit für die Sperrung eines SMGW

Grundsätzlich kann derjenige PKI-Teilnehmer, der ein SMGW-Zertifikat beantragt hat, auch sperren: GWH können Gütesiegelzertifikate sperren, GWAs können Wirkzertifikate sperren.

Eine Ausnahme davon trifft auf SMGW-Gütesiegelzertifikate zu. Wenn der GWH, der initial im Besitz eines Gütesiegelzertifikats war, die technische Verantwortung für das zum Gütesiegelzertifikat zugehörige SMGW auf einen GWA übertragen hat, dann kann der GWA - und nur noch er - das Gütesiegelzertifikat sperren.

Zur Übertragung der technischen Verantwortung für ein SMGW auf ein GWA sind folgende Schritte vom GWH erforderlich:

1. **Bekanntmachung des GWAs bei der Sub-CA durch den GWH**

   Der GWA, auf den die technische Verantwortung für ein oder mehrere Geräte übertragen werden soll, wird vom GWH per signierter und verschlüsselter E-Mail bei GWAdriga Smart Energy CA bekanntgemacht:

- Nennung der technischen Ansprechpartner des GWAs und der E-Mail-Adressen, ggf. S/MIME-Zertifikate der Ansprechpartner,
- Benennung der Sub-CA (einschließlich zugehöriger Webseite), von welcher der GWA Zertifikate bezieht,
- Kommunikationsdaten des GWA zur Nutzung der Webservice-Schnittstelle für GeneralMessage-Meldungen.

Hierzu steht ein Formular zur Verfügung, das auf der in Abschnitt 1.5 angeführten Webseite veröffentlicht ist. GWAdriga Smart Energy CA nimmt per genannten Ansprechpartnern Kontakt zum GWA auf, um die Angaben bestätigen zu lassen.

2. Übertragung der technischen Verantwortung

Ein oder mehrere SMGWs können einmalig vom GWH auf den zuvor bekanntgemachten GWA übertragen werden. Diese Übertragung soll per Webservice gemäß [TR-03109-4] erfolgen. Der GWH erstellt dafür einen Datensatz in welchem eines oder mehrere SMGWs und der dafür zuständige GWA benannt sind. Dieser Datensatz wird mit dem privaten Schlüssel CSIG(GWH) signiert und per Web-Service an GWAdriga Smart Energy CA gesendet, von welcher die Gütesiegelzertifikate bezogen wurden. Die Übertragung der technischen Verantwortlichkeit an den GWA ist mit sofortiger Wirkung gültig, sobald GWAdriga Smart Energy CA den Datensatz erfolgreich verarbeitet hat. Der GWA wird von GWAdriga Smart Energy CA per Webservice (GeneralMessage) informiert werden, sobald die Übertragung der Verantwortlichkeit abgeschlossen ist.

3.5.1.2. Sperrung eines SMGW

Die Zertifikate eines SMGW müssen per Webservice gemäß [TR-03109-4] gesperrt werden.

Sperrung von Gütesiegelzertifikaten

Die Sperrung von Gütesiegelzertifikaten wird von dem PKI-Teilnehmer vorgenommen, der die Verantwortung hat:

- sofern noch keine Übertragung der Verantwortung stattgefunden hat: vom GWH, der das Gütesiegelzertifikat initial beantragt,
- sofern eine Übertragung stattgefunden hat: vom GWA, an den übertragen wurde

Sperrung von Wirkzertifikaten

Die Sperrung von Wirkzertifikaten wird von dem GWA ausgeführt, der das jüngste Zertifikatetripelbeantragt hat. Dies gilt insbesondere auch bei einem Wechsel des GWA: der neue GWA kann die Wirkzertifikate eines SMGW nur dann sperren, wenn die vom al-ten GWA beantragten Wirkzertifikate gegen neue Wirkzertifikate, die vom neuen GWA bean-tragt wurden, ersetzt

wurden. Bis zu diesem Zeitpunkt, kann die Sperrung der SMGW nur vom alten GWA vorgenommen werden.

Die Sperrung wird jeweils am Webservice unter Verwendung der Zertifikate des Antragstellers beantragt. Jede Sperrung wird in der Sperrliste gemäß [RFC-5280] unmittelbar veröffentlicht. In Ausnahmefällen können Sperrungen von SMGW-Zertifikaten auch per Formular und signiert/verschlüsselter Mail beantragt werden.

3.5.2. Initiative durch GWAdriga Smart Energy CA selbst

Eine Identifizierung und Authentifizierung bei Sperrungen entfällt.

Sperrgründe können sein:

- ein erkannter Verstoß gegen Betriebsauflagen (insbesondere gegen die Anforderungen für die Teilnahme an der SM-PKI (s. Tabelle 11),
- erkannte (erhebliche) Schwächen in der eingesetzten Kryptografie oder Kryptoimplementierung,
- Änderungen in den zentralen Vorgaben (z. B. der [TR-03109-4]),
- Änderung der Zertifikatsdaten (z. B. des Organisationsnamens),
- eine erkannte Schlüsselkompromittierung oder
- die Einstellung des Betriebs bzw. die Außerbetriebnahme der betroffenen Komponente.

3.5.3. Initiative durch die Root-CA

Die Sperrgründe der Root-CA sind wie in 3.5.2 für die Sub-CA angegeben.

Die Root-CA stellt formlos einen Sperrantrag:

- per signierter E-Mail mit den bekannten Ansprechpartnern der Root-CA

Der berechtigte Ansprechpartner der Root-CA sendet eine mittels $C_{S/MIME}$ (ASP) signierte E-Mail an den Betreiber der CA. Dieser prüft die Authentizität der Information und sperrt das Zertifikat.

3.6. Identifizierung und Authentifizierung von Anträgen auf Suspendierung

GWAdriga Smart Energy CA implementiert alle Regelungen zur Suspendierung gemäß [SM-PKI-Policy], Abschnitt 3.6.

Einige wichtige Details sind:

- Eine Suspendierung ist ausschließlich für SMGW-Wirkzertifikate möglich,
- in der Regel wird eine Suspendierung per Webservice beantragt, nur in Ausnahmefällen per S/MIME-Kommunikation,
- für den Antrag auf Suspendierung gelten die in Abschnitt 3.5 beschriebenen Regelungen, insbesondere Abschnitt 3.5.1.2, Absatz „Sperrung von Wirkzertifikaten“,

- eine Suspendierung muss alle SMGW-Zertifikate eines Triples umfassen.

4. Betriebsanforderungen für den Zertifikatslebenszyklus

Abschnitt 4 definiert die Prozeduren und Verantwortlichkeiten für den Lebenszyklus von Zertifikaten hinsichtlich

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

Personengebundene Kommunikation erfolgt ausschließlich per S/MIME-verschlüsselter und signierter E-Mail. Für alle beteiligte Personen, insbesondere die Ansprechpartner, werden individuelle/persönliche S/MIME-Zertifikate vorausgesetzt. Für die S/MIME-Kommunikation gelten die Regelungen von [TR-03116-4].

4.1. Zertifikatsantrag

Dieser Abschnitt beschreibt alle Regelungen der GWAdriga Smart Energy CA zum Zertifikatsantrag.

4.1.1. Wer kann einen Zertifikatsantrag stellen?

Für ein Zertifikat unterhalb der GWAdriga Smart Energy CA können Zertifikatsrequests ausschließlich von einer Organisation gestellt werden. Befugte Organisationen sind GWAs, GWHs, EMTs, die sich gemäß Abschnitte 3.2.2.1, 3.2.2.2, 3.2.2.3 registrieren lassen. Darüber hinaus ist die GWAdriga Smart Energy CA befugt, sich selbst ein TLS-Zertifikat CTLS(Sub-CA) unterhalb der GWAdriga Smart Energy CA auszustellen.

Als natürliche Personen handeln die Ansprechpartner der Organisationen für diese, wenn sie dazu bevollmächtigt sind. Die Vollmacht für mindestens zwei Ansprechpartner stellt die Geschäftsleitung bei der Einreichung des Antragschreibens aus. Weitere Ansprechpartner können zusätzlich von gleicher Stelle bevollmächtigt werden.

Ebenso ist beim Ausscheiden benannter und identifizierter Mitarbeiter die Unterschrift der Geschäftsleitung erforderlich und es ist zu beachten, dass die Mindestanzahl an Ansprechpartnern von 2 Personen nicht unterschritten wird.

Bei Ansprechpartnern für GWA- und GWH-Organisationen ist erforderlich, dass die Identifizierung der bevollmächtigten Personen im Rahmen eines persönlichen Termins erfolgt.

4.1.2. Beantragungsprozess und Zuständigkeiten

Der Beantragungsprozess wird von der Registration Authority der GWAdriga Smart Energy CA durchgeführt.

Je nach zu beantragendem Zertifikat treten unterschiedliche Antragsteller auf:

PKI-Teilnehmer (Zertifikat für)	Zertifikat für juristische Person	Gerätezertifikat	Antragsteller
EMT (EMT)	X		Selbst
GWA (GWA)	X		Selbst
GWH (GWH)	X		Selbst
SMGW (SMGW-Gütesiegelzertifikat)		X	GWH
SMGW (SMGW-Wirkzertifikat)		X	GWA

Tabelle 10 Zuständige Antragsteller

Nicht alle in Abschnitt 1.3.3 aufgeführten PKI-Teilnehmer sind juristische Personen. Da der PKI-Teilnehmer SMGW Gerätezertifikate erhält, tritt für deren Beantragung eine Organisation ein. Je nach Zertifikatsprofil SMGW-Gütesiegel- bzw. Wirkzertifikat ist der Antragsteller der Hersteller (GWH) oder der Administrator (GWA) des SMGW.

Die Übermittlungswege für Zertifikatsrequests können sich je Zertifikatstyp unterscheiden:

PKI-Teilnehmer (Zertifikat für)	Initiales Zertifikat	Folgezertifikat
EMT (EMT)	Per signierter Mail	Per Webservice; im Ausnahmefall: Per signierter Mail
GWA (GWA)	Per signierter Mail	Per Webservice; im Ausnahmefall: Per signierter Mail
GWH (GWH)	Per signierter Mail	Per Webservice; im Ausnahmefall: Per signierter Mail
SMGW (SMGW-Gütesiegelzertifikat)	Per Webservice	-
SMGW (SMGW-Wirkzertifikat)	-	Per Webservice

Tabelle 11 Übermittlungswege Zertifikatsrequests

Im Folgenden werden die weiteren Schritte im Zertifikatslebenszyklus beschrieben:

- in Abschnitt 4.2: die Verarbeitung von initialen Zertifikatsanträgen,
- in Abschnitt 4.3: die Annahme von Zertifikaten,
- in Abschnitt4.4: die Verwendung von Schlüsselpaar und Zertifikat,
- in Abschnitt 4.5: die Zertifikatserneuerung
- in Abschnitt 4.6: die Zertifizierung nach Schlüsselerneuerung
- in Abschnitt 4.7: Änderungen am Zertifikat,
- in Abschnitt 4.8: die Sperrung von Zertifikaten,

- in Abschnitt 4.9: die Statusabfrage von Zertifikaten,
- in Abschnitt 4.10: die Beendigung der Teilnahme und
- in Abschnitt 4.11: die Hinterlegung und Wiederherstellung von Schlüsseln

4.2. Verarbeitung von initialen Zertifikatsanträgen

Initiale Zertifikatsanträge bestehen grundsätzlich aus zwei Anteilen:

- einem formalen schriftlichen Antrag, der zur Identifizierung und Authentifizierung von Personen - sowohl juristischen als auch natürlichen dient, und
- einem initialen Zertifikatsrequest(-Paket).

Eine Ausnahme davon stellen die initialen Zertifikatsanträge für SMGWs dar. Diese Anträge können ausschließlich von bereits genehmigten PKI-Teilnehmern gestellt werden. Damit entfällt auch der formale Antrag und sie werden über die Webservice-Schnittstelle gesendet, vgl. 4.2.1.2.

Im Testbetrieb und ggf. bei EMT-Teilnehmern sind nicht alle Forderungen an die Verarbeitung der initialen Anträge zu erfüllen. Sofern einzelne Punkte entfallen, ist dieses kennzeichnet mit „**(im Testbetrieb nicht erforderlich)**“.

4.2.1. Durchführung der Identifizierung und Authentifizierung

Pos.	Schritte	Zuständig
1	**Einreichen der Registrierungsunterlagen (sofern bisher keine Registrierung erfolgt ist)** Falls noch keine Registrierung der Organisation für die Rolle, für die ein Zertifikat erstellt werden soll, vorliegt: Einsenden der für die Registrierung erforderlichen Unterlagen gemäß Abschnitte 3.2.2.1, 3.2.2.2, 3.2.2.3 per Post bzw. alternativ per E-Mail als PDF mit mindestens der qualifizierten digitalen Signatur des Vertretungsberechtigten.	Antragsteller EMT/GWA/GWH
2	**Terminvereinbarung für Präsenztermin** **(im Testbetrieb und bei EMT-PKI-Teilnehmern nicht erforderlich)** Für GWA- und GWH-Zertifikate ist es erforderlich, dass die benannten Ansprechpartner persönlich identifiziert und authentifiziert werden. Dazu vereinbart GWAdriga Smart Energy CA einen Präsenztermin bei der Registrierungsstelle RA des Trustcenters des Betreibers.	RA
3	**Austausch der S/MIME-Zertifikate** Der Antragsteller sichert das mit Senden der Bestätigung verschickte Zertifikat aus der Signatur z. B. im Mail-Programm.	TS, Antragsteller EMT/GWA/GWH

Pos.	Schritte	Zuständig
	Anschließend verschlüsselt der Antragsteller mit diesem Zertifikat eine Mail an pki@gwadriga.de und signiert sie mit seinem eigenen Zertifikat. Zusätzlich schickt der Antragsteller in dieser oder einer weiteren verschlüsselten und signierten Mail die Zertifikate aller weiteren Ansprechpartner inklusive der zur Verifikation erforderlichen Zertifikatskette (bei Trusted Root-Teilnehmern nicht erforderlich) an pki@gwadriga.de.	
4	**Persönlicher Termin der Ansprechpartner** **(im Testbetrieb und bei EMT-PKI-Teilnehmern nicht erforderlich)** Alle Ansprechpartner erscheinen zu einem Präsenztermin (der ggf. für mehrere Personen auch in mehreren Terminen stattfinden kann) zur Feststellung der persönlichen Identität. Bis zur Ausstellung eines Zertifikats müssen mindestens zwei Ansprechpartner vorher identifiziert worden sein. Im Rahmen des Präsenztermins können weitere Nachweise mitgebracht werden, vgl. 3.2.2.	RA, Antragsteller GWA/GWH
5	**Prüfung der Unterlagen** Die RA-Mitarbeiter der GWAdriga Smart Energy CA prüfen die eingereichten Dokumente und Nachweise. Wenn die Unterlagen bzw. Nachweise unvollständig oder fehlerhaft sind, wird der Antragsteller (die in den Antragsunterlagen genannten Ansprechpartner) informiert und zur Nachlieferung aufgefordert. Sind alle Unterlagen vollständig und korrekt, werden die formalen Voraussetzungen für die Teilnahme als PKI-Teilnehmer in der wahrgenommenen Rolle EMT/GWA oder GWH an der GWAdriga Smart Energy CA mit einer signierten Mail eines RA-Mitarbeiters bestätigt.	RG

Tabelle 12 Einzelschritte zur Durchführung der Identifizierung und Authentifizierung

4.2.1.1. Eingang des initialen Zertifikatsrequests per signierter Mail

Pos.	Schritte	Zuständig
6	**Übergabe bzw. Einsenden des initialen Zertifikatsrequest-Pakets** Das Zertifikatsrequest-Paket kann der GWAdriga Smart Energy CA vorab zugesendet werden an pki@gwadriga.de , so dass (ggf. vor dem Präsenztermin bei der Registrierungsstelle RA des Trustcenters des Betreibers – nur bei GWA/GWH zwingend erforderlich) eine Überprüfung auf Konformität erfolgen kann. Der Antragsteller legt einen Hashwert (SHA 256) vor. Gemäß [TR-03109-4]) MUSS der Hashwert in gedruckter Form mit der Bestätigung durch die Unterschrift eines autorisierten Ansprechpartners vorliegen. Der Hashwert wird dabei über die binär-codierte Request-Datei gebildet, welche das Zertifikatsrequest-Paket gemäß [TR-03109-4] enthält (einschließlich der initialen Zertifikatsrequests für das Signatur- (CSig(ENu)), das Verschlüsselungs- (CEnc(ENu)) und das TLS-Zertifikat (CTLS(ENu))), und als base64-codierter Ausdruck in diesem Prozess verwendet. Die eigentlichen Zertifikatsrequests werden im Request-Paket als signierte E-Mail bzw. für GWA/GWH auch möglich im Rahmen des Präsenztermins als Dateien übergeben – wenn nicht schon zuvor geschehen, s. Pos. 4.	RA, Antragsteller EMT/GWA/GWH

Tabelle 13 Einzelschritte zum Einsenden des initialen Zertifikatsrequests per Mail

4.2.1.2. Eingang des initialen Zertifikatsrequests per Webservice-Schnittstelle

Pos.	Schritte	Zuständig
7	**Zertifikatsrequest-Pakete per Webservice-Schnittstelle:** **Initiale Zertifikate SMGW (Gütesiegel)** Ein initiales SMGW-Zertifikatsrequest-Paket besitzt immer eine Autorisierungssignatur, vgl. [TR-03109-4]): Für SMGW (Gütesiegel): Autorisierungssignatur: CSig(GWH) signiert. Das signierte Zertifikatsrequest-Paket wird an die per TLS-Kanal gesicherte Webservice-Schnittstelle der GWAdriga Smart Energy CA gesendet: https://soap.gwadriga.de/smartsm	GWH per Webservice

Tabelle 14 Einzelschritte zum Einsenden des initialen Zertifikatsrequests per Webservice

4.2.2. Annahme oder Ablehnung von initialen Zertifikatsanträgen

Initiale SMGW-Zertifikatsanträge:

Zur Verarbeitung des initialen SMGW-Zertifikatsrequest-Pakete wird mit Pos. 11 fortgefahren.

Initiale GWA-, GWH- und EMT-Zertifikatsanträge:

Nach erfolgreicher Identifizierung und Authentifizierung sind

- die Organisation als PKI-Teilnehmer genehmigt,
- die Ansprechpartner als bevollmächtigte Vertreter autorisiert und
- die Bestätigung zur Einhaltung dieser Policy, der Nutzungsbedingungen der GWAdriga Smart Energy CA und die Datenschutzerklärungen vorhanden.

Damit liegen diese Informationen als Registrierungsdaten vor. Das eingegangene Zertifikatsrequest-Paket kann zertifiziert werden.

Pos.	Schritte	Zuständig
8	**Prüfung der Aktualität der Registrierungsdaten durch den Zertifizierer** Es wird vom Zertifizierer geprüft: • hat der Antragsteller die aktuelle Version der SM-GWAdriga Policy bestätigt, • falls nein, muss eine Verständigung über die aktuelle Dokumentenlage herbeigeführt werden. Die Registrierungsdaten sind entsprechend anzupassen.	Zertifizierer, ggf. Antragsteller
9	**Prüfung aller initialen Zertifikatsrequests hinsichtlich CN**	Zertifizierer

Pos.	Schritte	Zuständig
	Der CN aller Requests wird gegen die Angabe im Antrag geprüft, die CNs müssen übereinstimmen. Falls nicht ist die Prüfung der Requests nicht erfolgreich.	
10	**Annahme des initialen Zertifikatsrequest-Paketes** Der Zertifizierer übergibt das Zertifikatsrequest-Paket in die Zertifizierung. Dafür wird das Request-Paket vom APC des Zertifizierers auf ein Serververzeichnis des Webservices übertragen, zu dem nur Berechtigte Zugang haben.	Zertifizierer
11	**Automatische Zertifizierung** Das Zertifikatsrequest-Paket wird validiert hinsichtlich Aufbau des Pakets sowie jeden einzelnen enthaltenen Request. Unter anderem prüft die Validierung bei einem initialen Request-Paket: • je Request: den Besitz des privaten Schlüssels des Antragstellers durch Verifizierung der (inneren) Signatur des Requests, vgl. 3.2.1. • je Request: Überprüfung der Sequenznummer im initialen Request: bei SMGW-G-Zertifikaten muss der Wert 0 sein,andere müssen mit 1 beginnen	CA-System

Tabelle 15 Einzelschritte zu Annahme oder Ablehnung initialer Zertifikatsanträge

Falls

- die Organisation oder mindestens 2 Vertreter nicht erfolgreich identifiziert und authentifiziert wurden oder
- Fehler bei der Prüfung auftraten (ein einziger Fehler in einem der Requests reicht aus)

werden auch keine Zertifikatsrequests(-Pakete) angenommen respektive verarbeitet. Der Antragsteller wird entweder per verschlüsselter und signierter E-Mail – sofern 2 Ansprechpartner für diesen Kommunikationsweg zur Verfügung stehen - oder per Post über die Ablehnung informiert.

Auch wenn für die SMGWs keine direkten Ansprechpartner benannt sind, da diese Aufgaben von GWH/GWAs übernommen werden, gilt hier analog:

Wurden die antragstellende GWA-/GWH-Organisation oder mindestens 2 Vertreter nicht erfolgreich identifiziert und authentifiziert, werden auch keine SMGW-Zertifikatsrequests(-Pakete) angenommen. Diese Anforderung wird bereits durch die Anforderungen an die Webservice-Schnittstelle hinsichtlich Autorisierungssignatur und äußerer Signatur abgedeckt, vgl. Abschnitt 4.2.1.2.

4.2.3. Fristen für die Bearbeitung von Zertifikatsanträgen

4.2.3.1. Ausgabe von initialen Sub-CA Zertifikaten

Die GWAdriga Smart Energy CA ist selbst eine Sub-CA. Sie stellt sich selbst das Sub-CA-Zertifikat CTLS(Sub-CA) unmittelbar nach Erhalt der Sub-CA-Zertifikate von der Root-CA aus.

4.2.3.2. Ausgabe von initialen Endnutzer-Zertifikaten

Die in den Abschnitten 4.2.1 und 4.2.2 beschriebenen Schritte zur Ausstellung von Endnutzer-Zertifikaten per Mail (betrifft alle initialen Anträge EMT, GWA oder GWH) lassen sich zu Arbeitsschritten zusammenfassen; zu jedem Arbeitsschritt ist ein maximaler Zeitrahmen angegeben:

Arbeits-schritt	Pos.	Beschreibung des Arbeitsschritts	Max. Zeitrah-men in Arbeits-tagen
1	1	Start des Beantragungsprozesses durch den Endnutzer (GWA,GWH oder EMT)	0
2	2	Nur bei GWA und GWH erforderlich, bei EMT, wenn ge-wünscht: Kontaktaufnahme zur Terminvereinbarung durch GWAdriga Smart Energy CA (GWAdriga Smart Energy CA er-möglicht dabei einen Termin (für Arbeitsschritt 4)) innerhalb der nachfolgenden 3 Arbeitstage	6
3	4, 6	Übergabe der Dokumente / Nachweise ggf. im Rahmen eines persönlichen Termins	0
4	5	Vorprüfung der Unterlagen und Rückmeldung an den An-tragsteller	5
5	5	(optional) Nachlieferungsfrist für den Endnutzer	15
6	5, 8, 9, 10	Prüfung der Unterlagen durch die Sub-CA inkl. Rückmeldung an den Antragsteller	5
7	11, 12, 13, 14	Ausgabe der Zertifikate für Endnutzer	2
		Summe aller Arbeitsschritte	33

Tabelle 16 Zusammenfassung der Schritte zur Ausgabe von initialen Endnutzer-Zertifikaten (GWA, GWH, EMT)

Anmerkung: Die in Arbeitsschritt 7 gelisteten Pos. 12 bis 14 sind Vorwärtsverweise auf Abschnitt 4.2.4.

4.2.4. Ausgabe von Zertifikaten

Pos.	Schritte	Zuständig
12	**Sichere Verwahrung der erstellten Zertifikate** Die bei der Zertifizierung erstellten Zertifikats-Pakete, vgl. Pos. 11, erhalten genau denselben eindeutigen Namen (mit einer anderen Extension), den das Request-Paket erhalten hatte und werden sicher auf dem CA-System verwahrt, zu dem nur nach dem Rollenkonzept Berechtigte Zugang haben.	CA-System

Tabelle 17 Erster Einzelschritt zur Ausgabe der Zertifikate

4.2.4.1. Ausgabe des initialen Zertifikats per signierter Mail

Pos.	Schritte	Zuständig
13	**Ausgabe bzw. Versenden des Zertifikats-Pakets** Nach erfolgreicher Zertifizierung wird das eindeutig zuordenbare Zertifikats-Paket gemäß [TR-03109-4]#3.4.2 per verschlüsselter und signierter Mail von pki@gwadriga.de an den Antragsteller versendet: „Es dürfen ausschließlich Zertifikate für korrekt signierte Zertifikatsrequests bzw. Zertifikatsrequest-Pakete ausgestellt werden.“ … „Auf Endnutzer-Ebene wird immer ein Zertifikatstripel ausgestellt.“.	TS

Tabelle 18 Weitere Einzelschritte zur Ausgabe der Zertifikate per S/MIME-Kommunikation

4.2.4.2. Ausgabe des initialen Zertifikats per Webservice

Pos.	Schritte	Zuständig
14	**Ausgabe bzw. Versenden des Zertifikats-Pakets** Nach erfolgreicher Zertifizierung werden Zertifikats-Pakete gemäß [TR-03109-4]#3.4.2 ausgegeben: „Es dürfen ausschließlich Zertifikate für korrekt signierte Zertifikatsrequests bzw. Zertifikatsrequest-Pakete ausgestellt werden.“ … „Auf Endnutzer-Ebene wird immer ein Zertifikatstripel ausgestellt.“ Das Zertifikats-Paket wird in der Regel synchron (im gleichen Aufruf wie das Einreichen des Request-Pakets) ausgegeben. Optional kann eine asynchrone Kommunikation erfolgen. Dies setzt voraus, dass der Antragssteller die asynchrone Kommunikation bei der GWAdriga Smart Energy CA per signierter S/MIME-Kommunikation von einem Ansprechpartner des Antragsstellers mitteilt und die hierfür erforderliche Web Service URL (WSDL-URL) benennt.	Webservice

Tabelle 19 Weitere Einzelschritte zur Ausgabe der Zertifikate per Webservice

4.2.5. Benachrichtigung des Zertifikatsnehmers über die Ausgabe des Zertifikats

4.2.5.1. Benachrichtigung über Ausgabe des initialen Zertifikats per Mail

Die Benachrichtigung des Zertifikatsnehmers erfolgt durch die verschlüsselte und signierte Mail (Abschnitt 4.2.4.1) mit dem ausgestellten Zertifikatspaket (Pos. 13).

4.2.5.2. Benachrichtigung über Ausgabe des initialen Zertifikats per Webservice

Pos.	Schritte	Zuständig
15	**Benachrichtigung zum Zertifikatspaket** **Bei erfolgreicher Zertifizierung** wird mit Ausgabe des Zertifikatspakets auch ein passender Status übergeben: • bei synchroner Ausgabe des Zertifikats-Pakets: `ok_cert_available` • bei asynchroner Ausgabe des Zertifikats-Pakets: `ok_syntax` oder `ok_reception_ack`	Webservice

Tabelle 20 Einzelschritt zur Benachrichtigung nach Ausgabe der Zertifikate per Webservice

Pos.	Schritte	Zuständig
16	**Benachrichtigung zum Zertifikatspaket** **Bei nicht erfolgreicher Zertifizierung** wird ein Nachrichtenpaket mit Fehlerstatus übergeben: Ist das Request-Paket fehlerhaft an den Webservice übergeben worden, wird ein Fehlerstatus zurückgegeben: • failure_syntax_soap • failure_synchronous_processing_not_possible Ist mindestens einer der Requests im Paket fehlerhaft, wird ein Fehlerstatus zurückgegeben: • failure_inner_signature • failure_outer_signature • failure_domain_parameters • failure_expired • failure_request_not_accepted • failure_syntax_request Sind sonstige Fehler bei der Zertifizierung aufgetreten, wird ein Fehlerstatus zurückgegeben: • failure_internal_error	Webservice

Tabelle 21 Einzelschritt zur Benachrichtigung über Fehler bei der Ausgabe der Zertifikate per Webservice

4.3. Annahme von Zertifikaten

Prüfung auf Korrektheit und Vollständigkeit

Nach Eingang der Endnutzer-Zertifikate müssen diese auf Seiten des Antragstellers und Zertifikatsnehmers gemäß den Vorgaben zur Zertifikatsvalidierung aus [TR-03109-4], Abschnitt 3.3, vom jeweilig autorisierten Ansprechpartner auf Korrektheit und Vollständigkeit geprüft werden.

Kommunikationsschnittstelle für Fehlermeldungen

Um ein Zertifikat zurückzuweisen schickt der Ansprechpartner eine Nachricht an

pki@gwadriga.de

mit:

- Angabe des Grundes für die Verweigerung der Annahme und
- bei fehlerhaften Zertifikaten: Benennung der fehlerhaften bzw. unvollständigen Einträge (sofern möglich)

Bei einem SMGW kann diese Prüfung durch den GWH oder den GWA automatisiert z. B. bei dem Erhalt oder der Einbringung der Zertifikate erfolgen. In jedem Fall muss der Empfänger von SMGW-Zertifikaten diese wie o.a. prüfen und insbesondere die Regelungen der [TR-03109-4] in Abschnitt 3.3.2 zum Spezialfall SMGW umsetzen. Die Prüfung der SMGW-Zertifikate schließt die Prüfung der Zertifikatskette ein. Auch hier ist im Fehlerfall das oben angegebene Postfach zu nutzen.

4.3.1. Veröffentlichung von Zertifikaten durch die CA

Alle ausgestellten Zertifikate werden unmittelbar nach der Ausstellung in den LDAP-Verzeichnisdienst der GWAdriga Smart Energy CA eingetragen, vgl. Abschnitt 2.1.

Gemäß [TR-03109-4]#2.2.3 ist dieser nicht-öffentlich, da er den Teilnehmern der SM-PKI vorbehalten ist.

Weitere Angaben gemäß [TR-03109-4]#3.5

- Protokoll/Adresse:
  - LDAPS-Protokoll / Port 636
  - TLS-Authentisierung mit SM-PKI-Zertifikaten
  - URL: ldaps://ldap.gwadriga.de

4.4. Verwendung von Schlüsselpaar und Zertifikat

4.4.1. Verwendung des privaten Schlüssels und des Zertifikats durch den Zertifikatsnehmer

Zertifikate und die zugehörigen privaten Schlüssel werden ausschließlich für ihren Verwendungszweck eingesetzt. Gemäß [TR-03109-4], Abschnitt 3 sind die Verwendungszwecke:

- **TLS-Zertifikat (CTLS):** Gegenseitige Authentisierung zwischen zwei Kommunikationspartnern sowie Aufbau eines verschlüsselten, integritätsgesicherten TLS-Kanals zwischen beiden.
- **Verschlüsselungszertifikat (CEnc):** Ende-zu-Ende-Verschlüsselung von Daten für den Endempfänger (Datenebene, unabhängig von TLS-Verbindungen).

- **Signaturzertifikat (CSig):** Prüfung von elektronischen Signaturen von Daten (Datenebene, unabhängig von TLS-Verbindungen). Finden bei der TLS-Authentisierung keine Anwendung.

Vgl. die Beschreibung der Verwendungszwecke jedes Zertifikats je PKI-Teilnehmer in Abschnitt 1.4.1, insbesondere **Tabelle 6**, Spalte „Verwendungszweck".

Der private Schlüssel muss stets eindeutig sein, auch innerhalb eines Zertifikatsrequest-Pakets, vgl. 3.2.1.

Zertifikate eines Zertifikatspakets werden stets mit der gleichen Gültigkeit ausgestellt. Sobald ein Fehler bei einem der drei Requests im Paket aufritt, wird das ganze Zertifikatsrequest-Paket nicht verarbeitet, vgl. Abschnitt 4.2.2.

Die Verwendungszeit für den zugehörigen privaten Schlüssel entspricht der im Zertifikat angegebenen Gültigkeit, vgl. [TR-03109-4]#3.2. Die Gültigkeiten für die Endnutzer-Zertifikate sind somit wie folgt:

Endnutzer-Zertifikate	Gültigkeit
CTLS(EMT) CTLS(GWH) CTLS(SMGW)	2 Jahre
CEnc(EMT) CEnc(GWH) CEnc(SMGW)	
CSig(EMT) CSig(GWH) CSig(SMGW)	
CTLS(GWA) CEnc(GWA) CSig(GWA)	3 Jahre

Tabelle 22 Gültigkeiten der Endnutzer-Zertifikate

4.4.2. Verwendung des öffentlichen Schlüssels und des Zertifikats durch Zertifikatsnutzer

Mit dem im ausgestellten Zertifikat der GWAdriga Smart Energy CA enthaltenen öffentlichen Schlüssel wird die Authentizität des jeweiligen Zertifikatsinhabers bescheinigt.

Dieser wird insbesondere bei der Feststellung eines authentischen SMGW eingesetzt: Mit Hilfe der Gütesiegelzertifikate authentisiert sich ein SMGW bei Inbetriebnahme gegenüber dem GWA als echtes SMGW, vgl. [TR-03109-6]#2.3.6.1.

4.5. Zertifikatserneuerung

Zertifikatserneuerung im Sinne von Ausstellen eines neuen Zertifikats für einen schon verwendeten öffentlichen Schlüssel erfolgt nicht.

4.6. Zertifizierung nach Schlüsselerneuerung

4.6.1. Bedingungen der Zertifizierung nach Schlüsselerneuerungen

Die verantwortlichen Ansprechpartner jedes PKI-Teilnehmers EMT/GWA/GWH achten darauf, dass rechtzeitig vor Ablauf der Zertifikatslaufzeit ein neues Schlüsselpaar zu generieren und ein Zertifikat zu beantragen ist. Der Antrag soll

- bei Beantragung per Webservice mindestens 3 Arbeitstage
- bei Beantragung per E-Mail mindestens 10 Arbeitstage

vor Ende der Zertifikatslaufzeit bei der GWAdriga Smart Energy CA eingehen.

Die verantwortlichen Ansprechpartner des PKI-Teilnehmers verfügen über die erforderlichen und gültigen Kommunikations- bzw. Signaturzertifikate:

- zum Einreichen des Zertifikatsrequests(-Pakets) per Mail
  - über das Mail-Zertifikat des Antragstellers
  - für nicht routinemäßige Folgeanträge
  - Wichtig: nicht für SMGW-Zertifikate möglich
- zum Einreichen des Zertifikatsrequests(-Pakets) per Webservice
  - über eine gesicherte TLS-Verbindung (vgl. [TR-03116-3]) per TLS-Zertifikat
  - für routinemäßige Folgeanträge
- zum Einreichen von SMGW-Zertifikatsrequests(-Pakets)
  über das Signaturzertifikat, mit dem der GWA die Autorisierungssignatur erstellt.

Für ein SMGW achtet der zuständige GWA darauf, dass gemäß [TR-03109-4]#3.4.3) für die Erneuerung der Zertifikate eines SMGWs das Zertifikatsrequest-Paket vom SMGW rechtzeitig selbst erstellt wird. Der Request wird vom GWA abgerufen, geprüft und signiert (Autorisierungssignatur) und per Webservice durch den GWA an die zuständige Sub-CA weitergeleitet.

Unabhängig davon, ob Folgezertifikate routinemäßig mit dem Webservice oder nicht routinemäßig per signierter E-Mail beantragt werden, so sind die Anforderungen an die Requests im Zertifikatsrequest-Paket gleich:

- Es muss je Request ein neuer privater Schlüssel verwendet werden,
- der CN muss identisch mit dem CN des Vorgängerzertifikats sein,

- die Seriennummer soll sich von der Seriennummer des Vorgängerzertifikats unterscheiden (inkrementiert um 1).

4.6.2. Wer darf Zertifikate für Schlüsselerneuerungen beantragen?

Für eine Zertifikatserneuerung mit neuem Schlüssel unterhalb der GWAdriga Smart Energy CA können Zertifikatsrequests ausschließlich von registrierten Organisationen (gemäß Abschnitte 3.2.2.1, 3.2.2.2, 3.2.2.3) eingereicht werden.

Wie beim initialen Request handeln als natürliche Personen die autorisierten Ansprechpartner der Organisationen für diese, wenn sie dazu bevollmächtigt sind, vgl. Abschnitte 3.2.2 und 4.2.

4.6.3. Bearbeitung von Zertifikatsanträgen für Schlüsselerneuerungen

4.6.3.1. Verarbeitung und Ausgabe des Folgezertifikats-Pakets bei eingegangenem Request per Mail

Pos.	Schritte	Zuständig
17	**Einsenden des Zertifikatsrequest-Pakets für Folgezertifikate (nicht routinemäßige Folgeanträge)** Falls das TLS-Zertifikat des Vorgängerzertifikats ungültig ist, kann ein Zertifikatsrequest-Paket, das mit dem noch gültigen Signatur-Zertifikat signiert ist, per signierter Mail als Request-Paket für Folgezertifikate eingesendet werden. Falls das TLS-Zertifikat des Vorgängerzertifikats noch gültig ist, das Signaturzertifikat aber nicht, wird ein Zertifikatsrequest-Paket mit Folgerequests erzeugt, das mit dem noch gültigen TLS-Signatur-Zertifikat signiert wird und per signierter Mail eingesendet wird. Mit dem Hashwert ist wie in Pos. 6 beschrieben zu verfahren. Sind Signaturzertifikat und TLS-Zertifikat des Vorgängerzertifikats ungültig, dann wird wie bei einem initiale Zertifikatsrequest-Paket inklusive eines neuen Identifizierungsverfahrens verfahren, vgl. 4.2.1.1.	Antragsteller GWA/GWH/EMT
18	**Prüfung der Aktualität der Registrierungsdaten durch den Zertifizierer** Es wird vom Zertifizierer geprüft: hat der Antragsteller die aktuelle Version der SM-GWAdriga Policy bestätigt, falls nein, muss eine Verständigung über die aktuelle Dokumentenlage herbeigeführt werden. Die Registrierungsdaten sind entsprechend anzupassen.	Zertifizierer, ggf. Antragsteller

Pos.	Schritte	Zuständig
19	**Prüfung der Vorgängerzertifikate** Alle aktuell gültigen Zertifikate (die Vorgängerzertifikate zum Request-Paket) dürfen nicht gesperrt sein. Falls mindestens eines der Zertifikate gesperrt ist, ist die Prüfung des Request-Pakets nicht erfolgreich.	Zertifizierer
20	**Prüfung aller Zertifikatsrequests hinsichtlich CN und Seriennummer** Der CN aller Requests für Folgezertifikate wird gegen die Angabe im Antrag geprüft, die CNs müssen übereinstimmen. Die Seriennummer muss sich vom Vorgängerzertifikat unterscheiden. Falls nicht ist die Prüfung der Requests nicht erfolgreich.	Zertifizierer
21	**Annahme des Zertifikatsrequest-Paketes** Der Zertifizierer übergibt das Zertifikatsrequest-Paket in die Zertifizierung. Dafür wird das Request-Paket vom APC des Zertifizierers auf ein Serververzeichnis übertragen, zu dem nur nach dem Rollenkonzept Berechtigte Zugang haben.	Zertifizierer
22	**Automatische Zertifizierung** Das Zertifikatsrequest-Paket wird validiert hinsichtlich Aufbau des Pakets sowie jedes einzelnen enthaltenen Requests. Unter anderem prüft die Validierung bei einem Folgerequest: • je Request muss ein neuer privater Schlüssel verwendet werden, vgl. 4.5, • das den Request signierende Zertifikat ist ein gültiges Vorgängerzertifikat (jedes noch gültige Vorgängerzertifikat, nicht nur das zuletzt ausgestellte Vorgängerzertifikat ist möglich), • der CN muss identisch mit dem CN des Vorgängerzertifikats sein, • die Seriennummer im DN (Sequenznummer) muss sich von der Seriennummer des Vorgängerzertifikats unterscheiden (inkrementiert um 1); ist dies nicht der Fall, wird die Sequenznummer entsprechend gesetzt	CA-System
23	**Ausgabe bzw. Versenden des Folgezertifikats-Pakets** Nach erfolgreicher Zertifizierung werden Zertifikats-Pakete gemäß [TR-03109-4]#3.4.2 per signierter Mail von pki@gwadriga.de versendet: „Es dürfen ausschließlich Zertifikate für korrekt signierte Zertifikatsrequests bzw. Zertifikatsrequest-Pakete ausgestellt werden.“ … „Auf Endnutzer-Ebene wird immer ein Zertifikatstripel ausgestellt.“.	TS

Tabelle 23 Einzelschritte zur Ausgabe der Folgezertifikate per Mail (nicht routinemäßig)

Falls

- die Überprüfung der Aktualität der Registrierungsdaten nicht erfolgreich war,
- gesperrte oder abgelaufene Vorgängerzertifikate vorlagen oder
- Fehler bei der Prüfung des Zertifikatsrequest-Pakets per Checkliste auftraten

wird das Zertifikatsrequest-Paket für die Folgezertifikate nicht angenommen respektive verarbeitet.

Dies wirkt sich ggf. auch auf die Zertifikate der SMGWs aus:

Wurden die Folgezertifikatsrequest-Pakete von GWA-/GWH-Organisationen nicht erfolgreich geprüft und in der Folge auch keine Zertifikate ausgestellt, dann können nach Ablauf der Gültigkeit der Vorgängerzertifikate auch keine SMGW-Zertifikatsrequests(-Pakete) angenommen werden. Diese Anforderung wird bereits durch die Anforderungen an den Webservice hinsichtlich Autorisierungssignatur und äußerer Signatur abgedeckt, vgl. Abschnitt 4.2.1.2.

Für die Ausgabe des Zertifizierungsergebnisses an den Antragsteller gelten die gleichen Regelungen wie bei einem initialen Zertifikatsantrag, vgl. Abschnitt 4.2.4.1 „Ausgabe des initialen Zertifikats per signierter Mail“. Dort ist auch beschrieben, wie im Fall eines bei der Zertifizierung auftretenden Fehlers verfahren wird.

4.6.3.2. Verarbeitung und Ausgabe des Folgezertifikats-Pakets bei eingegangenem Request per Webservice

Pos.	Schritte	Zuständig
24	**Zertifikatsrequest-Pakete per Web-Schnittstelle:** **routinemäßige Folgezertifikate GWA, GWH, EMT, SMGW** Ein Zertifikatsrequest-Paket besitzt immer eine äußere Signatur, vgl. [TR-03109-4]) und ggf. auch eine Autorisierungssignatur: • Für SMGW (Wirkbetrieb): äußere Signatur mit dem Vorgängerzertifikat SMGW signiert und Autorisierungssignatur: CSig(GWA) signiert • Für GWA-, GWH und EMT-Zertifikate: äußere Signatur mit dem Vorgängerzertifikat: CSig(GWA/GWH/EMT) signiert Das signierte Zertifikatsrequest-Paket wird an die per TLS-Kanal gesicherte Webservice-Schnittstelle der GWAdriga Smart Energy CA gesendet: https://soap.gwadriga.de/smartsm	Webservice
25	**Ausgabe bzw. Versenden des Folgezertifikats-Pakets** Nach erfolgreicher Zertifizierung werden Zertifikats-Pakete gemäß [TR-03109-4]#3.4.2 ausgegeben: „Es dürfen ausschließlich Zertifikate für korrekt signierte Zertifikatsrequests bzw. Zertifikatsrequest-Pakete ausgestellt werden.“ … „Auf Endnutzer-Ebene wird immer ein Zertifikatstripel ausgestellt.“ Das Zertifikats-Paket wird in der Regel synchron (im gleichen Aufruf wie das Einreichen des Request-Pakets) ausgegeben. Optional kann eine asynchrone Kommunikation erfolgen. Dies setzt voraus, dass der Antragssteller die asynchrone Kommunikation bei der GWAdriga Smart Energy CA per signierter S/MIME-Kommunikation von einem Ansprechpartner des Antragsstellers mitteilt und die hierfür erforderliche Web Service URL (WSDL-URL) benennt.	Webservice

Tabelle 24 Einzelschritte zur Ausgabe der Folgezertifikate per Webservice (routinemäßig)

Für die Ausgabe des Zertifizierungsergebnisses an den Antragsteller gelten die gleichen Regelungen wie bei einem initialen Zertifikatsantrag, vgl. Abschnitte 4.2.4.2 „Ausgabe des initialen Zertifikats per

Webservice“ und 4.2.5.2 „Benachrichtigung über Ausgabe des initialen Zertifikats per Webservice“. In Abschnitt 4.2.5.2 ist auch beschrieben, wie im Fall eines bei der Zertifizierung auftretenden Fehlers verfahren wird.

4.6.4. Benachrichtigung des Zertifikatsnehmers über die Ausgabe eines Nachfolgezertifikats

4.6.4.1. Benachrichtigung über Ausgabe des Folgezertifikats per Mail

Die Benachrichtigung des Zertifikatsnehmers erfolgt durch die verschlüsselte und signierte Mail (Abschnitt 4.6.3.1) mit dem ausgestellten Folgezertifikatspaket (Pos. 22).

4.6.4.2. Benachrichtigung über Ausgabe des Folgezertifikats per Webservice

Die Benachrichtigung über die Ausgabe des Folgezertifikatspakets per Webservice erfolgt analog zur Ausgabe des initialen Zertifikats-Pakets – Fehlermeldungen eingeschlossen. Alle Schritte aus Abschnitt 4.2.5.2 gelten hier ebenso.

4.6.5. Verhalten für die Annahme von Zertifikaten für Schlüsselerneuerungen

Alle Regelungen für die Annahme der initialen Zertifikate gelten in gleicher Weise für die Folgezertifikate, siehe Abschnitt 4.3.

4.6.6. Veröffentlichung von Zertifikaten für Schlüsselerneuerungen durch die CA

Alle Regelungen für die Veröffentlichung der initialen Zertifikate gelten in gleicher Weise für die Folgezertifikate, siehe Abschnitt4.3.1.

4.6.7. Benachrichtigung anderer PKI-Teilnehmer über die Ausgabe eines Nachfolgezertifikats

Alle ausgestellten Zertifikate werden direkt nach der Ausstellung in dem Verzeichnisdienst der GWAdriga Smart Energy CA veröffentlicht, vgl. Abschnitte 4.3.1 und 4.6.6.

4.7. Änderungen am Zertifikat

Änderungen an den Zertifikatsinhalten für einen registrierten PKI-Teilnehmer sind nicht vorgesehen, es sei denn es handelt sich um Folgezertifikate, die wie spezifiziert einen neuen Schlüssel enthalten.

Sind Änderungen erforderlich, z. B. durch eine Umfirmierung einer registrierten Organisation (d.h. die Änderung des Firmennamens oder der Gesellschaftsform), ist eine erneute Registrierung gemäß Abschnitt 3.2 vorzunehmen einschließlich eines neuen initialen Zertifikatsrequests(-Pakets). Die alten Zertifikate werden gesperrt, sobald der betroffene PKI-Teilnehmer einen Sperrantrag für nicht mehr benötigte Zertifikate stellt.

4.8. Sperrung und Suspendierung von Zertifikaten

4.8.1. Sperrung von Zertifikaten

Die Initiierung einer Sperrung eines Zertifikats kann durch den Zertifikatsnehmer, die für das Zertifikat zuständige CA und die Root beantragt bzw. eingeleitet werden. Die Identifizierung und Authentifizierung von Anträgen auf Sperrung sind in Abschnitt 3.5 beschrieben.

Die Sperrung eines SMGW-Zertifikatstripels muss über die von der GWAdriga Smart Energy CA betriebene Webservice-Schnittstelle zu erfolgen. Die Sperrung anderer Zertifikate erfolgt hat grundsätzlich per S/MIME-Antrag zu erfolgen (Formular zum Sperrantrag auf unserer Webseite, das ausgefüllt per Mail von einem autorisierten Ansprechpartner signiert und verschlüsselt eingesendet wird). Im Ausnahmefall (z.B. Geräteverlust) kann ein Sperrantrag per Mail auch für SMGW-Zertifikate verwendet werden.

4.8.1.1. Auswirkungen von zu sperrenden Zertifikaten

Je nachdem, von welchem PKI-Teilnehmer die Sperrung eines zu sperrenden Zertifikats ausgeht, sind die Auswirkungen auf die Zahl der von der GWAdriga Smart Energy CA zu sperrenden Zertifikate unterschiedlich:

Initiative durch Instanz	Zu sperrendes Zertifikat	Konsequenzen	Beteiligung Root-CA
Root-CA	Sub-CA-Zertifikat der GWAdriga Smart Energy CA	Sind noch aktive Zertifikate vorhanden, die von der Sub-CA GWAdriga Smart Energy CA ausgestellt wurden, erfolgt deren Sperrung in Abstimmung mit der Root-CA.	X
Sub-CA GWAdriga Smart Energy CA	Sub-CA GWAdriga Smart Energy CA	Sind noch aktive Zertifikate vorhanden, die von der Sub-CA GWAdriga Smart Energy CA ausgestellt wurden, erfolgt deren Sperrung in Abstimmung mit der Root-CA.	X
GWA	GWA-Zertifikat	Sofern vom GWA-Zertifikat noch gültige SMGW-Zertifikate abhängen, sind diese zu identifizieren und mitzuteilen. Es ist eine Einigung zu erzielen, ob und wann auch diese Zertifikate gesperrt werden müssen.	X
EMT	EMT-Zertifikat	Nur das beantragte EMT-Zertifikat wird gesperrt.	

Tabelle 25 Auswirkungen von zu sperrenden Zertifikaten

Anmerkung: die Sperrung von SMGW-Zertifikaten ist in Abschnitt 4.8.2 beschrieben

4.8.1.2. Durchführung der Sperrung

E-Mails mit Sperranträgen werden an von montags bis freitags von 8-17 Uhr bearbeitet. Die E-Mail wird an die Ansprechpartner des Betreibers, vgl. Abschnitt 3.5.1 gesendet, damit die Vorgaben an die Reaktionszeiten hinsichtlich Sperraufträge eingehalten werden.

Mit der Entgegennahme der Sperranfrage prüft der Sperrservice den Sperrantrag:

- hinsichtlich Berechtigung des Ansprechpartners, vgl. 3.5, und
- ob der genannte Sperrgrund zur Sperrung berechtigt, vgl. 3.5.1.

GWAdriga Smart Energy CA sperrt die Zertifikate von GWA, GWH oder eines EMT in folgenden Schritten:

- Sind systemrelevante Auswirkungen zu befürchten, informiert die GWAdriga Smart Energy CA die Root vorab und stimmt das weitere Vorgehen mit ihr ab.
- Sperrungen von GWA-Zertifikaten erfolgen wegen ihrer systemrelevanten Bedeutung grundsätzlich in Abstimmung mit der Root-CA, vgl. auch 5.2.10.
- Ist ein Antrag auf Sperrung berechtigt, wird die Sperrung unverzüglich umgesetzt.
- Um sicherzustellen, dass jedes gesperrte Zertifikat innerhalb von 24 Stunden in die Sperrliste aufgenommen ist, wird die Sperrliste entsprechend aktualisiert.

Die Veröffentlichung der aktualisierten Sperrliste erfolgt gemäß den Vorgaben der [TR-03109-4].

Ein einmal gesperrtes Zertifikat bleibt gesperrt. Der PKI-Teilnehmer kann ein neues Zertifikat beantragen und geht dabei wie in Abschnitt 0 vor.

4.8.1.3. Veröffentlichung und Verwendung der Sperrliste

Die Veröffentlichung der Sperrliste erfolgt gemäß den Vorgaben der [TR-03109-4]:

- bei einer anlassbezogenen Sperrung wird innerhalb von 24 Stunden aktualisiert,
- im Allgemeinen wird die Sperrliste der GWAdriga Smart Energy CA, sofern kein Anlass vorliegt, täglich veröffentlicht, mindestens aber innerhalb von 7 Tagen aktualisiert.

Die GWAdriga Smart Energy CA bietet 24 Stunden am Tag, 7 Tage in der Woche (Ausnahme: kurzzeitige Wartungsfenster, die vorher allen registrierten Teilnehmern angekündigt werden) beide Alternativen der Sperrliste an:

- Als öffentlich zugängliche Version via http:
  Protokoll/Adresse:
  - http-Protokoll / Port 80
  - öffentlich
  - URI.1 = http://crl.gwadriga.de/GWAdriga-SmartEnergy.CA. <*Serial Number im DN*>.crl
- Als öffentlich zugängliche Version via ldap:
  Protokoll/Adresse:
  - LDAP-Protokoll / Port 389
  - öffentlich
  - URI.2 = ldap://ldap.gwadriga.de/c=DE,o=SM-PKI-DE,cn=GWAdriga-SmartEnergy.CA,serialNumber=<*Serial Number im DN*>?certificateRevocationList

Anmerkung: Die Links URI.1 und URI.2 sind für jede <*Serial Number im DN*> eines Sub-CA-Zertifikats zu verwenden, indem jeweils die tatsächliche Serial Number (SN) aus dem Distinguished Name (DN) an-

stelle des Platzhalters in den Link einzusetzen ist. Die SN können auf der Downloadseite der GWAdriga Smart Energy CA, vgl. Abschnitt 1.5, eingesehen werden.

- Beispiel:
  Im Abschnitt „Sperrlisten“ befindet sich der Eintrag „GWAdriga-SmartEnergy.CA1“: Daraus ergeben sich die Links:
  - http://crl.gwadriga.de/GWAdriga-SmartEnergy.CA.**1**.crl
  - URI.2 = ldap://ldap.gwadriga.de/c=DE,o=SM-PKI-DE,cn=GWAdriga-SmartEnergy.CA,serialNumber=**1**?certificateRevocationList

Der Zertifikatsinhaber wird nach erfolgter Sperrung informiert – unabhängig von dem Initiator der Sperrung -, bei einem GWA-Zertifikat wird ebenso die Root-CA informiert.

Alle Teilnehmer MÜSSEN gemäß den Vorgaben aus [TR-03109-4] stets die aktuelle Sperrliste verwenden.

In besonderen Fällen (Erstinbetriebnahme oder auf Aufforderung einer CA-Instanz) werden neben den regelmäßigen Aktualisierungen auch neue Sperrlisten abgefragt.

Bei Erneuerung der Zertifikate der Smart Grid CA muss die vorliegende Policy CP angepasst werden, da weitere URI für CRLs einzufügen sind. Die betrifft insbesondere den vorliegenden Abschnitt.

4.8.2. Sperrung und Suspendierung von SMGW-Zertifikaten

GWAdriga Smart Energy CA implementiert alle Regelungen zur Sperrung und Suspendierung von SMGW-Zertifikaten gemäß [SM-PKI-Policy], Abschnitt 4.8.2.

Die Suspendierung ist ausschließlich für SMGW-Wirkzertifikate vorgesehen. Für den Antrag auf Suspendierung gelten die in Abschnitt 3.6 beschriebenen Regelungen.

Einige wichtige Details sind:

- Eine Suspendierung dauert maximal 30 Tage und schließt spätestens zu diesem Zeitpunkt mit einer Sperrung ab.
- Eine Rücknahme der Suspendierung ist temporär auf Antrag am Webservice durch den GWA möglich, damit dieser ein Folge-Wirkzertifikat beantragen kann.
- Erfolgt die Beantragung eines Folge-Wirkzertifikats im Zeitraum dieser 30 Tage nicht, wird das einmal suspendierte Wirkzertifikat ungeachtet dessen nach Ablauf der 30 Tage endgültig gesperrt.
- Initiiert der Zertifikatsnehmer eine Suspendierung, so MUSS er dies an einen Ansprechpartner der GWAdriga Smart Energy CA mittels signierter E-Mail als Sicherheitsvorfall melden. Hierbei MUSS der Grund für die Suspendierung genannt werden. GWAdriga Smart Energy CA MUSS

diese Begründung dokumentieren. Dies gilt auch für Suspendierungen, welche über die Webservice-Schnittstelle in Auftrag gegeben wurden.

4.8.3. Annullierung von SMGW-Zertifikaten

Zertifikate des Typs SMGW-Gütesiegelzertifikat dürfen in Ausnahmefällen mehrfach mit identischem CN sowie der Sequenznummer 0 ausgestellt werden. Schlüsselmaterial darf in keinem Fall mehrfach zertifiziert werden. Damit die Mehrfachausstellung am Webservice der GWAdriga Smart Energy CA erfolgen kann, ist das unbrauchbare Zertifikatstripel zu annullieren.

Bei einer Annullierung wird das Zertifiaktstripel aus dem Zertifikatsspeicher LDAPS entfernt und in die Sperrliste eingetragen.

Andere PKI-Teilnehmerzertifikate (GWA, GWH, EMT, SMGW-W) können nicht annulliert werden.

Voraussetzungen für das Annullieren von Gütesiegelzertifikaten ist:

- Das ausgestellte und zu annullierende Gütesiegelzertifikats-Tripel ist noch gültig, d. h. es ist nicht abgelaufen oder gesperrt/annulliert/suspendiert/desuspendiert.
- Es wurden keine Wirkzertifikate zum betroffenen SMGW in den von Atos betriebenen Sub-CAen ausgestellt (keine Prüfung in den LDAPs der anderen Sub-CAen).

Die Annullierung kann auf zwei Wegen beauftragt werden:

- per Formular zum Sperren von Zertifikaten vgl. Abschnitt 2.2.1 oder
- per Sperr-Request mit Sperrgrund ‘9‘ (privileged withdrawn) am Webservice.

4.8.4. Aktualisierungs- und Prüfzeiten bei Sperrungen

GWAdriga Smart Energy CA implementiert alle Regelungen zu Aktualisierungs- und Prüfzeiten bei Sperrungen gemäß [SM-PKI-Policy], Abschnitt 4.8.3.

Aus diesen Regelungen ergeben sich Verpflichtungen für die PKI-Teilnehmer der GWAdriga Smart Energy CA:

Sollte eine Sperrliste nicht verfügbar bzw. abrufbar sein, MUSS ersatzweise mit der zuletzt bekannten Sperrliste weitergeprüft werden.

Die GWAdriga Smart Energy CA MUSS hierüber unverzüglich informiert werden (Kontakt siehe Abschnitt 1.5). Die GWAdriga Smart Energy CA stellt dann auf anderem Wege eine aktuelle Sperrliste zur Verfügung, die zur Prüfung herangezogen wird.

4.9. Service zur Statusabfrage von Zertifikaten

Statusabfragen erfolgen per Sperrlisten, vgl. Abschnitte 2.3 und 4.8.

Es wird kein OCSP-Responder eingesetzt.

4.10. Beendigung der Teilnahme

4.10.1. Beendigung der Teilnahme der Sub-CA GWAdriga Smart Energy CA

Sollte die Sub-CA GWAdriga Smart Energy CA aufgelöst werden, wird die Beendigung der Teilnahme durch GWAdriga Smart Energy CA selbst oder die Root-CA eingeleitet werden.

Vor Einstellung des Dienstes werden zur Abstimmung der Beendigung und zur Übergabe der Aufgaben und Verpflichtungen folgende Schritte durchgeführt:

Pos.	Schritte	Zuständig
26	**Abstimmung Zeitablauf** GWAdriga Smart Energy CA und ggf. eine Nachfolgeorganisation stimmen einen zeitlichen Ablauf mit der Root-CA ab.	Sub-CA, Nachfolge-Sub-CA/ Root-CA
27	**Information der Zertifikatsnutzer** GWAdriga Smart Energy CA informiert jedes Unternehmen (EMT, GWH und GWA) welches Zertifikatsnutzer ist und direkt von einer Beendigung der Teilnahme der Sub-CA betroffen ist.	Sub-CA/EMT/GWA/GWH
28	**Abstimmung des Zeitplans zum Zertifikatsaustausch** GWAdriga Smart Energy CA stimmt sich mit jedem Unternehmen bezüglich des notwendigen Zeitrahmens zum Austausch der Zertifikate, insbesondere der SMGW-Zertifikate, ab.	Sub-CA/EMT/GWA/GWH

Tabelle 26 Einzelschritte zur Abstimmung und zur Übergabe der Aufgaben und Verpflichtungen vor Beendigung der GWAdriga Smart Energy CA

Die Beendigung gliedert sich in vier Schritte:

Pos.	Schritte	Zuständig
29	**Übertragung der Aufgaben und Verpflichtungen** Die Aufgaben und Verpflichtungen werden für eine Übergangszeit aufrechterhalten oder bei einer endgültigen Auflösung von einer Nachfolgeorganisation übernommen, einschließlich der Bereitstellung von Sperrinformationen für die Restlaufzeit der ausgegebenen Zertifikate.	Sub-CA/ Nachfolge-Sub-CA
30	**Widerruf aller ausgestellten Zertifikate** Nach Ablauf des Zeitrahmens und Rückmeldung aller Teilnehmer zum erfolgten Zertifikatsaustausch werden alle von der Sub-CA GWAdriga Smart Energy CA ausgestellten Zertifikate widerrufen.	Sub-CA/ Root-CA
31	**Zerstörung von Schlüssel- und Zertifikatsinformationen** Nach Einstellung der Tätigkeiten werden die Zertifikatsinformationen und zugehörigen Kundendaten nach Einhaltung der Aufbewahrungsfristen zerstört werden; private Schlüssel der Teilnehmer liegen zu keinem Zeitpunkt vor, vgl. Abschnitt 4.5.	Sub-CA
32	**Sperren der Berechtigung der benannten Ansprechpartner** Nach Löschen der privaten Schlüssel der GWAdriga Smart Energy CA werden die Ansprechpartner von der Root-CA hinsichtlich Ihrer Berechtigung gesperrt, Aussagen gegenüber der übergeordneten CA tätigen zu dürfen.	Sub-CA/ Root-CA

Tabelle 27 Einzelschritte zur Beendigung der GWAdriga Smart Energy CA

4.10.2. Beendigung der Teilnahme eines Zertifikatsnehmers unterhalb der Sub-CA GWAdriga Smart Energy CA

Die Beendigung der Teilnahme eines Zertifikatsnehmers kann durch den Zertifikatsnehmer selbst oder die zugehörige CA eingeleitet werden. Die Beendigung gliedert sich in drei Schritte:

Pos.	Schritte	Zuständig
34	**Information der betroffenen Zertifikatsnutzer** Durch den Zertifikatsinhaber werden alle Zertifikatsnutzer informiert, die direkt von der Beendigung der Teilnahme eines PKI-Teilnehmers betroffen sind. Es muss hierbei durch den Zertifikatsinhaber jedes Unternehmen (EMT, GWH und GWA) informiert werden, welches im Rahmen der Nutzung der Zertifikate mit dem Zertifikatsinhaber in Kontakt stand.	Ansprechpartner GWA/GWH/EMT
34	**Austausch der betroffenen Zertifikate** Austausch der von der Sperrung betroffenen Zertifikate, so dass ein kontinuierlicher Betrieb gewährleistet werden kann. Zeitrahmen: es erfolgt eine entsprechende Abstimmung zwischen den Beteiligten bezüglich des dazu notwendigen Zeitrahmens. Ausnahme: die Sperrung von Zertifikaten aufgrund von Gefahren für den sicheren Betrieb der SM-PKI, vgl. 4.8.1	Sub-CA/Ansprechpartner GWA/GWH/EMT/Webservice GWA/GWH/EMT
35	**Sperrung aller Zertifikate des Zertifikatsnehmers** Sperrung aller Zertifikate des Zertifikatsnehmers sowie entsprechende Kennzeichnung der CS/MIME(ASP) Zertifikate der benannten Ansprechpartner zum betroffenen Zertifikatsnehmer, so dass die Nutzung der Zertifikate für eine vertrauliche und authentische Kommunikation unterbunden wird.	Sub-CA
36	**Sperren der Berechtigung der benannten Ansprechpartner** Nach Löschen der privaten Schlüssel des Zertifikatnehmers werden die Ansprechpartner von der GWAdriga Smart Energy CA hinsichtlich Ihrer Berechtigung gesperrt, Aussagen gegenüber der GWAdriga Smart Energy CA tätigen zu dürfen.	Ansprechpartner GWA/GWH/EMT Sub-CA

Tabelle 28 Einzelschritte bei Beendigung eines PKI-Teilnehmers der GWAdriga Smart Energy CA

4.10.3. Außerbetriebnahme eines SMGWs

Bei der Außerbetriebnahme eines SMGWs MÜSSEN alle Zertifikate des SMGWs gesperrt werden. Dazu nutzt der GWA oder ggf. der GWH die Webservice-Schnittstelle, vgl. Abschnitt 4.8.2.

4.11. Hinterlegung und Wiederherstellung von Schlüsseln

Hinterlegung und Wiederherstellung von Schlüsseln ist zwar theoretisch für Sub-CAs und andere PKI-Teilnehmer von der übergeordneten Policy vorgesehen, aber praktisch nur für die Sub-CA möglich.

4.11.1. Schlüssel der Sub-CA

Das Sub-CA-Zertifikat der GWAdriga Smart Energy CA kann dem LDAP-Verzeichnis der Root-CA entnommen werden. Es ist prüfbar gegen das ebenfalls veröffentlichte Root-CA-Zertifikat. Der Fingerprint des Sub-CA-Zertifikat der GWAdriga Smart Energy CA wird auf der Webseite der GWAdriga Smart Energy CA veröffentlicht.

Schlüssel-Backup and -Restore für die Sub-CA-Zertifikate der GWAdriga Smart Energy CA sind vorgesehen und es werden dafür die Sicherheitsvorgaben aus den im Folgenden beschriebenen Abschnitten 5 und 6 eingehalten, u. a.:

- Backup der privaten Schlüssel: 5.3, 6.1.3
- Sicherheit bei der Hinterlegung: 5.2.8, 6.1.4,
- Sichere Handhabung und Lagerung von Schlüsselmaterial:6.1.5, 6.2.5,
- Übertragung des privaten Schlüssels (auch zur Wiederherstellung): 6.2.3.

4.11.2. Schlüssel der PKI-Teilnehmer unterhalb der GWAdriga Smart Energy CA

Private Schlüssel der Endnutzer sind in der GWAdriga Smart Energy CA nicht vorhanden. Für die Endnutzer-Zertifikate werden die Zertifikatsrequests eingereicht, die mit dem privaten Schlüssel signiert sind – nicht aber die privaten Schlüssel selbst. Deshalb erfolgt auch keine Hinterlegung der privaten Schlüssel.

Eine Wiederherstellung z. B. bei verlorenen Schlüsseln/Zertifikaten ist folglich ausgeschlossen.

5. Organisatorische, betriebliche und physikalische Sicherheitsanforderungen

Für die PKI-Teilnehmer EMT, GWA und GWH sowie SMGW der hier vorliegenden GWAdriga Smart Energy CA Policy gelten die Anforderungen hinsichtlich organisatorischer, betrieblicher und physikalischer Sicherheit, die in übergeordneten Sicherheitsanforderungen [SM-PKI-Policy] in Abschnitt 5 aufgeführt sind. Die nachfolgenden Tabellen zeigen auf, inwiefern die GWAdriga Smart Energy CA diese Anforderungen selbst erfüllt:

- Die erste Spalte gibt die Abschnittsnummer an, wie sie sich aus der [SM-PKI-Policy] ergibt.
- Die zweite Spalte enthält jeweils ein oder mehrere Auszüge aus der [SM-PKI-Policy] und gibt die Anforderungen an eine Sub-CA zur jeweiligen Abschnittsnummer wieder.
- Die dritte Spalte beschreibt die Umsetzung der Anforderungen aus der [SM-PKI-Policy] durch den Betreiber der GWAdriga Smart Energy CA.

5.1. Generelle Sicherheitsanforderungen

5.1	Für die Einhaltung der generellen Sicherheitsanforderungen ist die Zertifizierung nach ISO 27001 relevant. Eine ISO 27001-Zertifizierung KANN nativ [ISO/IEC 27001] oder auf Basis von IT-Grundschutz (gemäß BSI-Standard 100-2) vorgenommen werden.	Die Einhaltung der generellen Sicherheitsanforderungen im Trustcenter des Betreibers der GWAdriga Smart Energy CA als Sub-CA unterhalb der Smart Metering Root PKI wird in einer Zertifizierung nach ISO 27001 (nativ) nachgewiesen.

5.1.1. Erforderliche Zertifizierungen der PKI-Teilnehmer

5.1.1	**Sub-CA**: Die Zertifizierung nach ISO 27001 sowie eine Zertifizierung nach [TR-03145] MUSS vorhanden sein und nachgewiesen werden.	Für das Atos Trustcenter als Betreiber der GWAdriga Smart Energy CA als Sub-CA unterhalb der Smart Metering Root PKI ist jeweils eine Zertifizierung nach ISO 27001 und [TR-03145-1] vorhanden. Zu den Zertifizierungen liegen Urkunden vor, die einsehbar sind und vorgelegt werden können, vgl. [Secure-CA].

5.1.2. Anforderungen an die ISO 27001-Zertifizierung

5.1.2	Die Zertifizierung gemäß ISO/IEC 27001 MUSS bei einer CA alle Geschäftsprozesse und IT-Systeme des Registrierungs- und Zertifizierungsbetriebs der betreffenden PKI-Infrastruktur umfassen. Hierbei muss von einem hohen Schutzbedarf ausgegangen werden.	Die ISO 27001-Zertifizierung erfasst alle Systeme der CA, auch an verschiedenen Standorten. Grundlage der Zertifizierung ist ein Sicherheitskonzept, das für die GWAdriga Smart Energy CA von einem hohen Schutzbedarf ausgeht.
5.1.2	Allgemein MUSS die Zertifizierung nach [ISO/IEC 27001] die Überprüfung beinhalten, dass alle Anforderungen aus [TR-03109-4] und aus … SM-PKI Policy eingehalten werden. Das Ergebnis MUSS im Auditbericht dokumentiert werden, damit es bei Bedarf vorgelegt werden kann.	Die Prüfungen nach ISO 27001 und [TR-03145-1] werden im Verbund ausgeführt und berücksichtigen die Anforderungen der zugrundeliegenden Anforderungen aus [TR-03145-1] und [SM-PKI-Policy].

		Die Ergebnisse der Konformitätsprüfungen zu [TR-03109-4] und der [SM-PKI-Policy] sind in Auditberichten dokumentiert.
5.1.2	Werden Fach- oder Administrationsprozesse per Remote-Management realisiert MUSS dieses per 2-Faktor-Authentisierung abgesichert werden. Das Remote-Management MUSS im Sicherheitskonzept behandelt werden und MUSS als Bestandteil der Zertifizierung gemäß [ISO/IEC 27001] überprüft werden. Zugehörige WAN-Verbindungen MÜSSEN vom Sicherheitsniveau vergleichbar mit den WAN-Verbindungen gemäß [TR-03109-6] sein.	Fach- und Administrationsprozesse werden nicht per Remote-Management realisiert.

5.2. Erweiterte Sicherheitsanforderungen

5.2.1. Betriebsumgebung und Betriebsabläufe

5.2.1	Nachfolgend werden die Anforderungen an eine sichere Betriebsumgebung und an sichere Betriebsabläufe für … Sub-CA … definiert. …. –**Objektschutz**: Die betrieblichen Prozesse MÜSSEN vor Störung geschützt werden. –**Zutrittssicherheit**: Es MÜSSEN Vorkehrungen zur Sicherung des Zutritts vor Unbefugten zu den jeweiligen Betriebsräumen getrof-	Die von der übergeordneten SM-PKI Policy geforderten Maßnahmen an eine sichere Betriebsumgebung und an sichere Betriebsabläufe für eine Sub-CA sind für die GWAdriga Smart Energy CA umgesetzt: - Die betrieblichen Prozesse sind vor Störungen geschützt (**Objektschutz**), - Die jeweiligen Betriebsräume sind vor dem Zutritt von Unbefugten gesichert (**Zutrittssicherheit**).

	fen werden. –**Geschäftsfortführung**: Die Wiederaufnahme der Betriebsabläufe sowie die Wiederherstellung der notwendigen Ressourcen (Personal, Technologie, Standort, Information) MÜSSEN nach einer Unterbrechung unverzüglich erfolgen. –**Informationsträger**: Bei der Verarbeitung und Aufbewahrung von Informationen in IT-Systemen MUSS der Schutz vor unautorisiertem oder unbeabsichtigtem Gebrauch gewährleistet werden. Wenn nicht mehr benötigt, MUSS der Informationsträger sicher und unwiederherstellbar zerstört werden.	- Die unverzügliche Wiederaufnahme der Betriebsabläufe sowie die Wiederherstellung der notwendigen Ressourcen (Personal, Technologie, Standort, Information) nach einer Unterbrechung sind in einem Notfall-Konzept festgelegt (**Geschäftsfortführung**). - Der Schutz vor unautorisiertem oder unbeabsichtigtem Gebrauch von Informationen in IT-Systemen bei der Verarbeitung und Aufbewahrung ist gewährleistet und Gegenstand von Sicherheits- und Rollenkonzept; nicht mehr benötigte Informationsträger werden sicher und unwiederherstellbar zerstört (**Informationsträger**).
5.2.1	Für die CAs gelten überdies die folgenden Anforderungen: –**Brandschutz**: Es MÜSSEN bei den CAs Maßnahmen getroffen werden, die der Entstehung eines Brandes und der Ausbreitung von Feuer vorbeugen sowie wirksame Löscharbeiten ermöglichen. –**Strom**: Eine gesicherte Stromversorgung einschließlich Redundanzkonzept für Strom SOLLTE bei den CAs gewährleistet werden.	Die von der übergeordneten SM-PKI Policy zusätzlich geforderten Maßnahmen einer CA sind für die GWAdriga Smart Energy CA umgesetzt: - Es sind Maßnahmen getroffen, die der Entstehung eines Brandes und der Ausbreitung von Feuer vorbeugen sowie wirksame Löscharbeiten ermöglichen (**Brandschutz**). - Eine gesicherte Stromversorgung einschließlich Redundanzkonzept für Strom ist gewährleistet (**Strom**).

	–**Wasserschaden**: Die IT-Infrastruktur SOLLTE bei CAs gegen das Eintreten eines Wasserschadens geschützt werden. –**Notfall-Management und Wiederherstellung**: Die CAs MÜSSEN ihre Systeme durch Backup-Mechanismen sichern, um die Wiederherstellung des Betriebs nach einer Störung oder einem Notfall zu ermöglichen. Nur vertrauenswürdiges Betriebspersonal SOLLTE Backup- und Wiederherstellungsprozesse durchführen.	- Die IT-Infrastruktur ist gegen das Eintreten eines Wasserschadens geschützt (**Wasserschaden**). - Die Systeme sind durch Backup-Mechanismen gesichert, um die Wiederherstellung des Betriebs nach einer Störung oder einem Notfall zu ermöglichen. Nur vertrauenswürdiges Betriebspersonal führt die Backup- und Wiederherstellungsprozesse durch (**Notfall-Management und Wiederherstellung**).

5.2.2. Verfahrensanweisungen

5.2.2	Für den Betrieb der … Sub-CA … MÜSSEN folgende Verfahrensanweisungen umgesetzt werden: –**Einhaltung von Verpflichtungen**: Basierend auf den verschiedenen Aufgaben MÜSSEN die Mitarbeiter die Pflichten entsprechend ihren Rollen bei ihren Tätigkeiten einhalten. –**Vertreterregelung**: Für jede definierte Rolle MUSS ein Vertreter ernannt werden. –**Verantwortungsbereiche**: Die Verantwortungsbereiche der Mitarbeiter MÜSSEN klar definiert werden. Für die Verantwortungsbereiche MÜSSEN klare Rollen definiert werden. –**Vier-Augen-Prinzip**: Kritische Vorgänge erfordern die Einhaltung des Vier-Augen-Prinzips (siehe Definition in Anhang C *der [SM-PKI-Policy]*). Nach Möglichkeit soll das Vier-Augen-Prinzip auch technisch durchgesetzt werden. Es ist immer zu dokumentieren, welche beiden Personen einen kritischen Vorgang durchgeführt haben.	Die von der übergeordneten SM-PKI Policy zusätzlich geforderten Maßnahmen einer CA sind für die GWAdriga Smart Energy CA umgesetzt: - Die Mitarbeiter halten die Pflichten entsprechend ihrer Rollen bei ihren Tätigkeiten/Aufgaben ein (**Einhaltung von Verpflichtungen**). - Für jede im Rollenkonzept definierte Rolle ist ein Vertreter ernannt (**Vertreterregelung**). - Für die Verantwortungsbereiche der Mitarbeiter sind Rollen im Rollenkonzept festgelegt (**Verantwortungsbereiche**). - Kritische Vorgänge werden im Vier-Augen-Prinzip durchgeführt. Entsprechende organisatorische Regelungen sind in Arbeitsanweisungen beschrieben. Soweit möglich ist das Vier-Augen-Prinzip technisch umgesetzt. Jeder Vorgang, der im Vier-Augen-Prinzip durchgeführt wird, wird entweder technisch (in Logdateien) oder manuell (in Logbüchern) mit Angabe der Personen dokumentiert (**Vier-Augen-Prinzip**).

	–**Beschränkung der Anzahl Mitarbeiter**: Die Anzahl der Personen, die sicherheitsrelevante oder kritische Funktionen durchführen, MUSS auf die unbedingt notwendige Anzahl begrenzt sein. –**Eskalationsmanagement**: Es MUSS ein gut definiertes und eindeutiges Eskalationsmanagement umgesetzt werden.	- Die Anzahl der Personen, die sicherheitsrelevante oder kritische Funktionen durchführen, ist auf die unbedingt notwendige Anzahl begrenzt (**Beschränkung der Anzahl Mitarbeiter**)**.** - Die Bearbeitung von Eskalationen sind als Incident- bzw. Notfallmanagement im Sicherheits- respektive Notfallkonzept [Betr_NotfK] festgelegt (**Eskalationsmanagement**).

5.2.3. Personal

5.2.3	Der Betrieb der … Sub-CA … MUSS durch angemessen geschultes und erfahrenes Personal erfolgen. Insbesondere sollen folgende Anforderungen umgesetzt werden: –**Rollen und Verantwortungen**: Die Rollen und Verantwortlichkeiten sind gemäß der Anforderungen in Kapitel 5.2.2 zu dokumentieren. In Bezug auf kritische Aufgaben/Funktionen bezüglich des Schlüssel- und Zertifikatsmanagement-Lebenszyklus MÜSSEN die Verantwortlichkeiten klar definiert werden. –**Rollenbeschreibungen**: Für temporäres und permanentes Personal MÜSSEN Rollenbeschreibungen definiert werden, welche	Für den Betrieb der GWAdriga Smart Energy CA wird angemessen geschultes und erfahrenes Personal eingesetzt: - Die Rollen sind dokumentiert, vgl. 5.2.2, dies gilt insbesondere für die Aufgaben/Funktionen/Verantwortlichkeiten bezüglich des Schlüssel- und Zertifikatsmanagement-Lebenszyklus (**Rollen und Verantwortungen**). - Die Rollenbeschreibungen sind definiert, vgl. 5.2.2, Personaleinsatz (temporär bzw. permanent), Aufgabentrennung, Mindestberechtigungen, Sicherheitsprüfungen, Verpflichtung zu Mitarbeiter- und Sensibilisierungsschulungen sind im Sicherkonzept enthalten (**Rollenbeschreibungen**).

	Aufgabentrennung, Mindestberechtigungen, Sicherheitsprüfungen, Verpflichtung zu Mitarbeiter- und Sensibilisierungsschulungen enthalten. –**Einhaltung der ISMS-Anforderungen**: Das Personal MUSS administrative und betriebliche Verfahren und Prozesse im Einklang mit dem Standard ISO 27001 durchführen. Für den Betrieb einer CA gilt darüber hinaus: –**Qualifiziertes Personal**: Die CA MUSS Personal beschäftigen, welches über die erforderlichen Fachkenntnisse, Erfahrung und Qualifikation für das Aufgabenfeld und die angebotenen Dienste verfügt. –**Sicherheitsüberprüfung**: Die CA MUSS sicherstellen, dass an kritischen und sicherheitsrelevanten Prozessen beteiligte Personen bezüglich der persönlichen Eignung geprüft und die Prüfung dokumentiert wurde..	- Die Durchführung der administrativen und betrieblichen Verfahren/Prozesse erfolgt gemäß ISO 27001, vgl. 5.1.2 (**Einhaltung der ISMS-Anforderungen**). Der Betrieb der GWAdriga Smart Energy CA erfüllt die zusätzlichen Anforderungen an das Personal einer CA gemäß SM-PKI Policy: - Es wird ausschließlich Personal mit der erforderlichen Fachkenntnis, Erfahrung und Qualifikation für das Aufgabenfeld und der angebotenen Dienste eingesetzt (**Qualifiziertes Personal**). - Zu allen im GWAdriga Smart Energy CA eingesetzten Mitarbeitern liegt ein polizeiliches Führungszeugnis vor oder sie sind nach dem Sicherheitsüberprüfungsgesetz sicherheitsüberprüft (**Sicherheitsüberprüfung**). Das Führungszeugnis muss nach eigenen Vorgaben des Betreibers der GWAdriga Smart Energy CA alle zwei Jahre neu vorgelegt werden. Die Aktualisierung wird jährlich überwacht.

5.2.4. Monitoring

5.2.4	Folgende Ereignisse MÜSSEN erkannt und aufgezeichnet bzw. dokumentiert werden: … Sub-CA: –Die aus der ISO 27001 für den Betrieb, Prozesse und Infrastruktur relevanten Kontrollen –Schlüsselmanagement (siehe Definition in Anhang C der [SM-PKI-Policy]) auf dem Kryptografiemodul –Nutzung des privaten Schlüssels der CA, insbesondere zur Erstellung von Zertifikaten –Nicht routinemäßige Ausstellung von Zertifikaten –Backup der privaten und öffentlichen Schlüssel und angemessene Maßnahmen für die Archivierung der öffentlichen Schlüssel MÜSSEN in der Zertifizierung nach [ISO 27001] nachgewiesen werden (siehe Anhang B der [SM-PKI-Policy]).	Die IT-Systeme der GWAdriga Smart Energy CA erkennen und dokumentieren die relevanten Ereignisse.

	–Es MUSS sichergestellt werden, dass unautorisierter oder unbeabsichtigter Gebrauch von PKI-relevanten Systemen erkannt wird. –Regelmäßige Prüfung der Überwachungsmaßnahmen durch externe Auditoren. –Remote-Anbindung über WAN: •Mehrfach ungültige Login-Versuche über die WAN-Schnittstelle	

5.2.5. Archivierung von Aufzeichnungen

5.2.5	Es MUSS sichergestellt sein, dass die Systeme über angemessene Archivierungsfunktionen verfügen. Die Zeiträume sind in Anhang B der [SM-PKI-Policy] dokumentiert. Folgende Anforderungen MÜSSEN berücksichtigt werden: … Sub-CA: –**Archivierung der öffentlichen Schlüssel:** Die Beteiligten MÜSSEN sicherstellen, dass die relevanten Informationen zu den öffentlichen Schlüsseln des Zertifikates archiviert werden.	Die IT-Systeme der GWAdriga Smart Energy CA verfügen über angemessene Archivierungsfunktionen: - Die relevanten Informationen zu allen ausgegebenen öffentlichen Zertifikatsschlüsseln werden archiviert (**Archivierung der öffentlichen Schlüssel**). - Die jeweiligen Zertifikate sind eindeutig den registrierten Benutzern zuordenbar (**Eindeutige Zuordnung von Zertifikaten**). - Durch die Backup- und Wiederherstellungsmechanismen der Standard-

	–**Eindeutige Zuordnung von Zertifikaten:** Die Beteiligten MÜSSEN in der Lage sein, die jeweiligen Zertifikate eindeutig den registrierten Benutzern zuzuordnen. –**Verfügbarkeit:** Mit Hilfe einer angemessenen Archivierung klar definierter Daten der verbreiteten öffentlichen Zertifikatsschlüssel MUSS nach einer vollständigen Wiederherstellung die Verfügbarkeit der Dienste gewährleistet werden. –**Datenbanken:** Die Aktualität, Integrität und Vertraulichkeit der Datenbanken MÜSSEN gewährleistet sein, insbesondere bezüglich der Konsistenz der Datenbanken zur Verbreitung von Zertifikaten und der Datenbank zur Nutzer-Registrierung. –**Definition der zu archivierenden Informationen:** Die Informationen, welche für das Tracking und die Wiederherstellung von öffentlichen Schlüsseln benötigt werden, MÜSSEN klar definiert werden. –**Die zu archivierenden Informationen für öffentliche Schlüssel**	Datensicherung, die die verbreiteten öffentlichen Zertifikatsschlüssel einschließt, ist die Verfügbarkeit der Dienste nach einer vollständigen Wiederherstellung gewährleistet **(Verfügbarkeit)**. **-** Durch die Backup- und Wiederherstellungsmechanismen der Standard-Datensicherung, die die Sicherung der Datenbanken einschließt, ist die Verfügbarkeit der Dienste nach einer vollständigen Wiederherstellung gewährleistet **(Datenbanken)**. - Die Informationen, die für das Tracking und die Wiederherstellung von öffentlichen Schlüsseln benötigt werden, sind klar definiert (**Definition der zu archivierenden Informationen)**. **Es werden die folgenden Informationen protokolliert:** **- für öffentliche Schlüssel:** •Registrierungsinformationen •Essentielle CA-Ereignisse (z. B. Generierung von Zertifikaten)

	MÜSSEN enthalten: •Registrierungsinformationen •Essentielle CA-Ereignisse (z. B. Generierung von Zertifikaten) •Schlüsselverwaltung •Zertifizierungsereignisse •Für jedes Ereignis MUSS der Zeitpunkt der Archivierung präzise festgelegt werden. –**Zu archivierende Ereignisse:** Die wesentlichen Ereignisse, die archiviert werden, umfassen: •Zertifikatserstellung •Erneuerung und Aktualisierung der öffentlichen Zertifikats-Schlüssel	•Schlüsselverwaltung •Zertifizierungsereignisse •Für jedes Ereignis wird der Zeitpunkt der Archivierung im Protokollierungs-konzept [Betr_Prot] festgelegt. **- für weitere Ereignisse:** •Zertifikatserstellung •Erneuerung der öffentlichen Zertifikats-Schlüssel für den Sub-CA-Schlüssel; die Aktualisierung des öffentlichen Zertifikatsschlüssels im Sinne von Erstellen eines neuen Zertifikatsrequests für einen schon verwendeten öffentlichen Schlüssel der Sub-CA erfolgt nicht. •Incident- oder Notfall-Management bezüglich Zertifikats-relevanter Vorfälle. Key-Recovery und damit auch das Wiederherstellen von verlorenen Schlüs-seln/Zertifikaten ist ausgeschlossen, vgl. Abschnitt 4.6 „Zertifikatserneuerung

	•Incident- oder Notfall-Management bezüglich Zertifikats-relevanter Vorfälle. –**Verlorene Schlüssel / Zertifikate:** Daten von verbreiteten Schlüsseln / Zertifikaten DÜRFEN NICHT wiederhergestellt werden. Es MÜSSEN neue Schlüssel / Zertifikate beantragt werden.	… erfolgt nicht“ **(Verlorene Schlüssel / Zertifikate)**.

5.2.6. Schlüsselwechsel einer Zertifizierungsstelle

5.2.6	Der Schlüsselwechsel einer Zertifizierungsstelle kann einerseits geplant und andererseits ungeplant erfolgen: –**Geplanter Schlüsselwechsel:** Im Fall eines planbaren Schlüsselwechsels einer Zertifizierungsstelle MÜSSEN die in Kapitel 5.2.7 beschriebenen Verfahren berücksichtigt werden und entsprechende Prozesse vorhanden sein. –**Ungeplanter Schlüsselwechsel:** Für den Fall, dass ein unvorhergesehener Schlüsselwechsel einer Zertifizierungsstelle notwendig ist, MÜSSEN entsprechende Verfahren im Notfallmanagement	Der Schlüsselwechsel der Zertifizierungsstelle GWAdriga Smart Energy CA erfolgt stets im Vier-Augen-Prinzip: - geplant gemäß dem Sicherheitskonzept Prozessbeschreibung „Key Management“. - ungeplant gemäß dem Notfallmanagement.

	definiert werden. –Sowohl ein geplanter als auch ein ungeplanter Schlüsselwechsel einer Zertifizierungsstelle MUSS gemäß dem **Vier-Augen-Prinzip** erfolgen.	

5.2.7. Auflösen einer Zertifizierungsstelle

5.2.7	**Sub-CA:** Wenn eine Sub-CA aufgelöst wird, MÜSSEN alle von ihr ausgestellten Zertifikate gesperrt werden. Insbesondere gelten folgende Anforderungen: –**Übertragung der Aufgaben und Verpflichtungen:** Im Falle der Auflösung einer Sub-CA MÜSSEN deren Aufgaben und Verpflichtungen für eine Übergangszeit aufrechterhalten oder bei einer endgültigen Auflösung von einer Nachfolgeorganisation übernommen werden. Dies umfasst die Bereitstellung von Sperrinformationen für die Restlaufzeit der ausgegebenen Zertifikate. –**Informationspflicht:** Eine Sub-CA MUSS im Falle ihrer Auflösung alle beteiligten Teilnehmer sowie weitere Organisationen, mit denen Vereinbarungen bestehen, vor der Kündigung der Dienstleistung rechtzeitig informieren.	Sollte die Sub-CA GWAdriga Smart Energy CA aufgelöst werden, - werden alle von ihr ausgestellten Zertifikate gesperrt, - Die Aufgaben und Verpflichtungen werden für eine Übergangszeit aufrechterhalten oder bei einer endgültigen Auflösung von einer Nachfolgeorganisation übernommen, einschließlich die Bereitstellung von Sperrinformationen für die Restlaufzeit der ausgegebenen Zertifikate (**Übertragung der Aufgaben und Verpflichtungen**). Nach Einstellung der Tätigkeiten werden die Zertifikatsinformationen und zugehörigen Kundendaten nach Einhaltung der Aufbewahrungsfristen zerstört werden; private Schlüssel der Teilnehmer liegen zu keinem Zeitpunkt vor, vgl. 6.2.9.

	–**Zerstörung von Schlüssel- und Zertifikatsinformationen:** Nach Einstellung der Tätigkeiten MÜSSEN alle privaten Schlüssel einschließlich Zertifikatsinformationen und zugehörige Kundendaten zerstört werden.	(**Zerstörung von Schlüssel- und Zertifikatsinformationen**).

5.2.8. Aufbewahrung der privaten Schlüssel

5.2.8	**Kryptografiemodule:** Die Schlüssel MÜSSEN in vertrauenswürdigen Kryptografiemodulen gespeichert werden (siehe Abschnitt 6.2). Wenn private Schlüssel der … Sub-CA …und ggf. von Teilnehmern außerhalb des Sicherheitsmoduls (z. B. als Backup) aufbewahrt werden, MÜSSEN diese mit dem gleichen Schutzniveau, wie bei der Schlüsselerstellung verarbeitet werden. … Sub-CA … MÜSSEN sicherstellen, dass folgende Anforderungen umgesetzt werden (die diesbezüglichen Anforderungen an die GWA sind Teil von [TR-03109-6]): –**Schutz der Speichermedien:** Die Speichermedien MÜSSEN gegen nicht autorisierte Nutzung, Schäden durch Personen und weitere Bedrohungen (z. B. Feuer) gesichert werden (siehe auch 5.2.1).	Die Speicherung der Sub-CA-Schlüssel erfolgt in HSMs und deren Backups (vgl. Abschnitt Backups können sein: Exporte der Schlüssel als verschlüsselte Dateien, die im gesicherten Archiv verwahrt werden oder, Backup auf einem HSM-Backup). Private Schlüssel von Teilnehmern sind nicht vorhanden und deshalb hier nicht zu berücksichtigen. GWAdriga Smart Energy CA setzt folgende Anforderungen für das Speichermedium HSM um: - HSMs sind gegen nicht autorisierte Nutzung, Schäden durch Personen und weitere Bedrohungen (z. B. Feuer) gesichert (siehe auch 5.2.1) **(Schutz der Speichermedien)**.

	–**Schlüsselaufbewahrung:** Die Speichermedien MÜSSEN sich in einem physisch und logisch hoch gesicherten Bereich befinden. Der Zutritt MUSS auf eine klar definierte Anzahl von Personen eingeschränkt werden. –**Vertrauenswürdiges Personal:** Der private Schlüssel DARF NUR durch vertrauenswürdiges Personal erzeugt, gespeichert und für Signaturen verwendet werden. –**Abfallbeseitigung:** Es MUSS sichergestellt werden, dass Abfälle nicht unberechtigt genutzt und vertrauliche Informationen veröffentlicht werden können. –**Gehärtete IT-Systeme :** Es MUSS sichergestellt werden, dass die Anforderungen an gehärtete IT-Systeme und -Netzwerke sowie an die physische Sicherheit eingehalten werden. Eine Basis für umzusetzende Maßnahmen kann aus dem BSI-Grundschutzkatalog entnommen werden.	- Speichermedien (HSM, verschlüsselte Dateien oder Backup-HSMs) befinden sich in einem physisch und logisch hoch gesicherten Bereich. In allen Fällen ist der Zutritt ist auf eine klar definierte Anzahl von Personen eingeschränkt. **(Schlüsselaufbewahrung)**. - Der private Schlüssel der Sub-CA wird durch vertrauenswürdiges Personal erzeugt, gespeichert und für Signaturen verwendet **(Vertrauenswürdiges Personal)**. - Es ist sichergestellt, dass Abfälle nicht unberechtigt genutzt und vertrauliche Informationen nicht veröffentlicht werden können **(Abfallbeseitigung)**. - Alle eingesetzten Betriebssysteme der GWAdriga Smart Energy CA werden nach Security-Baselines des Betreibers gehärtet **(Gehärtete IT-Systeme)**.

5.2.9. Behandlung von Vorfällen und Kompromittierung

5.2.9	Nachfolgend wird beschrieben, wie bei Vorfällen und Kompromittierungen verfahren werden MUSS:	Bei Vorfällen und Kompromittierungen verfährt die GWAdriga Smart Energy CA wie folgt:

	–Bei einer Kompromittierung oder einem begründeten Verdacht auf Kompromittierung eines privaten Schlüssels MUSS das zugehörige Zertifikat unverzüglich gesperrt und DARF NICHT wiederverwendet werden. –Ein Fall von Kompromittierung sowie Verdachtsfälle MÜSSEN durch den Schlüsselinhaber dokumentiert werden. –Jeder Verdacht auf Kompromittierung oder Missbrauch des privaten Schlüssels ist aufzuklären. –Die Generierung neuer Schlüssel und Zertifikate MUSS überwacht und dokumentiert werden.	– Bei jeder Kompromittierung bzw. jedem begründeten Verdacht auf Kompromittierung des privaten Schlüssels der Sub-CA GWAdriga Smart Energy CA wird das zugehörige Zertifikat gesperrt, eine Wiederverwendung ist ausgeschlossen. – Jeder Fall von Kompromittierung sowie Verdachtsfälle werden durch den Schlüsselinhaber dokumentiert. – Jeder Verdacht auf Kompromittierung oder Missbrauch des privaten Schlüssels wird aufgeklärt. – Die Generierung neuer Schlüssel und Zertifikate wird überwacht und dokumentiert.

5.2.10. Meldepflichten

5.2.10	Bei Kompromittierung oder anderweitigen sicherheitsrelevanten Vorfällen MUSS eine Meldung aufbereitet und an die zuständige CA kommuniziert werden. Bei der Kompromittierung eines GWA MUSS zusätzlich die Root informiert werden.	Bei Kompromittierung oder anderweitigen sicherheitsrelevanten Vorfällen wie - Verstoß gegen relevante Betriebsauflagen - Betreiber der CA ist nicht mehr aktiv (Bsp.: Insolvenz) – Aufforderung zur Sperrung oder Suspendierung eines Zertifikates

	Folgende Vorkommnisse sind Beispiele für eine Meldepflicht: Meldepflicht liegt auf Seiten des Zertifikatsnehmers: –Kompromittierung des privaten Schlüsselmaterials –Verstoß gegen relevante Betriebsauflagen –Betreiber derCA ist nicht mehr aktiv (Bsp.: Insolvenz) –Aufforderung zur Sperrung oder Suspendierung eines Zertifikates Folgende Angaben MÜSSEN der Meldung mindestens beigefügt werden: –Was wurde kompromittiert bzw. was wurde betroffen –Wann ist das Vorkommnis passiert bzw. wann wurde der Vorfall bemerkt	wird eine Meldung aufbereitet und an die zuständige CA kommuniziert. Bei der Kompromittierung eines GWA wird zusätzlich stets auch die Root informiert. Jede Meldung beinhaltet die Angaben: - Was kompromittiert wurde bzw. was betroffen war, – Wann das Vorkommnis passierte bzw. wann der Vorfall bemerkt wurde, – Wer das Vorkommnis festgestellt hat, – Ort des Vorkommnisses, – Wie das Vorkommnis vermutlich abgelaufen ist, – Welche Maßnahmen schon durchgeführt bzw. eingeleitet wurden.

	–Wer hat das Vorkommnis festgestellt –Ort des Vorkommnisses –Wie ist das Vorkommnis vermutlich abgelaufen –Wenn schon eine Maßnahme durchgeführt wurde: Welche Maß-nahmen wurden schon eingeleitet	

5.3. Notfall-Management

5.3	Die … Sub-CA … MÜSSEN gewährleisten, dass die Wiederherstellung des Normalbetriebs nach einer Störung oder nach einem Notfall innerhalb einer angemessenen Frist erfolgt. Notfall-Szenarien betreffen u.a.: – Kompromittierung des privaten Schlüssels – Entdeckte Schwachstellen in den verwendeten kryptografischen Verfahren – Nichtverfügbarkeit von Sperrlisten Insbesondere gelten folgende Anforderungen, welche erfüllt werden MÜSSEN: –**Notfallmanagement:** Die … Sub-CA … MÜSSEN rechtzeitig angemessen auf Störungen oder Notfälle reagieren, um Schäden zu minimieren und den Geschäftsbetrieb zu gewährleisten. –**Kompromittierung:** Wenn die Vermutung besteht, dass Schlüsselmaterial kompromittiert ist, so DARF KEIN PKI-Teilnehmer die-	Das Notfallmanagement der GWAdriga Smart Energy CA ist in einem Notfallkonzept geregelt, das u.a. auch die Szenarien - Kompromittierung des privaten Schlüssels – Entdeckte Schwachstellen in den verwendeten kryptografischen Verfahren – Nichtverfügbarkeit von Sperrlisten berücksichtigt. Die Sub-CA GWAdriga Smart Energy CA gewährleistet mit einem Notfallkonzept, dass rechtzeitig angemessen auf Störungen oder Notfälle reagiert wird, um Schäden zu minimieren und den Geschäftsbetrieb zu gewährleisten. Im Notfallkonzept ist zu jedem Notfallszenario ein Vorgehen festgelegt, zu dem jeweils beschrieben sind: - Vorgehensweise, - Dokumentation und - besondere Hinweise **(Notfallmanagement)**.

	ses weiter nutzen. –**Risikoreduktion / Schadensminderung**: Alle PKI-Teilnehmer SOLLTEN entsprechende Maßnahmen zur Minimierung von Risiken und Schäden anwenden. –**Vermeidung von Vorfällen:** Alle PKI-Teilnehmer MÜSSEN angemessene Maßnahmen vorbereiten sowie die Ursachen von Vorfällen ermitteln, um diese in Zukunft zu vermeiden. –**Notfallpläne:** Die … Sub-CA … MÜSSEN entsprechende Pläne vorbereiten, um die Geschäftsprozesse nach einem Notfall wiederherzustellen. –**Backups**: Die … Sub-CA … MÜSSEN Backups von privaten und öffentlichen Schlüsseln, ausgestellten Zertifikaten und Sperrinformationen durchführen. –**Vorgehen nach einer Störung:** Nach einer schweren Störung MÜSSEN alle PKI-Teilnehmer sicherstellen, dass die entstandene Sicherheitslücke geschlossen wird.	- Kein PKI-Teilnehmer darf einen kompromittierten Schlüssel weiter nutzen, auch nicht bei Verdacht. Im Verdachtsfall ist der entsprechende Endnutzer verpflichtet, das „verdächtige Zertifikat“ nicht zu nutzen, bis der Verdacht entkräftet wurde. Bestätigt sich andererseits der Verdacht, setzt die GWAdriga Smart Energy CA die Zertifikate zu diesen Schlüsseln auf ihre Sperrliste **(Kompromittierung)**. Es werden entsprechende Maßnahmen zur Minimierung von Risiken und Schäden angewendet (**Risikoreduktion / Schadensminderung**). - Angemessene Maßnahmen sind vorbereitet und die Ursachen von Vorfällen werden ermittelt, um diese in Zukunft zu vermeiden **(Vermeidung von Vorfällen)**. - Es liegen entsprechende Pläne vor, um die Geschäftsprozesse nach einem Notfall wiederherzustellen (**Notfallpläne**). – **Backups**: Die … Sub-CA … führt Backups von privaten und öffentlichen Schlüsseln, ausgestellten Zertifikaten und Sperrinformationen durch.

		- Nach einer schweren Störung ist sichergestellt, dass die entstandene Sicherheitslücke geschlossen wird (**Vorgehen nach einer Störung**).

6. Technische Sicherheitsanforderungen

Für die PKI-Teilnehmer EMT, GWA und GWH sowie SMGW der hier vorliegenden GWAdriga Smart Energy CA Policy gelten die Anforderungen hinsichtlich technischer Sicherheit, die in der übergeordneten Sicherheitsanforderungen [SM-PKI-Policy] in Abschnitt 6 aufgeführt sind. Die nachfolgenden Tabellen zeigen auf, inwiefern die GWAdriga Smart Energy CA diese Anforderungen selbst erfüllt.

6.1. Erzeugung und Installation von Schlüsselpaaren

6.1	Jeder Zertifikatsnehmer MUSS sein eigenes Schlüsselpaar generieren. Die technischen Anforderungen an die Erzeugung, Verwendung und Gültigkeit von Schlüsseln werden in [TR-03109-4] beschrieben.	Jeder Zertifikatsnehmer generiert sein eigenes Schlüsselpaar: - die Sub-CA GWAdriga Smart Energy CA im HSM, - die Teilnehmer unterhalb der Sub-CA in deren lokalem HSM bzw. kryptographischem Modul.

6.1.1. Generierung von Schlüsselpaaren für die Zertifikate

6.1.1.	Die PKI-Teilnehmer … Sub-CA … MÜSSEN sicherstellen, dass folgende Anforderungen umgesetzt werden: –**Generierung im Vier-Augen-Prinzip:** Das Schlüsselpaar MUSS während der Schlüsselzeremonie im Vier-Augen-Prinzip unter Teil-	Diese Sub-CA GWAdriga Smart Energy CA implementiert: - Das Schlüsselpaar für das Sub-CA-Zertifikat wird während der Schlüsselzeremonie im Vier-Augen-Prinzip unter Teilnahme zweier für den Schlüssel verantwortlichen Mitarbeiter (Keymanager) generiert **(Generierung im Vier-Augen-Prinzip)**.

	nahme des für den Schlüssel verantwortlichen Mitarbeiters generiert werden. –**Generierung eines Schlüsselpaars:** Die zur Schlüsselgenerierung eingesetzten Kryptographiemodule MÜSSEN je nach TYP entsprechend den in Kapitel 6.2 angegebenen Protection Profiles zertifiziert sein. –Der **technische Zugriff auf die Schlüssel in den Kryptografiemodulen** aller Zertifikatsnehmer MUSS durch ein Geheimnis geschützt werden (Passwort, PIN, o.ä.), welches ausschließlich die jeweiligen Operatoren kennen. Der Zugriff auf das Kryptografiemodul, insbesondere zur Schlüsselerzeugung, MUSS auf ein Minimum an Operatoren beschränkt sein.	- Das zur Schlüsselgenerierung eingesetzte Kryptografiemodul entspricht den in Kapitel 6.2 angegebenen Forderungen nach Protection Profile oder einem adäquaten Nachweis **(Generierung eines Schlüsselpaars)**. - Der technische Zugriff auf Schlüssel im HSM-Modul ist durch eine 2-Faktor-Authentisierung geschützt; Details dazu sind nur den lt. Rollenkonzept Berechtigten bekannt **(technischer Zugriff auf die Schlüssel in den Kryptografiemodulen)**.

6.1.2. Lieferung privater Schlüssel

6.1.2	Die Erstellung der privaten Schlüssel erfolgt dezentral durch die Zertifikatsnehmer der SM-PKI. Daher erfolgt keine Lieferung der privaten Schlüssel.	Es erfolgt keine Lieferung von privaten Schlüsseln durch die Sub-CA GWAdriga Smart Energy CA.

6.1.3. Lieferung öffentlicher Zertifikate

6.1.3	Alle Zertifikate werden in den jeweiligen Verzeichnissen der ausstellenden CAs abgelegt und sind somit für alle PKI-Teilnehmer	Alle ausgestellten Zertifikate werden unmittelbar nach der Ausstellung in dem LDAPS-Verzeichnisdienst der GWAdriga Smart Energy CA eingetragen, vgl.

	zugänglich.	#Veröffentlichung von Zertifikaten durch die CA in Abschnitt 4.3.1.

6.1.4. Schlüssellängen und kryptografische Algorithmen

6.1.4	Schlüssellängen und kryptografische Algorithmen der Schlüsselpaare MÜSSEN angemessene kryptografische Verfahren einhalten. Die zum jeweiligen Zeitpunkt konkret zu verwendenden kryptografischen Algorithmen und Schlüssellängen MÜSSEN der [TR-03116-3] entnommen werden.	Schlüssellänge und Algorithmen sind spezifiziert im Abschnitt 3 in Tabelle 4 von [TR-03116-3]. Die GWAdriga Smart Energy CA hält sich bei Erstellung der Zertifikate an diese Vorgabe, welche die Schlüssellänge und Algorithmen für von einer Sub-CA zu erstellenden Zertifikate festlegt, von zur Zeit noch auf „brainpoolP256r1“.
6.1.4	Bei der Erzeugung und Nutzung von statischen und temporären Schlüsseln im Rahmen der SM-PKI MUSS ein Zufallsgenerator verwendet werden, der konform zu den Anforderungen aus [TR-03116-3] ist. Des Weiteren MUSS bei statischen Schlüsseln ein Kryptografiemodul gemäß Abschnitt 6.2 eingesetzt werden.	Bei der Erzeugung und Nutzung von statischen und temporären Schlüsseln setzt GWAdriga Smart Energy CA im Rahmen der SM-PKI ein Kryptomodul ein, dass den geforderten Zufallsgenerator verwendet, vgl. die Ausführungen in Abschnitte 6.2.6 und 6.2.10.

6.1.5. Festlegung der Parameter der Schlüssel und Qualitätskontrolle

6.1.5	**Sichere Handhabung und Lagerung von Schlüsselmaterial:** Software- und Hardware-Komponenten zur Erzeugung, Handhabung und Lagerung der privaten Schlüssel MÜSSEN angemessene Maßnahmen zur sicheren Handhabung und Lagerung von Schlüsselmaterial einhalten. –**Defektes Krypto-Modul (KM):** Im Falle eines defekten KM ist sicherzustellen, dass das Schlüssel-Backup sicher und im Vier-	Für die Software- und Hardware-Komponenten zur Erzeugung, Handhabung und Lagerung der privaten Schlüssel sind angemessene Maßnahmen zur sicheren Handhabung und Lagerung von Schlüsselmaterial eingerichtet **(Sichere Handhabung und Lagerung von Schlüsselmaterial)**: - Im Falle eines defekten KM ist sichergestellt, dass bereits eine Backup-HSM bereitsteht (unter Einhaltung des Vier-Augen-Prinzips/ des Rollenkonzepts eingerichtet), das die Aufgabe des defekten KMs übernimmt, vgl. auch **(Defek-**

	Augen-Prinzip in ein neues KM nach angemessenen Maßnahmen zur sicheren Handhabung und Lagerung von Schlüsselmaterial importiert wird. –**Schutz vor Angriff auf den privaten Schlüssel:** Es MUSS sichergestellt werden, dass der private Schlüssel nicht von einem Angreifer für kryptografische Operationen missbraucht werden kann und dass angemessene Maßnahmen (siehe Abschnitt 6.2.3. bis 6.2.6) zur sicheren Handhabung und Lagerung von Schlüsselmaterial und gehärteten IT-Systemen und -Netzwerken eingehalten werden. –**Unverschlüsselter / unberechtigter Export des privaten Schlüssels:** Es MUSS sichergestellt werden, dass der private Schlüssel nicht unverschlüsselt oder unberechtigt aus dem Schlüsselspeicher exportiert werden kann. Es MÜSSEN angemessene Maßnahmen zur sicheren Handhabung und Lagerung von Schlüsselmaterial eingehalten werden. Die zum jeweiligen Zeitpunkt konkret zu verwendenden kryptografischen Algorithmen und Schlüssellängen MÜSSEN den jeweils aktuellen Empfehlungen aus [TR-02102-1] entsprechen. –Die Testteilnahme erfolgt auf Basis von **Testschlüsseln (Testes Krypto-Modul (KM))**. - Angemessene Maßnahmen zur sicheren Handhabung und Lagerung von Schlüsselmaterial und gehärteten IT-Systemen und -Netzwerken sind eingehalten, vgl. Abschnitte 6.2.3. bis 6.2.6 **(Schutz vor Angriff auf den privaten Schlüssel)**. - Durch SmartCards, einer 2-Faktor-Authentifizierung, dem Vier-Augen-Prinzip und Anwendung des Rollenkonzepts für Zugriff auf das HSM ist ausgeschlossen, dass der private Schlüssel der Sub-CA unverschlüsselt oder unberechtigt aus dem Schlüsselspeicher exportiert werden kann. Ebenso ist die Lagerung eines exportierten Backups des Schlüssels mehrfach geschützt durch verschlüsseltes Backup, das Rollenkonzept, 2-Faktor-Authentifizierung am HSM für den Export, sichere Lagerung. Zur Verschlüsselung des Backups werden kryptografische Algorithmen und Schlüssellängen nach den Vorgaben von [TR-02102-1] genutzt, vgl. Abschnitt 6.2.4. **(Unverschlüsselter / unberechtigter Export des privaten Schlüssels)**. - Die Testteilnahme der Sub-CA GWAdriga Smart Energy CA erfolgt unter Einhaltung der Anforderungen an den Wirkbetrieb aus [TR-03109-4] und der Root SM-PKI Policy, vgl. Anhang Testbetrieb. Die verwendeten Testschlüssel werden ausschließlich für den Testbetrieb erzeugt und nicht im Wirkbetrieb des

	PKI, siehe Abschnitt 1.3.1**)** unter Einhaltung der Anforderungen an den Wirkbetrieb aus [TR-03109-4] und … SM-PKI Policy. Die verwendeten Testschlüssel werden ausschließlich für den Testbetrieb erzeugt und DÜRFEN NICHT im Wirkbetrieb des SM-PKI Umfeldes eingesetzt werden.	SM-PKI Umfeldes eingesetzt **(Testschlüsseln, Test-PKI)**.

6.1.6. Verwendungszweck der Schlüssel

6.1.6	Die Schlüssel DÜRFEN ausschließlich für die in Kapitel 1.4.1 beschrieben Verwendungszwecke eingesetzt werden. Der Verwendungszweck ist in der jeweils aktuellen Fassung der [TR-03109-4] konkretisiert.	Der Verwendungszweck der Schlüssel wird eingehalten, vgl. Abschnitte 1.4.1 und 1.4.2.

6.2. Sicherung des privaten Schlüssels und Anforderungen an kryptografische Module

6.2	Die Teilnehmer der SM-PKI MÜSSEN Kryptografiemodule zur Generierung, Speicherung und Nutzung ihrer privaten Schlüssel zu ihren Zertifikaten aus der SM-PKI verwenden. Die Sicherheitsanforderungen an Kryptografiemodule zum Schutz der privaten Schlüssel zu den Zertifikaten der SM-PKI werden in Kapitel 6.2.10 definiert.	Die vorliegende Sub-CA GWAdriga Smart Energy CA setzt Kryptografiemodule zur Generierung, Speicherung und Nutzung ihrer privaten Schlüssels ein, die die Anforderungen am Kryptografiemodule für den Wirkbetrieb der GWAdriga Smart Energy CA erfüllen, vgl. Abschnitt 6.2.10. Für die GWAdriga Smart Energy CA liegt der Nachweis durch den HSM-Hersteller vor: vgl. [HSM-Nachweis].
6.2	Neben dem Einsatz eines sicheren Kryptografiemodules MUSS auch ein sicherer Umgang mit den privaten Schlüsseln sicherge-	Die Anforderungen an den sicheren Umgang mit privaten Schlüsseln sowie an deren Lebenszyklus werden erfüllt, vgl.

	stellt werden. Daher MÜSSEN die Anforderungen an den Lebenszyklus und die Einsatzumgebung aus [KeyLifecSec] – Security Level 2 eingehalten werden (Ausnahme SMGW). Die in diesem Kapitel definierten Anforderungen ergänzen die Anforderungen aus [KeyLifecSec]. Dabei gelten vorrangig die Vorgaben aus der CP.	- Mehrpersonen-Zugriffssicherung in Abschnitt 6.2.1, - Ablage, Backup, Archivierung privater Schlüssel in den Abschnitten 6.2.2, 6.2.3 und 6.2.4, - Transfer von privaten Schlüsseln in oder aus und Speicherung in krytographische Module in Abschnitten 6.2.5 und 6.2.6, - Aktivierung und Deaktivierung privater Schlüssel in Abschnitten 6.2.7 und 6.2.8 sowie - Beurteilung der der eingesetzten kryptographischen Module in Abschnitt 6.2.10 – auch hinsichtlich der Einhaltung der Anforderungen an den Lebenszyklus und die Einsatzumgebung aus [KeyLifeSec] – Security Level 2.
6.2	Die Anforderung an Kryptografiemodule für den Einsatz in der Test-PKI ist in C.1 definiert.	Die vorliegende Sub-CA GWAdriga Smart Energy CA setzt bei der Teilnahme als Sub-CA in der Test-PKI Kryptografiemodule zur Generierung, Speicherung und Nutzung ihrer privaten Schlüssels ein, die die Anforderungen an Kryptografiemodule für den Testbetrieb erfüllen, vgl. Anhang Testbetrieb.

6.2.1. Mehrpersonen-Zugriffssicherung zu privaten Schlüsseln

6.2.1	Das Schlüsselmanagement bei … Sub-CA … MUSS im Vier-Augen-Prinzip, unter entsprechender Dokumentation und Protokollierung insbesondere der Rollen und eindeutiger Identifikation der teilnehmenden Personen, durchgeführt werden.	Das Schlüsselmanagement der Sub-CA GWAdriga Smart Energy CA wird im Vier-Augen-Prinzip, unter entsprechender Dokumentation und Protokollierung insbesondere der Rollen und eindeutiger Identifikation der teilnehmenden Personen, durchgeführt. Vgl. auch Abschnitt 5.2.4 für Dokumentation und Protokollierung.

6.2.2. Ablage privater Schlüssel

6.2.2	Es MUSS sichergestellt werden, dass die Daten der privaten Schlüssel nach den Anforderungen aus Kapitel 5 zur sicheren Handhabung und Lagerung von Schlüsselmaterial gespeichert werden.	Die Daten der privaten Schlüssel sind nach den Anforderungen aus Kapitel 5 der [SM-PKI-Policy] zur sicheren Handhabung und Lagerung von Schlüsselmaterial gespeichert, vgl. Abschnitt 5 im vorliegenden Dokument.

6.2.3. Backup privater Schlüssel

6.2.3	Die … Sub-CA … MÜSSEN sicherstellen, dass Maßnahmen zum sicheren Backup der privaten Schlüssel umgesetzt werden. Insbesondere MÜSSEN folgende Anforderungen eingehalten werden: –Die Vorgaben aus 6.2.5 **Transfer** privater Schlüssel in oder aus kryptografischen Modulen MÜSSEN eingehalten werden. –**Bestandteil des ISMS nach ISO 27001:** Die technischen Maßnahmen zum Backup privater Schlüssel MÜSSEN in der Auditierung nach [ISO/IEC 27001] berücksichtigt werden. –**Sichere Schlüssel-Backups:** Die Durchführung von sicheren Backups der privaten Schlüssel MUSS nach den Vorgaben zur sicheren Handhabung und Lagerung von Schlüsselmaterial durchgeführt werden. –**Durchführung des Schlüssel-Backups:** Das Schlüssel-Backup MUSS während der Schlüsselzeremonie gemäß dem Vier-Augen-Prinzip unter Teilnahme des für den Schlüssel verantwortlichen Mitarbeiters durchgeführt werden. Automatisierte Prozesse zur	Die Sub-CA GWAdriga Smart Energy CA setzt die geforderten Maßnahmen zum sicheren Backup der privaten Schlüssel um: - Die Vorgaben aus [SM-PKI-Policy]#6.2.5 zum Transfer privater Schlüssel in oder aus kryptografischen Modulen werden eingehalten, vgl. Abschnitt 6.2.5. - Die technischen Maßnahmen zum Backup privater Schlüssel werden in der Auditierung nach [ISO/IEC 27001] berücksichtigt werden **(Bestandteil des ISMS nach ISO 27001)**. - Sichere Backups der privaten Schlüssel werden nach den Vorgaben zur sicheren Handhabung und Lagerung von Schlüsselmaterial durchgeführt werden, vgl. Abschnitt 6.1.5# Sichere Handhabung und Lagerung von Schlüsselmaterial **(Sichere Schlüssel-Backups)**. - Das Schlüssel-Backup wird während der Schlüsselzeremonie im Vier-Augen-Prinzip unter Teilnahme zweier für den Schlüssel verantwortlicher Mitarbeiter (Keymanager) durchgeführt. **(Durchführung des Schlüssel-Backups)**. - Die Backup-Daten des öffentlichen Schlüssels sind nach den Vorgaben zur

	Übertragung der Schlüssel auf ein weiteres HSM (z. B. für ein Cold-Standby-Backup) DÜRFEN genutzt werden. –**Schlüsselspeicherung:** Es MUSS sichergestellt werden, dass die Backup-Daten des öffentlichen Schlüssels nach den Vorgaben zur sicheren Handhabung und Lagerung von Schlüsselmaterial gespeichert werden. –**Zugriff auf Backup-Daten:** Es MUSS sichergestellt werden, dass nur vertrauenswürdige Mitarbeiter Zugriff auf die Schlüsselspeicher- und Backup-Daten haben.	sicheren Handhabung und Lagerung von Schlüsselmaterial gespeichert, vgl. Abschnitt 6.1.5 **(Schlüsselspeicherung)**. - Ausschließlich dafür im Rollenkonzept autorisierte Personen (unter Einhaltung von Regelungen zur Sicherheitsüberprüfung von Mitarbeitern) haben Zugriff auf Schlüsselspeicher- und Backup-Daten **(Zugriff auf Backup-Daten)**.
6.2.3	Der private Schlüssel KANN als Backup wie folgt exportiert werden: –Verschlüsselter Dateicontainer: •Datenstruktur, die den geheimen Schlüssel enthält und mit einem KEK (Key Encryption Key) verschlüsselt ist (Für die Verschlüsselung sind jeweils die aktuellen Empfehlungen aus [TR-02102-1] einzuhalten). •Die Nutzung des Dateicontainers erfordert den Import in ein Kryptografiemodul, das die Anforderungen aus Kapitel 6.2 erfüllt.	Der private Schlüssel der Sub-CA GWAdriga Smart Energy CA wird als Backup wie folgt exportiert: – Verschlüsselter Dateicontainer: •Datenstruktur, die den geheimen Schlüssel enthält und mit einem KEK (Key Encryption Key) – nachfolgend MasterBackupKey genannt - mit • Krypt. Algorithmus AES, • Schlüssellänge 256 Bit verschlüsselt ist (Für die Verschlüsselung ist hinsichtlich krypt. Algorithmus und Schlüssellänge damit die aktuelle Empfehlung aus [TR-02102-1] eingehal-

	•Der Zugriff auf den verschlüsselten Dateicontainer MUSS auf das Betriebspersonal beschränkt sein. •Die Wiederherstellung des Dateicontainers ist technisch ausschließlich im 4-Augen-Prinzip möglich. –Backup Kryptografiemodul: •Der private Schlüssel wird verschlüsselt direkt in das Backup-Kryptografiemodul transferiert (siehe Abschnitt 6.2.5). •Der Zugang zum Backup-Kryprografiemodul MUSS auf das Betriebspersonal beschränkt sein.	ten). •Für den Import des Dateicontainers wird ein Kryptografiemodul verwendet, das die Anforderungen aus [SM-PKI-Policy]#Kapitel 6.2 erfüllt, vgl. [HSM-Nachweis]. •Der Zugriff auf den verschlüsselten Dateicontainer ist im Rollenkonzept geregelt und auf die Rolle des Keymanagers beschränkt. •Die Wiederherstellung des Dateicontainers ist technisch ausschließlich im Vier-Augen-Prinzip möglich – Backup Kryptografiemodul: •Der private Schlüssel wird verschlüsselt direkt in das Backup-Kryptografiemodul transferiert (siehe Abschnitt 6.2.5). •Der Zugang zum Backup-Kryptografiemodul im Rollenkonzept geregelt und auf die Rolle des Keymanagers beschränkt

6.2.4. Archivierung privater Schlüssel

6.2.4	Es wird keine Archivierung gesperrter oder abgelaufener privater	Eine Archivierung gesperrter oder abgelaufener privater Schlüssel der Sub-CA

	Schlüssel durchgeführt. Diese privaten Schlüssel MÜSSEN unter Beachtung der Einschränkungen aus Kapitel 6.2.9 zerstört werden.	GWAdriga Smart Energy CA wird nicht durchgeführt. Sobald ein Schlüssel-Backup wg. Sperrung oder Gültigkeitsende nicht mehr erforderlich ist, wird es zerstört. Dies ist im [Löschkonzept] berücksichtigt mit Einhaltung der Vorgaben aus Abschnitt 6.2.9.

6.2.5. Transfer privater Schlüssel in oder aus kryptografischen Modulen

6.2.5	Der private Schlüssel KANN zwischen kryptografischen Modulen transferiert werden. –Voraussetzung für den Transfer privater Schlüssel ist, dass nur Kryptografiemodule verwendet werden, welche die Anforderungen aus Abschnitt 6.2 erfüllen. –Der private Schlüssel MUSS hierbei verschlüsselt und integritätsgesichert transferiert werden. Die Ver-/Entschlüsselung MUSS in den Kryptografiemodulen erfolgen. –Der KEK zur Ver-/Entschlüsselung des privaten Schlüssels MUSS vertraulich und integritätsgesichert ausgetauscht werden. –Bei der Durchführung eines manuellen Transfers MUSS das Vier-	Wenn der private Schlüssel der GWAdriga Smart Energy CA zwischen Kryptografiemodulen transferiert wird, dann werden die nachfolgenden Bedingungen eingehalten: - Es werden Kryptografiemodule verwendet, welche die Anforderungen aus Abschnitt 6.2 an die BSI-Zertifizierung erfüllen. - Der private Schlüssel ist beim Transfer verschlüsselt und integritätsgesichert. Die Ver-/Entschlüsselung erfolgt in den Kryptografiemodulen, vgl. Abschnitt 6.2.4. - Der KEK, hier MasterBackup zur Ver-/Entschlüsselung des privaten Schlüssels, wird vertraulich und integritätsgesichert ausgetauscht: Nach Import des MBK von zwei verschiedenen SmartCards für zwei verschiedene Personen, die die Rolle Keymanager innehaben, wird der MBK dauerhaft im HSM gespeichert.

	Augen-Prinzip eingehalten werden.	- Bei der Durchführung eines manuellen Transfers wird das Vier-Augen-Prinzip eingehalten.

6.2.6. Speicherung privater Schlüssel in kryptografischen Modulen

6.2.6	Grundsätzlich MÜSSEN die privaten Schlüssel eines PKI-Teilnehmers auf einem Kryptografiemodul gespeichert werden. •Die einzige Ausnahme bilden die client- und serverseitigen TLS-Schlüssel bei Sub-CA und Root-CA, die bei der Root-CA und den Sub-CAs zur TLS-Authentisierung an der Web-Service-Schnittelle und am Verzeichnisdienst verwendet werden. Hier SOLLTE ein Kryptografiemodul eingesetzt werden. –Auf einem HSM DÜRFEN private Schlüssel von PKI-Teilnehmern derselben PKI-Rolle gespeichert werden (Bsp.: es dürfen mehrere CA-Schlüssel auf demselben HSM gespeichert werden). Diese MÜSSEN aber in getrennten Sicherheitsdomänen (Trennung auf Anwendungsebene) verwaltet werden. Entsprechend MÜSSEN diese im HSM logisch getrennt sein.	Alle privaten Schlüssel der Sub-CA GWAdriga Smart Energy CA sind in einem Kryptografiemodul gespeichert, einschließlich der TLS- Schlüssel der Sub-CA. Verschiedene private Schlüssel für die Rolle als Sub-CA werden vom Betreiber (z.B. als Eigenbetrieb und Fremdbetrieb) auf einem HSM in getrennten Sicherheitsdomänen (Instanzentrennung, Trennung auf Anwendungsebene, logische Trennung) gespeichert und verwaltet.
6.2.6	–Auf einem HSM DÜRFEN KEINE privaten Schlüssel von verschie-	Da GWAdriga Smart Energy CA ausschließlich die Rolle als Sub-CA ausübt,

	denen PKI-Rollen gespeichert werden. Es darf entsprechend keine Vermischung von Schlüsseln von unterschiedlichen PKI-Rollen auf einem HSM erfolgen (Bsp.: es dürfen keine CA- und GWA-Schlüssel auf demselben HSM gespeichert werden). –Die privaten Schlüssel der PKI-Teilnehmer aus einer Testumgebung MÜSSEN von der Produktivumgebung getrennt werden.	liegen keine privaten Schlüssel für andere Rollen vor. Private Schlüssel zur Teilnahme der GWAdriga Smart Energy CA an der Test-PKI für die Rolle als Sub-CA werden auf einem Testbetriebs-HSM gespeichert und verwaltet.

6.2.7. Aktivierung privater Schlüssel

6.2.7	Die Aktivierung eines Schlüssels in einem Kryptografiemodul erfordert die Einhaltung des Vier-Augen-Prinzips.	Die Aktivierung eines Schlüssels der Sub-CA GWAdriga Smart Energy CA in einem Kryptografiemodul wird im Vier-Augen-Prinzip durchgeführt.

6.2.8. Deaktivierung privater Schlüssel

6.2.8	Im deaktivierten Zustand der Schlüssel DÜRFEN diese NICHT genutzt werden können.	Deaktivierte Schlüssel (das sind nicht aktive/nicht konfigurierte CA-Schlüssel) der Sub-CA GWAdriga Smart Energy CA werden nicht genutzt. Deaktivierte Schlüssel sind: 1. ein für die zukünftige Nutzung vorgesehener Schlüssel, der erst ab einem bestimmten zukünftigen Datum verwendet werden soll, 2. ein Schlüssel, der nicht mehr verwendet wird, da er durch einen Nachfolgeschlüssel ersetzt wurde; 3. ein aus anderen Gründen für einen bestimmten Zeitraum nicht verwendeter Schlüssel.

6.2.9. Zerstörung privater Schlüssel

6.2.9	Die privaten Schlüssel eines CA-Betreibers MÜSSEN in folgenden Fällen sicher und unwiederherstellbar zerstört werden: –Der Gültigkeitszeitraum des CA-Schlüssels ist abgelaufen –Der Schlüssel der CA wurde gesperrt. Die Backups der Schlüssel MÜSSEN ebenfalls berücksichtigt werden. Die Zerstörung der privaten Schlüssel MUSS durch einen sicheren Lösch-Mechanismus im Kryptografiemodul (falls vorhanden) oder durch die unwiederherstellbare mechanische Zerstörung erfolgen. Für diesen Prozess gelten die Anforderungen aus [KeyLifecSec]. 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, MUSS dieser zerstört werden.	Die privaten Schlüssel der Sub-CA GWAdriga Smart Energy CA werden in folgenden Fällen sicher und unwiederherstellbar zerstört: – Der Gültigkeitszeitraum des CA-Schlüssels ist abgelaufen. – Der Schlüssel der CA wurde gesperrt. Die Backups der Schlüssel werden ebenfalls berücksichtigt, vgl. 6.2.4. Die Zerstörung von ENC-Schlüsseln entfällt: Private Schlüssel für ENC-Zertifikate fallen in der GWAdriga Smart Energy CA nicht an. ENC-Zertifikate kommen für Endnutzer als eines der Zertifikate eines Tripels vor. Aber: die privaten Schlüssel zu allen ENC-Zertifikaten verbleiben beim Zertifikatsinhaber, der Inhaber schickt lediglich einen Antrag, der mit dem privaten Schlüssel signiert wurde.

6.2.10. Beurteilung kryptografischer Module

6.2.10	Die Sicherheitsanforderungen an Kryptografiemodule zum Schutz der privaten Schlüssel zu den Zertifikaten der SM-PKI werden in Kapitel 6.2 definiert.	Die Sicherheitsanforderungen an Kryptografiemodule zum Schutz der privaten Schlüssel zu den Zertifikaten sind in [SM-PKI-Policy]#Kapitel 6.2 definiert und werden von der vorliegenden Sub-CA GWAdriga Smart Energy CA eingehalten, vgl. Abschnitt 6.2.
6.2.10	**Geltungsbereich:** Innerhalb der PKI können verschiedene Produktklassen von Kryptografiemodulen eingesetzt werden, z.B. Hardware-Sicherheitsmodule (HSM), Chipkarten und Secure Elements (vgl. Kategorien der Schutzprofile in [KeyLifecSec]).	Die vorliegende Sub-CA GWAdriga Smart Energy CA setzt ausschließlich Hardware-Sicherheitsmodule (HSM) ein.
6.2.10	**Sicherheitsanforderungen:** Um ein Kryptografiemodul in der SM-PKI einsetzen zu können, MUSS dieses konform zu den Anforderungen an Kryptografiemodule aus [KeyLifecSec] – Security Level 2[1] sein. Hinsichtlich der Anforderungen an den Zufallsgenerator des Kryptografiemodules gelten die Anforderung aus [TR-03116-3]. Ergänzend zu [KeyLifecSec] KANN für GWA, GWH und EMT auch ein	**Sicherheitsanforderungen/Übergangsregelung:** Die Sub-CA GWAdriga Smart Energy CA setzt für den Wirkbetrieb Krytomodule ein, die die Anforderungen der Übergangsregelung erfüllen. Die Anforderungen der [SM-PKI-Policy] hinsichtlich des Key-Lifecycle im ISMS, vgl. Sicherheitskonzept [Betr_Siko], berücksichtigt.

[1] Informativ: Derzeit erstellt das BSI basierend auf BSI-CC-PP-0077 und zugehöriger TR ein adaptiertes PP für den serverseitigen Einsatz des Sicherheitsmoduls, welches auf dem Sicherheitsniveau Security Level 2 in die CP aufgenommen werden soll.

	Kryptografiemodul eingesetzt werden, das nach BSI-CC-PP-0095 zertifiziert ist. **Übergangsregelung:** Die für ein Kryptografiemodul in Security Level 2 geforderte Zertifizierung KANN bis auf Widerruf alternativ durch den Nachweis der in der [SM-PKI-Policy] in Tabelle 11 bzw. 12 aufgeführten Anforderungen erfüllt werden. Bzgl. der Anforderungen wird insbesondere zwischen einer zertifizierten und einer nicht zertifizierten Einsatzumgebung unterschieden. Bei einer zertifizieren Einsatzumgebung MÜSSEN die Anforderungen aus der SM-PKI Policy speziell hinsichtlich des Key-Lifecycle im ISMS berücksichtigt werden.	Für den Testbetrieb werden Krytomodule eingesetzt, die den Anforderungen der [SM-PKI-Policy] zum Testbetrieb genügen.

6.3. Andere Aspekte des Managements von Schlüsselpaaren

6.3.1. Archivierung öffentlicher Schlüssel

6.3.1	Die Zertifikate eines Teilnehmers der SM-PKI MÜSSEN inklusive der Statusdaten archiviert werden (siehe Anhang B der [SM-PKI-Policy]).	Die Zertifikate der Teilnehmer der Sub-CA GWAdriga Smart Energy CA werden inklusive der Statusdaten archiviert für die Archivierungszeit gemäß [SM-PKI-Policy]#Anhang B: -Zertifikate der Sub-CA: Zertifikatslaufzeit + 10 ½ Jahre

		-Zertifikate durch Sub-CA GWAdriga Smart Energy CA ausgestellt für EMT, GWA, GHW, SMGW: Zertifikatslaufzeit + 2 ½ Jahre

6.3.2. Gültigkeitszeitraum von Zertifikaten und Schlüsselpaaren

6.3.2	Der Gültigkeitszeitraum von Zertifikaten und Schlüsseln wird in [TR-03109-4] definiert. Unabhängig vom Gültigkeitszeitraum MÜSSEN die folgenden Zertifikate spätestens in dem hierzu angegebenen Intervall gewechselt werden: Instanz: Zertifikat: Sub-CA C(Sub-CA)	Als Gültigkeitszeitraum für Sub-CA-Zertifikate gemäß [TR-03109-4]#Tabelle 11 in Abschnitt 3.2 sind 5 Jahre vorgesehen. Gemäß [SM-PKI-Policy]#6.3.2 wird der Sub-CA-Schlüsselwechsel im Intervall von 2 Jahren durchgeführt. Dementsprechend wird rechtzeitig (**mindestens 3 Tage**, in der Regel 2 Wochen) vor Erreichen der Intervallgrenze ein neuer CA-Schlüssel für GWAdriga Smart Energy CA generiert, ein Zertifikatsrequest erzeugt und zur Zertifizierung an die Root-CA eingereicht.
6.3.2	Sobald eine CA über ein neues Zertifikat verfügt, MUSS dieses zum Ausstellen neuer Zertifikate und der zugehörigen Sperrlisten verwendet werden.	Sobald zum eingereichten Request das neue GWAdriga Smart Energy CA Zertifikat eintrifft, wird auf dem HSM ein Schlüsselwechsel durchgeführt und das neue Zertifikat zum Ausstellen neuer Zertifikate und der zugehörigen Sperrlisten verwendet.

6.4. Aktivierungsdaten

6.4	Die Aktivierungsdaten für die Kryptografiemodule MÜSSEN sicher aufbewahrt werden.	Die Aktivierungsdaten (Admin-SmartCards) für die Verwaltung der Kryptografiemodule (als HSM-Administrator) werden sicher aufbewahrt.

6.5. Sicherheitsanforderungen für die Rechneranlagen

6.5	Nachfolgend werden die Anforderung an die Rechneranlagen definiert, die von den jeweiligen PKI-Teilnehmern umgesetzt werden MÜSSEN: –**… Sub-CA …: Netzwerkkontrolle:** Es MÜSSEN entsprechende Maßnahmen umgesetzt werden, um das interne Netzwerk vom externen zu trennen und vor unbefugtem Zugriff zu schützen. –… **Sub-CA …: Intrusion Detection Systeme (IDS):** Der Einsatz von Intrusion-Detection-Systemen (IDS) im gesicherten Netzsegment MUSS berücksichtigt werden. Die Log-Dateien des IDS MÜSSEN regelmäßig kontrolliert werden. –…**Sub-CA …:** Die CA-Server, die zur Erstellung von Zertifikaten verwendet werden, MÜSSEN gehärtet werden. Dies umfasst die Konfiguration und Einstellung der verwendeten Hardware- und Software-Komponenten. –**… Sub-CA: System-Konfiguration:** Die Konfigurationsoptionen und –einstellungen DÜRFEN nur die minimal benötigten Funktio-	Die für die Sub-CA eingesetzte IT-Infrastruktur erfüllt die in [SM-PKI-Policy]#6.5 geforderten Anforderungen: - Es sind Maßnahmen umgesetzt, um das interne Netzwerk vom externen zu trennen und vor unbefugtem Zugriff zu schützen **(Netzwerkkontrolle)**. - Es wird ein Intrusion Detection and Prevention System IDS/IPS eingesetzt. Die dabei aufkommenden Events werden regelmäßig kontrolliert. (**Intrusion Detection System (IDS)**). - Die CA-Server, die zur Erstellung von Zertifikaten verwendet werden, sind gehärtet. Dies umfasst die Konfiguration und Einstellung der verwendeten Hardware- und Software-Komponenten. - Die Konfigurationsoptionen und –einstellungen enthalten nur die minimal benötigten Funktionalitäten für den CA-Betrieb **(System-Konfiguration)**. - Die Netzwerke, in denen sich die CA-Server befinden, sind durch geeignete Maßnahmen geschützt **(Netzwerk-Separierung)**.

	nalitäten für den CA Betrieb enthalten. –… **Sub-CA: Netzwerk-Separierung:** Die Netzwerke, in denen sich die CA-Server befinden, MÜSSEN durch geeignete Maßnahmen geschützt werden. –**Alle PKI-Teilnehmer: Software-Updates:** Software-Updates MÜSSEN bei sicherheitsrelevanten Änderungen schnellstmöglich eingespielt werden, andere Updates SOLLTEN regelmäßig aktualisiert werden. –… **Sub-CA: Vertraulichkeit und Integrität:** Die CA MUSS sensitive Daten vor unbefugtem Zugriff oder Veränderung schützen. –… **Sub-CA: Logging und Audit-Trails:** Log -Dateien und Audit-Trails MÜSSEN regelmäßig geprüft werden, und automatisierte Benachrichtigungen MÜSSEN auf Abweichung vom vorgesehenen Betrieb hinweisen. –… **Sub-CA: Speicherort von Log-Dateien:** Die Dateien der Audit-Trails SOLLEN NICHT auf dem CA-Server, der für die Verwaltung	Software-Updates werden bei sicherheitsrelevanten Änderungen schnellstmöglich eingespielt, andere Updates werden regelmäßig aktualisiert (**Software-Updates**). - Log-Dateien und Audit-Trails werden regelmäßig geprüft, und automatisierte Benachrichtigungen weisen auf Abweichung vom vorgesehenen Betrieb hin. Es wird ein Icinga Monitoring System in Verbindung mit einer Mailing Notification betrieben **(Logging und Audit-Trails)**. **-** Die Dateien der Audit-Trails werden nicht auf dem CA-Server, der für die Verwaltung von Zertifikaten verwendet wird, gespeichert. Einige Log-Dateien werden auf dem CA-Server, der für die Verwaltung von Zertifikaten verwendet wird, vorübergehend gespeichert und von dort regelmäßig gesichert **(Speicherort von Log-Dateien)**. - Die IT-Systeme verfügen über eine angemessene Benutzerverwaltung. - Die CA begrenzt den Zugriff auf die benötigten Systemfunktionen und Hilfsprogramme **(Systemfunktionen)**.

	von Zertifikaten verwendet wird, gespeichert werden. Der Speicherort für Log-Dateien KANN temporär der CA-Server sein. Die Log-Dateien MÜSSEN dann regelmäßig auf einen anderen Speicherort ausgelagert werden. –**Alle PKI-Teilnehmer:** Das System MUSS über eine angemessene Benutzerverwaltung verfügen. –… **Sub-CA: Systemfunktionen:** Die CA MUSS den Zugriff auf die benötigten Systemfunktionen und Hilfsprogramme begrenzen. –**Alle PKI-Teilnehmer: Schutz vor Schadsoftware:** Die Integrität der System-Komponenten und Informationen MUSS gegen Viren, Schadsoftware sowie nicht zugelassene Programme geschützt werden.	**-** Die Integrität der System-Komponenten und Informationen ist gegen Viren, Schadsoftware sowie nicht zugelassene Programme geschützt (**Schutz vor Schadsoftware)**.

6.6. Zeitstempel

6.6	Keine	N/A

6.7. Validierungsmodell

6.7	Die Anforderungen an die Zertifikatsvalidierung werden in der [TR-	Die GWAdriga Smart Energy CA validiert Zertifikatsrequests nach den in [TR-

	03109-4] spezifiziert.	03109-4]#3.2.1 spezifizierten Anforderungen an die V:alidierung.

7. Profile für Zertifikate und Sperrlisten

Die Profile für

- Zertifikate,
- Zertifikatsrequests,
- Sperrlisten sowie
- das Sperrmanagement

sind in [TR-03109-4] spezifiziert.

Das Namensschema zu den Zertifikaten ist in Anhang A der [SM-PKI-Policy] definiert und im Abschnitt 3.1 dieses Dokuments für GWAdriga Smart Energy CA spezifiziert worden.

8. Überprüfung und andere Bewertungen

8.1. Inhalte, Häufigkeit und Methodik

8.1.1. Testbetrieb

Die vorliegende Sub-CA GWAdriga Smart Energy CA stellt eine Testumgebung zur Verfügung, vgl. Anhang Testbetrieb, in welcher Testaufgaben zum Test der Funktionalitäten der PKI-Infrastruktur und –Prozesse durchlaufen werden müssen:

- Die Sub-CA selbst:
  um ihre Testaufgaben in Richtung Root-CA zu erfüllen, vgl. Abschnitt 8.1.1.1, und
- ihre antragstellenden PKI-Teilnehmer GWA, EMT und GWH:
  um Testaufgaben im Zusammenwirken mit der Sub-CA GWAdriga Smart Energy CA zu erfüllen, vgl. Abschnitt 8.1.1.2.

8.1.1.1. Testbetrieb der Sub-CA

Zur vorliegenden Sub-CA GWAdriga Smart Energy CA sind alle Nachweise gegenüber der Root-CA aus dem Testbetrieb erfüllt:

- Nachweis der vollständigen und korrekten Funktion der Zertifikatsantragstellung und Zertifikatsannahme.
  Basis: Webservice-Schnittstelle

Die für den Testbetrieb genutzte Testumgebung steht zur Verfügung, um mit dem Antragsteller den Test der Funktionalitäten ihrer PKI-Infrastruktur und –Prozesse durchzuführen. Dieser Test muss nachgewiesen werden, um Teilnehmer der Wirk-PKI werden zu können (siehe 3.2).

8.1.1.2. Testbetrieb der Endnutzer-Zertifikate

Zur Teilnahme von GWA und GWH am Testbetrieb der Sub-CA GWAdriga Smart Energy CA wird geprüft:

- vollständige und korrekte Funktion der Zertifikatsantragstellung und Zertifikatsannahme
  Basis: S/MIME-Kommunikation für initiale Requests und Zertifikate sowie Webservice-Schnittstelle für Folgerequests und –zertifikate mit den einzelnen Prüfpunkten:
  - Erfolgreiche Registrierung für den Testbetrieb,
  - Sichere E-Mail Kommunikation (S/MIME),
  - Erstellung initialer Requests des GWA bzw. GWH und Annahme der Zertifikate,
  - Nutzung des Webservice der Sub-CA (für Beantragung von SMGW-W-Zertifikatstripel und -Folgezertifikate durch den GWA bzw. für Beantragung von SMGW-G-Zertifikatstripel durch den GWH),
  - Nutzung des Webservice der Sub-CA (GWA- bzw. GWH-Folgezertifikat) oder Beantragung eines Folgezertifikats per S/MIME,
  - Erfolgreiche Sperrung eines Zertifikates des GWA bzw. GWH oder eines SMGW-Zertifikats, das vom GWA bzw. GWH verwaltet wird

Zur Teilnahme von EMT am Testbetrieb der Sub-CA GWAdriga Smart Energy CA wird geprüft:

- Konformität der Zertifikatsrequests mit den einzelnen Prüfpunkten:
  - Erfolgreiche Registrierung für den Testbetrieb
  - Sichere E-Mail Kommunikation
  - Erstellung initialer Requests des EMT und Annahme der Zertifikate
  - Nutzung des Webservice der Sub-CA (EMT-Folgezertifikate) oder Beantragung eines Folgezertifikats per S/MIME,
  - Erfolgreiche Sperrung eines EMT-Zertifikates

Nach erfolgreicher Teilnahme wird dem Antragsteller eine verschlüsselte und signierte E-Mail zugesendet.

8.1.2. Beantragung Teilnahme an SM-PKI

8.1.2.1. Teilnahme als Sub-CA

Die Beantragung zur Teilnahme der vorliegenden Sub-CA GWAdriga Smart Energy CA bei der Root-CA ist erfolgt.

Vorausgegangen ist die Prüfung der Anforderungen an eine Sub-CA:

- ISO 27001-Zertifizierung nativ der Sub-CA Services des Sub-CA-Betreibers
  (geprüft durch einen zertifizierten ISO 27001 Lead Auditor,
  Nachweis: Zertifikat)
- Zertifizierung nach [TR-03145-1] der Sub-CA Services des Sub-CA-Betreibers
  (geprüft durch einen zertifizierten [TR-03145-1] Auditor,
  Nachweis: Zertifikat)
- Erfolgreiche Tests

(geprüft durch Prüfer der Root-CA,
Nachweis: Signierte E-Mail der Root-CA über erfolgreiche Tests mit der Test-Sub-CA der GWAdriga Smart Energy CA)

8.1.2.2. Teilnahme als GWH, GWA, EMT

Die vorliegende Sub-CA GWAdriga Smart Energy CA ermöglicht nach erfolgreichem Testbetrieb GWH, GWA und EMT die Teilnahme an der SM-PKI, vgl. Abschnitt 8.1.1.2.

Zur Beantragung sind erforderlich:

- Für GWH:
  - Die Antragsunterlagen wie ausgeführt in Abschnitt 3.2.2.3,
  - Die erforderliche Zertifizierung gemäß [SM-PKI-Policy]#Abschnitt 5.1.1 als PKI-Teilnehmer GWH: Ein Gateway-Hersteller benötigt ein Common-Criteria-Zertifikat auf Basis von [BSI-CC-PP-0073] für sein Produkt SMGW, um die Sicherheit seiner Produktionsumgebung nachzuweisen.
  - Darüber hinaus: Das im Common-Criteria-Zertifikat benannte SMGW des GWH muss gemäß [TR-03109-1] zertifiziert sein.
- Für GWA:
  - Die Antragsunterlagen wie ausgeführt in Abschnitt 3.2.2.2,
  - Die erforderliche Zertifizierung gemäß [SM-PKI-Policy]#Abschnitt 5.1.1 als PKI-Teilnehmer GWA: Ein GWA MUSS alle Anforderungen gemäß [TR-03109-6] erfüllen und das entsprechende Zertifikat nachweisen: Der Nachweis wird durch einen Auditbericht gemäß ISO 27001-Zertifizierung auf Basis von IT-Grundschutz oder eine Zertifizierung nach ISO/IEC 27001 erbracht, der das Auditierungsschema gemäß [TR-03109-6] einhält.
- Für EMT:
  - Die Antragsunterlagen wie ausgeführt in Abschnitt 3.2.2.1,
  - Die erforderliche Zertifizierung gemäß [SM-PKI-Policy]#Abschnitt 5.1.1 als PKI-Teilnehmer EMT: Ein passiver EMT MUSS ein Sicherheitskonzept erstellen und umsetzen,, in dem die Anforderungen aus der [SM-PKI-Policy] berücksichtigt werden. Ein aktiver EMT (siehe Abschnitt 1.3.3) MUSS eine ISO 27001-Zertifizierung vorweisen bzw. nachweisen, dass ein nach ISO 27001 zertifizierter Dritter die Leistung für ihn erbringt.

8.1.3. Wirkbetrieb

Die vorausgesetzten Nachweise/Zertifizierungen der GWAdriga Smart Energy CA werden im Wirkbetrieb auf Basis der Prüf-/Zertifizierungsschemas aufrechterhalten. Dafür werden Audits und Re-Zertifizierungen des Sub-CA-Betreibers regelmäßig durchgeführt. Die Mitteilung an die Root-CA über die Ergebnisse der Überwachungsmaßnahmen erfolgt wie in Abschnitt 3.2.7 beschrieben.

Ein autorisierter Ansprechpartner der GWAdriga Smart Energy CA teilt einem Ansprechpartner der Root-CA per S/MIME-Kommunikation jede Änderung des vorliegenden Dokuments mit.

8.2. Reaktionen auf identifizierte Vorfälle

Zu Reaktionen auf identifizierte Vorfälle vergleiche Abschnitt 5.2.10.

9. Sonstige finanzielle und rechtliche Regelungen

9.1. Preise

Preise für Sub-CA-Dienstleistungen werden auf Anfrage mitgeteilt.

9.2. Finanzielle Zuständigkeiten

Als Betreiber von Sub-CA-Instanzen sind wir finanziell eigenständig und unabhängig.

10. Glossar, Abkürzungen etc.

10.1. Glossar

Begriff (Ggf. alternativer Begriff)	Erläuterung
Aktiver EMT	Ein aktiver EMT nutzt ein SMGW, um über dieses nachgelagerte Gerät (Controllable Local Systems, CLS) anzusprechen. Die entsprechenden Anwendungsfälle zur Steuerung von CLS an der HAN-Schnittstelle durch einen EMT sind in der [TR-03109-1] definiert.
Ansprechpartner	Ansprechpartner sind die Vertreter des Zertifikatsnehmers, siehe Vertreter.
Antragsteller	Antragsteller sind die Zertifikatsnehmer / Teilnehmer, die ein Zertifikat beantragen und für die noch kein Zertifikat ausgestellt wurde.
Dienstleister	Dienstleister können als Auftragnehmer Zertifikatsnehmer für eine andere Organisation sein.
EMT	Ein externer Marktteilnehmer (EMT) erhält von einer Sub-CA der SM-PKI Zertifikate, mit denen er insbesondere mit den SMGWs sicher kommunizieren kann. Überdies kann der Datenaustausch mit den anderen Teilnehmern der SM-PKI (z. B. einem GWA) abgesichert werden.
Endnutzer	GWA oder GWH oder EMT oder SMGW
GWA	Ein Gateway-Administrator 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 einer Sub-CA Zertifikate, mit

Begriff (Ggf. alternativer Begriff)	Erläuterung
	denen er - die Beantragung und Verwaltung der Wirkzertifikate der SMGWs durchführen, - die Administration der SMGWs durchführen und - den Datenaustausch mit den anderen Teilnehmern der SM-PKI (z. B. EMT) absichern kann.
GWH	Ein Hersteller von Gateway-Komponenten erhält von einer Sub-CA der SM-PKI Zertifikate, mit denen er insbesondere die Prozesse zur Beantragung und Verwaltung von Gütesiegelzertifikaten für SMGWs durchführen kann.
SMGW	Ein Smart Meter Gateway ist die zentrale Kommunikationseinheit des intelligenten Messsystems. Smart Meter Gateways sorgen für die sichere und verschlüsselte Kommunikation der einzelnen Bausteine im Energiesystem und werden dafür vom BSI zertifiziert. Sie sind in der Lage, nicht nur Stromzähler, sondern über gesonderte Schnittstellen auch Erzeugungs- und Verbrauchsanlagen wie Solaranlagen, Elektromobile, Stromspeicherheizungen und Wärmepumpen in das intelligente Energienetz zu integrieren. Quelle : http://www.bmwi-energiewende.de/EWD/Redaktion/Newsletter/2015/16/Meldung/smart-meter.html
Teilnehmer (Participant)	Nutzer der Zertifikate (diejenigen, die diesen vertrauen).
Transport Layer Security	Protokoll zur Verschlüsselung von Datenübertragungen im Internet
Vertreter	Vertreter sind stets natürliche Personen, die autorisiert sind eine Organisation, die als Zertifikatsnehmer auftritt, zu vertreten. Vertreter besitzen ein personenbezogenes S/MIME-Zertifikat für den verschlüsselten E-Mail-Austausch.
Zertifikatsinhaber (Subscriber)	Der Inhaber eines Zertifikates. Dies können Services, Personen, Server, Router oder ähnliche sein. In der vorliegenden Policy sind dies Organisationen oder technische Geräte.
Zertifikatsnehmer	Teilnehmer (Subscriber)

10.2. Abkürzungen

Abkürzung	Begriff
APC	Arbeitsplatzrechner
ASP	Ansprechpartner
CA	Certification Authority

Abkürzung	Begriff
CC	Common Criteria
CENC	Certificate for Encryption / Verschlüsselungszertifikat
CLS	Controllable Local Systems
CP	Certificate Policy
CPS	Certificate Practices Statement
CRL	Certificate Revocation List / Zertifikatssperrliste
CSIG	Certificate for Signature /Signaturzertifikat
CTLS	Certificate for TLS / TLS-Zertifikat
DRG	Deterministic RNG / Funktionsklasse für Zufallszahlengeneratoren
EMT	Externer Marktteilnehmer
ENC	Encryption / Verschlüsselung
ENu	Endnutzer
GWA	Gateway-Administrator
GWH	Gateway-Hersteller
HAN	Home Area Network
HSM	Hardware Security Module
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ID	Identifier
ISMS	Information Security Management System
ISO	International Organization for Standardization
KEK	Key Encryption Key
KM	Krypto-Modul
LDAP	Lightweight Directory Access Protocol
LDAPS	LDAP over SSL
MBK	Master Backup Key
NTG	Non-physical TRNG / Funktionsklasse für Zufallsgeneratoren
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PIN	Personal Identifikation Number
PKI	Public Key Infrastructure
PP	Protection Profile

Abkürzung	Begriff
PTG	Physical TRNG / Funktionsklasse für Zufallsgeneratoren
QA	Quality Assurance
RA	Registration Authority
RNG	Random Number Generator
RG	Registrator
SHA	Secure Hash Algorithm
SSL	Secure Sockets Layer
SMGW	Smart Meter Gateway
SM-PKI	Smart Metering PKI
TRNG	True Random Number Generator
TLS	Transport Layer Security
TS	Teilnehmerservice
URI	Uniform Resource Identifier
URL	Uniform Resource Locator

10.3. Mitgeltende Dokumente

Referenz	Dokument
[CPS]	Certification Practice Statement der GWAdriga Smart Energy CA, ist implizit im SM-GWAdriga Policy enthalten
[Betr_NotfK]	Anhang 4 – Notfallkonzept des Betreibers
[Betr_Prot]	Anhang 7 zu [Betr_Siko] – Protokollierungskonzept des Betreibers
[Betr_RegPruef]	Anhang 5 zu [Betr_Siko] – Regelmäßige Prüfungen des Betreibers
[Betr_Roko]	Rollenkonzept des Betreibers
[Betr_Siko]	Sicherheitskonzept des Betreibers
[Auditbericht]	Auditbericht TR03109-Konformität des Sub-CA-Betreibers
[Betriebskonzepte]	Betriebskonzepte GWAdriga Smart Energy CA
[BSI CC-PP-0045]	Protection Profile Cryptografic Modules, Security Level "Enhanced", Version 1.01, 2008
[BSI-CC-PP-0073]	Protection Profile for the Gateway of a Smart Metering System (Smart Meter Gateway PP) - Schutzprofil für die Kommunikationseinheit eines intelligenten Messsystems für Stoff- und Energiemengen - SMGW-PP – Version 1.3, 31 March 2014 (Final Release) – Certification-ID: BSI-CC-PP-0073

Referenz	Dokument
BSI-CC-PP-0077	BSI: Protection Profile for the Security Module of a Smart Meter Gateway (Security Module PP)
[BSI-CC-PP-0095]	BSI: Protection Profile for the Security Module of a Smart Meter Mini-HSM (Mini-HSM Security Module PP), Version 1.0, 2017
[DIN 43863-5]	Herstellerübergreifende Identifikationsnummer für Messgeräte
[HSM-HB]	HSM-Handbuch Schlüsselzeremonie
[KeyLifeSec]	BSI: Key Lifecycle Security Requirements Version 1.0.2
[Löschkonzept]	Analyse Löschkonzept Trustcenter
[MsbG]	Messstellenbetriebsgesetz
[RFC-5280]	IETF RFC 5280, D. Cooper, S. Santesson, S. Farrell, S. Boyen, R. Housley, W. Polk, Internet X.509 Public Key Infrastructures - Certificates and Certificate Revocation List (CRL) Profiles, 2008
[RFC-5480]	IETF RFC 5480, S. Turner, R. Housley, T. Polk, Elliptic Curve Cryptography Subject Public Key Information
[Secure-CA]	https://www.bsi.bund.de/SharedDocs/Zertifikate_TR/Secure_CA/BSI-K-TR-0402-2020.html Datum: 26.10.2020
[SM-PKI-Policy]	Certificate Policy der Smart Metering-PKI, Version 1.1.2, 25.01.2023
[TR-02102-1]	BSI TR-02102-1, Kryptographische Verfahren: Empfehlungen und Schlüssellängen, Version: 2023-01, Stand: 09. Januar 2023
[TR-03109-1]	Technische Richtlinie BSI TR-03109-1: Anforderungen an die Interoperabilität der Kommunikationseinheit eines intelligenten Messsystems - Version: 1.1, Datum: 2021-09-17
[TR-03109-3]	Technische Richtlinie BSI TR-03109-3: Kryptographische Vorgaben für die Infrastruktur von intelligenten Messsystemen - Version: 1.1, 17.04.2014
[TR-03109-4]	Technische Richtlinie BSI TR-03109-4: Smart Metering PKI - Public Key Infrastruktur für Smart Meter Gateways, Version 1.2.1, 09.08.2017
[TR-03109-6]	BSI TR-03109-6: Smart Meter Gateway Administration, Version 1.0, Datum 26.11.2015
[TR-03116-3]	BSI TR-03116-3, , Kryptographische Vorgaben für Projekte der Bundesregierung, Teil 3: Intelligente Messsysteme, Stand 2023, Datum: 6. Dezember 2022
[TR-03116-4]	BSI TR-03116-4: Kryptographische Vorgaben für Projekte der Bundesregierung, Teil 4: Kommunikationsverfahren in Anwendungen, 2022, Datum: 24. Januar 2022
[TR-03145-1]	BSI TR-03145-1 Secure CA operation, Part 1, Generic requirements for Trust Centers instantiating as Certification Authority (CA) in a Public-Key Infrastructure (PKI)

Referenz	Dokument
	with security level 'high', Version 1.1, Datum: 27.03.2017
[HSM-Nachweis]	Nachweis zum HSM für den Einsatz in der Smart-Metering-PKI durch eine durch das BSI für Common Criteria-Evaluierungen akkreditierte Prüfstelle. Details daraus: –sicherer Zufallszahlengenerators der folgenden Klasse: -–DRG.4, –Tamper-Schutz gegen Attack Potential "moderate" und „high“; –Seitenkanalresistenz gegen Attack Potential "moderate" und „high“. Datum: 8.07.2016
[Zertifikat]	ISO/IEC 27001 Multisite-Zertifikat

Anhang Testbetrieb

Dieser Anhang beschreibt, wie GWAdriga Smart Energy CA die Anforderungen der übergeordneten Policy an die Teilnahme in der Test-PKI umsetzt:

C.1 Test-PKI Sicherheitsanforderungen	Als Teilnehmer der SM-Test-PKI generiert, speichert und nutzt GWAdriga Smart Energy CA seine Sub-CA-Schlüssel in Kryptografiemodulen. Das in der SM-Test-PKI eingesetzte Kryptografiemodul ist konform zu den Anforderungen an Kryptografiemodule aus [KeyLifeSec] – Security Level 1: • Der Zugriff auf die Kryptografiemodule ist durch eine Zwei-Faktorautorisierung geschützt, vgl. [Betr_Siko]. Zudem wird auch im Testbetrieb das Vier-Augen-Prinzip nach [Betr_Roko] angewendet. • Die Anzahl von berechtigten Personen, die auf die Kryptografiemodule zugreifen, ist durch das Rollenkonzept [Betr_Roko] eingeschränkt und auf das notwendige Maß reduziert. • Durch die o.a. Maßnahmen sind die privaten Schlüssel vor unautorisiertem Zugriff und Kompromittierung geschützt. • Die Zufallszahlengenerierung wird vom eingesetzten Kryptografiemodul wie gefordert mit DRG.4 oder PTG.3 gemäß [AIS 20/31] oder [TR-02102] umgesetzt.
C.2.1 Test-PKI …Sub-CA Anforderungen - Allgemein	Der Betrieb der GWAdriga Smart Energy CA (Test-PKI) erfolgt generell analog den Vorgaben für die Wirkumgebung, um das Testen unter funktionalen Echtbedingungen zu ermöglichen, ausgenommen sind die in diesem Anhang be-

	schriebenen Vereinfachungen gegenüber dem Wirkbetrieb.
C.2.2 Test-PKI …Sub-CA Anforderungen - Identifizierung und Authentifizierung	GWAdriga Smart Energy CA (Test-PKI) hat sich bei der Root der Test-PKI mit Verwendung der zugehörigen Formulare auf der Web-Seite der Root registrieren lassen.
C.2.3 Test-PKI …Sub-CA Anforderungen - Verzeichnisdienste	GWAdriga Smart Energy CA (Test-PKI) veröffentlicht die von ihr ausgestellten Zertifikate in einem Verzeichnis mit dem DN der Form 'dc=Certificates, dc=SM-Test-PKI-DE'. Informationen zum Testbetrieb inkl. dem Verzeichnisdienst können der Webseite: https://www.gwadriga.de/pki/test-pki/ entnommen werden. Der Zugriff auf den Verzeichnisdienst erfolgt analog zum Wirkbetrieb durch Einschränkung auf die Teilnehmer der SM-Test-PKI.
C.2.4 Test-PKI …Sub-CA Anforderungen - Technische Sicherheitsanforderungen	Auch wenn nicht zwingend erforderlich: Beim Betrieb der GWAdriga Smart Energy CA Testumgebung werden die Vorgaben zum 4-Augen-Prinzip weitestgehend und zur Speicherung der Schlüssel auf einem HSM stets eingehalten.
C.2.5 Test-PKI …Sub-CA Anforderungen - Überprüfung und andere Bewertungen	Die GWAdriga Smart Energy CA Testumgebung wird für die geforderten Funktionalitätstests eingesetzt, vgl. Abschnitt 8.1.1.
C.2.6 Test-PKI …Sub-CA Anforderungen - Namensschema	In der Testumgebung wird bis auf die nachfolgende Abweichung das Namensschema der Wirkumgebung, vgl. Abschnitt eingesetzt: im DN wird der Attributtyp „organisation“ mit „SM-Test-PKI-DE“ statt mit „SM-PKI-DE“ belegt.

C.2.6 Test-PKI …Sub-CA Anforderungen -Archivierung	Die Archivierung erfolgt in der Testumgebung analog zur Wirkumgebung.