

# Inhaltsverzeichnis

<b>1. EINLEITUNG .....</b>	<b>4</b>
1.1. Überblick .....	4
1.2. Name und Identifizierung des Dokumentes.....	4
1.3. PKI-Teilnehmer .....	4
1.4. Verwendung von Zertifikaten .....	4
1.5. Administration und Pflege der GÖRLITZ PKI Policy.....	4
<b>2. VERANTWORTLICHKEIT FÜR VERÖFFENTLICHUNG UND VERZEICHNISSE.....</b>	<b>5</b>
2.1. Verzeichnisse .....	5
2.2. Veröffentlichung von Informationen zur Zertifikatserstellung.....	5
2.3. Zeitpunkt und Häufigkeit der Veröffentlichungen.....	5
2.4. Zugriffskontrollen auf Verzeichnisse .....	5
<b>3. IDENTIFIZIERUNG UND AUTHENTIFIZIERUNG.....</b>	<b>6</b>
3.1. Regeln für die Namensgebung .....	6
3.2. Initiale Überprüfung zur Teilnahme .....	6
3.2.1. Authentifizierung von Organisationszugehörigkeiten .....	6
3.2.2. Aktualisierung der Zertifizierungs- / Registrierungsinformationen der Teilnehmer .....	6
3.3. Anträge auf Schlüsselerneuerung (Routinemäßiger Folgeantrag).....	6
3.4. Anträge auf Schlüsselerneuerung (nicht routinemäßiger Folgeantrag).....	6
3.5. Anträge zur Sperrung .....	6
3.6. Anträge zur Suspendierung .....	7
<b>4. BETRIEBSANFORDERUNGEN FÜR DEN ZERTIFIKATSLEBENSZYKLUS.....</b>	<b>8</b>
4.1. Zertifikatsantrag .....	8
4.2. Verarbeitung von initialen Zertifikatsanträgen .....	8
4.2.1. Fristen für die Bearbeitung von Zertifikatsanträgen .....	8
4.3. Annahme von Zertifikaten.....	9
4.4. Verwendung von Schlüsselpaar und Zertifikat .....	9
4.5. Zertifikatserneuerung .....	9
4.6. Zertifizierung nach Schlüsselerneuerung.....	9
4.7. Änderungen am Zertifikat.....	9
4.8. Sperrung und Suspendierung von Zertifikaten.....	10
4.8.1. Sperrung und Suspendierung von SMGW-Wirkzertifikaten .....	10
4.9. Service zur Statusabfrage von Zertifikaten .....	10
4.10. Beendigung der Teilnahme.....	10
<b>5. ORGANISATORISCHE, BETRIEBLICHE UND PHYSIKALISCHE SICHERHEITSANFORDERUNGEN .....</b>	<b>11</b>
5.1. Generelle Sicherheitsanforderungen.....	11
5.2. Erweiterte Sicherheitsanforderungen.....	11
5.2.1. Schlüsselwechsel einer Zertifizierungsstelle .....	11
5.3. Beendigung der Teilnahme der Sub-CA.....	11
5.4. Notfall-Management.....	12

<b>6.</b>	<b>TECHNISCHE SICHERHEITSANFORDERUNGEN</b>	<b>13</b>
6.1.	Erzeugung und Installation von Schlüsselpaaren	13
6.1.1.	Lieferung öffentlicher Zertifikate	13
6.1.2.	Schlüssellängen und kryptografische Algorithmen	13
6.1.3.	Festlegung der Parameter der Schlüssel und Qualitätskontrolle	13
6.2.	Anforderungen an kryptographische Module	13
6.3.	Andere Aspekte des Managements von Schlüsselpaaren	13
6.4.	Aktivierungsdaten	14
6.5.	Sicherheitsanforderungen für die Rechneranlagen	14
6.6.	Validierungsmodell	14
<b>7.</b>	<b>PROFILE FÜR ZERTIFIKATE UND SPERRLISTEN</b>	<b>15</b>
7.1.	Profile für Zertifikate und Zertifikatsrequests	15
7.2.	Profile für Sperrlisten	15
7.3.	Profile für OCSP Dienste	15
<b>8.</b>	<b>ÜBERPRÜFUNG UND ANDERE BEWERTUNGEN</b>	<b>16</b>
8.1.	Inhalte, Häufigkeit und Methodik	16
8.1.1.	Testbetrieb	16
8.1.2.	Beantragung Teilnahme an SM-PKI	16
8.1.3.	Wirkbetrieb	16
8.2.	Reaktionen auf identifizierte Vorfälle	16
<b>9.</b>	<b>SONSTIGE FINANZIELLE UND RECHTLICHE REGELUNGEN</b>	<b>17</b>
9.1.	Preise	17
9.2.	Finanzielle Zuständigkeiten	17
<b>10.</b>	<b>REFERENZDOKUMENTE</b>	<b>18</b>

## Inhalt

Bezeichnung	Certificate Policy (CP) der GÖRLITZ AG
Version	1.2
OID	1.3.6.1.4.1.43336.1.1 Test-PKI 1.3.6.1.4.1.43336.1.2 Wirk-PKI
Datum	19.11.2018
Zweck und Anwendungsbereich	Rahmenbedingungen der GÖRLITZ Sub-CA. Informationen und Anforderungen für Nutzer und Teilnehmer.
Verantwortlich	GÖRLITZ AG August-Thyssen Str. 32 56070 Koblenz
Ansprechpartner	<b>Timo Holtkamp</b> Timo.Holtkamp@goerlitz.com 0261 / 9285 0
E-Mail	caoperator@goerlitz.com
Webseite	<a href="https://www.goerlitz.com/sub-ca">https://www.goerlitz.com/sub-ca</a>

## **1. Einleitung**

Dieses Dokument orientiert sich an der Certificate Policy der Smart Metering PKI des Bundesamt für Sicherheit in der Informationstechnik [CP der SM-PKI]. Daher sind die Inhalte und Gliederung aus diesem Dokument abgeleitet und es wird auf dieses Referenzdokument verwiesen (Version 1.1.1; 09.08.2017).

### **1.1. Überblick**

Dieses Dokument richtet sich an alle Interessierten und Teilnehmer der Sub-CA der GÖRLITZ AG. In diesem Dokument werden alle relevanten Rahmenbedingungen und Anforderungen zur Nutzung dokumentiert, weiterhin werden Betriebsrelevante Informationen für Nutzer zusammengefasst und aufbereitet.

### **1.2. Name und Identifizierung des Dokumentes**

Bei diesem Dokument handelt es sich um die Certificate Policy (CP) der GÖRLITZ AG. Die genauen Angaben zur Identifikation dieses Dokumentes befinden sich am Anfang des Dokumentes.

Die jeweils gültige Fassung ist auf den Interseite der GÖRLITZ AG zu finden:  
<https://www.goerlitz.com/sub-ca>

### **1.3. PKI-Teilnehmer**

Alle Teilnehmer der PKI der GÖRLITZ AG verpflichten sich zur Einhaltung dieses Dokumentes. Registrierte Teilnehmer werden aktiv mittels verschlüsselter E-Mail über Änderungen informiert. Teilnehmer müssen den Erhalt und die Einhaltung neuer Versionen dieses Dokumentes bestätigen, wird eine Version nicht bestätigt oder der Teilnehmer verstößt gegen Regelungen in diesem Dokument so führt dies zur Deaktivierung des Teilnehmers.

Das entsprechende Kapitel der [CP der SM-PKI] ist gültig und anzuwenden.

### **1.4. Verwendung von Zertifikaten**

Die Verwendung von Zertifikaten wird aus den Vorgaben der [CP der SM-PKI] übernommen. Die dort getroffenen Festlegungen haben ebenfalls Gültigkeit für die PKI der GÖRLITZ AG.

### **1.5. Administration und Pflege der GÖRLITZ PKI Policy**

Die für dieses Dokument verantwortliche Organisation ist die GÖRLITZ AG. Kontaktdaten, Adresse und relevante Angaben sind zu Beginn dieses Dokumentes zu finden.

## 2. Verantwortlichkeit für Veröffentlichung und Verzeichnisse

### 2.1. Verzeichnisse

Ausgestellte und noch gültige Zertifikate der Görlitz Sub-CA werden in einem Lightweight Directory Access Protocol Verzeichnis (LDAP-Verzeichnis) geführt. Hierzu wurden zwei redundante LDAP-Server über einen LoadBlancer Cluster installiert. Das LDAP-Verzeichnis für die Test-PKI ist unter den folgenden Namen zu erreichen:

- [sub-ca-test.rzgoerlitz.com](http://sub-ca-test.rzgoerlitz.com)
- [ldap-sub-ca-test.rzgoerlitz.com](http://ldap-sub-ca-test.rzgoerlitz.com)

Weiterhin wird unter [ldap-sub-ca-test.rzgoerlitz.com](http://ldap-sub-ca-test.rzgoerlitz.com) die tagesaktuelle Sperrliste veröffentlicht, in der alle gesperrten Zertifikate der Görlitz SubCA während ihres Gültigkeitszeitraums aufgeführt sind.

### 2.2. Veröffentlichung von Informationen zur Zertifikatserstellung

Alle laut [CP der SM-PKI] relevanten Informationen zur Zertifikatserstellung finden Sie auf der oben angegebenen Internetseite der GÖRLITZ AG.

### 2.3. Zeitpunkt und Häufigkeit der Veröffentlichungen

Die Zeitpunkte der Veröffentlichungen richten sich nach den Vorgaben der [CP der SM-PKI] und erfolgen in der Regel mittels oben beschriebenem LDAP-Verzeichnis.

### 2.4. Zugriffskontrollen auf Verzeichnisse

Gemäß den Vorgaben des BSI erhalten nur berechtigte und teilnehmende Organisationen Zugriff auf den Verzeichnisdienst. Dieser Zugriff ist ausschließlich mittels zertifikatsbasierter Authentisierung möglich.

Der Massenabruf von Zertifikaten ist dabei ausgeschlossen und technisch unterbunden, es wird nur eine begrenzte Anzahl an Suchergebnissen geliefert.

Lediglich der lesende Zugriff auf die Sperrlisten erfolgt ohne Authentifikation.

### **3. Identifizierung und Authentifizierung**

Dieses Kapitel beschreibt die durchzuführenden Prozeduren, um die Identität und die Berechtigung eines Antragstellers vor dem Ausstellen eines Zertifikats festzustellen.

#### **3.1. Regeln für die Namensgebung**

Das entsprechende Kapitel der [CP der SM-PKI] ist gültig und anzuwenden.

#### **3.2. Initiale Überprüfung zur Teilnahme**

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

Bestandteil dieser Prozeduren sind auch die Prüfungen nach den Anforderungen aus Abschnitt 8.1 der [CP der SM-PKI].

##### **3.2.1. Authentifizierung von Organisationszugehörigkeiten**

**Die folgenden Regelungen sind für alle Antragsteller zwingend zu beachten.**

Zur initialen Autorisierung muss das Unternehmen authentifiziert und mindestens zwei bevollmächtigte Vertreter des Betreibers persönlich bei dem Betreiber der Root-CA identifiziert und authentifiziert werden. Dazu ist das entsprechende Formular auf der oben genannten Webseite zu nutzen. Alle relevanten Angaben und Anweisungen sind diesem Formular zu entnehmen. Ein Zertifikatsrequest darf nicht von einer Einzelperson (natürliche Person), sondern muss von einer Organisation (juristische Person) gestellt werden. Alle eingereichten Anträge werden von der GÖRLITZ AG auf Korrektheit geprüft, sollten dabei Fragen auftreten so ist die GÖRLITZ AG vom Antragsteller bei der Feststellung der Richtigkeit zu unterstützen.

##### **3.2.2. Aktualisierung der Zertifizierungs- / Registrierungsinformationen der Teilnehmer**

Sind zur Anmeldung Zertifizierungen notwendig, so ist mit Abgabe der Anmeldung über die Ergebnisse der Auditierung zu informieren und soweit ausgestellt auch das entsprechende Zertifikat zur Verfügung zu stellen. Sollte der Teilnehmer die Zertifizierung nicht mehr erhalten, so wird das Zertifikat / die Zertifikate aus der PKI gesperrt.

Jeder Teilnehmer muss unverzüglich mitteilen, falls sich Änderungen bzgl. seiner Registrierungsdaten ergeben. Ergänzend wird der Teilnehmer eine jährliche Abfrage der zu seinen Registrierungsdaten von der GÖRLITZ AG erhalten, diese ist innerhalb von vier Wochen zu beantworten, ansonsten kann dies ebenfalls zur Sperrung des Zertifikats / der Zertifikate führen.

#### **3.3. Anträge auf Schlüsselerneuerung (Routinemäßiger Folgeantrag)**

Zur Beantragung von Schlüsselerneuerungen gelten die entsprechenden Vorgaben des Kapitels 3.3 der [CP der SM-PKI]. Routinemäßige Folgeanträge müssen spätestens **vier Wochen vor Ablauf** des vorherigen Zertifikats gestellt werden.

#### **3.4. Anträge auf Schlüsselerneuerung (nicht routinemäßiger Folgeantrag)**

Zur Beantragung von Schlüsselerneuerungen mittels nicht routinemäßigem Folgeantrag gelten die entsprechenden Vorgaben des Kapitels 3.4 der [CP der SM-PKI]

#### **3.5. Anträge zur Sperrung**

Das entsprechende Kapitel (3.5) der [CP der SM-PKI] ist gültig und anzuwenden.

**3.6. Anträge zur Suspendierung**

Das entsprechende Kapitel (3.6) der [CP der SM-PKI] ist gültig und anzuwenden.

## 4. Betriebsanforderungen für den Zertifikatslebenszyklus

In diesem Kapitel werden die Prozeduren und Verantwortlichkeiten für den Lebenszyklus von Zertifikaten definiert. Dies umfasst insbesondere folgende Bereiche:

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

Innerhalb der Prozesse des Zertifikatslebenszyklus muss die relevante personenbezogene Kommunikation verschlüsselt und signiert erfolgen, wofür individuelle/personenbezogene Zertifikate einzusetzen sind. Für alle beteiligten Personen wird der Besitz von individuellen/persönlichen CS/MIME(ASP)-Zertifikaten vorausgesetzt.

### 4.1. Zertifikatsantrag

Ein Zertifikatsrequest darf ausschließlich von einer Organisation gestellt werden. Befugte Organisationen sind GWA, GWH, EMT, die sich gemäß Abschnitt "Initiale Überprüfung zur Teilnahme" identifiziert haben. Der Zertifikatsrequest muss als Folgeantrag (siehe oben) unter Nutzung der vorhandenen Zertifikate gestellt werden. Für die Bearbeitung eines Zertifikatsantrags ist die Registration Authority (RA) der GÖRLITZ AG verantwortlich.

Die ausgegebenen Zertifikate (ENC, SIG, TLS) werden im Format ".pem" (Base64) an den Antragsteller übergeben.

### 4.2. Verarbeitung von initialen Zertifikatsanträgen

Der Zertifikatsnehmer übergibt durch seinen benannten Ansprechpartner, die Unterlagen und Nachweise für die initiale Zertifikatsbeantragung an die RA der GÖRLITZ AG. Die RA-Mitarbeiter prüfen die eingereichten Dokumente / Nachweise. Sollten die Unterlagen / Nachweise nicht vollständig oder fehlerhaft sein, informieren diese den Antragsteller bzw. Ansprechpartner des Zertifikatsnehmers und fordern ihn zur Nachlieferung auf. Sollte einer der benannten und identifizierten Mitarbeiter ausscheiden, muss sich mindestens ein neuer Vertreter im Rahmen eines persönlichen Termins identifizieren lassen. Die Benennung des neuen Vertreters bzw. der neuen Vertreter sowie die Information über das Ausscheiden des bisherigen Vertreters muss von einem der benannten Ansprechpartner des Teilnehmers bestätigt werden.

Für die SMGWs werden keine direkten Ansprechpartner benannt, da diese Aufgaben von den GWAs übernommen werden. Bei allen Prozessen zur Beantragung, Ausgabe und Verwaltung der Zertifikate muss hinsichtlich der eingesetzten Kryptografie immer die aktuelle Version der [TR-03116-3] bei der Nutzung des Webservices bzw. sollte die [TR-03116-4] zu der Absicherung der E-Mail-Kommunikation via S/MIME berücksichtigt werden.

Die vorliegenden bzw. nachgelieferten Unterlagen / Nachweise werden von den RA-Mitarbeitern gegen die Vorgaben aus dieser Richtlinie geprüft. Im Positivfall wird der Zertifikatsantrag formell freigegeben und der benannte Ansprechpartner per signierter E-Mail darüber informiert. Durch die RA werden im Rahmen der Prüfung auch der vorliegende Zertifikatsrequest für die initialen Zertifikate formal und die Übereinstimmung der gedruckten Hashwerte in den Unterlagen mit denen der Zertifikatsrequests überprüft.

Im Negativfall wird der Zertifikatsantrag formell abgelehnt und der benannte Ansprechpartner per signierter E-Mail über die Ablehnung (incl. entsprechender Begründung) informiert. Der Beantragungsprozess ist mit diesem Schritt beendet und muss durch den Zertifikatsnehmer ggf. neu initiiert werden.

#### 4.2.1. Fristen für die Bearbeitung von Zertifikatsanträgen

Die in den nachfolgenden Abschnitten aufgeführten Zeiten sind als Richtwerte für die einzelnen Arbeitsschritte bei der initialen Ausgabe von Zertifikaten anzusehen. Die Ausgabe von Folgezertifikaten bzw. Ersatzzertifikaten nach der Sperrung von Zertifikaten können von den angegebenen Werten



situationsabhängig abweichen. Die Auflistung orientiert sich am entsprechenden Kapitel der [CP der SM-PKI].

Arbeitsschritt	Beschreibung	Zeitraumen
1	Start des Beantragungsprozess durch den Antragsteller	
2	Kontaktaufnahme zur Terminvereinbarung durch die GÖRLITZ AG	3 Arbeitstage ab Antragseingang
3	Übergabe der Dokumente / Nachweise im Rahmen eines persönlichen Termins	Termin innerhalb 3 Arbeitstagen wird ermöglicht. Maximal 6 Wochen nach Antragseingang.
4	Vorprüfung der Unterlagen und Rückmeldung an den Antragsteller	5 Arbeitstage
5 (optional)	Nachlieferungsfrist für den Antragsteller	15 Arbeitstage
6	Prüfung der Unterlagen inkl. Rückmeldung	5 Arbeitstage
7	Zertifikatsausstellung	2 Arbeitstage

Für die Einhaltung der hier definierten Zeiträume ist eine fristgerechte und fachliche Lieferung / Mitwirkung des Antragstellers Voraussetzung. Sollten sich die Lieferungen / Zuarbeiten des Antragstellers verzögern, können sich die Zeiten verlängern.

Die Ausgabe von Endnutzer-Zertifikaten erfolgt über die Web-Service-Schnittstelle. Ein Versand von Endnutzer-Zertifikaten per E-Mail ist nur bei der initialen Ausstellung von Zertifikaten vorgesehen, in diesem Fall erhält der Ansprechpartner des Antragsstellers nach der Ausstellung eines initialen Zertifikats eine entsprechende E-Mail.

#### 4.3. Annahme von Zertifikaten

Bei den Endnutzer-Zertifikaten muss der Ansprechpartner des Antragstellers nach Erhalt die Angaben im Zertifikat auf Korrektheit und Vollständigkeit prüfen. Um ein Zertifikat zurückzuweisen, muss der Ansprechpartner eine Nachricht an die RA der GÖRLITZ AG schicken. In einer solchen Nachricht ist der Grund für die Verweigerung der Annahme anzugeben. Bei fehlerhaften Zertifikaten sind, soweit möglich, die fehlerhaften bzw. unvollständigen Einträge zu benennen. Bei einem SMGW kann diese Prüfung durch den GWH oder den GWA automatisiert z.B. bei dem Erhalt oder der Einbringung der Zertifikate erfolgen.

Bei Fehlermeldungen hat der Kontakt über den CA-Operator zu erfolgen.

Alle ausgestellten Zertifikate werden direkt nach der Ausstellung im Verzeichnisdienst veröffentlicht.

#### 4.4. Verwendung von Schlüsselpaar und Zertifikat

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

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

#### 4.5. Zertifikatserneuerung

Zertifikatserneuerung bedeutet das Ausstellen eines neuen Zertifikats für einen öffentlichen Schlüssel, der bereits zertifiziert wurde. Zertifikatserneuerungen sind in der [CP der SM-PKI] untersagt und werden daher nicht durchgeführt.

#### 4.6. Zertifizierung nach Schlüsselerneuerung

Das entsprechende Kapitel (4.6) der [CP der SM-PKI] ist gültig und anzuwenden.

#### 4.7. Änderungen am Zertifikat

Änderungen an den Zertifikatsinhalten, abgesehen vom Schlüsselmaterial und den Seriennummern im SubjectDN, sind nicht vorgesehen. Sollte sich Änderungsbedarf ergeben, muss ein neues initiales Zertifikat gemäß den Vorgaben dieses Dokumentes beauftragt und das alte Zertifikat gesperrt werden.

#### **4.8. Sperrung und Suspendierung von Zertifikaten**

Die Initiierung der Sperrung eines Zertifikats kann durch den Zertifikatsnehmer mittels entsprechender Anfrage bei der GÖRLITZ AG eingeleitet werden. Dies geschieht über den Sperrantrag welcher auf der Homepage der GÖRLITZ AG heruntergeladen werden kann. Hierzu ist auch das Sperrpasswort notwendig. Die Sperrung/Suspendierung eines SMGWs erfolgt über die GWA-Software automatisiert. Alle Zertifikate werden über die bereitgestellten Schnittstellen/Prozesse gesperrt. Eine Sperrung kann nicht zurückgenommen werden. Eine Ausnahme stellt der Spezialfall Suspendierung dar (siehe unten). Alle Sperrungen werden unverzüglich geprüft, entsprechend umgesetzt und in die neue Sperrlisten aufgenommen. Die Veröffentlichung erfolgt gemäß den Vorgaben der [TR-03109-4]. Ist dem Sperrenden der genaue Zeitpunkt für den Eintritt des Sperrgrundes bekannt, so ist dieser bei der Sperrung anzugeben, ansonsten erfolgt der Eintrag in die Sperrliste ohne diesen Parameter. Alle Teilnehmer verpflichten sich gemäß den Vorgaben aus [TR-03109-4] immer die aktuelle Sperrliste zu verwenden. In besonderen Fällen (Erstinbetriebnahme oder auf Aufforderung) müssen neben den regelmäßigen Aktualisierungen auch neue Sperrlisten abgefragt werden.

##### **4.8.1. Sperrung und Suspendierung von SMGW-Wirkzertifikaten**

Das entsprechende Kapitel (4.8.2) der [CP der SM-PKI] ist gültig und anzuwenden. Alle Teilnehmer müssen gemäß den Vorgaben der [CP der SM-PKI] immer die aktuelle Sperrliste verwenden.

#### **4.9. Service zur Statusabfrage von Zertifikaten**

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

#### **4.10. Beendigung der Teilnahme**

Die Beendigung der Teilnahme eines Zertifikatsnehmers kann durch diesen selbst oder die Sub-CA der GÖRLITZ AG eingeleitet werden.

Die Beendigung gliedert sich in drei Schritte:

1. Information des Zertifikatsnehmers.
2. Aufforderung zum Austausch der von der Sperrung betroffenen Zertifikate, so dass ein kontinuierlicher Betrieb gewährleistet werden kann (hierzu muss eine entsprechende Abstimmung zwischen den Beteiligten bezüglich des dazu notwendigen Zeitrahmens erfolgen. Ausgenommen hiervon ist die Sperrung von Zertifikaten aufgrund von Gefahren für den sicheren Betrieb der SM-PKI).
3. Sperrung aller Zertifikate des Zertifikatsnehmers sowie entsprechende Kennzeichnung der bekannten CS/MIME(ASP) Zertifikate der benannten Ansprechpartner zum betroffenen Zertifikatsnehmer, so dass die Nutzung der Zertifikate für eine vertrauliche und authentische Kommunikation unterbunden wird.

Bei der Außerbetriebnahme eines SMGWs müssen die Zertifikate des SMGW gesperrt werden. Die Sperrung muss der zugehörigen CA über deren Webservice-Schnittstelle mitgeteilt werden (siehe [TR-03109-4]).

## 5. Organisatorische, betriebliche und physikalische Sicherheitsanforderungen

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

### 5.1. Generelle Sicherheitsanforderungen

Das entsprechende Kapitel (5.1) der [CP der SM-PKI] ist gültig und anzuwenden.

### 5.2. Erweiterte Sicherheitsanforderungen

Die erweiterten Sicherheitsanforderungen werden in der [CP der SM-PKI] in den Unterkapiteln des Kapitel 5.2 beschrieben. Ohne weitere Ergänzungen oder Einschränkungen, gelten die folgenden Kapitel:

- 5.2.1 Betriebsumgebung und Betriebsabläufe
- 5.2.2 Verfahrensanweisungen
- 5.2.3 Personal
- 5.2.4 Monitoring
- 5.2.5 Archivierung von Aufzeichnungen
- 5.2.6 Schlüsselwechsel einer Zertifizierungsstelle
- 5.2.8 Aufbewahrung der privaten Schlüssel
- 5.2.9 Behandlung von Vorfällen und Kompromittierung
- 5.2.10 Meldepflichten

Zusätzlich sind für für einen GWA alle Vorgaben der [TR-03109-6] einzuhalten. Weiterhin werden folgende Festlegungen zu erweiterten Sicherheitsanforderungen getroffen.

#### 5.2.1. Schlüsselwechsel einer Zertifizierungsstelle

Wenn eine Sub-CA aufgelöst wird, müssen alle von ihr ausgestellten Zertifikate gesperrt werden. Daher definiert die GÖRLITZ AG folgendes:

- Übertragung der Aufgaben und Verpflichtungen: Im Falle der Auflösung erhält die GÖRLITZ AG alle relevanten Aufgaben und Verpflichtungen für eine Übergangszeit aufrecht. Bei einer endgültigen Auflösung verpflichtet sich die GÖRLITZ AG zur Suche einer Nachfolgeorganisation die entsprechende Dienste übernehmen kann. Dies umfasst ebenfalls die Bereitstellung von Sperrinformationen für die Restlaufzeit der ausgegebenen Zertifikate.
- Informationspflicht: Im Falle ihrer Auflösung informiert die GÖRLITZ AG alle beteiligten Teilnehmer sowie weitere Organisationen, mit denen Vereinbarungen bestehen, vor der Kündigung der Dienstleistung rechtzeitig.
- Zerstörung von Schlüssel- und Zertifikatsinformationen: Nach Einstellung der Tätigkeiten werden alle privaten Schlüssel einschließlich Zertifikatsinformationen und zugehörige Kundendaten zerstört bzw. ausgegebene Zertifikate widerrufen oder gesperrt.

### 5.3. Beendigung der Teilnahme der Sub-CA

Sollte die Firma GÖRLITZ AG die Teilnahme an der Sub-CA beenden, werden die folgenden Aktionen ausgeführt:

- Alle Aufgaben und Verpflichtungen werden aufrechterhalten solange die Laufzeit der Sub-CA Zertifikate ihre Gültigkeit besitzen. Dies umfasst die Bereitstellung von Sperrinformationen für die Restlaufzeit der ausgegebenen Zertifikate.

- Alle Zertifikatsnehmer der GÖRLITZ Sub-CA, sowie alle weiteren Organisationen mit denen Vereinbarungen bzgl. Sub-CA bestehen werden über die Beendigung rechtzeitig informiert.
- Mit der Beendigung und Einstellung der Tätigkeiten werden alle privaten Schlüssel einschließlich der Zertifikatsinformationen und zugehörigen Kundendaten zerstört.

#### **5.4. Notfall-Management**

Das entsprechende Kapitel (5.3) der [CP der SM-PKI] ist gültig und anzuwenden.

## 6. Technische Sicherheitsanforderungen

Jeder Zertifikatsnehmer muss sein eigenes Schlüsselpaar generieren. Die technischen Anforderungen an die Erzeugung, Verwendung und Gültigkeit von Schlüsseln werden in [TR-03109-4] beschrieben.

### 6.1. Erzeugung und Installation von Schlüsselpaaren

Die GÖRLITZ AG stellt als Sub-CA die folgenden Anforderungen sicher:

- Generierung im Vier-Augen-Prinzip: Das Schlüsselpaar wird während der Schlüsselzeremonie im Vier-Augen-Prinzip unter Teilnahme des für den Schlüssel verantwortlichen Mitarbeiters generiert.
- Generierung eines Schlüsselpaars: Die zur Schlüsselgenerierung eingesetzten Kryptographiemodule sind entsprechend den in Kapitel "Anforderungen an kryptographische Module" angegebenen Schutzprofilen zertifiziert.
- Der technische Zugriff auf die Schlüssel in den Kryptografiemodulen aller Zertifikatsnehmer ist durch ein Geheimnis geschützt, welches ausschließlich die jeweiligen Operatoren kennen. Der Zugriff auf das Kryptografiemodul, insbesondere zur Schlüsselerzeugung, ist auf ein Minimum an Operatoren beschränkt.

Antragstellende GWA und GWH müssen diese Anforderungen ebenfalls sicherstellen. Ein EMT muss nur die Anforderung "Generierung eines Schlüsselpaars" umsetzen.

#### 6.1.1. Lieferung öffentlicher Zertifikate

Alle öffentlichen Zertifikate werden in den entsprechenden LDAP-Verzeichnissen abgelegt und sind somit für alle Teilnehmer zugänglich.

#### 6.1.2. Schlüssellängen und kryptografische Algorithmen

Schlüssellängen und kryptografische Algorithmen der Schlüsselpaare entsprechen den Anforderungen der [TR-03116-3].

#### 6.1.3. Festlegung der Parameter der Schlüssel und Qualitätskontrolle

Das entsprechende Kapitel (6.1.5) der [CP der SM-PKI] ist gültig und anzuwenden.

### 6.2. Anforderungen an kryptographische Module

Die GÖRLITZ AG setzt gemäß den Anforderungen der [CP der SM-PKI] Kapitel 6.2 entsprechende Kryptografiemodule ein. Somit auch die dort geforderte Einhaltung der Anforderungen der [KeyLifecSec] in Security Level 2 an den Lebenszyklus und die Einsatzumgebung. Die Anforderungen dieses Kapitels gelten entsprechend für dieses Dokument. Daher gelten die folgenden Unterkapitel der [CP der SM-PKI] Kapitel 6.2 für dieses Dokument:

- 6.2.1 Mehrpersonen-Zugriffssicherung zu privaten Schlüsseln
- 6.2.2 Ablage privater Schlüssel
- 6.2.3 Backup privater Schlüssel
- 6.2.4 Archivierung privater Schlüssel
- 6.2.5 Transfer privater Schlüssel in oder aus kryptografischen Modulen
- 6.2.6 Speicherung privater Schlüssel in kryptografischen Modulen
- 6.2.7 Aktivierung privater Schlüssel
- 6.2.8 Deaktivierung privater Schlüssel
- 6.2.9 Zerstörung privater Schlüssel
- 6.2.10 Beurteilung kryptografischer Module

Die Einhaltung dieser Vorgaben wird mittels interner Vorgaben sichergestellt und durch interne und externe Audits überwacht.

### 6.3. Andere Aspekte des Managements von Schlüsselpaaren

Die Zertifikate eines Teilnehmers werden inklusive der Statusdaten sicher gespeichert und abgelegt.

In den folgenden Tabellen sind die Laufzeiten von Schlüssel und Zertifikaten gemäß [CP der SM-PKI] und [TR03109-4] zusammengefasst. Diese gelten verbindlich für alle Teilnehmer.

Zertifikat	Gültigkeitszeit
Root-CRL-Signer-Zertifikat	4 Jahre
Root-TLS-Signer-Zertifikat	4 Jahre
Sub-CA-Zertifikat	5 Jahre
TLS-Zertifikate der Root-CA und der Sub-CA	2 Jahre
GWA-Zertifikate (TLS/Sign/Enc)	3 Jahre
Andere Endnutzerzertifikate (TLS/Sign/Enc)	2 Jahre

Unabhängig vom Gültigkeitszeitraum müssen die folgenden Zertifikate gemäß den Vorgaben der [CP der SM-PKI] spätestens in dem hierzu angegebenen Intervall gewechselt werden.

Instanz	Zertifikat	Intervall
Root-CA	C(Root)	Alle 3 Jahre
	Ccrl-s(Root)	Alle 3 Jahre
	Ctls-s(Root)	Alle 2 Jahre
Sub-CA	C(Sub-CA)	Alle 2 Jahre

#### 6.4. Aktivierungsdaten

Die Aktivierungsdaten der Kryptografiemodule werden entsprechend den Anforderungen sicher Aufbewahrt.

#### 6.5. Sicherheitsanforderungen für die Rechneranlagen

Das entsprechende Kapitel (6.1.5) der [CP der SM-PKI] ist gültig und anzuwenden. Für alle verwendeten Anlagen sind die entsprechenden Anforderungen umgesetzt.

#### 6.6. Validierungsmodell

Die Anforderungen an die Zertifikatsvalidierung werden in [TR-03109-4] spezifiziert und durch die GÖRLITZ AG umgesetzt.

## **7. Profile für Zertifikate und Sperrlisten**

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

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

### **7.1. Profile für Zertifikate und Zertifikatsrequests**

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

### **7.2. Profile für Sperrlisten**

Die Anforderungen an die Sperrlisten (Certification Revocation List, CRL)-Profile werden in der der [TR-03109-4] definiert und sind durch die GÖRLITZ AG erfüllt.

### **7.3. Profile für OCSP Dienste**

Es werden keine OCSP-Dienste eingesetzt.

## **8. Überprüfung und andere Bewertungen**

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

### **8.1. Inhalte, Häufigkeit und Methodik**

#### **8.1.1. Testbetrieb**

Die GÖRLITZ AG stellt Testumgebungen zur Verfügung, welche die Antragsteller zum Test der Funktionalitäten ihrer PKI-Infrastruktur und -Prozesse durchlaufen müssen, bevor diese Teilnehmer der PKI werden.

#### **8.1.2. Beantragung Teilnahme an SM-PKI**

Zur Beantragung der Teilnahme an der PKI müssen die Anforderungen der [CP der SM-PKI] Kapitel 8.1.2 (Tabelle 15) erfüllt werden.

#### **8.1.3. Wirkbetrieb**

Die vorausgesetzten Nachweise/Zertifizierungen müssen im Wirkbetrieb auf Basis des jeweiligen Prüf-/Zertifizierungsschemas aufrechterhalten werden. Sollte eine Zertifizierung nicht mehr gültig sein, so ist dies der GÖRLITZ AG umgehend mitzuteilen.

### **8.2. Reaktionen auf identifizierte Vorfälle**

Die Reaktionen auf identifizierte Vorfälle sind in Kapitel 5.2.10 Meldepflichten der [CP der SM-PKI] definiert.



## **9. Sonstige finanzielle und rechtliche Regelungen**

### **9.1. Preise**

Die Preise für CA-Dienstleistungen können bei der GÖRLITZ AG angefragt werden.

### **9.2. Finanzielle Zuständigkeiten**

Die GÖRLITZ AG als Betreiber der Sub-CA ist finanziell eigenständig und unabhängig.

## 10. Referenzdokumente

Referenz	Titel	Version
[CP der SM-PKI]	Certificate Policy der Smart Metering PKI	1.1.1 (09.08.2017)
[TR-03109-6]	Smart Meter Gateway Administration	1.0 (26.11.2015)
[TR-03109-4]	Smart Metering PKI - Public Key Infrastruktur für Smart Meter Gateways	1.2.1 (09.08.2017)
[KeyLifecSec]	Key Lifecycle Security Requirements	1.0.1 (29.11.2016)
[TR-03116-3]	Kryptographische Vorgaben für Projekte der Bundesregierung	23.04.2018