 Stadtwerke Saarbrücken	Certificate Policy SEN.CA	Version: 3.0
		Seite: 1/99
SWIT- 1961468859- 1355		Gültig ab: 01.12.2022
Status: Freigegeben	Klassifizierung: Öffentlich	Druckdatum: 01.12.2022

Eigentümer: 
www.co-met.info

co.met GmbH
Hohenzollernstraße 75
66117 Saarbrücken
www.co-met.info

Betreiber:  **Stadtwerke
Saarbrücken**

Stadtwerke Saarbrücken GmbH
Hohenzollernstraße 104-106
66117 Saarbrücken
www.sw-sb.de

Certificate Policy SEN.CA

Version	3.0
Geltungsbereich	ISMS-IT
Klassifizierung	Öffentlich
Dokumenteneigner	Klein Thomas
Verteiler	ISMS SEN, Kunden der SEN.CA
Dokumentenstatus	Freigegeben
Dokumententyp	Richtlinie (RL)
Autor	Schorr Christian
Gültig ab	01.12.2022
Ersetzt Dokument	SW-IT-A.10-RL-002.docx

 Stadtwerke Saarbrücken	Certificate Policy SEN.CA	Version: 3.0
		Seite: 2/99
SWIT- 1961468859- 1355		Gültig ab: 01.12.2022
Status: Freigegeben	Klassifizierung: Öffentlich	Druckdatum: 01.12.2022

Prüfung und Freigabe

Rolle	Name	Firma	Datum
QS	Klein Thomas	Stadtwerke Saarbrücken GmbH	01.12.2022
ISB	Knauth Julia	co.met GmbH	01.12.2022
Weitere Genehmiger 1	-	-	-
Weitere Genehmiger 2	-	-	-
Weitere Genehmiger 3	-	-	-
Weitere Genehmiger 4	-	-	-
Weitere Genehmiger 5	-	-	-

Dieses Dokument hat den elektronischen Freigabe-Prozess durchlaufen und ist ohne Unterschrift gültig.

 Stadtwerke Saarbrücken	Certificate Policy SEN.CA	Version: 3.0
		Seite: 3/99
SWIT- 1961468859- 1355		Gültig ab: 01.12.2022
Status: Freigegeben	Klassifizierung: Öffentlich	Druckdatum: 01.12.2022

Inhalt

1.	Einleitung	10
1.1.	Überblick.....	11
1.2.	Name und Identifizierung des Dokuments.....	12
1.3.	PKI-Teilnehmer	13
1.3.1.	Zertifizierungsstellen	14
1.3.2.	Registrierungsstellen.....	16
1.3.3.	Zertifikatsnehmer.....	18
1.3.4.	Zertifikatsnutzer	19
1.3.5.	Andere Teilnehmer.....	19
1.4.	Verwendung von Zertifikaten	20
1.4.1.	Erlaubte Verwendung von Zertifikaten.....	20
1.4.2.	Verbotene Verwendung von Zertifikaten	21
1.5.	Administration der SEN.CA CP.....	22
1.5.1.	Pflege der SEN.CA CP	22
1.5.2.	Zuständigkeit für das Dokument	22
1.5.3.	Ansprechpartner / Kontaktpersonen	22
1.5.4.	Zuständiger für die Anerkennung eines CPS	23
1.5.5.	SEN.CA CPS-Aufnahmeverfahren	23
2.	Verantwortlichkeit für Veröffentlichungen und Verzeichnisse	23
2.1.	Verzeichnisse	23
2.2.	Veröffentlichung von Informationen zur Zertifikatserstellung	23
2.3.	Zeitpunkt und Häufigkeit der Veröffentlichungen	24
2.4.	Zugriffskontrollen auf Verzeichnisse.....	24
3.	Identifizierung und Authentifizierung	24
3.1.	Regeln für die Namensgebung	24
3.1.1.	Arten von Namen	24
3.1.2.	Notwendigkeit für aussagefähige Namen.....	25
3.1.3.	Anonymität oder Pseudonymität von Zertifikatsnehmern.....	25
3.1.4.	Eindeutigkeit von Namen	25
3.1.5.	Anerkennung, Authentifizierung und die Rolle von Markennamen.....	25
3.2.	Initiale Überprüfung zur Teilnahme an der PKI	26
3.2.1.	Methoden zur Überprüfung bzgl. Besitz des privaten Schlüssels.....	26

3.2.2. Authentifizierung von Organisationszugehörigkeiten	26
3.2.2.1. Sub-CA.....	26
3.2.2.2. EMT.....	26
3.2.2.3. GWA.....	28
3.2.2.4. GWH.....	29
3.2.2.5. SMGW.....	30
3.2.3. Anforderungen zur Identifizierung und Authentifizierung des Zertifikats-Antragstellers....	31
3.2.4. Ungeprüfte Angaben zum Zertifikatsnehmer.....	32
3.2.5. Prüfung der Berechtigung zur Antragsstellung.....	32
3.2.6. Kriterien für den Einsatz interoperierender Systeme / Einheiten	32
3.2.7. Aktualisierung / Anpassung der Zertifizierungsinformationen der Teilnehmer	32
3.2.8. Aktualisierung / Anpassung der Registrierungsinformationen der Teilnehmer.....	32
3.3. Identifizierung und Authentifizierung von Anträgen auf Schlüsselerneuerung (routinemäßiger Folgeantrag)	33
3.4. Identifizierung und Authentifizierung von Anträgen auf Schlüsselerneuerung (Nicht routinemäßiger Folgeantrag)	33
3.4.1. Allgemeines.....	33
3.4.2. Schlüsselerneuerung nach Sperrung	35
3.5. Identifizierung und Authentifizierung von Anträgen auf Sperrungen	35
3.5.1. Initiative des Zertifikatsinhabers.....	35
3.5.1.1. Verantwortlich für die Sperrung eines SMGW	36
3.5.1.2. Sperrung eines SMGW	37
3.5.2. Initiative des Betreibers der Certificate Authority	37
3.6. Identifizierung und Authentifizierung von Anträgen auf Suspendierung.....	38
4. Betriebsanforderungen für den Zertifikatslebenszyklus.....	38
4.1. Zertifikatsantrag.....	38
4.1.1. Wer kann einen Zertifikatsantrag stellen?	39
4.1.2. Beantragungsprozess und Zuständigkeiten	39
4.2. Verarbeitung von initialen Zertifikatsanträgen	39
4.2.1. Durchführung der Identifizierung und Authentifizierung	39
4.2.2. Annahme oder Ablehnung von initialen Zertifikatsanträgen.....	40
4.2.3. Fristen für die Bearbeitung von Zertifikatsanträgen	41
4.2.4. Ausgabe von Zertifikaten	42
4.2.5. Benachrichtigung des Zertifikatsnehmers über die Ausgabe des Zertifikats.....	43

4.3.	Annahme von Zertifikaten	43
4.3.1.	Veröffentlichung von Zertifikaten durch die CA	44
4.4.	Verwendung von Schlüsselpaar und Zertifikat	44
4.4.1.	Verwendung des privaten Schlüssels und des Zertifikats durch den Zertifikatsnehmer ...	44
4.4.2.	Verwendung des öffentlichen Schlüssels und des Zertifikats durch den Zertifikatsnutzer	44
4.5.	Zertifikatserneuerung	44
4.6.	Zertifizierung nach Schlüsselerneuerung	44
4.6.1.	Bedingungen der Zertifizierung nach Schlüsselerneuerungen	44
4.6.2.	Zulässige Antragsteller von Zertifikaten für Schlüsselerneuerungen	44
4.6.3.	Bearbeitung von Zertifikatsanträgen für Schlüsselerneuerungen	44
4.6.4.	Benachrichtigung des Zertifikatsnehmers über die Ausgabe eines Nachfolgezertifikats ..	45
4.6.5.	Verhalten für die Annahme von Zertifikaten für Schlüsselerneuerungen	45
4.6.6.	Veröffentlichung von Zertifikaten für Schlüsselerneuerungen durch die SEN.CA.....	45
4.6.7.	Benachrichtigung anderer PKI-Teilnehmer über die Ausgabe eines Nachfolgezertifikats	46
4.7.	Änderungen am Zertifikat.....	46
4.8.	Sperrung und Suspendierung von Zertifikaten	46
4.8.1.	Sperrung.....	46
4.8.2.	Sperrung und Suspendierung von SMGW-Zertifikaten	47
4.8.2.1.	Maximale Dauer einer Suspendierung	48
4.8.3.	Aktualisierung und Prüfzeiten bei Sperrung	48
4.9.	Service zur Statusabfrage von Zertifikaten.....	49
4.10.	Beendigung der Teilnahme	49
4.11.	Hinterlegung und Wiederherstellung von Schlüsseln.....	50
5.	Organisatorische, betriebliche und physikalische Sicherheitsanforderungen.....	51
5.1.	Generelle Sicherheitsanforderungen	51
5.1.1.	Erforderliche Zertifizierungen der PKI-Teilnehmer	51
5.1.2.	Anforderungen an die Zertifizierung gemäß [ISO/IEC 27001]	53
5.2.	Erweiterte Sicherheitsanforderungen	53
5.2.1.	Betriebsumgebung und Betriebsabläufe.....	53
5.2.2.	Verfahrensanweisungen	54
5.2.3.	Personal	55
5.2.4.	Monitoring.....	55
5.2.5.	Archivierung von Aufzeichnungen	56

5.2.6. Schlüsselwechsel einer Zertifizierungsstelle	57
5.2.7. Auflösen der Zertifizierungsstelle	57
5.2.8. Aufbewahrung der privaten Schlüssel	58
5.2.9. Behandlung von Vorfällen und Kompromittierung	58
5.2.10. Meldepflichten	59
5.3. Notfall-Management	59
6. Technische Sicherheitsanforderungen	60
6.1. Erzeugung und Installation von Schlüsselpaaren	60
6.1.1. Generierung von Schlüsselpaaren für die Zertifikate	60
6.1.2. Lieferung privater Schlüssel	61
6.1.3. Lieferung öffentlicher Zertifikate	61
6.1.4. Schlüssellängen und kryptografische Algorithmen	61
6.1.5. Festlegung der Parameter der Schlüssel und Qualitätskontrolle	61
6.1.6. Verwendungszweck der Schlüssel	62
6.2. Sicherung des privaten Schlüssels und Anforderungen an kryptografische Module	62
6.2.1. Mehrpersonen-Zugriffssicherung zu privaten Schlüsseln	62
6.2.2. Ablage privater Schlüssel	62
6.2.3. Backup privater Schlüssel	63
6.2.4. Archivierung privater Schlüssel	64
6.2.5. Transfer privater Schlüssel in oder aus kryptografischen Modulen	64
6.2.6. Speicherung privater Schlüssel in kryptografischen Modulen	64
6.2.7. Aktivierung privater Schlüssel	64
6.2.8. Deaktivierung privater Schlüssel	65
6.2.9. Zerstörung privater Schlüssel	65
6.2.10. Beurteilung kryptografischer Module	65
6.3. Andere Aspekte des Managements von Schlüsselpaaren	67
6.3.1. Archivierung öffentlicher Schlüssel	67
6.3.2. Gültigkeitszeitraum von Zertifikaten und Schlüsselpaaren	67
6.4. Aktivierungsdaten	68
6.5. Sicherheitsanforderungen für die Rechneranlagen	68
6.6. Zeitstempel	69
6.7. Validierungsmodell	69
7. Profile für Zertifikate und Sperrlisten	69

**SWIT-
1961468859-
1355**

Certificate Policy SEN.CA

Gültig ab: 01.12.2022

Status: Freigegeben

Klassifizierung: Öffentlich

Druckdatum: 01.12.2022

7.1.	Profile für Zertifikate und Zertifikatsrequests	69
7.1.1.	Zugriffsrechte.....	69
7.1.2.	Zertifikatserweiterung	69
7.2.	Profile für Sperrlisten.....	69
7.3.	Profile für OCSP Dienste	69
8.	Überprüfung und andere Bewertungen.....	69
8.1.	Inhalte, Häufigkeit und Methodik.....	70
8.1.1.	Testbetrieb.....	70
8.1.2.	Beantragung der Teilnahme an der SEN.CA	71
8.1.3.	Wirkbetrieb	73
8.2.	Reaktionen auf identifizierte Vorfälle	73
9.	Sonstige finanzielle und rechtliche Regelungen	73
9.1.	Preise.....	73
9.1.1.	Nutzungsentgelte für Zertifikatsausstellung und -erneuerung	73
9.1.2.	Nutzungsentgelte für Zertifikate	73
9.1.3.	Nutzungsentgelte für Sperr- oder Statusinformationen	73
9.1.4.	Gebühren für andere Dienste	73
9.1.5.	Rückerstattung	73
9.2.	Finanzielle Zuständigkeiten.....	74
9.3.	Vertraulichkeit von Geschäftsdaten	74
9.3.1.	Geltungsbereich von vertraulichen Informationen.....	74
9.3.2.	Informationen, die nicht zu den vertraulichen Informationen gehören	74
9.3.3.	Zuständigkeit für den Schutz vertraulicher Informationen.....	74
9.4.	Datenschutz und Personendaten.....	74
9.4.1.	Richtlinie zur Verarbeitung personenbezogener Daten	74
9.4.2.	Vertraulich zu behandelnde Daten.....	75
9.4.3.	Nicht vertraulich zu behandelnde Daten.....	75
9.4.4.	Verantwortlicher Umgang mit personenbezogenen Daten	75
9.4.5.	Nutzung personenbezogener Daten	75
9.4.6.	Offenlegung bei gerichtlicher Anordnung oder im Rahmen einer gerichtlichen Beweisführung.....	75
9.4.7.	Andere Umstände einer Veröffentlichung.....	75
9.5.	Rechte am geistigen Eigentum	75

**SWIT-
1961468859-
1355**
Certificate Policy SEN.CA

Gültig ab: 01.12.2022

Status: Freigegeben
Klassifizierung: Öffentlich

Druckdatum: 01.12.2022

9.6.	Zusicherungen und Gewährleistungen	76
9.6.1.	Zusicherungen und Gewährleistungen der CA.....	76
9.6.2.	Zusicherungen und Gewährleistungen der RA.....	76
9.6.3.	Zusicherungen und Gewährleistungen der Zertifikatsinhaber	76
9.6.4.	Zusicherungen und Gewährleistungen der Zertifikatsnutzer.....	76
9.6.5.	Zusicherungen und Gewährleistungen für weitere Teilnehmer	76
9.7.	Gewährleistung	76
9.8.	Haftungsbeschränkungen	76
9.9.	Haftungsfreistellung.....	77
9.10.	Inkrafttreten und Aufhebung	77
9.10.1.	Inkrafttreten	77
9.10.2.	Aufhebung.....	77
9.10.3.	Konsequenzen der Aufhebung	77
9.11.	Individuelle Mitteilungen und Absprachen mit Teilnehmern.....	77
9.12.	Änderungen	77
9.12.1.	Verfahren bei Änderungen.....	77
9.12.2.	Benachrichtigungsmethode und -fristen.....	78
9.12.3.	Bedingungen für die Änderung des Richtlinienbezeichners (OID)	78
9.13.	Bestimmungen zur Schlichtung von Streitfällen	78
9.14.	Gerichtsstand	78
9.15.	Einhaltung geltenden Rechts	78
9.16.	Sonstige Bestimmungen	78
9.16.1.	Vollständigkeitserklärung.....	78
9.16.2.	Abtretung der Rechte.....	78
9.16.3.	Salvatorische Klausel.....	79
9.16.4.	Rechtliche Auseinandersetzungen / Erfüllungsort	79
9.17.	Andere Regelungen	79
Anhang A – Namensschema.....		80
A.1	Root-CA (informell)	81
A.2	Sub-CA.....	83
A.3	EMT.....	84
A.4	GWA.....	85
A.5	GWH	86

 Stadtwerke Saarbrücken	Certificate Policy SEN.CA	Version: 3.0
SWIT- 1961468859- 1355		Seite: 9/99
Status: Freigegeben	Klassifizierung: Öffentlich	Gültig ab: 01.12.2022 Druckdatum: 01.12.2022

A.6 SMGW.....	86
A.7 Alternativnamen.....	88
A.7.1 SubjectAltNames.....	88
A.7.2 IssuerAltName.....	89
Anhang B – Archivierung.....	89
Anhang C – Definitionen.....	91
Anhang D – Literaturverzeichnis.....	93
Glossar.....	96
Stichwort- und Abkürzungsverzeichnis.....	97

 Stadtwerke Saarbrücken	Certificate Policy SEN.CA	Version: 3.0
		Seite: 10/99
SWIT- 1961468859- 1355		Gültig ab: 01.12.2022
Status: Freigegeben	Klassifizierung: Öffentlich	Druckdatum: 01.12.2022

1. Einleitung

Der Einsatz intelligenter Strommesssysteme (Smart Metering Systems) bietet dem Endverbraucher eine höhere Transparenz über den eigenen Energieverbrauch und schafft die Basis für eine flexible Anpassung des Energieverbrauchs an die Verfügbarkeit von Energie. Die zentrale Kommunikationseinheit des intelligenten Messsystems stellt das Smart Meter Gateway (SMGW oder im Folgenden auch Gateway genannt) in den Haushalten der Endverbraucher dar. Diese Einheit trennt das Weitverkehrsnetz (WAN), d. h. das Netz zu den Backendsystemen von Smart Meter Gateway Administratoren (GWA) und externen Marktteilnehmern (EMT), von dem im Haushalt befindlichen Heimnetz (HAN) und den lokal angebundenen Zählern im metrologischen Netz (LMN). Die Hauptaufgaben des SMGW bestehen dabei in der technischen Separierung der angeschlossenen Netze, der sicheren Kommunikation in diese Netze, der Erfassung, Verarbeitung und Speicherung empfangener Messwerte verschiedener Zähler, der sicheren Weiterleitung der Messwerte an die Backendsysteme externer autorisierter Marktteilnehmer im WAN sowie der Verarbeitung von Administrationstätigkeiten durch den jeweiligen GWA.

Für die co.met GmbH (Eigentümer) betreibt die Stadtwerke Saarbrücken GmbH (Betreiber) kurz SWS genannt mit dem **SMART ENERGY NETWORK** im Folgenden kurz

SEN

genannt, einen ganzheitlichen Lösungsansatz für den Smart-Meter-Rollout, welcher alle derzeit bekannten Anforderungen vorkommender Rollen des Energiemarktes aus dem Gesetz über die Digitalisierung der Energiewende (GDEW) abdeckt.

Zur Absicherung der Kommunikation im WAN ist eine gegenseitige Authentisierung der Kommunikationspartner erforderlich. Die Kommunikation erfolgt dabei stets über einen verschlüsselten und integritätsgesicherten Kanal. Zudem werden Daten vom SMGW vor der Übertragung zur Integritätssicherung signiert und zur Gewährleistung des Datenschutzes für den Endempfänger verschlüsselt.

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

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

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

 Stadtwerke Saarbrücken	Certificate Policy SEN.CA	Version: 3.0
		Seite: 11/99
SWIT- 1961468859- 1355		Gültig ab: 01.12.2022
Status: Freigegeben	Klassifizierung: Öffentlich	Druckdatum: 01.12.2022

Die SWS betreibt hierbei für die co.met GmbH die im Folgenden als

SEN.CA

bezeichnete Sub-CA unter dem hoheitlichen Vertrauensanker der Root-CA des BSI, welche Zertifikate für alle berechtigten Marktrollen in der Smart-Metering-Infrastruktur bereitstellt.

Der eindeutige Name ("Distinguished Name") der **SEN.CA** lautet

C=DE, O=SM-PKI, CN=COMET-SEN.CA

Die **SEN.CA** ist als Sub-CA Teil der SM-PKI und unterwirft sich mit der **SEN.CA** CP der Certificate Policy der Smart Metering PKI (SM-PKI CP). Die **SEN.CA** Certificate Policy ist somit konform zu den prinzipiellen Vorgaben der Certificate Policy der Smart Metering PKI.

Die **SEN.CA** Certificate Policy, im Weiteren **SEN.CA** CP genannt, beschreibt dazu die technischen, personellen und organisatorischen Sicherheitsanforderungen und Vorgaben für die Ausstellung von Zertifikaten in der **SEN.CA**. Die konkreten und umfassenden Aussagen werden in dem Certification Practice Statement (CPS) der **SEN.CA** beschrieben (**SEN.CA** CPS).

Anforderungen und Regelungen zur Root-CA befinden sich in der [Certificate Policy der Smart Metering PKI](#) des BSI.

Die in der **SEN.CA** CP verwendeten Inhalte werden dem [RFC 2119](#) entsprechend mit folgenden deutschen Schlüsselworten beschrieben:

- **MUSS** bedeutet, dass es sich um eine normative Anforderung handelt, welche durch die **SEN.CA** entsprechend **umgesetzt** wird.
- **DARF NICHT / DARF KEIN** bezeichnet den normativen Ausschluss einer Eigenschaft in der **SEN.CA**.
- **SOLLTE / EMPFOHLEN** beschreibt eine dringende Empfehlung. Es müssen triftige Gründe vorliegen, um die Empfehlung nicht umzusetzen, wobei die Entscheidung dazu unter Abwägung aller Auswirkungen auf den jeweiligen Betrieb getroffen werden muss.
- **SOLLTE NICHT / SOLLTE KEIN** kennzeichnet die dringende Empfehlung, eine Eigenschaft auszuschließen.
- **KANN / DARF** bedeutet, dass die Eigenschaften fakultativ oder optional sind.

Die Kapitel der **SEN.CA** CP sind grundsätzlich als normativ anzusehen. Informative Kapitel werden explizit am Anfang gekennzeichnet.

1.1. Überblick

Das Dokument richtet sich an die Teilnehmer der **SEN.CA** und ist in Anlehnung an [RFC 3647](#) strukturiert und definiert. Nachfolgend wird die Struktur erläutert:

Nach der Einleitung (Kapitel 1) werden in Kapitel 2 zunächst die Verzeichnisdienste beschrieben. Hierunter fallen, neben der Darstellung der Verzeichnisse, Details dazu, welche Informationen

 Stadtwerke Saarbrücken	Certificate Policy SEN.CA	Version: 3.0
		Seite: 12/99
SWIT- 1961468859- 1355		Gültig ab: 01.12.2022
Status: Freigegeben	Klassifizierung: Öffentlich	Druckdatum: 01.12.2022

durch die **SEN.CA** zu veröffentlichen sind, 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 beschreibt die Betriebsanforderungen für den Zertifikatslebenszyklus (Ausgabe, Sperrung, Ablauf) sowie den Sonderfall der Außerbetriebnahme der **SEN.CA**.

Kapitel 5 beschäftigt sich mit organisatorischen, betrieblichen und physikalischen Sicherheitsanforderungen für die Betriebsumgebungen der **SEN.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 **SEN.CA**.

In Kapitel 8 finden sich Bewertungsrichtlinien für die einzelnen Parteien.

Kapitel 9 geht auf weitere rechtliche und finanzielle Regelungen ein.

Die Verantwortlichkeit für die SM-PKI Policy sowie den Betrieb der Root obliegt dem Bundesamt für Sicherheit in der Informationstechnik (BSI) als Inhaber der Wurzelzertifikate der SM-PKI.


Eigentümer der **SEN.CA** ist die co.met GmbH. Verantwortlich für die **SEN.CA** CP und den Betrieb der **SEN.CA** zeichnet die Stadtwerke Saarbrücken GmbH.

1.2. Name und Identifizierung des Dokuments

Identifikator	Wert
Titel	Certificate Policy SEN.CA
Version	3.2
OID	1.3.6.1.4.1.35262.1.5.1.42.1.0

Tabelle 1: Identifikation des Dokuments

Dieses Dokument kann öffentlich unter <https://support.sen-cloud.de/SEN-PKI> bezogen werden.

 Stadtwerke Saarbrücken	Certificate Policy SEN.CA	Version: 3.0
		Seite: 13/99
SWIT- 1961468859- 1355		Gültig ab: 01.12.2022
Status: Freigegeben	Klassifizierung: Öffentlich	Druckdatum: 01.12.2022

1.3. PKI-Teilnehmer

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

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

Tabelle 2: Übersicht der PKI-Teilnehmer

Unternehmen können mit mehreren Instanzen ihrer Organisation an der **SEN.CA** teilnehmen. Voraussetzung ist eine klare technische und organisatorische Separierung der Aufgabenbereiche sowie die Erfüllung aller Sicherheitsvorgaben der jeweiligen Instanz (siehe dazu auch die Maßnahmen zur Trennung der Instanzen im Abschnitt 6.2.6). Zusätzlich MUSS bei den ausführenden Personen der Unternehmen darauf geachtet werden, dass kein Interessenkonflikt bei der Erfüllung der Aufgaben auftreten darf.

Dies gilt insbesondere bei den Personen, die administrative Aufgaben im System wahrnehmen. Es DARF NICHT möglich sein (etwa durch eine Kumulierung von Berechtigungen bei einer Person), die definierte Trennung zwischen den einzelnen Instanzen zu umgehen. Dies gilt insbesondere für die Prozesse zur Ausgabe einer Berechtigung, zur Beantragung von GWA-/GWH-/EMT-/SMGW-Zertifikaten und zur eigentlichen Beantragung dieser Zertifikate.

Personen mit Managementrollen bzw. Rollen in der Sicherheitsorganisation KÖNNEN diese auch für mehrere Instanzen wahrnehmen. Hierbei MÜSSEN die Aufgabenbearbeitung, die jeweilige Funktion und die Berechtigungen der Person eindeutig sein.

Beispiel: Ein Mitarbeiter, der die Verantwortung für den Betrieb einer Sub-CA innehat, DARF NICHT gleichzeitig die Verantwortung für den Betrieb eines GWA haben.

 Stadtwerke Saarbrücken	Certificate Policy SEN.CA	Version: 3.0
		Seite: 14/99
SWIT- 1961468859- 1355		Gültig ab: 01.12.2022
Status: Freigegeben	Klassifizierung: Öffentlich	Druckdatum: 01.12.2022

1.3.1. Zertifizierungsstellen

Die Zertifizierungsstellen (Certification Authority – CA) stellen Sperrlisten sowie Zertifikate aus. Möglich sind folgende Arten von Zertifikaten:

- TLS-Zertifikate zur gegenseitigen Authentisierung zwischen SMGW und autorisierten Marktteilnehmern
- Verschlüsselungszertifikate für die Ende-zu-Ende-Verschlüsselung von Daten auf der Dateninhaltsebene unabhängig von der TLS-Verbindung
- Signaturzertifikate

Neben dem Wirksystem MUSS die **SEN.CA** für Testzwecke (z.B. bei der Erst-Registrierung und zum Test systemkritischer Vorgänge wie dem Wechsel des Vertrauensankers) auch eine *Test-CA*, im Folgenden **TEST-SEN.CA** genannt, bereitstellen. Mit der **TEST-SEN.CA** wird eine *Test-PKI* betrieben. Die technische Infrastruktur der **TEST-SEN.CA** MUSS funktional der einer Wirk-CA entsprechen. Hierbei MUSS die **TEST-SEN.CA** informationstechnisch von der Wirk-CA getrennt sein, und die verwendeten Schlüssel MÜSSEN unterschiedlich sein.

In Erweiterung der regulatorischen Anforderungen, betreibt die Stadtwerke Saarbrücken GmbH zur Wahrung des geforderten Sicherheitsniveaus und der bereitgestellten Verfügbarkeit, eine dreistufige Systemlandschaft mit jeweils separierten Sub-CAs (siehe Abbildung 1 - SM-PKI Systemlandschaft SEN.CA).

**SWIT-
1961468859-
1355**

Certificate Policy SEN.CA

Gültig ab: 01.12.2022

Status: Freigegeben

Klassifizierung: Öffentlich

Druckdatum: 01.12.2022

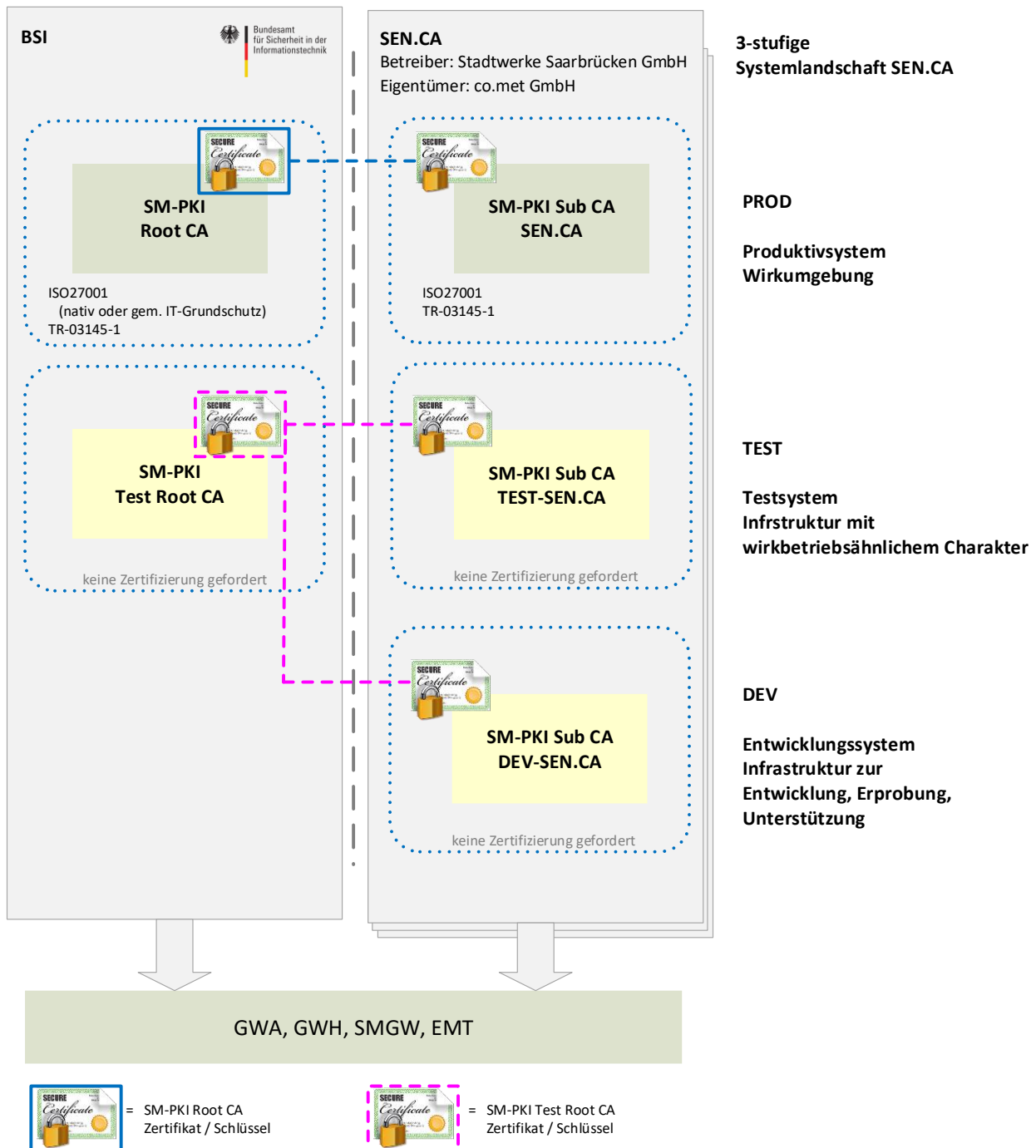



Abbildung 1 - SM-PKI Systemlandschaft SEN.CA

3. Stufe – PROD – Produktivumgebung
2. Stufe – TEST – Testumgebung
1. Stufe – DEV – Entwicklungsumgebung

 Stadtwerke Saarbrücken	Certificate Policy SEN.CA	Version: 3.0
		Seite: 16/99
SWIT- 1961468859- 1355		Gültig ab: 01.12.2022
Status: Freigegeben	Klassifizierung: Öffentlich	Druckdatum: 01.12.2022

1.3.1.1. Root-CA

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) ist Inhaber der Zertifikate der Wurzelzertifizierungsstelle (Root) der Smart-Metering-Public-Key-Infrastruktur (SM-PKI) und ist somit verantwortlich für die Smart-Metering-PKI-Root-Certificate Authority (**SM-PKI-Root-CA**).

Die SM-PKI-Root-CA bildet den hoheitlichen Vertrauensanker der SM-PKI. Die Aufgabe der SM-PKI ist die Absicherung der Kommunikation in der WAN-Infrastruktur der Smart Meter Gateways (SMGW). Die Zertifikate aus der SM-PKI werden insbesondere für die gegenseitige Authentisierung der Kommunikationspartner in der Infrastruktur eingesetzt. Die Kommunikation erfolgt dabei stets über einen verschlüsselten und integritätsgesicherten Kanal. Zudem werden Daten von einem SMGW vor der Übertragung zur Integritätssicherung signiert und zur Gewährleistung des Datenschutzes für den Endempfänger verschlüsselt.

Der Betrieb der Root wird von einem Zertifizierungsdiensteanbieter für das BSI durchgeführt.

1.3.1.2. Sub-CA

Die Stadtwerke Saarbrücken GmbH betreiben unter der ROOT-CA des BSI für die co.met GmbH die **SEN.CA** als Sub-CA, welche Zertifikate für Endbenutzer ausstellt. Die **SEN.CA** ist dazu von der Root-CA zur Ausstellung von Zertifikaten für Endbenutzer autorisiert. Die **SEN.CA** wird unternehmensübergreifend betrieben und kann die unterschiedlichsten Marktteilnehmer mit Zertifikaten versorgen. Folgende Endbenutzer können Zertifikate aus der **SEN.CA** beziehen:

- Externe Marktteilnehmer (EMT)
- Gateway-Administrator (GWA)
- Gateway-Hersteller (GWH)
- Smart Meter Gateway (SMGW)

Zu den externen Marktteilnehmern gehören im Kontext der PKI alle Marktteilnehmer, die potenzielle Kommunikationspartner eines Smart Meter Gateways im WAN sind, etwa Verteilnetzbetreiber, Messstellenbetreiber oder Lieferanten.

1.3.2. Registrierungsstellen

Den Registrierungsstellen (RA) obliegt die Überprüfung der Identität und Authentizität von Zertifikatsnehmern vor der Ausstellung eines Zertifikats. Der **SEN.CA** ist eine ausgezeichnete RA zugeordnet, welche sich in zwei Ebenen gliedert.

1. Ebene RA-FirstLevel-Instanz (durch den Betreiber der **SEN.CA** autorisierte Instanz)
2. Ebene RA-SecondLevel-Instanz (ausgezeichnete RA Instanz der **SEN.CA**)

Die Anforderungen an den Betrieb einer RA-FirstLevel-Instanz sind in Tabelle 15 zusammengestellt.


 Stadtwerke Saarbrücken	Certificate Policy SEN.CA	Version: 3.0
		Seite: 17/99
SWIT- 1961468859- 1355		Gültig ab: 01.12.2022
Status: Freigegeben	Klassifizierung: Öffentlich	Druckdatum: 01.12.2022

Nur die ausgezeichnete RA-SecondLevel-Instanz der **SEN.CA** RA darf zur initialen Registrierung von der unmittelbar vorgelagerten RA-FirstLevel-Instanzen eingesetzt werden. Hierzu MUSS die RA-SecondLevel-Instanz der **SEN.CA** die Autorisierung der RA der RA-FirstLevel-Instanz vornehmen und entsprechende verantwortliche identifizierte und authentifizierte Vertreter autorisieren. Die Registrierung weiterer Zertifikatsnehmer KANN über beide Ebenen durchgeführt werden, MUSS jedoch immer durch die RA-SecondLevel-Instanz geprüft und genehmigt werden. Die Einhaltung der **SEN.CA** CP muss jeweils schriftlich gegenüber dem Betreiber der **SEN.CA** zugesichert werden. Ebenso ist die Benennung und Entbindung von RAs der FirstLevel-Instanz zu dokumentieren und zu kommunizieren.

Zur Autorisierung und Aufnahme einer neuen RA-FirstLevel-Instanz in die ausgezeichnete **SEN.CA** RA MÜSSEN das Unternehmen authentifiziert und mindestens zwei bevollmächtigte Vertreter der RA-FirstLevel-Instanz (RA-FirstLevel-Operator) persönlich bei dem Betreiber der **SEN.CA** identifiziert, authentifiziert und autorisiert werden.

Notwendige Unterlagen und Daten für die Registrierung sind:

- Antragsschreiben zur Aufnahme einer neuen RA-FirstLevel-Instanz in die ausgezeichnete **SEN.CA** RA
 - 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 RA-FirstLevel-Operatoren (unter Beachtung einer Vertreterregelung)
 - eine Sicherheitserklärung der benannten RA-FirstLevel-Operatoren
 - eine Sicherheitserklärung des beantragenden Unternehmens in welchem die RA-FirstLevel-Operatoren beschäftigt sind
 - Bestätigung der Geschäftsführung des Unternehmens bzw. der Leitung der Institution, in der der Vertreter (RA-FirstLevel-Operator) des Betreibers berechtigt wird, den Antrag für eine neue RA-FirstLevel-Instanz zu stellen und in der Sache dazu verbindliche Aussagen und Angaben zu machen.
- Persönliche/individuelle Zertifikate für die gesicherte E-Mail-Kommunikation der benannten RA-FirstLevel-Operatoren (C_{S/MIME}(RAFL)) inklusive der zur Verifikation erforderlichen Zertifikatskette
- Die RA-FirstLevel-Instanz MUSS eine Erklärung zur Einhaltung der Sicherheitsvorgaben aus dieser SEN.CA Certificate Policy für die Teilnahme an der ausgezeichneten **SEN.CA** RA (s. Tabelle 15) vorlegen.
- Die RA-FirstLevel-Instanz fungiert als Dienstleister und MUSS für initiale Prozesse und zum Betrieb der RA-FirstLevel-Instanz dem Betreiber der **SEN.CA** eine Bestätigung des beauftragenden Unternehmens vorlegen, welches den Dienstleister zum Betrieb der RA-FirstLevel-Instanz berechtigt bzw. aus welchem die Vertragsbeziehung zwischen RA-FirstLevel-Instanz und beauftragenden Unternehmen hervorgeht.
- Vor der initialen Autorisierung MUSS der Betrieb der RA-FirstLevel-Instanz im Rahmen einer Testteilnahme unterhalb der **TEST-SEN.CA** erfolgreich erprobt worden sein. In diesem Test MÜSSEN mindestens einmalig die erforderlichen Prozesse erfolgreich

 Stadtwerke Saarbrücken	Certificate Policy SEN.CA	Version: 3.0
		Seite: 18/99
SWIT- 1961468859- 1355		Gültig ab: 01.12.2022
Status: Freigegeben	Klassifizierung: Öffentlich	Druckdatum: 01.12.2022

durchlaufen werden. Die erfolgreiche Teilnahme wird von einem Ansprechpartner der **SEN.CA** per signierter E-Mail bestätigt.

1.3.3. Zertifikatsnehmer

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

1.3.3.1. SMGW

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

1.3.3.2. Gateway-Administrator

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

Ein Gateway-Administrator (GWA) erhält von der **SEN.CA** Zertifikate, mit denen dieser insbesondere

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

1.3.3.3. Gateway-Hersteller

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

1.3.3.4. Externer Marktteilnehmer

Ein EMT ist ein datenumgangsberechtigter Marktteilnehmer nach § 49 Abs. 2 MsbG.

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

Ein EMT, welcher ein SMGW nutzt, um über dieses nachgelagerte Geräte (Controllable Local Systems, CLS) anzusprechen, wird als **aktiver EMT** bezeichnet. Die entsprechenden

 Stadtwerke Saarbrücken	Certificate Policy SEN.CA	Version: 3.0
		Seite: 19/99
SWIT- 1961468859- 1355		Gültig ab: 01.12.2022
Status: Freigegeben	Klassifizierung: Öffentlich	Druckdatum: 01.12.2022

Anwendungsfälle zur Steuerung von CLS an der HAN-Schnittstelle durch einen EMT sind in der BSI TR-03109-1 definiert.

Ein EMT, welcher keine nachgelagerten Geräte (CLSs) anspricht bzw. steuert, sondern nur Daten empfängt, um auf Basis dieser Informationen die eigenen Geschäftsprozesse fortzuführen, wird als **passiver EMT** bezeichnet.

Ein Unternehmen kann die Abwicklung der Kommunikation mit den SMGWs inkl. dem zugehörigen Zertifikatsmanagement auch als Dienstleistung einem datenumgangsberechtigten Marktteilnehmer (EMT) anbieten ohne selbst EMT zu sein. Dieses Unternehmen würde somit das EMT-Frontend des Auftraggebers realisieren. Gemäß § 52 Abs. 4 MsbG dürfen personenbezogene Daten, Stammdaten und Netzzustandsdaten nur zwischen den Teilnehmern der SM-PKI kommuniziert werden. Entsprechend MÜSSEN die verschiedenen Teilnehmer (z.B. Messstellenbetreiber) jeweils über ein eigenes Zertifikat verfügen, um die Kommunikation dieser Daten mit dem SMGW und untereinander durchzuführen. Daher MUSS jeder datenumgangsberechtigte Marktteilnehmer nach §49 Abs. 2 MsbG (EMT, z.B. ein Messstellenbetreiber) in seinem Namen ein PKI-Zertifikat bei seiner ausgewählten CA beantragen. Bei dem Aufbau einer solchen Systemstruktur MUSS darauf geachtet werden, dass die Übermittlung der Daten von dem Dienstleister zu dem Auftraggeber ein vergleichbares Sicherheitsniveau zu den in der [TR-03116-3] definierten Sicherheitsmechanismen einhält. Betreut ein solcher Dienstleister mehrere Auftraggeber, so MUSS eine klare Trennung zwischen den Auftraggebern erfolgen. Die Trennung kann durch technische und / oder organisatorische Maßnahmen realisiert werden. Der beauftragte Dienstleister nach § 49 Abs. 3 MsbG MUSS das PKI-Zertifikat im Auftrag des datenumgangsberechtigten Marktteilnehmers (EMT) nutzen. Der Dienstleister DARF für die beauftragten Aufgaben kein anderes Zertifikat verwenden. Der Dienstleister KANN im Auftrag des datenumgangsberechtigten Marktteilnehmers (EMT) entsprechende PKI-Zertifikate für diesen beantragen. Die Zertifikate MÜSSEN dabei jedoch auf den datenumgangsberechtigten Marktteilnehmer (EMT) ausgestellt werden. Diese Regelung gilt für jeden datenumgangsberechtigten Marktteilnehmer (EMT). Wie eine Registrierung in der **SEN.CA** mit einem Dienstleister generell erfolgen muss, ist in der Abschnitt 3.2.2.2 definiert.

1.3.4. Zertifikatsnutzer

Zertifikatsnutzer im Sinne dieser **SEN.CA** CP sind alle natürlichen und juristischen Personen bzw. technischen Komponenten, die Zertifikate aus der SEN.CA für die Erledigung von Geschäftsprozessen/Aufgaben verwenden.

1.3.5. Andere Teilnehmer

Teilnehmer (wie, z.B. Endverbraucher), welche keine Verpflichtung im Rahmen dieser **SEN.CA** CP eingegangen sind, sind nicht Bestandteil der **SEN.CA** CP und werden daher nicht berücksichtigt. Ergeben sich beispielsweise durch die internationale Anbindung anderer Infrastrukturen weitere Teilnehmer, so MÜSSEN sowohl deren Rollen als auch deren Interaktionen den Sicherheitsanforderungen dieser **SEN.CA** CP entsprechen.

 Stadtwerke Saarbrücken	Certificate Policy SEN.CA	Version: 3.0
		Seite: 20/99
SWIT- 1961468859- 1355		Gültig ab: 01.12.2022
Status: Freigegeben	Klassifizierung: Öffentlich	Druckdatum: 01.12.2022

1.4. Verwendung von Zertifikaten

In diesem Kapitel wird die erlaubte und verbotene Nutzung von Zertifikaten in der **SEN.CA** definiert.

1.4.1. Erlaubte Verwendung von Zertifikaten

Jeder SM-PKI-Teilnehmer benötigt für die Ausübung seiner PKI-Rolle entsprechende Zertifikate aus der SM-PKI. Ein Teilnehmer KANN über mehrere Zertifikate bzw. Zertifikatstriple verfügen (siehe [TR-03109-4] Abschnitt 4.1.1).

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


Der Verwendungszweck der Zertifikate für die Zertifikatsnehmer wird, außer für die Root-CA und Sub-CA, in folgender Tabelle dargestellt. Alle weiteren Informationen können der [TR-03109-4] entnommen werden.

Zertifikat eines Zertifikatsteilnehmer	Signiert durch	Verwendungszweck
C_{TLS}(EMT) C_{TLS}(GWA) C_{TLS}(GWH) C_{TLS}(SMGW)	Privater Schlüssel zu C(Sub-CA)	Zertifikat des entsprechenden Endnutzers zur Authentisierung beim Kommunikationspartner und zum Aufbau einer TLS-Verbindung (siehe [TR-03116-3]). Das Zertifikat C _{TLS} (GWA) wird zudem auch für die Authentifikation am Sicherheitsmodul des SMGW verwendet
C_{ENC}(EMT) C_{ENC}(GWA) C_{ENC}(GWH) C_{ENC}(SMGW)	Privater Schlüssel zu C(Sub-CA)	Zertifikat zur Verschlüsselung von Inhaltsdaten für den entsprechenden Endnutzer.
C_{SIG}(EMT) C_{SIG}(GWA) C_{SIG}(GWH) C_{SIG}(SMGW)	Privater Schlüssel zu C(Sub-CA)	Zertifikat zur Verifikation von Inhaltsdatensignaturen des entsprechenden Endnutzers.

Tabelle 3: Zertifikate der Zertifikatsnehmer

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

Für die Kommunikation der Ansprechpartner (ASP) in den unterschiedlichen Ebenen ist der Informationsaustausch mittels verschlüsselter und signierter E-Mails vorgesehen. Diese Zertifikate

 Stadtwerke Saarbrücken	Certificate Policy SEN.CA	Version: 3.0
		Seite: 21/99
SWIT- 1961468859- 1355		Gültig ab: 01.12.2022
Status: Freigegeben	Klassifizierung: Öffentlich	Druckdatum: 01.12.2022

werden nicht von der **SEN.CA** bereitgestellt. Die Anforderungen an diese Zertifikate sind in folgender Tabelle definiert:

Zertifikat eines Ansprechpartners	Verwendungszweck
C_{S/MIME}(ASP Root) C_{S/MIME}(ASP Sub-CA) C_{S/MIME}(GWA) C_{S/MIME}(GWH) C_{S/MIME}(EMT)	<p>Zertifikat für den privaten Schlüssel, der vom Ansprechpartner der Root, einer Sub-CA, eines GWA, eines GWH, eines EMT für die Signatur und Verschlüsselung der E-Mail-Kommunikation eingesetzt wird. Je nach Realisierung der ausstellenden CA KÖNNEN für die Signatur und die Verschlüsselung auch unterschiedliche Zertifikate eingesetzt werden. Es MUSS bei dem Zertifikat eine Zuordnung zwischen dem Ansprechpartner und den Angaben im Zertifikat möglich sein (personalisiertes bzw. persönliches Zertifikat). Der ergänzende Einsatz von Funktionspostfächern (Zugriff und Nutzung durch mehrere Anwender) ist nur zum Empfang von Mails gestattet, sofern die Kommunikation mit den identischen Mechanismen abgesichert wird (Funktionspostfach muss über ein entsprechendes Verschlüsselungszertifikat verfügen). Der Versand von allgemeinen bzw. öffentlichen Informationen kann optional auch unverschlüsselt erfolgen. Es wird EMPFOHLEN, dass Zertifikate den Anforderungen der [TR-03116-4] entsprechen. Grundsätzlich kommen hier die Zertifikate zum Einsatz, welche durch den Ansprechpartner bereitgestellt werden. Vor dem Ablauf des personenbezogenen Zertifikats muss der Ansprechpartner ein neues Zertifikat zur Verfügung stellen, so dass durchgehend ein sicherer Kommunikationskanal bereitgestellt wird. Die Übermittlung des neuen Zertifikats erfolgt dabei mittels einer mit dem alten, noch gültigen Zertifikat signierten E-Mail (alternativ mit einer entsprechenden E-Mail eines anderen Ansprechpartners).</p>

Tabelle 4: Kommunikationszertifikate der Ansprechpartner

1.4.2. Verbotene Verwendung von Zertifikaten

Die Zertifikate MÜSSEN gemäß ihres Verwendungszwecks eingesetzt werden, siehe Abschnitt 1.4.1.

 Stadtwerke Saarbrücken	Certificate Policy SEN.CA	Version: 3.0
		Seite: 22/99
SWIT- 1961468859- 1355		Gültig ab: 01.12.2022
Status: Freigegeben	Klassifizierung: Öffentlich	Druckdatum: 01.12.2022

1.5. Administration der SEN.CA CP

Für das vorliegende Dokument zuständig ist die SWS.

Organisation	Stadtwerke Saarbrücken GmbH
Adresse	Hohenzollernstraße 104 – 106 66117 Saarbrücken
Webseite	https://support.sen-cloud.de/SEN-PKI
eMail	trustcenter@sen-pki.de

Tabelle 5: Kontaktadresse

1.5.1. Pflege der SEN.CA CP

Jede aktualisierte Version der **SEN.CA** Certificate Policy wird den Anwendern unverzüglich über die angegebene Internetseite zur Verfügung gestellt (siehe Tabelle 5: Kontaktadresse).

1.5.2. Zuständigkeit für das Dokument

Zuständig für die Erweiterung und oder die nachträgliche Änderungen dieser **SEN.CA** CP ist die co.met GmbH.

1.5.3. Ansprechpartner / Kontaktpersonen

Ansprechpartner zu allen Fragestellungen im Zusammenhang mit dem vorliegenden Dokument sind:

Name	Dr.-Ing. Thomas Klein	Bernd Kraus
Bereich	VI – Informationsmanagement	VIS – IT Services
Funktion	Fachbereichsleiter	System Architect IT
E-Mail	thomas.klein@sw-sb.de	bernd.kraus@sw-sb.de
Telefon	+49 681 587 2017	+49 681 587 2680
Mobil	+49 160 369 4211	-
Fax	+49 681 587-297 2017	-

Tabelle 6: Ansprechpartner

 Stadtwerke Saarbrücken	Certificate Policy SEN.CA	Version: 3.0
		Seite: 23/99
SWIT- 1961468859- 1355		Gültig ab: 01.12.2022
Status: Freigegeben	Klassifizierung: Öffentlich	Druckdatum: 01.12.2022

1.5.4. Zuständiger für die Anerkennung eines CPS

Ein CPS (Certificate Practice Statement) einer CA ist ein internes Dokument. Dieses KANN bei Prüfungen des Betriebs herangezogen werden. Der Inhalt der **SEN.CA** CPS und der **SEN.CA** CP wird mindestens jedes Jahr durch einen internen PKI Ausschuss überprüft.

1.5.5. SEN.CA CPS-Aufnahmeverfahren

Die **SEN.CA** CPS MUSS die Anforderungen dieser **SEN.CA** CP umsetzen.

2. Verantwortlichkeit für Veröffentlichungen und Verzeichnisse

2.1. Verzeichnisse


Die **SEN.CA** stellt einen auf dem LDAP-Protokoll basierenden Verzeichnisdienst gemäß TR-03109-4 mit allen von ihr ausgestellten Zertifikaten zur Verfügung. Der Zugriff auf den Verzeichnisdienst ist dabei mittels zertifikatsbasierender TLS-Authentisierung auf die Teilnehmer der SM-PKI beschränkt.

Zudem erstellt die **SEN.CA** entsprechend der Anforderung wahlweise über HTTP oder LDAP eine Certificate Revocation List (CRL), im Deutschen ‚Zertifikatssperrliste‘ mit gesperrten Endnutzer-Zertifikaten. Dabei werden nur direkte CRLs ausgegeben, d.h. die Sperrliste enthält nur gesperrte Zertifikate, die von der **SEN.CA** selbst ausgegeben wurden. Hierüber kann die Gültigkeit aller von der **SEN.CA** ausgegebenen Zertifikate überprüft werden. Auf die Sperrliste kann frei zugegriffen werden. Die Sperrliste ist mit dem privaten Schlüssel zum aktuell gültigen **SEN.CA** Zertifikat signiert und enthält alle von der **SEN.CA** gesperrten Zertifikate während ihres Gültigkeitszeitraums.

2.2. Veröffentlichung von Informationen zur Zertifikatserstellung

Die **SEN.CA** veröffentlicht unter <https://support.sen-cloud.de/sen-pki/> folgende Informationen:

- Kontaktdaten der **SEN.CA**
- Parameter zur Einrichtung eines Zugriffs auf die Sperrliste bzw. das LDAP-Verzeichnis
- die vorliegende **SEN.CA** CP mit folgenden Inhalten:
 - die Anforderungen und somit die Einhaltung der SM-PKI Policy des BSIs.
 - die Beschreibung grundsätzlicher Prozesse für die Bereitstellung und Verwaltung der Zertifikate mit Verweis auf die entsprechenden Stellen in der SM-PKI Policy.
 - die für den Betrieb verantwortlichen Bereiche und Ansprechpartner.
- eine Beschreibung des Antragsverfahrens von Zertifikaten
- Formulare zur Beantragung von Zertifikaten
- Informationen zu den zu erstellenden jeweiligen Zertifikatsrequests
- Informationen zum Sperrprozess von Zertifikaten
- Hinweise zur Teilnahme am Testsystem

 Stadtwerke Saarbrücken	Certificate Policy SEN.CA	Version: 3.0
		Seite: 24/99
SWIT- 1961468859- 1355		Gültig ab: 01.12.2022
Status: Freigegeben	Klassifizierung: Öffentlich	Druckdatum: 01.12.2022

2.3. Zeitpunkt und Häufigkeit der Veröffentlichungen

Alle Zertifikate innerhalb der **SEN.CA** MÜSSEN unmittelbar nach der Ausstellung im jeweiligen LDAP-Verzeichnis veröffentlicht werden.

Sperrungen werden nach Durchführung durch eine Veröffentlichung in der Sperrliste der **SEN.CA** als solche wirksam. Eine Aufnahme in die Sperrliste sowie deren Veröffentlichung erfolgt gemäß den in der BSI TR-03109-4 festgelegten Zeiten. Nach Ablauf der im Zertifikat eingetragenen Gültigkeit MUSS der Eintrag aus der Sperrliste entfernt werden.

2.4. Zugriffskontrollen auf Verzeichnisse

Der lesende Zugriff auf die LDAP-Verzeichnisdienste MUSS auf die an der SM-PKI teilnehmenden Organisationen wie GWAs, GWHs sowie EMTs beschränkt werden. Ein SMGW verfügt über keine Schnittstellen zu den Verzeichnisdiensten, so dass diese Zertifikate für den Zugriff auch nicht freigeschaltet werden müssen. Der Zugriff wird über eine zertifikatsbasierte Authentisierung am jeweiligen Verzeichnisdienst mittels der TLS-Zertifikate der Zertifikatsnehmer gemäß der Anforderungen aus [TR-03116-3] sichergestellt.

Der Verzeichnisdienst der **SEN.CA** dient ausschließlich der Aktualisierung von angefragten Zertifikaten. Ein Massenabruf von Zertifikaten DARF NICHT erfolgen. Die vom Verzeichnisdienst zurückgegebene Anzahl von Suchergebnissen KANN hierfür durch die Betreiber der **SEN.CA** entsprechend begrenzt werden. Der Verzeichnisdienst der **SEN.CA** ist so konfiguriert, dass die Anzahl der zurückgegebenen Suchergebnisse auf 10 begrenzt ist.

Der lesende Zugriff auf die Sperrlisten der **SEN.CA** ist ohne Authentifikation und ohne Einschränkungen möglich.

3. Identifizierung und Authentifizierung

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

Das Profil eines Zertifikatsrequests MUSS konform zur BSI TR-03109-4 sein.

3.1. Regeln für die Namensgebung

3.1.1. Arten von Namen

In der **SEN.CA** wird eine einheitliche Namenshierarchie verwendet. Alle innerhalb der **SEN.CA** ausgestellten Zertifikate beinhalten eindeutige Namen (engl. Common Name, kurz CN) gemäß Anhang A – Namensschema. Ein CN enthält eine Folge von eindeutig kennzeichnenden Attributen, durch die jeder Zertifikatsnehmer eindeutig referenziert wird.

Ein CN entspricht dabei grundsätzlich folgendem Schema:

‘<org>.<function>[.<extension>]’

 Stadtwerke Saarbrücken	Certificate Policy SEN.CA	Version: 3.0
		Seite: 25/99
SWIT- 1961468859- 1355		Gültig ab: 01.12.2022
Status: Freigegeben	Klassifizierung: Öffentlich	Druckdatum: 01.12.2022

Tabelle 7 beschreibt die Bestandteile der CN für die Teilnehmer der **SEN.CA**:

Namensteil	Bedeutung	Länge, Kodierung, Ausnahmen
<org>	Kürzel der Identität/Organisation	Länge max. 48 Zeichen, erstes Zeichen muss ein Buchstabe oder eine Ziffer sein.
<function>	Funktionskennzeichnung innerhalb der SEN.CA	Länge max. 4 Zeichen. Feste Werte: CA, EMT, GWA, GWH oder SMGW
<extension>	Erweiterung, zusätzliche Informationen	Länge max. 10 Zeichen. Bezeichnung/Kürzel der RA-FirstLevel-Instanz

Tabelle 7: Namensschema (Kodierung Common Name)

3.1.2. Notwendigkeit für aussagefähige Namen

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

3.1.3. Anonymität oder Pseudonymität von Zertifikatsnehmern

Der Zertifikatsnehmer **DARF NICHT** anonym sein oder Pseudonyme verwenden. Über einen Zertifikatsantrag **MUSS** immer eine eindeutige Zuordnung zum Zertifikatsnehmer bestehen.

3.1.4. Eindeutigkeit von Namen

Eine Namensgleichheit, gleicher CN bei unterschiedlichem Zertifikatsnehmer, **MUSS** durch die **SEN.CA** verhindert werden. Entsprechend **DARF** die **SEN.CA** einen CN **NICHT** mehrfach vergeben.

Bei der Ausstellung von Zertifikaten ist ein Abgleich hinsichtlich der Eindeutigkeit von Namen zwischen verschiedenen Sub-CA's nicht erforderlich.

Sollten zwei oder mehr Zertifikatsnehmer den gleichen CN beantragen, besteht ein Konflikt, der durch die **SEN.CA** gelöst werden **MUSS**. Es behält der Teilnehmer seinen CN, der zuerst sein erstes Zertifikat mit diesem CN erhalten hat. Der oder die anderen Zertifikatsnehmer **MÜSSEN** sich ein neues Zertifikat mit einem anderem CN ausstellen lassen, um weiterhin an der **SEN.CA** teilnehmen zu **DÜRFEN**.

3.1.5. Anerkennung, Authentifizierung und die Rolle von Markennamen

Die Eintragungen der Firmennamen **MÜSSEN** gemäß den Vorgaben aus Abschnitt 3.1.1 auf Basis der Identität, die im Rahmen der initialen Überprüfung in das erste Zertifikat übernommen wurde, erfolgen.

 Stadtwerke Saarbrücken	Certificate Policy SEN.CA	Version: 3.0
		Seite: 26/99
SWIT- 1961468859- 1355		Gültig ab: 01.12.2022
Status: Freigegeben	Klassifizierung: Öffentlich	Druckdatum: 01.12.2022

3.2. Initiale Überprüfung zur Teilnahme an der PKI

Dieses Kapitel 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.

3.2.1. Methoden zur Überprüfung bzgl. Besitz des privaten Schlüssels

Zum Nachweis des Besitzes des privaten Schlüssels MUSS ein Zertifikatsrequest gemäß BSI TR-03109-4 eine sogenannte innere Signatur beinhalten.

Hierdurch MUSS bei der Antragsprüfung durch Verifikation der inneren Signatur mit dem im Zertifikatsrequest enthaltenen zugehörigen öffentlichen Schlüssel durch die **SEN.CA** geprüft werden, dass der Antragsteller im Besitz des privaten Schlüssels ist.

3.2.2. Authentifizierung von Organisationszugehörigkeiten

Innerhalb der **SEN.CA** dürfen der EMT, GWA und GWH Zertifikatsanträge stellen. Die detaillierten Prozesse zur Identifizierung, Registrierung und Zertifikatsbeantragung können der **SEN.CA** CPS entnommen werden.

3.2.2.1. Sub-CA

Es gelten die Anforderungen aus der Certificate Policy der Smart Meter PKI für den Betreiber der **SEN.CA**.

3.2.2.2. EMT

Die detaillierten Prozesse zur Identifizierung, Registrierung und Zertifikatsbeantragung können der **SEN.CA** CPS entnommen werden.

Zur Aufnahme eines neuen EMT in die **SEN.CA** MUSS durch die **SEN.CA** RA-SecondLevel-Instanz eine Überprüfung der Authentifikation des Unternehmens erfolgen.

Der Prozess DARF durch eine der RA-SecondLevel-Instanz vorgelagerte, durch die **SEN.CA** autorisierte, RA-FirstLevel-Instanz durchgeführt werden.

Die **SEN.CA** MUSS hierfür die erforderlichen Prozesse der RA-FirstLevel-Instanz bereitstellen.

Notwendige Unterlagen und Daten für die Registrierung sind:

- Antragsschreiben zur Ausgabe eines EMT-Zertifikats mit folgenden Daten bzw. beigefügten Informationen
 - 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

 Stadtwerke Saarbrücken	Certificate Policy SEN.CA	Version: 3.0
		Seite: 27/99
SWIT- 1961468859- 1355		Gültig ab: 01.12.2022
Status: Freigegeben	Klassifizierung: Öffentlich	Druckdatum: 01.12.2022

- 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.
- Persönliche/individuelle Zertifikate für die gesicherte E-Mail-Kommunikation der benannten Ansprechpartner(C_S/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.
 - Möchte ein passiver EMT nachträglich auch die Aufgaben eines aktiven EMTs, siehe Abschnitt 1.3.3.4, wahrnehmen oder möchte ein aktiver EMT nur noch als passiver EMT auftreten, so MUSS das Unternehmen dies der **SEN.CA** rechtzeitig und eigenverantwortlich mitteilen und die entsprechenden Unterlagen vorlegen
 - Die Aufgaben des aktiven EMT dürfen erst vom Antragssteller mit dem bestehenden Zertifikat ausgeübt werden, wenn die erfolgreiche Registrierung als aktiver EMT von der **SEN.CA** bestätigt wurde. Die Bestätigung MUSS per signierter E-Mail an den registrierten Ansprechpartner gesendet werden.
 - Die zusätzlichen Auflagen für den Betrieb des aktiven EMT fallen erst weg, wenn der Rollenwechsel von der **SEN.CA** bestätigt wurde. Die Bestätigung MUSS per signierter E-Mail an den registrierten Ansprechpartner gesendet werden.
- Erklärung zur Einhaltung der Sicherheitsvorgaben aus dieser **SEN.CA** Policy
 - Der EMT MUSS eine Erklärung zur Einhaltung der Sicherheitsvorgaben aus dieser **SEN.CA** Policy mit einreichen.
 - Der EMT MUSS den Nachweis des sicheren Betriebs gemäß den Vorgaben zu den Anforderungen für die Teilnahme an der **SEN.CA** gemäß Tabelle 15 erbringen.
 - Bei der Beauftragung eines Dienstleisters MUSS die sichere Kommunikation zwischen EMT und Dienstleister im Sicherheitskonzept (SiKo) des EMT definiert werden.
- Bestätigung der erfolgreichen Testteilnahme, ausgestellt von der **SEN.CA**
 - Vor der Wirksamkeitsaufnahme MÜSSEN die Prozesse zum Zertifikatsmanagement, insbesondere Registrierung, Zertifikatsbeantragung, -erneuerung, -sperrung, mit der **Test-SEN.CA** erfolgreich durchgeführt worden sein. Die erfolgreiche Teilnahme wird von einem Ansprechpartner der **SEN.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.
- Bei der Beauftragung eines Dienstleisters MUSS zusätzlich eine Vollmacht zur Teilnahme an der **SEN.CA** eingereicht werden, welche folgende Angaben beinhaltet:
 - Unternehmensdaten des datenumgangsberechtigten Marktteilnehmers

 Stadtwerke Saarbrücken	Certificate Policy SEN.CA	Version: 3.0
		Seite: 28/99
SWIT- 1961468859- 1355		Gültig ab: 01.12.2022
Status: Freigegeben	Klassifizierung: Öffentlich	Druckdatum: 01.12.2022

- Kontaktdaten der gesetzlichen Vertretungsberechtigten des datenumgangsberechtigten Marktteilnehmers
- Unternehmensdaten des bevollmächtigten Dienstleisters
- Kontaktdaten der gesetzlichen Vertretungsberechtigten des bevollmächtigten Dienstleisters
- Benennung und Kontaktdaten der autorisierten Ansprechpartner
- Handlungsbevollmächtigung für die definierten Prozesse

3.2.2.3.GWA

Die detaillierten Prozesse zur Identifizierung, Registrierung und Zertifikatsbeantragung können der **SEN.CA** CPS entnommen werden.

Zur Aufnahme eines neuen GWA in die **SEN.CA** MUSS das Unternehmen authentifiziert werden, und mindestens zwei bevollmächtigte Vertreter des GWA MÜSSEN persönlich bei der RA der **SEN.CA** identifiziert und authentifiziert werden.


Die Identifizierung und Authentifizierung vor Ort MUSS durch mindestens zwei bevollmächtigte Vertreter des GWA erfolgen und DARF hierbei von einer durch die **SEN.CA** autorisierten RA-FirstLevel-Instanz durchgeführt werden.

Die **SEN.CA** RA-SecondLevel-Instanz MUSS die hierfür erforderlichen Prozessschritte überwachen und notwendige Unterlagen und Daten der Registrierung überprüfen und freigeben.

Die **SEN.CA** MUSS hierfür die erforderlichen Prozesse der RA-FirstLevel-Instanz bereitstellen.

Notwendige Unterlagen und Daten für die Registrierung sind:

- Antragsschreiben zur Ausgabe eines GWA-Zertifikats mit folgenden Daten bzw. beigefügten Informationen
 - 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
 - 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
- Persönliche/individuelle Zertifikate für die gesicherte E-Mail-Kommunikation der benannten Ansprechpartner (CS/MIME(GWA)) inklusive der zur Verifikation erforderlichen Zertifikatskette
- Nachweise über die Einhaltung der Vorgaben zu den Anforderungen für die Teilnahme an der **SEN.CA**
- Bestätigung der erfolgreichen Testteilnahme
 - Vor der Wirksamkeitsaufnahme MÜSSEN die Prozesse zum Zertifikatsmanagement, insbesondere Registrierung, Zertifikatsbeantragung, -erneuerung, -sperrung von GWA- und SMGW-Zertifikaten mit der **TEST-SEN.CA**, siehe Abschnitt 1.3.1, erfolgreich durchgeführt worden sein. Die erfolgreiche Teilnahme wird von einem Ansprechpartner der **SEN.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

 Stadtwerke Saarbrücken	Certificate Policy SEN.CA	Version: 3.0
		Seite: 29/99
SWIT- 1961468859- 1355		Gültig ab: 01.12.2022
Status: Freigegeben	Klassifizierung: Öffentlich	Druckdatum: 01.12.2022

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.

- Es wird EMPFOHLEN, Zertifikatsrequests **SEN.CA** vorab zuzusenden, so dass vor dem Termin eine Überprüfung auf Konformität erfolgen kann.
- Bei der Beauftragung eines Dienstleisters MUSS zusätzlich eine Vollmacht zur Teilnahme an der **SEN.CA** eingereicht werden, welche folgende Angaben beinhaltet:
 - Unternehmensdaten des GWA
 - Kontaktdaten der gesetzlichen Vertretungsberechtigten des GWA
 - Unternehmensdaten des bevollmächtigten Dienstleisters
 - Kontaktdaten der gesetzlichen Vertretungsberechtigten des bevollmächtigten Dienstleisters
 - Benennung und Kontaktdaten der autorisierten Ansprechpartner
 - Handlungsbevollmächtigung für die definierten Prozesse

3.2.2.4.GWH

Die detaillierten Prozesse zur Identifizierung, Registrierung und Zertifikatsbeantragung können der **SEN.CA** CPS entnommen werden.

Zur Aufnahme eines neuen GWH in die **SEN.CA** MUSS das Unternehmen authentifiziert werden, und mindestens zwei bevollmächtigte Vertreter des GWH MÜSSEN persönlich bei der RA der **SEN.CA** identifiziert und authentifiziert werden.

Notwendige Unterlagen und Daten für die Registrierung sind:

- Antragsschreiben zur Ausgabe eines GWH-Zertifikats mit folgenden Daten bzw. beigefügten Informationen
 - 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)
 - 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
- Persönliche/individuelle Zertifikate für die gesicherte E-Mail-Kommunikation der benannten Ansprechpartner (C_{S/MIME}(GWH)) inklusive der zur Verifikation erforderlichen Zertifikatskette
- der GWH MUSS eine Erklärung zur Einhaltung der Sicherheitsvorgaben aus dieser SM-PKI Policy für die Teilnahme an der SM-PKI (s. Tabelle 15) vorlegen.
- Bestätigung der erfolgreichen Testteilnahme
 - Vor der Wirksamkeitsaufnahme MÜSSEN die Prozesse zum Zertifikatsmanagement, insbesondere Registrierung, Zertifikatsbeantragung, -erneuerung, -sperrung von GWH und SMGW-Gütesiegelzertifikaten mit der Test-Sub-CA des ausgewählten Sub-CA Betreibers erfolgreich durchgeführt worden sein, siehe Abschnitt 1.3.1. Die erfolgreiche Teilnahme wird von einem Ansprechpartner der Test-SubCA per signierter E-Mail bestätigt.

 Stadtwerke Saarbrücken	Certificate Policy SEN.CA	Version: 3.0
		Seite: 30/99
SWIT- 1961468859- 1355		Gültig ab: 01.12.2022
Status: Freigegeben	Klassifizierung: Öffentlich	Druckdatum: 01.12.2022

- 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.
 - Es wird EMPFOHLEN, Zertifikatsrequests dem Sub-CA-Betreiber vorab zuzusenden, so dass vor dem Termin eine Überprüfung auf Konformität erfolgen kann.
- Bei der Beauftragung eines Dienstleisters MUSS zusätzlich eine Vollmacht zur Teilnahme an der **SEN.CA** eingereicht werden welche folgende Angaben beinhaltet:
 - Unternehmensdaten des GWH
 - Kontaktdaten der gesetzlichen Vertretungsberechtigten des GWH
 - Unternehmensdaten des bevollmächtigten Dienstleisters
 - Kontaktdaten der gesetzlichen Vertretungsberechtigten des bevollmächtigten Dienstleisters
 - Benennung und Kontaktdaten der autorisierten Ansprechpartner
 - Handlungsbevollmächtigung für die definierten Prozesse

3.2.2.5.SMGW

Das SMGW kann selbst keine Zertifikate beantragen. Entsprechend beantragt eine dritte Partei stellvertretend für das SMGW die Zertifikate, siehe BSI TR03109-4. Hierbei wird zwischen der Beantragung der Gütesiegelzertifikate und der Zertifikate für die Wirkumgebung unterschieden.

- Im Rahmen der Produktion werden durch den GWH gemäß den definierten und geprüften Prozessen Gütesiegelzertifikate aufgebracht, welche in den nachfolgenden Prozessen zur Verifikation der Komponente verwendet werden (siehe Anforderungen in Abschnitt 8.1.).
- Bei der Integration des SMGWs in die Wirkumgebung MÜSSEN die Gütesiegelzertifikate vom GWA durch Wirkzertifikate ersetzt werden.

Aufbringen der Gütesiegelzertifikate

Grundvoraussetzung für das Aufbringen von Gütesiegel-Zertifikaten ist, dass der GWH bei der **SEN.CA** registriert ist und über gültige Zertifikate verfügt, siehe Abschnitt 3.2.2.3. Dabei MÜSSEN die Anforderungen aus Tabelle 15 eingehalten werden.

Der GWH ist für die Einhaltung der Rahmenbedingungen verantwortlich und MUSS den Prozess gemäß den Vorgaben nachvollziehbar dokumentieren.

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 (siehe BSI TR-03109-4). Das sogenannte Zertifikatsrequest-Paket wird mit dem C_{Sig}(GWH) signiert und an die **SEN.CA** über einen gesicherten Kommunikationskanal gesendet (Autorisierungssignatur, vgl. BSI TR-03109-4).

 Stadtwerke Saarbrücken	Certificate Policy SEN.CA	Version: 3.0
		Seite: 31/99
SWIT- 1961468859- 1355		Gültig ab: 01.12.2022
Status: Freigegeben	Klassifizierung: Öffentlich	Druckdatum: 01.12.2022

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

Austausch der Gütesiegelzertifikate gegen Wirkzertifikate

Grundvoraussetzung für den Austausch der Gütesiegelzertifikate gegen Wirkzertifikate ist, dass der für das SMGW zuständige GWA bei der **SEN.CA** registriert ist und über gültige Zertifikate verfügt, siehe Abschnitt 3.2.2.2.

Bei den SMGWs sind die Gütesiegelzertifikate im Rahmen der Personalisierung nach der BSI 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 eines sicheren TLS-Kanals zwischen SMGW und GWA unter Zuhilfenahme der aufgetragenen TLS-Gütesiegelzertifikate.
- Generierung neuer SMGW-Schlüsselpaare für TLS, Signatur und Verschlüsselung durch das Sicherheitsmodul des SMGW.
- Generierung der Zertifikatsrequests durch das SMGW gemäß BSI TR-03109-4. Die Zertifikatsrequests MÜSSEN mit einer äußeren Signatur gemäß BSI 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 Zertifikate beantragt werden.
- Der GWA erzeugt aus den drei Zertifikatsrequests und weiteren relevanten Daten ein Zertifikatsrequest-Paket, welches dann mit dem $C_{sig}(GWA)$ signiert wird (Autorisierungssignatur, siehe BSI TR-03109-4). Durch diese Signatur autorisiert der GWA die Beantragung.
- Das signierte Zertifikatsrequest-Paket MUSS über die per TLS-Kanal gesicherte Web-Service-Schnittstelle an die SEN.CA gesendet werden.
- Die Authentizität des Zertifikatsrequest-Pakets MUSS durch die **SEN.CA** geprüft werden siehe BSI TR-03109-4. Es DÜRFEN ausschließlich für authentische SMGWs Zertifikate ausgestellt werden, deren Beantragung durch den zugehörigen GWA autorisiert wurde.
- Die Zertifikate werden von der **SEN.CA** erzeugt und über die Web-Service-Schnittstelle an den GWA übertragen.
- Der GWA prüft die Zertifikate und installiert diese auf dem SMGW, vgl. BSI TR-03109-4.

3.2.3. Anforderungen zur Identifizierung und Authentifizierung des Zertifikats-Antragstellers

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

 Stadtwerke Saarbrücken	Certificate Policy SEN.CA	Version: 3.0
		Seite: 32/99
SWIT- 1961468859- 1355		Gültig ab: 01.12.2022
Status: Freigegeben	Klassifizierung: Öffentlich	Druckdatum: 01.12.2022

3.2.4. Ungeprüfte Angaben zum Zertifikatsnehmer

Die Registrierungsstelle MUSS die Angaben zum Zertifikatsnehmer im Zertifikatsrequest gegen die eingereichten Unterlagen auf Korrektheit prüfen siehe **SEN.CA** CPS Abschnitt 3.2.2.

3.2.5. Prüfung der Berechtigung zur Antragsstellung

Siehe Abschnitt 3.2.

3.2.6. Kriterien für den Einsatz interoperierender Systeme / Einheiten

Die für die Interoperation von wesentlichen Diensten, z. B. Registrierung und Zertifizierung, zugrunde gelegten Kriterien dürfen das Ergebnis der zweifelsfreien Identifizierung, z. B. in Form von eindeutigen Registrierungsdaten, nicht beeinträchtigen. Dies gilt für alle Betriebsprozesse, die Abschnitt 3.2 betreffen.

3.2.7. Aktualisierung / Anpassung der Zertifizierungsinformationen der Teilnehmer

Die für die Teilnehmer an der **SEN.CA** geforderten Zertifizierungen nach Tabelle 15 unterliegen in der Regel einem jährlichen Überwachungszyklus, für das z.B. ein Audit positiv abgeschlossen werden muss.

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

Sollte der Teilnehmer die Zertifizierung nicht mehr erhalten, MUSS / MÜSSEN das Zertifikat / die Zertifikate aus der **SEN.CA** gesperrt werden. Die Sperrung von systemrelevanten Zertifikaten erfolgt nur mit Abstimmung der ROOT.

Informationen über relevante Änderungen, die beispielsweise

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

erfordern, MUSS der Zertifikatsnehmer unverzüglich inklusive der entsprechenden Informationen und besonders die Ergebnisse der Zertifizierung **SEN.CA** zur Verfügung stellen.

Die **SEN.CA** MUSS anschließend die entsprechenden Registrierungsdaten zu dem jeweiligen Teilnehmer aktualisieren.

3.2.8. Aktualisierung / Anpassung der Registrierungsdaten der Teilnehmer

Jeder Teilnehmer MUSS der **SEN.CA** unverzüglich mitteilen, falls sich Änderungen bzgl. seiner Registrierungsdaten ergeben vgl. Abschnitt 4.7. Ergänzend SOLL die **SEN.CA** regelmäßig, z.B. jährliches Intervall, über die Ansprechpartner bei den Klienten anfragen ob Änderungen an den Registrierungsdaten vorliegen.

 Stadtwerke Saarbrücken	Certificate Policy SEN.CA	Version: 3.0
		Seite: 33/99
SWIT- 1961468859- 1355		Gültig ab: 01.12.2022
Status: Freigegeben	Klassifizierung: Öffentlich	Druckdatum: 01.12.2022

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

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

Bei einer Schlüsselerneuerung d.h. einem Folgeantrag zu einem bestehenden Zertifikat, ist zu beachten, dass von dem Antragsteller immer ein neuer Schlüssel erstellt werden **MUSS**.

Ein Zertifikatsinhaber ist dafür verantwortlich, rechtzeitig, d.h. vor dem Ablauf der von ihm betreuten Zertifikate, neue Zertifikate zu beantragen vgl. BSI TR-03109-4. Dies **MUSS** insbesondere bei den Gütesiegelzertifikaten und Wirkzertifikaten für SMGWs beachtet werden. Der Zeitraum **MUSS** so gewählt werden, dass die neuen Zertifikate rechtzeitig in die Systeme eingebracht werden können, so dass der Betrieb ohne Beeinträchtigungen fortgeführt werden kann. Beim GWA, GWH und EMT kann es nach der Ausstellung des neuen Zertifikats zu einem temporären Betrieb mit zwei gleichzeitig gültigen Zertifikaten kommen. Diese Phase dient dazu, allen relevanten Komponenten rechtzeitig das neue Zertifikat mitzuteilen.

Diese **SEN.CA** CP unterscheidet zwei Arten von Folgeanträgen, die nachfolgend beschrieben werden.

Der Antragsteller besitzt einen privaten Schlüssel des dem Betreiber zugeordneten TLS-Zertifikats, mit dem die Absicherung des Kommunikationskanals durchgeführt wird. Das Zertifikat zu diesem Schlüssel darf weder gesperrt noch abgelaufen sein. Der zu übermittelnde Zertifikatsrequest unabhängig von dem Zertifikatstyp bzw. das Zertifikatsrequest-Paket ist mit dem zuletzt gültigen Signaturschlüssel signiert worden, und das zugehörige Zertifikat ist noch gültig und nicht gesperrt.

Bei den SMGWs werden die Folgeanträge durch den GWA gestellt. Die Absicherung der Zertifikatsrequests erfolgt dabei über dessen TLS-Zertifikat und durch die Signatur mit seinem Signaturschlüssel siehe BSI TR-03109-4 (Autorisierungssignatur). Überdies **MUSS** über die äußere Signatur die Echtheit des SMGW nachgewiesen werden, siehe BSI TR-03109-4.


Nach der erfolgreichen Prüfung eines routinemäßigen Folgeantrags erfolgt die Ausstellung des beantragten Zertifikats.

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

3.4.1. Allgemeines

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

- der Antragssteller besitzt kein gültiges TLS-Zertifikat für die Beantragung
- der Zertifikatsrequest ist nicht mit der gültigen Signatur des vorherigen Signaturschlüssels versehen vgl. BSI TR 03109-4 (äußere Signatur).

 Stadtwerke Saarbrücken	Certificate Policy SEN.CA	Version: 3.0
		Seite: 34/99
SWIT- 1961468859- 1355		Gültig ab: 01.12.2022
Status: Freigegeben	Klassifizierung: Öffentlich	Druckdatum: 01.12.2022

Ist eine der beiden Absicherungen eines routinemäßigen Folgeantrags nicht gegeben KANN der vorher beschriebene Regelprozess nicht genutzt werden. Die weitere Vorgehensweise unterscheidet sich anhand der dem Antragsteller zu diesem Zeitpunkt noch zur Verfügung stehenden Sicherheitsmechanismen.

Beide Absicherungen fehlen

Sind beide Absicherungen d.h. gültiges TLS-Zertifikat und gültige äußere Signatur, nicht gegeben, MUSS ein neues initiales Zertifikatsrequest-Paket im Rahmen einer erneuten initialen Identifizierung des PKI-Teilnehmers vergleichbar Abschnitt 3.2 übergeben werden.

Ungültiges TLS-Zertifikat

Kann keine Authentifikation mittels des TLS-Zertifikats gegenüber der **SEN.CA** mehr erfolgen, MUSS die Übermittlung des Zertifikatsrequests über einen anderen gesicherten Kanal, z.B. eine verschlüsselte und signierte E-Mail des benannten ASP des Zertifikatsnehmers, durchgeführt werden. Bei der Beantragung MUSS immer auch ein neues TLS-Zertifikat beantragt werden. Dies ist auf Endnutzer-Ebene automatisch gegeben, da hier immer ein Zertifikatstripel beantragt wird. Durch die Erneuerung des TLS-Zertifikats müssen dann wieder routinemäßige Folgeanträge über die TLS-abgesicherten Webservice gestellt werden können. Die Beantragung von Zertifikaten MUSS, unabhängig vom Kommunikationskanal, immer über Zertifikatsrequest-Pakete gemäß BSI TR-03109-4 erfolgen.

Ungültige „Äußere Signatur“ (z.B. ungültiges Signatur-Zertifikat)

Kann die Autorisation des Zertifikatsrequests nicht mehr über Signatur mit einem vorherigen, noch gültigem Signaturschlüssel gegenüber der **SEN.CA** erfolgen, MUSS ein neues initiales Zertifikatsrequest-Paket übermittelt werden welches identisch mit dem Zertifikatsrequest bei der ersten Beantragung der Zertifikate ist.

Verfügt der PKI-Teilnehmer noch über ein gültiges TLS-Zertifikat, MUSS das neue initiale Zertifikatsrequest-Paket hiermit signiert und über einen gesicherten Kanal an die CA übermittelt werden. Dies KANN z.B. eine verschlüsselte und signierte E-Mail des benannten ASP des Zertifikatsnehmers sein.

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 binärcodierte Request-Datei gebildet, welche das Zertifikatsrequest-Paket gemäß TR-03109-4 enthält, und als base64-codierter Ausdruck in einer ISO 19005-1 konformen Datei versendet.

Nach einem positiven Abgleich des Hashwertes durch die Mitarbeiter der **SEN.CA** werden die Zertifikate zur Verfügung gestellt. Der erfolgreiche Abgleich des Hashwertes MUSS durch die **SEN.CA** mit Angabe der beteiligten Personen dokumentiert werden.

 Stadtwerke Saarbrücken	Certificate Policy SEN.CA	Version: 3.0
		Seite: 35/99
SWIT- 1961468859- 1355		Gültig ab: 01.12.2022
Status: Freigegeben	Klassifizierung: Öffentlich	Druckdatum: 01.12.2022

Sonderfall SMGW

Die beschriebenen Verfahren für einen nicht routinemäßigen Folgeantrag können nicht auf ein SMGW angewendet werden. Bei einem SMGW MUSS der entsprechende GWA darauf achten, dass diesen immer über gültige Zertifikate verfügt.

3.4.2. Schlüsselerneuerung nach Sperrung

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

3.5. Identifizierung und Authentifizierung von Anträgen auf Sperrungen

Die Sperrung eines Zertifikates kann von den folgenden Beteiligten initiiert werden:

- dem Zertifikatsinhaber
- dem Dienstleister des Zertifikatsinhabers
- der **SEN.CA**
- der ROOT CA

Bei einer Sperrung MÜSSEN dafür folgende Informationen übermittelt werden:


- Zertifikatstyp
- Identifier der **SEN.CA**
- Zertifikatsnummer d.h. der Wert des Felds "SerialNumber" des Zertifikats, siehe BSI TR-03109-4
- Sperrgrund für Sub-CA, GWA, GWH, EMT zwingend, für SMGW optional siehe Abschnitt 4.8
- Zeitpunkt, ab dem das Zertifikat als unsicher / gesperrt einzustufen ist; optional, nur wenn genauer Zeitpunkt bekannt ist. Wenn kein Zeitpunkt angegeben wird, wird das Zertifikat mit dem Zeitpunkt des Eintrages in die Sperrliste gesperrt.

3.5.1. Initiative des Zertifikatsinhabers

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

- eine Änderung der Zertifikatsdaten,
- eine Schlüsselkompromittierung oder
- die Einstellung des Betriebs.

Zur Einstellung von Sperranträgen stehen dem Zertifikatsinhaber zwei Wege zur Verfügung:

 Stadtwerke Saarbrücken	Certificate Policy SEN.CA	Version: 3.0
		Seite: 36/99
SWIT- 1961468859- 1355		Gültig ab: 01.12.2022
Status: Freigegeben	Klassifizierung: Öffentlich	Druckdatum: 01.12.2022

1. Hochladen / Ausfüllen des Sperrformulars im gesicherten **SEN.CA** Support Portal nach erfolgreicher Authentifizierung und Autorisierung. Hierbei wird der Antrag direkt in einem Supportticket erfasst und über die RA eindeutig dem Antragsteller zugeordnet.
2. Der Zertifikatsinhaber / benannte Ansprechpartner sendet eine mittels S/MIME (ASP) signierte E-Mail an den Betreiber der **SEN.CA**. Die Sperrung von systemrelevanten Zertifikaten erfolgt nur in Abstimmung mit der Root.

Der Betreiber (**SEN.CA**-Operator Rolle) prüft die Authentizität der Information und sperrt das Zertifikat.

Die Sperrung des jeweiligen Zertifikats wird über die Sperrliste der zuständigen CA veröffentlicht. Der Zertifikatsinhaber wird über den abgeschlossenen Sperrprozess per signierter E-Mail informiert.

Bei den SMGWs wird die Berechtigung zur Sperrung der Zertifikate von dem zuständigen GWH für Gütesiegelzertifikate bzw. GWA für Gütesiegel- und Wirkzertifikate, wahrgenommen. Der GWH überträgt den Besitz der Gütesiegel-Zertifikate an den entsprechenden GWA als neuer Besitzer des SMGW. Die Übergabe MUSS rechtssicher dokumentiert werden. Damit ein GWA ein Gütesiegel-Zertifikat sperren kann, MUSS dieser den Besitzübergang gegenüber der **SEN.CA** über diese Dokumentation nachweisen. Die Sperrung MUSS über die Web-Service-Schnittstelle der **SEN.CA** beantragt werden. Im Ausnahmefall, z.B. Web-Service-Schnittstelle steht nicht zur Verfügung, KANN dies auch über einen entsprechend abgesicherten, etablierten Kommunikationskanal, z.B. signierte E-Mail oder **SEN.CA** Support Portal, durchgeführt werden. Eine Sperrung eines SMGW MUSS immer als Paket erfolgen, siehe (Zertifikatstripel [TR-03109-4]). Eine Sperrung des jeweiligen Zertifikats MUSS über die Sperrliste der **SEN.CA** veröffentlicht werden. Der GWA als Zertifikatsverantwortlicher MUSS über den abgeschlossenen Sperrprozess informiert werden.

3.5.1.1. Verantwortlich für die Sperrung eines SMGW

Bei den SMGWs wird die Berechtigung zur Sperrung der Zertifikate von dem zuständigen GWH für Gütesiegelzertifikate bzw. GWA für Gütesiegel- und Wirkzertifikate wahrgenommen.

Ein GWA kann Gütesiegelzertifikate nur dann sperren, wenn seine technische Verantwortlichkeit für das betreffende SMGW in der **SEN.CA** registriert ist. Zur Durchführung dieser Registrierung KANN der GWH die Webservice-Schnittstelle der **SEN.CA** nutzen, alternativ kann er einen entsprechend abgesicherten, etablierten Kommunikationskanal, z.B. signierte E-Mail, verwenden.

Falls der GWH die Webservice-Schnittstelle nutzen möchte, erstellt er einen Datensatz gemäß [TR-03109-4], in welchem er eines oder mehrere SMGWs und den dafür zuständigen GWA benennt. Diesen Datensatz signiert er mit dem privaten Schlüssel von CSIG(GWH) und sendet ihn per Web-Service an die **SEN.CA**, von welcher er die Gütesiegelzertifikate bezogen hatte. Die Übertragung der technischen Verantwortlichkeit an den GWA ist mit sofortiger Wirkung gültig, sobald die **SEN.CA** den Datensatz erfolgreich verarbeitet hat.

Durch die Übertragung der technischen Verantwortlichkeit erhält der GWA die Berechtigung, die Gütesiegelzertifikate der betreffenden SMGWs zu sperren. Um Wirkzertifikate für das SMGW beantragen zu können, ist dieser Schritt nicht erforderlich.

 Stadtwerke Saarbrücken	Certificate Policy SEN.CA	Version: 3.0
		Seite: 37/99
SWIT- 1961468859- 1355		Gültig ab: 01.12.2022
Status: Freigegeben	Klassifizierung: Öffentlich	Druckdatum: 01.12.2022

Die Übertragung der technischen Verantwortlichkeit für SMGWs kann je SMGW nur einmalig vom zuständigen GWH initiiert werden.

Voraussetzung für die Übertragung der technischen Verantwortlichkeit ist, dass der GWH den GWA, an den übertragen werden soll, bei der **SEN-CA** bekannt gemacht hat, z.B. als Mitteilung der Kommunikationszertifikate der Ansprechpartner des GWA. Dies MUSS über einen sicheren Kommunikationskanal erfolgen. Der GWA MUSS von der **SEN.CA** informiert werden, sobald die Übertragung der Verantwortlichkeit abgeschlossen wurde.

3.5.1.2. Sperrung eines SMGW

Die Sperrung eines SMGW-Zertifikats MUSS über die Web-Service-Schnittstelle der **SEN.CA** als Paket beantragt werden (Zertifikatstripel, siehe [TR-03109-4]). Die **SEN.CA** MUSS bei der Bearbeitung von Sperranträgen für Gütesiegelzertifikate prüfen, ob der Absender und Unterzeichner des Sperrantrags für die zu sperrenden Zertifikate technisch verantwortlich ist. Wurde die technische Verantwortlichkeit für Gütesiegelzertifikate an einen GWA übertragen, so ist dieser alleinig sperrberechtigt. In allen anderen Fällen ist diejenige Instanz sperrberechtigt, die die Zertifikate beantragt hat.

Im Ausnahmefall wenn, z.B. die Web-Service-Schnittstelle nicht zur Verfügung steht, KANN die Sperrung auch über einen entsprechend abgesicherten, etablierten Kommunikationskanal erfolgen.


3.5.2. Initiative des Betreibers der Certificate Authority

Die **SEN.CA** hat die Aufgabe, bei erkannten Schwachstellen alle Tätigkeiten durchzuführen, welche die Integrität und Sicherheit der PKI sicherstellen. Die Schwachstellen sind direkt nach Bekanntwerden der SM-PKI Root zu melden. Die Einleitung weiterer Schritte ist ggf. in Absprache mit der SM-PKI Root vorzunehmen. Mögliche Gründe sind beispielsweise:

- ein erkannter Verstoß gegen Betriebsauflagen, insbesondere gegen die Anforderungen für die Teilnahme an der **SEN.CA** nach Tabelle 15: Anforderung für die Teilnahme an der **SEN.CA**,
- erkannte, erhebliche Schwächen in der eingesetzten Kryptographie oder Kryptoimplementierung
- Änderungen in den zentralen Vorgaben, z.B. der BSI TR-03109-4,
- Änderung der Zertifikatsdaten, z.B. des Organisationsnamens,
- eine erkannte Schlüsselkompromittierung oder
- die Einstellung des Betriebs bzw. die Außerbetriebnahme der betroffenen Komponente.

Sperrungen von Zertifikaten mit systemrelevanter Bedeutung - Sub-CA Zertifikat der **SEN.CA** und Zertifikat des GWA - MÜSSEN in Abstimmung mit der Root erfolgen.

Die Zertifikate eines SMGW, GWH oder eines EMT können in der eigenen Verantwortung durch die **SEN.CA** gesperrt werden. Sollten nach Ansicht der **SEN.CA** Sperrungen dieser Zertifikate systemrelevante Auswirkungen haben, MUSS sich die **SEN.CA** vorab mit der SM-PKI Root abstimmen.

 Stadtwerke Saarbrücken	Certificate Policy SEN.CA	Version: 3.0
		Seite: 38/99
SWIT- 1961468859- 1355		Gültig ab: 01.12.2022
Status: Freigegeben	Klassifizierung: Öffentlich	Druckdatum: 01.12.2022

Eine Sperrung des jeweiligen Zertifikats MUSS über die Sperrliste der **SEN.CA** veröffentlicht werden. Der Zertifikatsinhaber sowie die Root MÜSSEN im Fall von **SEN.CA** und GWA über den abgeschlossenen Sperrprozess informiert werden.

3.6. Identifizierung und Authentifizierung von Anträgen auf Suspendierung

Die Suspendierung der Wirk-Zertifikate eines SMGW MUSS vom zugehörigen GWA durchgeführt werden. Bei einer Suspendierung MÜSSEN dafür folgende Informationen an die **SEN.CA** übermittelt werden:

- Ausstellende Sub-CA
- Zertifikatsnummer, d.h. der Wert des Felds “SerialNumber“ des Zertifikats, siehe [BSI TR-03109-4]
- Der Sperrgrund „certificateHold“ gemäß [RFC5280]
- Begründung für die Suspendierung gemäß Abschnitt 4.8
- Die Suspendierung MUSS über die Web-Service-Schnittelle der **SEN.CA** beantragt werden. Im Ausnahmefall, z.B. wenn die Web-Service-Schnittstelle nicht zur Verfügung steht, kann dies auch über einen entsprechend abgesicherten, etablierten Kommunikationskanal, z.B. einer signierte E-Mail oder dem **SEN.CA** Support Portal, durchgeführt werden. Eine Suspendierung eines SMGW MUSS immer als Paket erfolgen, siehe [TR-03109-4].

Eine Suspendierung des jeweiligen Zertifikats MUSS über die Sperrliste der **SEN.CA** veröffentlicht werden. Der für das SMGW zuständige GWA MUSS über den abgeschlossenen Sperrprozess von der **SEN.CA** informiert werden; hierzu ist die Veröffentlichung der Sperrliste hinreichend.

4. Betriebsanforderungen für den Zertifikatslebenszyklus

4.1. Zertifikatsantrag

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

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

Für die gesicherte personenbezogene Kommunikation wird der Einsatz von $C_{S/MIME}(ASP)$ -Zertifikaten für alle beteiligten Parteien vorausgesetzt. Jegliche relevante personenbezogene Kommunikation MUSS verschlüsselt und signiert erfolgen. Für alle beteiligten Personen wird der Besitz von individuellen/personenbezogenen $C_{S/MIME}(ASP)$ -Zertifikaten vorausgesetzt.

E-Mails an zentrale Postfächer ohne sicherheitskritischen Inhalt KÖNNEN ggf. auch ohne Signatur und Verschlüsselung versendet werden.

 Stadtwerke Saarbrücken	Certificate Policy SEN.CA	Version: 3.0
		Seite: 39/99
SWIT- 1961468859- 1355		Gültig ab: 01.12.2022
Status: Freigegeben	Klassifizierung: Öffentlich	Druckdatum: 01.12.2022

4.1.1. Wer kann einen Zertifikatsantrag stellen?

Ein Zertifikatsrequest an die **SEN.CA** darf ausschließlich von einer Organisation gestellt werden. Befugte Organisationen sind GWA, GWH und EMT bzw. Dienstleister, die sich gemäß Abschnitt 3.2 gegenüber der **SEN.CA** identifiziert haben MÜSSEN.

Ein Endnutzer mit Ausnahme SMGW KANN, sofern erforderlich, weitere Zertifikate bzw. Zertifikatstriple, z.B. für Lastmanagement oder Ausfallsicherheit für sich beantragen, siehe [TR-03109-4].

Der Zertifikatsrequest MUSS als Folgeantrag unter Nutzung der vorhandenen Zertifikate bei der **SEN.CA** gestellt werden, siehe Abschnitt 3.3.

Die weiteren Zertifikate / Zertifikatstriple MÜSSEN eindeutig gekennzeichnet werden, siehe Anhang A – Namensschema.

Die Eindeutigkeit von Zertifikaten erfolgt aus der Kombination von Common Name, der Sequenznummer im Subject-DN, der Seriennummer des Zertifikats und dem Issuer-DN (Herausgeber/CA).

4.1.2. Beantragungsprozess und Zuständigkeiten

Für die Bearbeitung eines Zertifikatsantrags ist die Registration Authority (RA) der **SEN.CA** verantwortlich.

Die Kontaktadresse lautet wie folgt:

Organisation	Stadtwerke Saarbrücken GmbH
Adresse	Hohenzollernstraße 104 – 106 66117 Saarbrücken
Webseite	https://support.sen-cloud.de/SEN-PKI
eMail	trustcenter@sen-pki.de

4.2. Verarbeitung von initialen Zertifikatsanträgen

4.2.1. Durchführung der Identifizierung und Authentifizierung

Der Zertifikatsnehmer übergibt durch seinen benannten Ansprechpartner, je nach Definition im Abschnitt 3.2, die zur Teilnahme an der **SEN.CA** erforderlichen Unterlagen und Nachweise für die initiale Zertifikatsbeantragung an die RA der **SEN.CA** bzw. an die durch die **SEN.CA** autorisierte RA-FirstLevel-Instanz der **SEN.CA**.

Die RA-Mitarbeiter der **SEN.CA** bzw. die RA-Mitarbeiter der **SEN.CA** First-level-Instanz prüfen die eingereichten Dokumente / Nachweise und nehmen bei Bedarf die Identifizierung und

 Stadtwerke Saarbrücken	Certificate Policy SEN.CA	Version: 3.0
		Seite: 40/99
SWIT- 1961468859- 1355		Gültig ab: 01.12.2022
Status: Freigegeben	Klassifizierung: Öffentlich	Druckdatum: 01.12.2022

Authentifizierung der Ansprechpartner vor. Sollten die Unterlagen / Nachweise nicht vollständig oder fehlerhaft sein bzw. die Authentifizierung / Identifizierung fehlschlagen, informieren diese den ASP des Zertifikatsnehmers und fordern ihn zur Nachlieferung auf. Im Positivfall werden die Informationen zur Prüfung und Autorisierung an die nachgelagerte RA-SecondLevel-Instanz der **SEN.CA** weitergeleitet.

Jede erfolgreiche Identifizierung und Authentifizierung durch die **SEN.CA** RA-First-level-Instanz MUSS durch die nachgelagerte **SEN.CA** RA-SecondLevel-Instanz bestätigt werden.

Erst nach einer erfolgreichen Bestätigung der RA-SecondLevel-Instanz DARF die positive Bestätigungsnachricht an den Antragsteller weitergeleitet werden.

Die von der **SEN.CA** autorisierte RA-FirstLevel-Instanz dient ausschließlich der Prozessinitialisierung und der persönlichen vor Ort Identifizierung und Authentifizierung der bevollmächtigten Ansprechpartner des Antragsstellers.

Sollte einer der benannten und identifizierten Mitarbeiter ausscheiden und dadurch die Mindestanzahl der erforderlichen ASPs unterschritten werden, MUSS sich mindestens ein neuer Vertreter im Rahmen eines persönlichen Termins, vergleichbar dem im Abschnitt 3.2 beschriebenen Prozess, bei der Registration Authority der **SEN.CA** 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.

Bei allen Prozessen zur Beantragung, Ausgabe und Verwaltung der Zertifikate MUSS bei der **SEN.CA** 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. Dabei MÜSSEN die Prozessdaten ein vergleichbares Sicherheitsniveau gemäß dieser Certificate Policy aufweisen.

4.2.2. Annahme oder Ablehnung von initialen Zertifikatsanträgen

Die vorliegenden bzw. nachgelieferten Unterlagen / Nachweise werden von den RA-Mitarbeitern gegen die Vorgaben aus der **SEN.CA** CP geprüft.

Im Positivfall wird der Zertifikatsantrag formell freigegeben und der benannte Ansprechpartner per signierter E-Mail durch die **SEN.CA** darüber informiert.

Erfolgt die Überprüfung der Unterlagen / Nachweise durch eine von der **SEN.CA** autorisierte **SEN.CA** RA-FirstLevel-Instanz so DARF diese im Negativfall zur Nachlieferung von Unterlagen auffordern. Im Positivfall werden alle Unterlagen / Nachweise an die nachgelagerte **SEN.CA** RA-SecondLevel-Instanz zur Überprüfung/Bestätigung weitergeleitet.

Gegen eine Ablehnung des Teilnahmeantrags durch die RA-FirstLevel-Instanz der **SEN.CA** darf der Antragsteller begründeten Einspruch bei der **SEN.CA** erheben.

Jede Annahme von Teilnehmern der **SEN.CA** MUSS durch die RA-SecondLevel-Instanz der **SEN.CA** nach entsprechender Prüfung bestätigt/genehmigt werden.

 Stadtwerke Saarbrücken	Certificate Policy SEN.CA	Version: 3.0
		Seite: 41/99
SWIT- 1961468859- 1355		Gültig ab: 01.12.2022
Status: Freigegeben	Klassifizierung: Öffentlich	Druckdatum: 01.12.2022

Durch die RA der **SEN.CA** MÜSSEN 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 werden.

Im Negativfall MUSS der Zertifikatsantrag durch die **SEN.CA** formell abgelehnt und der benannte Ansprechpartner per signierter E-Mail über die Ablehnung, inkl. entsprechender Begründung, informiert werden. Der Beantragungsprozess ist mit diesem Schritt beendet und MUSS durch den Zertifikatsnehmer ggf. neu initiiert werden.

Sonderfall SMGW:

Die beschriebenen Verfahren für einen initialen Zertifikatsantrag können nicht auf ein SMGW angewendet werden. Bei einem SMGW MUSS der entsprechende GWA darauf achten, dass dieses immer über gültige Zertifikate verfügt. Initialanträge von SMGWs MÜSSEN an der **SEN.CA** über deren Webservice-Schnittstelle eingereicht werden. Es erfolgt keine Freigabe durch die **SEN.CA** und keine Benachrichtigung der benannten Ansprechpartner per signierter E-Mail.

4.2.3. Fristen für die Bearbeitung von Zertifikatsanträgen

Die in den nachfolgenden Absätzen 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.

4.2.3.1. Ausgabe von initialen Endnutzer-Zertifikaten

Die Bearbeitung der Zertifikatsanträge gliedert sich in folgende Arbeitsschritte:

 Stadtwerke Saarbrücken	Certificate Policy SEN.CA	Version: 3.0
		Seite: 42/99
SWIT- 1961468859- 1355		Gültig ab: 01.12.2022
Status: Freigegeben	Klassifizierung: Öffentlich	Druckdatum: 01.12.2022

Arbeitsschritt	Beschreibung des Arbeitsschrittes	Zeitraumen
1	Start des Beantragungsprozesses durch den Endnutzer (GWA, GWH oder EMT)	-
2	Kontaktaufnahme zur Terminvereinbarung durch die RA der SEN.CA	3 Arbeitstage (Die SEN.CA soll dabei einen Termin, für Arbeitsschritt 3, innerhalb der nachfolgenden 3 Arbeitstage ermöglichen)
3	Übergabe der Dokumente / Nachweise ggf. im Rahmen eines persönlichen Termins	-
4	Vorprüfung der Unterlagen und Rückmeldung an den Endnutzer	1 Kalenderwoche
5	Nachlieferungsfrist für den Antragsteller	6 Kalenderwochen
6	Prüfung der Unterlagen durch die SEN.CA inkl. Rückmeldung an den Endnutzer	1 Kalenderwoche
7	Ausstellung der Zertifikate für Endnutzer	2 Arbeitstage

Tabelle 8: Zeitablauf für die initiale Ausgabe von Endnutzer-Zertifikaten

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

4.2.4. Ausgabe von Zertifikaten

Folgende Zertifikate werden durch die **SEN.CA** über Web-Services bereitgestellt:

Zertifikat eines Zertifikatsteilnehmer	Signiert durch	Verwendungszweck
C_{TLS}(EMT) C_{TLS}(GWA) C_{TLS}(GWH) C_{TLS}(SMGW)	Privater Schlüssel zu C(Sub-CA)	Zertifikat des entsprechenden Endnutzers zur Authentisierung beim Kommunikationspartner und zum Aufbau eines TLS-Kanals. Das Zertifikat C _{TLS} (GWA) wird zudem auch für die Authentifikation am Sicherheitsmodul des SMGW verwendet.

Zertifikat eines Zertifikatsteilnehmer	Signiert durch	Verwendungszweck
C_{ENC}(EMT) C_{ENC}(GWA) C_{ENC}(GWH) C_{ENC}(SMGW)	Privater Schlüssel zu C(Sub-CA)	Zertifikat zur Verschlüsselung von Inhaltsdaten für den entsprechenden Endnutzer.
C_{SIG}(EMT) C_{SIG}(GWA) C_{SIG}(GWH) C_{SIG}(SMGW)	Privater Schlüssel zu C(Sub-CA)	Zertifikat zur Verifikation von Inhaltsdatensignaturen des entsprechenden Endnutzers.

Tabelle 9: Über Web-Services bereitgestellte Zertifikate

Die initialen Zertifikate **MÜSSEN**, Folgezertifikate **KÖNNEN** per E-Mail an den Ansprechpartner gesendet werden. Der Versand per E-Mail **KANN** unverschlüsselt erfolgen.

Die Ausgabe von SMGW-Zertifikaten erfolgt ausschließlich über die Web-Service-Schnittstelle.

Endnutzer-Zertifikaten werden, abgesehen von den initialen Zertifikaten, über die Web-Service-Schnittstelle ausgegeben. Folgezertifikate für datenumgangsberechtigte Marktteilnehmer können auch über weiter definierte Schnittstellen ausgegeben werden.

4.2.5. Benachrichtigung des Zertifikatsnehmers über die Ausgabe des Zertifikats

Der Ansprechpartner **MUSS** nach der Ausstellung eines initialen Zertifikats per E-Mail durch die **SEN.CA** informiert werden. Initiale Zertifikate werden als Anlage übermittelt.

4.3. Annahme von Zertifikaten

Bei den Endnutzer-Zertifikaten **MUSS** der Ansprechpartner des Zertifikatsnehmers bzw. des berechtigten Dienstleisters, nach Erhalt die Angaben im Zertifikat auf Korrektheit und Vollständigkeit prüfen. Um ein Zertifikat zurückzuweisen, **MUSS** der Ansprechpartner des Zertifikatsnehmers eine Nachricht an die **SEN.CA** 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 erfolgen, z.B. bei dem Erhalt oder der Einbringung der Zertifikate.

Für registrierte Ansprechpartner und Kunden wird unter der URL: <https://support.sen-cloud.de> ein **SEN.CA** Support Portal bereitgestellt. Folgende Prozesse sind hierüber abrufbar:

- Request Fulfilment (Service-Auftragsmanagement)
- Incident Management (IT-Störungsmanagement)

 Stadtwerke Saarbrücken	Certificate Policy SEN.CA	Version: 3.0
		Seite: 44/99
SWIT- 1961468859- 1355		Gültig ab: 01.12.2022
Status: Freigegeben	Klassifizierung: Öffentlich	Druckdatum: 01.12.2022

- Change Management (IT-Änderungsmanagement)
- Service Process Automation (Services zur Prozessautomatisierung)
- Service Reporting
- Service Statistik

4.3.1. Veröffentlichung von Zertifikaten durch die CA

Alle ausgestellten Zertifikate MÜSSEN direkt nach der Ausstellung in dem Verzeichnisdienst der **SEN.CA** veröffentlicht werden.

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 MÜSSEN gemäß ihrem Verwendungszweck eingesetzt werden, vgl. BSI TR-03109-4.

4.4.2. Verwendung des öffentlichen Schlüssels und des Zertifikats durch den Zertifikatsnutzer

Die Verwendung des öffentlichen Schlüssels und des Zertifikats MUSS gemäß BSI TR-03109-4 erfolgen.

4.5. Zertifikatserneuerung

Zertifikatserneuerung bedeutet das Ausstellen eines neuen Zertifikats für einen öffentlichen Schlüssel, der bereits zertifiziert wurde. Zertifikatserneuerungen DÜRFEN NICHT erfolgen.

4.6. Zertifizierung nach Schlüsselerneuerung

4.6.1. Bedingungen der Zertifizierung nach Schlüsselerneuerungen

Es gelten die Anforderungen aus Abschnitt 3.3.

4.6.2. Zulässige Antragsteller von Zertifikaten für Schlüsselerneuerungen

Jeder Teilnehmer der **SEN.CA** MUSS darauf achten, rechtzeitig vor Ablauf der Zertifikatslaufzeit ein neues Schlüsselpaar zu generieren und ein Zertifikat zu beantragen. Für ein SMGW MUSS dies vom zuständigen GWA durchgeführt werden.

4.6.3. Bearbeitung von Zertifikatsanträgen für Schlüsselerneuerungen

Es gibt zwei unterschiedliche Arten der Folgeanträge:

- Folgeanträge über eine automatisierte Web-Service-Schnittstelle, vgl. BSI TR-03109-4, oder

 Stadtwerke Saarbrücken	Certificate Policy SEN.CA	Version: 3.0
		Seite: 45/99
SWIT- 1961468859- 1355		Gültig ab: 01.12.2022
Status: Freigegeben	Klassifizierung: Öffentlich	Druckdatum: 01.12.2022

- Folgeanträge über eine abgesicherte E-Mail-Kommunikation

Folgeanträge über eine automatisierte Schnittstelle (synchron bzw. asynchron)

Hier wird über eine gesicherte TLS-Verbindung, siehe [TR-03116-3], ein Zertifikatsrequest gemäß [TR-03109-4] an die **SEN.CA** gesendet.

Die **SEN.CA** SOLLTE einen Zertifikatsrequest synchron beantworten, so dass die beantragten Zertifikate unmittelbar in der Response enthalten sind. Eine zeitverzögerte Zustellung der Zertifikate per Webservice KANN über einen asynchronen Callback erfolgen, sofern beide Kommunikationspartner dies unterstützen. Wenn der Antragssteller asynchrone Kommunikation mit **SEN.CA** durchführen möchte, MUSS der benannte Ansprechpartner des Antragsstellers der **SEN.CA** die hierfür erforderliche Web Service URL (WSDL-URL) per signierter E-Mail mitteilen.

Folgeanträge über eine abgesicherte E-Mail Kommunikation

Bei einem Folgeantrag über die E-Mail-Schnittstelle wird der Zertifikatsrequest gemäß BSI TR-03109-4 vom benannten Ansprechpartner des Zertifikatsnehmers an die **SEN.CA** in einer verschlüsselten und signierten E-Mail gesendet.

Unabhängig von der gewählten Kommunikationsverbindung wird bei einem routinemäßigen Antrag gemäß Abschnitt 3.3 gehandelt und das Zertifikat wird direkt ausgestellt. Bei einem nicht routinemäßigen Folgeantrag MUSS wie in Abschnitt 3.4 beschrieben verfahren werden.

4.6.4. Benachrichtigung des Zertifikatsnehmers über die Ausgabe eines Nachfolgezertifikats

Der Beantragende wird durch die Zustellung des Nachfolgezertifikats durch die **SEN.CA** informiert.

Die sonstigen Teilnehmer der PKI werden grundsätzlich nicht durch die **SEN.CA** individuell über die Ausgabe von Zertifikaten zur Schlüsselerneuerung informiert. Eine Benachrichtigung erfolgt nur über die Veröffentlichung im Verzeichnisdienst, siehe Abschnitt 4.6.7.


4.6.5. Verhalten für die Annahme von Zertifikaten für Schlüsselerneuerungen

Bei den GWA/GWH/EMT-Zertifikaten MUSS der Ansprechpartner des Zertifikatsnehmers nach Erhalt die Angaben im Zertifikat auf Korrektheit und Vollständigkeit prüfen. Um ein Zertifikat zurückzuweisen, MUSS der Ansprechpartner des Zertifikatsnehmers eine Nachricht an die **SEN.CA** 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 erfolgen, z.B. bei dem Erhalt oder der Einbringung der Zertifikate.

4.6.6. Veröffentlichung von Zertifikaten für Schlüsselerneuerungen durch die SEN.CA

Alle ausgestellten Zertifikate MÜSSEN unmittelbar nach der Ausstellung in dem Verzeichnisdienst der **SEN.CA** veröffentlicht werden.

 Stadtwerke Saarbrücken	Certificate Policy SEN.CA	Version: 3.0
		Seite: 46/99
SWIT- 1961468859- 1355		Gültig ab: 01.12.2022
Status: Freigegeben	Klassifizierung: Öffentlich	Druckdatum: 01.12.2022

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

Alle ausgestellten Zertifikate MÜSSEN unmittelbar nach der Ausstellung in dem Verzeichnisdienst der **SEN.CA** veröffentlicht werden.

4.7. Änderungen am Zertifikat

Änderungen an den Zertifikatsinhalten, abgesehen vom Schlüsselmaterial, sind nicht vorgesehen. Sollte sich Änderungsbedarf, z.B. durch eine Umfirmierung eines Zertifikatsnehmers, ergeben, MUSS ein neues initiales Zertifikat gemäß Abschnitt 3.2 beauftragt und das alte Zertifikat nach einer angemessenen Übergangsfrist durch die **SEN.CA** gesperrt werden.

4.8. Sperrung und Suspendierung von Zertifikaten

Die Initiierung der Sperrung eines Zertifikats kann durch den Zertifikatsnehmer, die **SEN.CA** und die SM-PKI Root eingeleitet werden. Die Sperrberechtigung für SMGW-Zertifikate liegt außerdem beim GWA bzw. vor der Übergabe beim GWH, vgl. Abschnitt 3.2.6.

4.8.1. Sperrung

Alle Zertifikate werden über die von der **SEN.CA** bereitgestellten Schnittstellen/Prozesse gesperrt. Eine Sperrung kann nicht zurückgenommen werden. Eine Ausnahme stellt der Spezialfall Suspendierung dar, siehe Abschnitt 4.8.2. Alle Sperrungen MÜSSEN unverzüglich durch die **SEN.CA** umgesetzt und in die neue Sperrlisten aufgenommen werden. Die Veröffentlichung erfolgt gemäß den Vorgaben der [TR-03109-4]. Ist dem Sperrenden der genaue Zeitpunkt für den Eintritt des Sperrgrundes bekannt, MUSS dieser bei der Sperrung angegebenen werden, ansonsten erfolgt der Eintrag in die Sperrliste ohne diesen Parameter. Alle Teilnehmer MÜSSEN gemäß den Vorgaben aus [TR-03109-4] immer die aktuelle Sperrliste verwenden. In besonderen Fällen, z.B. der Erstinbetriebnahme oder auf Aufforderung einer CA-Instanz, MÜSSEN neben den regelmäßigen Aktualisierungen auch neue Sperrlisten abgefragt werden.

Die Sperrung eines GWA-Zertifikates unterliegt einer besonderen Systemrelevanz und bedingt die Beteiligung der SM-PKI Root CA.

Hinweis: Die Aufforderung zur Sperrung oder Suspendierung eines Zertifikates sind meldepflichtige Ereignisse. Es gelten die Regelungen aus Abschnitt 5.2.10.

Notwendige Angaben für die Sperrung von Zertifikaten in der **SEN.CA** sind:

- Unternehmensdaten
- Kontaktdaten eines bevollmächtigten Ansprechpartners
- Angaben zum Zertifikat
 - Zu sperrendes Zertifikat (SerialNumber)
 - Fingerabdruck des Zertifikat
- Zertifikatstyp (GWA/GWH/EMT/SMGW Güte- oder Wirkzertifikat)
- Sperrgrund

 Stadtwerke Saarbrücken	Certificate Policy SEN.CA	Version: 3.0
		Seite: 47/99
SWIT- 1961468859- 1355		Gültig ab: 01.12.2022
Status: Freigegeben	Klassifizierung: Öffentlich	Druckdatum: 01.12.2022

- Änderungen der Zertifikatsdaten
- Schlüsselkompromittierung oder sicherheitsrelevanter Vorfall, siehe Abschnitt 5.2.10
 - Was wurde kompromittiert bzw. was wurde betroffen?
 - Wann ist das Vorkommnis passiert bzw. wann wurde der Vorfall bemerkt?
 - Wer hat das Vorkommnis festgestellt?
 - Ort des Vorkommnisses
 - Wie ist das Vorkommnis vermutlich abgelaufen?
 - Wenn schon eine Maßnahme durchgeführt wurde: Welche Maßnahmen wurden schon eingeleitet?
- Einstellen des Betrieb
- Sonstige

4.8.2. Sperrung und Suspendierung von SMGW-Zertifikaten

Bei SMGW-Wirkzertifikaten, nicht jedoch bei SMGW-Gütesiegelzertifikaten, kann alternativ zu einer Sperrung auch eine Suspendierung erfolgen, vgl. Abschnitt 3.6. Die Suspendierung stellt einen Spezialfall der Sperrung dar. Suspendierte Zertifikate werden in die Sperrliste aufgenommen und speziell gekennzeichnet, siehe [TR-03109-4]. Bei diesen Zertifikaten kann die Sperrung innerhalb eines begrenzten Zeitraums vorübergehend wieder zurückgenommen werden, um neue Zertifikate zu erhalten und somit wieder in den Wirkbetrieb aufgenommen zu werden.

Eine Sperrung MUSS gemäß den Vorgaben in Abschnitt 4.8.1 verarbeitet werden und wird, z.B. bei der Außerbetriebnahme des SMGW, durchgeführt.

Initiiert der Zertifikatsnehmer eine Suspendierung, so MUSS er dies an einen Ansprechpartner der **SEN.CA** mittels signierter E-Mail als Sicherheitsvorfall melden, siehe auch Abschnitt 5.2.10. Hierbei MUSS der Grund für die Suspendierung genannt werden. Die **SEN.CA** MUSS diese Begründung dokumentieren. Dies gilt auch für Suspendierungen, welche über die Webservice-Schnittstelle in Auftrag gegeben wurden.

Eine Suspendierung von SMGW-Zertifikaten wird beispielsweise bei unklaren Sachverhalten genutzt, wenn die Vertrauenswürdigkeit eines SMGW in Frage gestellt wird. Liegen belastbare Erkenntnisse vor, dass das SMGW nicht mehr vertrauenswürdig ist, MUSS die Kennzeichnung als „suspendiert“ in der Sperrliste entfernt werden, siehe [TR-03109-4]. Eine Rücknahme der Sperrung ist dann nicht mehr möglich. Eine Suspendierung ermöglicht eine Prüfung, inwieweit das betroffene Gerät weiter verwendet werden kann.

Im Positivfall d.h. ein SMGW ist weiterhin vertrauenswürdig, KANN der GWA innerhalb der in Abschnitt 4.8.2.1 definierten Frist die Suspendierung zurücknehmen, um anschließend mittels Zertifikatsrequest neue Zertifikate für das SMGW beantragen zu können. Dabei werden die suspendierten Zertifikate für die Neubeantragung temporär von der Sperrliste entfernt. Die Rücknahme der Suspendierung erfolgt, ebenso wie die Suspendierung, durch den GWA über die von der **SEN.CA** angebotene Schnittstelle, d.h. Webservice oder alternativ durch per S/MIME verschlüsselte und signierte E-Mail. Anschließend MUSS der GWA sicherstellen, dass die - vorübergehend wieder gültigen- SMGW-Zertifikate ausschließlich für die Neubeantragung

 Stadtwerke Saarbrücken	Certificate Policy SEN.CA	Version: 3.0
		Seite: 48/99
SWIT- 1961468859- 1355		Gültig ab: 01.12.2022
Status: Freigegeben	Klassifizierung: Öffentlich	Druckdatum: 01.12.2022

verwendet werden. Sobald die neuen Zertifikate auf dem SMGW installiert sind, MUSS der GWA die alten Zertifikate endgültig sperren lassen, so dass diese wieder in die Sperrliste eingetragen werden.

Die **SEN.CA** MUSS bei der Verarbeitung des Zertifikatsrequests

– die Signatur des GWA als Nachweis für die Rechtmäßigkeit zur Ausgabe der neuen Zertifikate und

– die Signatur des SMGW als Nachweis, dass das Gerät neue Zertifikate beziehen darf, prüfen.

Sind die Bedingungen erfüllt, werden die neuen Zertifikate erstellt und sind durch den GWA in das SMGW einzubringen. Der Entscheidungsprozess für die Beauftragung der neuen Zertifikate MUSS vom GWA sorgfältig und nachvollziehbar dokumentiert werden.

Dieser Zusatzschritt wird bei den SMGW vorgenommen, um ggf. einen zum Zeitpunkt des Auftretens nicht nachweisbaren Verdacht des Verlusts der Vertrauenswürdigkeit des SMGW-Zertifikats innerhalb eines angemessenen Zeitraums untersuchen zu können.

Suspendierte Zertifikate MÜSSEN von allen Teilnehmern der **SEN.CA** als gesperrte Zertifikate behandelt werden.

4.8.2.1. Maximale Dauer einer Suspendierung

Die maximale Dauer einer Suspendierung beträgt 30 Tage.

Unabhängig von der Klärung der Vertrauenswürdigkeit des SMGW durch den GWA, unabhängig von einer eventuellen Rücknahme der Suspendierung und unabhängig von der Beantragung neuer SMGW-Zertifikate MUSS die **SEN.CA** einmal suspendierte SMGW-Zertifikate nach Ablauf dieses Zeitraums endgültig sperren, sofern der GWA dies nicht zwischenzeitlich selbst veranlasst hat. Die Kennzeichnung in der Sperrliste als „suspendiert“ entfällt dabei.

Wurde ein SMGW, dessen Zertifikate suspendiert worden sind, bis zum Fristablauf nicht mit neuen Zertifikaten versorgt, DÜRFEN KEINE neuen Zertifikate für dieses SMGW mehr ausgestellt werden.

4.8.3. Aktualisierung und Prüfzeiten bei Sperrung

In der folgenden Tabelle sind die minimal erforderlichen Aktualisierungs- und Prüfungszeiten der Sperrlisten für die **SEN.CA** definiert. Es wird zwischen regelmäßigen Aktualisierungen, verursacht durch den Ablauf der Gültigkeitszeit einer Sperrliste, und anlassbezogenen Aktualisierungen, verursacht durch die Sperrung von Zertifikaten, unterschieden. Voraussetzung für die anlassbezogene Aktualisierung ist, dass die CA, wie in Tabelle 10 definiert, erreichbar ist.

Nach Eintreffen eines Antrags für eine Sperrung MUSS dieser von der **SEN.CA** unverzüglich geprüft werden. Ist der Antrag valide MUSS dieser zeitlich, wie in Tabelle 10 definiert, umgesetzt werden.

Die Gültigkeit einer Sperrliste darf max. 3 Tage länger sein, als das in Tabelle 10 definierte Aktualisierungsintervall.

 Stadtwerke Saarbrücken	Certificate Policy SEN.CA	Version: 3.0
		Seite: 49/99
SWIT- 1961468859- 1355		Gültig ab: 01.12.2022
Status: Freigegeben	Klassifizierung: Öffentlich	Druckdatum: 01.12.2022

Sollte eine Sperrliste nicht verfügbar bzw. abrufbar sein, MUSS ersatzweise mit der zuletzt bekannten Sperrliste weitergeprüft werden. Die **SEN.CA** MUSS hierüber unverzüglich, über Kontaktadresse in dieser CP, informiert werden. Diese MUSS dann auf anderem Wege eine aktuelle Sperrliste zur Verfügung stellen. Steht nach 3 Tagen immer noch keine aktualisierte Sperrliste zur Verfügung, MUSS die **SEN.CA** die Root-CA informieren.

PKI Teilnehmer	Regelmäßige Aktualisierung der Sperrliste	Erreichbarkeit für Sperrungen	Anlassbezogene Aktualisierung der Sperrliste	Abruf der Sperrliste	Prüfung der Zertifikate auf Sperrung
Sub-CA	Innerhalb von 7 Tagen	Täglich	Unverzüglich	Täglich	Täglich
Endnutzer (außer SMGW)	Entfällt (Erstellt keine Sperrliste)	Entfällt	Entfällt (Erstellt keine Sperrliste)	Täglich	Bei jeder Verwendung
Endnutzer SMGW	Entfällt (Erstellt keine Sperrliste)	Entfällt	Entfällt (Erstellt keine Sperrliste)	Täglich durch GWA bzw. anlassbezogen	Täglich durch GWA bzw. anlassbezogen

Tabelle 10: Zeitliche Anforderungen bei Sperrung

4.9. Service zur Statusabfrage von Zertifikaten


Für die **SEN.CA** ist kein OCSP-Dienst vorgesehen. Statusabfragen hinsichtlich einer Sperrung können über die entsprechende CRL erfolgen, siehe Abschnitt 2.2.

4.10. Beendigung der Teilnahme

Die Beendigung der Teilnahme eines Zertifikatsnehmers kann durch den Zertifikatsnehmer selbst oder die **SEN.CA** eingeleitet werden.

Die Beendigung gliedert sich in drei Schritte:

- Information der Zertifikatsnutzer, die direkt von einer Beendigung der Teilnahme des Zertifikatsinhabers betroffen sind, durch den Zertifikatsinhaber oder Dienstleister. Es muss hierbei durch den Zertifikatsinhaber jedes Unternehmen (EMT, GWH und GWA) informiert werden, welches im Rahmen der Nutzung der Zertifikate mit dem Zertifikatsinhaber oder Dienstleister in Kontakt stand.
- 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

 Stadtwerke Saarbrücken	Certificate Policy SEN.CA	Version: 3.0
		Seite: 50/99
SWIT- 1961468859- 1355		Gültig ab: 01.12.2022
Status: Freigegeben	Klassifizierung: Öffentlich	Druckdatum: 01.12.2022

ist die Sperrung von Zertifikaten aufgrund von Gefahren für den sicheren Betrieb der **SEN.CA**.

- 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.

Bei der Außerbetriebnahme eines SMGWs MÜSSEN die Zertifikate des SMGW gesperrt werden. Die Sperrung MUSS der **SEN.CA** über deren Web-Service-Schnittelle mitgeteilt werden, siehe [TR-03109-4].

4.11. Hinterlegung und Wiederherstellung von Schlüsseln

Die **SEN.CA** KANN optional für ihre Teilnehmer eine Hinterlegung, z.B. für die Katastrophenfallvorsorge, gemäß den definierten Sicherheitsanforderungen durchführen. Der entsprechende Hinterlegungsprozess MUSS nachvollziehbar dokumentiert werden. Die entsprechenden Prozesse MÜSSEN in der **SEN.CA** CPS beschrieben sein.

 Stadtwerke Saarbrücken	Certificate Policy SEN.CA	Version: 3.0
		Seite: 51/99
SWIT- 1961468859- 1355		Gültig ab: 01.12.2022
Status: Freigegeben	Klassifizierung: Öffentlich	Druckdatum: 01.12.2022

5. Organisatorische, betriebliche und physikalische Sicherheitsanforderungen

Die **SEN.CA** CP spezifiziert technische und organisatorische Sicherheitsanforderungen an alle **SEN.CA** Teilnehmer, die im Kontext der SM-PKI relevant sind, um die Sicherheit der SM-PKI zu gewährleisten. Alle Teilnehmer der **SEN.CA** MÜSSEN die Sicherheitsvorgaben der **SEN.CA** CP beachten. Weiterführende rollenabhängige Sicherheitsanforderungen an die Teilnehmer der **SEN.CA** sind nicht Bestandteil der folgenden Betrachtung.

In der **SEN.CA** CP findet der Einsatz der Modalverben, wie in Abschnitt 1.1, beschrieben Verwendung.

Ein **MUSS** bedeutet demnach, dass es sich um eine normative Anforderung handelt, welche durch die **SEN.CA** entsprechend **umgesetzt wird**.

5.1. Generelle Sicherheitsanforderungen

In diesem Kapitel werden die generellen Sicherheitsanforderungen an die Teilnehmer der SM-PKI definiert. Diese bilden den Sicherheitsrahmen für alle SM-PKI Teilnehmer basierend auf den definierten Vorgaben der SM-PKI Root CA. Hierauf aufbauend werden in dieser **SEN.CA** CP ergänzende Sicherheitsanforderungen definiert.

Für die Einhaltung der generellen Sicherheitsanforderungen durch die **SEN.CA** ist die Zertifizierung nach ISO/IEC 27001 relevant. Voraussetzung zur Zertifizierung und Grundlage für einen Audit- und Zertifizierungsprozess, ist der Konformitätsnachweis nach TR-03145 welcher

1. der **SEN.CA** bescheinigt, dass die Vertrauenswürdigkeit der **SEN.CA** auf einem angemessenen Sicherheitsniveau organisatorische und technische Maßnahmen implementiert und Regeln für alle Teilnehmer aufstellt,
2. die Sicherheitsmaßnahmen der **SEN.CA** transparent dokumentiert werden, um Vertrauen aufzubauen.

Die TR-03145-1 beinhaltet hierbei generelle Anforderungen an die **SEN.CA**, welche eine Certification Authority mit Sicherheitslevel "hoch" betreiben.

Die **SEN.CA** ist entsprechend den Anforderungen der ISO/IEC 27001 sowie der BSI TR-03145 zertifiziert und erfüllt die in dieser Richtlinie definierten generellen Sicherheitsanforderungen. Die **SEN.CA** erfüllt somit die gestellten Anforderungen der Certificate Policy der Smart Meter PKI.

Die genaue Umsetzung der Maßnahmen welche zur Einhaltung der generellen Sicherheitsanforderungen durch den Betreiber der **SEN.CA** getroffen wurden, sind Bestandteil der **SEN.CA** CPS und den Dokumenten im ISMS (Informations-Sicherheits-Management-System) der **SEN.CA**.

5.1.1. Erforderliche Zertifizierungen der PKI-Teilnehmer

Nachfolgend werden die durch die PKI-Teilnehmer zu erbringenden Zertifizierungen aufgelistet.

 Stadtwerke Saarbrücken	Certificate Policy SEN.CA	Version: 3.0
		Seite: 52/99
SWIT- 1961468859- 1355		Gültig ab: 01.12.2022
Status: Freigegeben	Klassifizierung: Öffentlich	Druckdatum: 01.12.2022

SEN.CA: Die **SEN.CA** ist entsprechend den Anforderungen der ISO/IEC 27001:2013 sowie der BSI TR-03145 zertifiziert und erfüllt die in dieser Richtlinie definierten generellen Sicherheitsanforderungen.

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


GWA: Ein GWA MUSS alle Anforderungen gemäß BSI TR-03109-6 erfüllen und das entsprechende Zertifikat nachweisen.

SMGW: Ein SMGW MUSS über ein Common-Criteria-Zertifikat auf Basis von BSI-CC-PP-0073 verfügen.

Der Zeitpunkt zur Nachweispflicht hinsichtlich der Interoperabilität gemäß [TR-03109-1] wird durch das BSI festgelegt und im Gateway-Standardisierungsausschuss bekannt gegeben. Ein Nachweis zur Interoperabilität gemäß [TR-03109-1] MUSS ab diesem Zeitpunkt für ein SMGW vorhanden sein. Dieser Nachweis MUSS dem GWA vorgelegt werden.

EMT:

- **Passiver EMT:** Ein passiver EMT MUSS ein Sicherheitskonzept erstellen, in dem die Anforderungen aus dieser Certificate Policy berücksichtigt werden. Gegenüber der **SEN.CA** bestätigt er dieses im Rahmen des Registrierungsprozesses. Das Sicherheitskonzept MUSS NICHT als Nachweis des sicheren Betriebs, den Betreibern der **SEN.CA** vorgelegt werden. Das Sicherheitskonzept und die Umsetzung der Maßnahmen KANN im Schadensfall herangezogen werden.
 - Im Falle der Beauftragung eines Dienstleisters handelt dieser im Auftrag des datenumgangsberechtigten Marktteilnehmers (EMT) und nutzt dessen PKI-Zertifikat. Zwischen dem EMT und Dienstleister besteht ein Innenverhältnis. Beide kommunizieren über eine geschützte interne Infrastruktur, z.B. ein VPN. Die sichere Kommunikation zwischen EMT und Dienstleister MUSS dabei im Sicherheitskonzept des EMT definiert werden.
 - Sicherheitstechnisch muss die Weiterverarbeitung der Daten gleichwertig zur Authentisierung und Verschlüsselung mit den PKI-Zertifikaten aus der SM-PKI geschützt werden. Dies bedeutet insbesondere den Einsatz vergleichbarer Kryptographie, siehe Abschnitt 1.3.3.4.
- **Aktiver EMT:** Ein aktiver EMT, siehe Abschnitt 1.3.3.4, MUSS eine Zertifizierung gemäß [ISO/IEC 27001] vorweisen bzw. nachweisen, dass ein nach [ISO/IEC 27001] zertifizierter Dritter die Leistung für ihn erbringt. Bei einem Wechsel der Rollen zwischen aktiven und passiven EMT MUSS dieses rechtzeitig und eigenverantwortlich der **SEN.CA** angezeigt und die entsprechenden Prozesse durchlaufen werden, siehe Abschnitt 3.2.2.2.
 - Die Aufgaben des aktiven EMT dürfen erst vom Antragsteller mit den bestehenden Zertifikaten ausgeübt werden, wenn die erfolgreiche Registrierung als aktiver EMT von der **SEN.CA** bestätigt wurde. Die Bestätigung erfolgt per signierter E-Mail an den registrierten Ansprechpartner.

 Stadtwerke Saarbrücken	Certificate Policy SEN.CA	Version: 3.0
		Seite: 53/99
SWIT- 1961468859- 1355		Gültig ab: 01.12.2022
Status: Freigegeben	Klassifizierung: Öffentlich	Druckdatum: 01.12.2022

- Die zusätzlichen Auflagen für den Betrieb des aktiven EMT fallen erst weg, wenn der Rollenwechsel von der **SEN.CA** bestätigt wurde. Die Bestätigung erfolgt per signierter E-Mail an den registrierten Ansprechpartner.

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

Die Zertifizierung gemäß [ISO/IEC 27001] umfasst bei der **SEN.CA** alle Geschäftsprozesse und IT-Systeme des Registrierungs- und Zertifizierungsbetriebs der betreffenden PKI-Infrastruktur. Hierbei wird von einem hohen Schutzbedarf ausgegangen.

Bei einem aktiven EMT MUSS eine entsprechende Zertifizierung alle für die PKI relevanten Geschäftsprozesse und IT-Systeme, insbesondere hinsichtlich Beantragung, Empfang und Nutzung von Schlüsseln und Zertifikaten, umfassen.

Allgemein MUSS die Zertifizierung nach [ISO/IEC 27001] die Überprüfung beinhalten, dass alle Anforderungen aus [TR-03109-4] und aus der Certificate Policy der SM-PKI eingehalten werden.

Das Ergebnis MUSS im Auditbericht dokumentiert werden, damit es bei Bedarf vorgelegt werden kann. 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. Bei den Systemen der TEST-**SEN.CA** ist keine Zertifizierung entsprechend [ISO/IEC 27001] erforderlich, siehe CP-SM-PKI Anhang C.1.

5.2. Erweiterte Sicherheitsanforderungen

5.2.1. Betriebsumgebung und Betriebsabläufe

Nachfolgend werden die Anforderungen an eine sichere Betriebsumgebung und an sichere Betriebsabläufe der **SEN.CA**, GWH und EMT definiert. Entsprechende Anforderungen an den GWA sind in der BSI TR-03109-6 spezifiziert.

- **Objektschutz:** Die betrieblichen Prozesse MÜSSEN vor Störung geschützt werden.
- **Zutrittssicherheit:** Es MÜSSEN Vorkehrungen zur Sicherung des Zutritts vor Unbefugten zu den jeweiligen Betriebsräumen getroffen 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.

Für die **SEN.CA** gelten überdies die folgenden Anforderungen:

 Stadtwerke Saarbrücken	Certificate Policy SEN.CA	Version: 3.0
		Seite: 54/99
SWIT- 1961468859- 1355		Gültig ab: 01.12.2022
Status: Freigegeben	Klassifizierung: Öffentlich	Druckdatum: 01.12.2022

- **Brandschutz:** Es MÜSSEN bei der **SEN.CA** 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 der **SEN.CA** gewährleistet werden.
- **Wasserschaden:** Die IT-Infrastruktur SOLLTE bei der **SEN.CA** gegen das Eintreten eines Wasserschadens geschützt werden.
- **Notfall-Management und Wiederherstellung:** Die **SEN.CA** MUSS ihre Systeme durch Backup-Mechanismen sichern, um die Wiederherstellung des Betriebs nach einer Störung oder einem Notfall zu ermöglichen. Nur vertrauenswürdige Betriebspersonal DARF Backup- und Wiederherstellungsprozesse durchführen.

5.2.2. Verfahrensanweisungen

Für den Betrieb der **SEN.CA**, GWH, GWA und eines aktiven EMT 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.
- **Vertreterreglung:** 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. Die Rollen innerhalb der **SEN.CA** MÜSSEN im Benutzer-Rollen- und Rechtekonzept festgelegt sein.
- **Vier-Augen-Prinzip:** Kritische Vorgänge erfordern die Einhaltung des Vier-Augen-Prinzips. Nach Möglichkeit SOLL das Vier-Augen-Prinzip auch technisch durchgesetzt werden. Es MUSS immer dokumentiert werden, welche beiden Personen einen kritischen Vorgang durchgeführt haben.
- **Beschränkung der Anzahl an Mitarbeitern:** 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.

Informativ: Ein passiver EMT MUSS folgende der oben aufgeführten Verfahrensanweisungen umsetzen:

- **Einhaltung von Verpflichtungen**
- **Beschränkung der Anzahl an Mitarbeitern**
- **Eskalationsmanagement**

Informativ: Der Betrieb eines GWA MUSS gemäß [TR-03109-6] erfolgen und wird nicht in diesem Dokument beschrieben.

 Stadtwerke Saarbrücken	Certificate Policy SEN.CA	Version: 3.0
		Seite: 55/99
SWIT- 1961468859- 1355		Gültig ab: 01.12.2022
Status: Freigegeben	Klassifizierung: Öffentlich	Druckdatum: 01.12.2022

5.2.3. Personal

Der Betrieb der **SEN.CA**, GWH, GWA und EMT 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 Abschnitt 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 Aufgabentrennung, Mindestberechtigungen, Sicherheitsprüfungen sowie die 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/IEC 27001 durchführen.

Für den Betrieb der **SEN.CA** gilt darüber hinaus:

- **Qualifiziertes Personal:** Die **SEN.CA** MUSS Personal beschäftigen, welches über die erforderlichen Fachkenntnisse, Erfahrung und Qualifikation für das Aufgabenfeld und die angebotenen Dienste verfügt.
- **Sicherheitsüberprüfung:** Die **SEN.CA** MUSS sicherstellen, dass an kritischen und sicherheitsrelevanten Prozessen beteiligte Personen bezüglich der persönlichen Eignung geprüft und die Prüfung dokumentiert wurde.


Die Regelungen zum Personal eines GWA werden nicht innerhalb dieses Dokumentes beschrieben, da diese in der [TR-03109-6] enthalten sind.

5.2.4. Monitoring

Folgende Ereignisse MÜSSEN erkannt und aufgezeichnet bzw. dokumentiert werden:

SEN.CA:

- Die aus der ISO/IEC 27001 für den Betrieb, Prozesse und Infrastruktur relevanten Kontrollen.
- Schlüsselmanagement auf dem Kryptografiemodul, siehe Anhang C der SM-PKI Policy.
- Nutzung des privaten Schlüssels der **SEN.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/IEC 27001 nachgewiesen werden, siehe Anhang B der SM-PKI Policy.
- 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

 Stadtwerke Saarbrücken	Certificate Policy SEN.CA	Version: 3.0
		Seite: 56/99
SWIT- 1961468859- 1355		Gültig ab: 01.12.2022
Status: Freigegeben	Klassifizierung: Öffentlich	Druckdatum: 01.12.2022

Informativ: GWA:

- Durchführung der Überwachungsmaßnahmen gemäß BSI TR-03109-6
- Schlüsselmanagement auf dem Kryptografiemodul
- Direkter Zugriff auf das SecMod des SMGWS (External Authentication am SecMod)

Informativ: GWH:

- Schlüsselmanagement auf dem Kryptografiemodul
- Zertifikatsanträge von SMGWs für Gütesiegel-Zertifikate

Informativ: EMT:

- Schlüsselmanagement auf dem Kryptografiemodul
- EMT aktiv: Ansprechen und Steuern von Geräten über ein SMGW

5.2.5. Archivierung von Aufzeichnungen

Es MUSS sichergestellt sein, dass die Systeme über angemessene Archivierungsfunktionen verfügen. Die Zeiträume sind in Anhang B – Archivierung dokumentiert. Folgende Anforderungen MÜSSEN berücksichtigt werden:

SEN.CA:

- **Archivierung der öffentlichen Schlüssel:** Die Beteiligten MÜSSEN sicherstellen, dass die relevanten Informationen zu den öffentlichen Schlüsseln des Zertifikates archiviert werden.
- **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 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

 Stadtwerke Saarbrücken	Certificate Policy SEN.CA	Version: 3.0
		Seite: 57/99
SWIT- 1961468859- 1355		Gültig ab: 01.12.2022
Status: Freigegeben	Klassifizierung: Öffentlich	Druckdatum: 01.12.2022

- Erneuerung und Aktualisierung der öffentlichen Zertifikatsschlüssel
- Incident- oder Notfall-Management bezüglich zertifikatsrelevanter Vorfälle.
- **Verlorene Schlüssel / Zertifikate:** Daten von verbreiteten Schlüsseln / Zertifikaten DÜRFEN NICHT wiederhergestellt werden. Es MÜSSEN neue Schlüssel / Zertifikate beantragt werden.

Informativ: Ein GWA MUSS folgende der oben aufgeführten Verfahrensanweisungen umsetzen:

- **Zu archivierende Ereignisse im Kontext Kommunikation mit der SEN.CA:**
 - Zertifikatsbeantragung
 - Incident- oder Notfall-Management bezüglich zertifikatsrelevanter Vorfälle.

Informativ: Ein EMT MUSS folgende der oben aufgeführten Verfahrensanweisungen umsetzen:

- **Archivierung der öffentlichen Schlüssel**
- **Definition zu archivierender Informationen**
- **Zu archivierende Ereignisse**
 - Zertifikatsbeantragung
 - Incident- oder Notfall-Management bezüglich zertifikatsrelevanter Vorfälle.

5.2.6. Schlüsselwechsel einer Zertifizierungsstelle

Der Schlüsselwechsel der **SEN.CA** kann einerseits geplant und andererseits ungeplant erfolgen:

- **Geplanter Schlüsselwechsel:** Im Fall eines planbaren Schlüsselwechsels einer Zertifizierungsstelle MÜSSEN die gemäß der Certificate Policy der SM-PKI 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 definiert werden.
- Sowohl ein geplanter als auch ein ungeplanter Schlüsselwechsel einer Zertifizierungsstelle MUSS gemäß dem **Vier-Augen-Prinzip** erfolgen.

5.2.7. Auflösen der Zertifizierungsstelle

SEN.CA: Wenn die **SEN.CA** aufgelöst wird, MÜSSEN alle von ihr ausgestellten Zertifikate widerrufen werden. Insbesondere gelten folgende Anforderungen:

- **Übertragung der Aufgaben und Verpflichtungen:** Im Falle der Auflösung der **SEN.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:** Die **SEN.CA** MUSS im Falle ihrer Auflösung alle beteiligten Teilnehmer sowie weitere Organisationen, mit denen Vereinbarungen bestehen, vor der Kündigung der Dienstleistung rechtzeitig informieren.

 Stadtwerke Saarbrücken	Certificate Policy SEN.CA	Version: 3.0
		Seite: 58/99
SWIT- 1961468859- 1355		Gültig ab: 01.12.2022
Status: Freigegeben	Klassifizierung: Öffentlich	Druckdatum: 01.12.2022

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

5.2.8. Aufbewahrung der privaten Schlüssel

Alle Teilnehmer der **SEN.CA** MÜSSEN folgende Anforderung umsetzen:

- **Kryptografiemodule:** Die Schlüssel MÜSSEN in vertrauenswürdigen Kryptografiemodulen gespeichert werden, siehe Abschnitt 6.2. Wenn private Schlüssel der **SEN.CA**, GWA 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.


Die **SEN.CA**, GWH und EMT MÜSSEN sicherstellen, dass folgende Anforderungen umgesetzt werden. Die diesbezüglichen Anforderungen an die GWA sind Teil der BSI TR-03109-6 definiert.

- **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.
- **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.
- **Vertrauenswürdigen Personal:** Der private Schlüssel DARF NUR durch vertrauenswürdigen 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.

5.2.9. Behandlung von Vorfällen und Kompromittierung

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

- 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.

 Stadtwerke Saarbrücken	Certificate Policy SEN.CA	Version: 3.0
		Seite: 59/99
SWIT- 1961468859- 1355		Gültig ab: 01.12.2022
Status: Freigegeben	Klassifizierung: Öffentlich	Druckdatum: 01.12.2022

5.2.10. Meldepflichten

Bei Kompromittierung oder anderweitigen sicherheitsrelevanten Vorfällen MUSS eine Meldung aufbereitet und an die **SEN.CA** kommuniziert werden. Bei der Kompromittierung eines GWA MUSS zusätzlich durch die **SEN.CA** die Root informiert werden.

Folgende Vorkommnisse sind Beispiele für eine Meldepflicht:

Meldepflicht liegt auf Seiten des Zertifikatsnehmers:

- Kompromittierung des privaten Schlüsselmaterials
- Verstoß gegen relevante Betriebsauflagen
- Betreiber der **SEN.CA** ist nicht mehr aktiv
- 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?
- Wer hat das Vorkommnis festgestellt?
- Ort des Vorkommnisses
- Wie ist das Vorkommnis vermutlich abgelaufen?
- Wenn schon eine Maßnahme durchgeführt wurde: Welche Maßnahmen wurden schon eingeleitet?

EMT:

Ein EMT MUSS dem zugehörigen GWA mitteilen, wenn

- dieser Anomalien bei den von einem SMGW empfangen Daten feststellt, die auf eine Fehlfunktion oder Kompromittierung hindeuten könnten, oder
- dieser, auch wiederholt, unberechtigte Kommunikationsversuche von einem oder mehreren gesperrten SMGWs feststellt

5.3. Notfall-Management

Die **SEN.CA**, GWA, GWH und EMT 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 **SEN.CA** GWA und EMT 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, DARF KEIN Teilnehmer der **SEN.CA** dieses weiter nutzen.

 Stadtwerke Saarbrücken	Certificate Policy SEN.CA	Version: 3.0
		Seite: 60/99
SWIT- 1961468859- 1355		Gültig ab: 01.12.2022
Status: Freigegeben	Klassifizierung: Öffentlich	Druckdatum: 01.12.2022

- **Risikoreduktion / Schadensminderung:** Alle **SEN.CA** Teilnehmer SOLLTEN entsprechende Maßnahmen zur Minimierung von Risiken und Schäden anwenden.
- **Vermeidung von Vorfällen:** Alle **SEN.CA** Teilnehmer MÜSSEN angemessene Maßnahmen vorbereiten sowie die Ursachen von Vorfällen ermitteln, um diese in Zukunft zu vermeiden.
- **Notfallpläne:** Die **SEN.CA** und GWA MÜSSEN entsprechende Pläne vorbereiten, um die Geschäftsprozesse nach einem Notfall wiederherzustellen.
- **Backups:** Die **SEN.CA** und GWA MÜSSEN Backups von privaten und öffentlichen Schlüsseln, ausgestellten Zertifikaten und Sperrinformationen durchführen.
- **Vorgehen nach einer Störung:** Nach einer schweren Störung MÜSSEN alle **SEN.CA**-Teilnehmer sicherstellen, dass die entstandene Sicherheitslücke geschlossen wird.

6. Technische Sicherheitsanforderungen

Die detaillierten Maßnahmen welche zur Einhaltung der technischen Sicherheitsanforderungen durch die **SEN.CA** getroffen wurden sind Bestandteil der CPS und den Dokumenten des ISMS (Informations-Sicherheits-Management-Systems) der **SEN.CA**.

6.1. Erzeugung und Installation von Schlüsselpaaren

Jeder Zertifikatsnehmer MUSS sein eigenes Schlüsselpaar generieren.

Die technischen Anforderungen an die Erzeugung, Verwendung und Gültigkeit von Schlüsseln werden in der BSI TR-03109-4 beschrieben.

6.1.1. Generierung von Schlüsselpaaren für die Zertifikate

Die PKI-Teilnehmer **SEN.CA**, GWA und GWH MÜSSEN sicherstellen, dass folgende Anforderungen umgesetzt werden:

- **Generierung im Vier-Augen-Prinzip:** Das Schlüsselpaar MUSS während der Schlüsselzeremonie im Vier-Augen-Prinzip unter Teilnahme des für den Schlüssel verantwortlichen Mitarbeiters generiert werden.
- **Generierung eines Schlüsselpaars:** Die zur Schlüsselgenerierung eingesetzten Kryptografiemodule MÜSSEN je nach TYP entsprechend den in Abschnitt 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.

Der EMT MUSS nur folgende der oben aufgeführten Anforderungen bei der Generierung von Schlüsselpaaren umsetzen:

 Stadtwerke Saarbrücken	Certificate Policy SEN.CA	Version: 3.0
		Seite: 61/99
SWIT- 1961468859- 1355		Gültig ab: 01.12.2022
Status: Freigegeben	Klassifizierung: Öffentlich	Druckdatum: 01.12.2022

– **Generierung eines Schlüsselpaars**

6.1.2. Lieferung privater Schlüssel

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

6.1.3. Lieferung öffentlicher Zertifikate

Alle Zertifikate der **SEN.CA** werden in den jeweiligen Verzeichnissen abgelegt und sind somit für alle PKI-Teilnehmer zugänglich.


6.1.4. Schlüssellängen und kryptografische Algorithmen

Schlüssellängen und kryptografische Algorithmen der Schlüsselpaare MÜSSEN angemessene kryptografische Verfahren einhalten. Die zum jeweiligen Zeitpunkt konkret zu verwendenden kryptografischen Algorithmen und Schlüssellängen MÜSSEN der BSI TR-03116-3 entnommen werden.

Bei der Erzeugung und Nutzung von statischen und temporären Schlüsseln innerhalb der **SEN.CA** 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.

6.1.5. Festlegung der Parameter der Schlüssel und Qualitätskontrolle

- **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-Augen-Prinzip in ein neues KM nach angemessenen Maßnahmen zur sicheren Handhabung und Lagerung von Schlüsselmaterial importiert wird.
- **Schutz vor Angriffen 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

 Stadtwerke Saarbrücken	Certificate Policy SEN.CA	Version: 3.0
		Seite: 62/99
SWIT- 1961468859- 1355		Gültig ab: 01.12.2022
Status: Freigegeben	Klassifizierung: Öffentlich	Druckdatum: 01.12.2022

Algorithmen und Schlüssellängen MÜSSEN den jeweils aktuellen Empfehlungen aus der BSI TR-02102-1 entsprechen.

- Die Testteilnahme erfolgt auf Basis von **Testschlüsseln** der **Test-SEN.CA**, unter Einhaltung der Anforderungen an den Wirkbetrieb aus der BSI TR-03109-4 und dieser **SEN.CA** CP, siehe Abschnitt 1.3.1. Die verwendeten Testschlüssel werden ausschließlich für den Testbetrieb erzeugt und DÜRFEN NICHT im Wirkbetrieb des **SEN.CA** Umfeldes eingesetzt werden.

6.1.6. Verwendungszweck der Schlüssel

Die Schlüssel der **SEN.CA** DÜRFEN ausschließlich für die in Abschnitt 1.4.1 beschriebenen Verwendungszwecke eingesetzt werden. Der Verwendungszweck ist in der jeweils aktuellen Fassung der BSI TR-03109-4 konkretisiert.

6.2. Sicherung des privaten Schlüssels und Anforderungen an kryptografische Module

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

Neben dem Einsatz eines sicheren Kryptografiemodules MUSS auch ein sicherer Umgang mit den privaten Schlüsseln sichergestellt werden. Daher MÜSSEN die Anforderungen an den Lebenszyklus und die Einsatzumgebung aus [KeyLifecSec] – Security Level 2 mit Ausnahme SMGW eingehalten werden.

Die in diesem Kapitel definierten Anforderungen ergänzen die Anforderungen aus [KeyLifecSec]. Dabei gelten vorrangig die Vorgaben aus der Certificate Policy der SM-PKI.

Die Anforderung an Kryptografiemodule für den Einsatz in der **TEST-SEN.CA** ist in Anhang C der CP der SM-PKI definiert.

6.2.1. Mehrpersonen-Zugriffssicherung zu privaten Schlüsseln

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

6.2.2. Ablage privater Schlüssel

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.

 Stadtwerke Saarbrücken	Certificate Policy SEN.CA	Version: 3.0
		Seite: 63/99
SWIT- 1961468859- 1355		Gültig ab: 01.12.2022
Status: Freigegeben	Klassifizierung: Öffentlich	Druckdatum: 01.12.2022

6.2.3. Backup privater Schlüssel

Die **SEN.CA** und GWA MÜSSEN sicherstellen, dass Maßnahmen zum sicheren Backup der privaten Schlüssel umgesetzt werden. Insbesondere MÜSSEN folgende Anforderungen eingehalten werden:

- Die Vorgaben aus Abschnitt 6.2.5 **Transfer** privater Schlüssel in oder aus kryptografischen Modulen MÜSSEN eingehalten werden.
- **Bestandteil des ISMS nach ISO/IEC 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 Übertragung der Schlüssel auf ein weiteres HSM DÜRFEN genutzt werden, z.B. für ein Cold-Standby-Backup.
- **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.

Informativ: Es wird EMPFOHLEN, dass der EMT und der GWH ein Backup durchführen. Sobald ein Backup durchgeführt wird, SOLLTEN die vorstehenden Anforderungen eingehalten werden.

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 der BSI TR-02102-1 einzuhalten.
 - Die Nutzung des Dateicontainers erfordert den Import in ein Kryptografiemodul, das die Anforderungen aus Abschnitt 6.2 erfüllt.
 - 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-Kryptografiemodul MUSS auf das Betriebspersonal beschränkt sein.

 Stadtwerke Saarbrücken	Certificate Policy SEN.CA	Version: 3.0
		Seite: 64/99
SWIT- 1961468859- 1355		Gültig ab: 01.12.2022
Status: Freigegeben	Klassifizierung: Öffentlich	Druckdatum: 01.12.2022

6.2.4. Archivierung privater Schlüssel

Es wird keine Archivierung gesperrter oder abgelaufener privater Schlüssel durchgeführt. Die privaten Schlüssel der **SEN.CA** MÜSSEN unter Beachtung der Einschränkungen aus Abschnitt 6.2.9 zerstört werden.

6.2.5. Transfer privater Schlüssel in oder aus kryptografischen Modulen


- 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 des Transfers MUSS das Vier-Augen-Prinzip eingehalten werden.

6.2.6. Speicherung privater Schlüssel in kryptografischen Modulen

- Grundsätzlich MÜSSEN die privaten Schlüssel der **SEN.CA** auf einem Kryptografiemodul gespeichert werden.
 - Die einzige Ausnahme bilden die client- und serverseitigen TLS-Schlüssel der **SEN.CA** und Root-CA, die zur TLS-Authentisierung an der Web-Service-Schnittelle und am Verzeichnisdienst verwendet werden. Hier SOLLTE ein Kryptografiemodul eingesetzt werden.
- Informativ: Auf einem HSM DÜRFEN private Schlüssel von PKI-Teilnehmern derselben PKI-Rolle gespeichert werden. Dabei DÜRFEN mehrere CA-Schlüssel auf demselben HSM gespeichert werden. Die kryptografischen Schlüssel mehrerer Mandaten DÜRFEN auf einem Kryptografiemodul gespeichert werden, MÜSSEN jedoch logisch getrennt werden. Die Trennung der Schlüssel KANN durch einen Mechanismus des Kryptografiemoduls, z.B. eigene Partition / Slot, oder serverseitig auf Anwendungsebene über ein Berechtigungsmanagement erfolgen. Hierbei MUSS sichergestellt werden, dass ein Mandat ausschließlich auf seine Schlüssel zugreifen kann. Passiver EMT und aktiver EMT gehören beide zur PKI-Rolle EMT. Entsprechend können passive und aktive EMT-Schlüssel auf demselben HSM gespeichert werden.
- Informativ: Auf einem HSM DÜRFEN KEINE privaten Schlüssel von verschiedenen PKI-Rollen gespeichert werden. Es DARF KEINE Vermischung von Schlüsseln unterschiedlicher PKI-Rollen auf einem HSM erfolgen. Beispielsweise DÜRFEN KEINE CA- und GWA-Schlüssel auf demselben HSM gespeichert werden.
- Die privaten Schlüssel der **SEN.CA** aus einer Testumgebung MÜSSEN von der Produktivumgebung getrennt werden.

6.2.7. Aktivierung privater Schlüssel

Die Aktivierung eines Schlüssels der **SEN.CA** in einem Kryptografiemodul MUSS unter Einhaltung des Vier-Augen-Prinzips erfolgen.

 Stadtwerke Saarbrücken	Certificate Policy SEN.CA	Version: 3.0
		Seite: 65/99
SWIT- 1961468859- 1355		Gültig ab: 01.12.2022
Status: Freigegeben	Klassifizierung: Öffentlich	Druckdatum: 01.12.2022

6.2.8. Deaktivierung privater Schlüssel

Im deaktivierten Zustand DÜRFEN die Schlüssel der **SEN.CA** NICHT genutzt werden können.

6.2.9. Zerstörung privater Schlüssel

Die privaten Schlüssel der **SEN.CA** MÜSSEN in den folgenden Fällen sicher und unwiederherstellbar zerstört werden:

- Der Gültigkeitszeitraum des **SEN.CA**-Schlüssels ist abgelaufen
- Der Schlüssel der **SEN.CA** wurde gesperrt.

Die Backups der Schlüssel der **SEN.CA** MÜSSEN ebenfalls berücksichtigt werden.

Die Zerstörung der privaten Schlüssel der **SEN.CA** MUSS durch einen sicheren Löschanforderung Mechanismus im Kryptografiemodul 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 ebenfalls zerstört werden.

6.2.10. Beurteilung kryptografischer Module

Die Sicherheitsanforderungen an Kryptografiemodule zum Schutz der privaten Schlüssel zu den Zertifikaten der **SEN.CA** werden in Abschnitt 6.2 definiert.

Geltungsbereich: Alle PKI-Teilnehmer mit Ausnahme SMGW

Innerhalb der PKI können verschiedene Produktklassen von Kryptografiemodulen wie z.B. Hardware-Sicherheitsmodule (HSM), Chipkarten und Secure Elements eingesetzt werden, vgl. Kategorien der Schutzprofile in [KeyLifecSec]. Die SMGWs bzw. der Betrieb von SMGWs ist ausgenommen von den Anforderungen aus [KeyLifecSec].

Sicherheitsanforderungen

Um ein Kryptografiemodul in der **SEN.PKI** einsetzen zu können, MUSS dieses konform zu den Anforderungen an Kryptografiemodule aus [KeyLifecSec] – Security Level 2 sein. Ergänzend zu [KeyLifecSec] KANN für GWA, GWH und EMT auch ein Kryptografiemodul eingesetzt werden, das nach [BSI-CC-PP-0095] zertifiziert ist.

Hinsichtlich der Anforderungen an den Zufallsgenerator des Kryptografiemoduls gelten die Anforderungen aus [TR-03116-3].

Übergangsregelung

Die für ein Kryptografiemodul in Security Level 2 geforderte Zertifizierung KANN bis auf Widerruf alternativ durch die in Tabelle 11 und Tabelle 12 aufgeführten Nachweise erfüllt werden.

 Stadtwerke Saarbrücken	Certificate Policy SEN.CA	Version: 3.0
		Seite: 66/99
SWIT- 1961468859- 1355		Gültig ab: 01.12.2022
Status: Freigegeben	Klassifizierung: Öffentlich	Druckdatum: 01.12.2022

Bzgl. der Anforderungen wird insbesondere zwischen einer zertifizierten und einer nicht zertifizierten Einsatzumgebung unterschieden.

Bei einer zertifizierten Einsatzumgebung MÜSSEN die Anforderungen aus der SM-PKI Certificate Policy speziell hinsichtlich des Key-Lifecycle im ISMS berücksichtigt werden.


Zertifizierte Einsatzumgebung						
	EMT passiv	EMT aktiv	GWH	GWA	Sub-CA	Root
Anforderungen an die Betriebsumgebung	Siehe Tabelle 15	Siehe Tabelle 15	Siehe Tabelle 15	Siehe Tabelle 15	Siehe Tabelle 15	Siehe Tabelle 15
Nachweise	Erforderlichkeit					
Sicher Zufallszahlengenerator gemäß [TR-03116-3].	MUSS	MUSS	MUSS	MUSS	MUSS	MUSS
Tamper-Schutz gegen Attack Potential "moderate"	SOLLTE	SOLLTE	SOLLTE	SOLLTE	SOLLTE	MUSS
Seitenkanalresistenz gegen Attack Potential "moderate"	SOLLTE	SOLLTE	SOLLTE	SOLLTE	SOLLTE	MUSS

Tabelle 11: Übergangsregelungen Anforderungen HSM (zertifizierte Einsatzumgebung)

Nicht zertifizierte Einsatzumgebung						
	EMT passiv	EMT aktiv	GWH	GWA	Sub-CA	Root
Nachweise	Erforderlichkeit					
Sicher Zufallszahlengenerator gemäß [TR-03116-3].	MUSS	Entfällt	Entfällt	Entfällt	Entfällt	Entfällt
Tamper-Schutz gegen Attack Potential "moderate"	MUSS	Entfällt	Entfällt	Entfällt	Entfällt	Entfällt
Seitenkanalresistenz gegen Attack Potential "moderate"	MUSS	Entfällt	Entfällt	Entfällt	Entfällt	Entfällt

Tabelle 12: Übergangsregelungen Anforderungen HSM (nicht zertifizierte Einsatzumgebung)

Die in der Tabelle dargestellten Nachweise für eine Übergangslösung MÜSSEN jeweils durch eine durch das BSI für Common Criteria-Evaluierungen anerkannte Prüfstelle erbracht werden. Die

 Stadtwerke Saarbrücken	Certificate Policy SEN.CA	Version: 3.0
		Seite: 67/99
SWIT- 1961468859- 1355		Gültig ab: 01.12.2022
Status: Freigegeben	Klassifizierung: Öffentlich	Druckdatum: 01.12.2022

Prüfstelle MUSS in den letzten 5 Jahren mindestens die Prüfung eines Zufallszahlengenerators gemäß [AIS 20]/[AIS 31] im Rahmen eines CC-Zertifizierungsverfahrens erfolgreich abgeschlossen haben. Die Prüfungen werden eigenverantwortlich durch die Prüfstelle durchgeführt. Dabei kann die Prüfstelle für die Nachweise auch Ergebnisse heranziehen, die auf CC-Zertifizierungen des Kryptografiemoduls basieren, die nicht auf Grundlage eines Schutzprofils aus [KeyLifecSec] - Security Level 2 durchgeführt wurden.

Die **SEN.CA** MUSS für ihr Kryptografiemodul eine Bestätigung bzw. eine Sicherheitsaussage des Herstellers, dass diese Nachweise durch eine entsprechende Prüfstelle erbracht wurden, besitzen.

Das Vorhandensein der Bestätigung zu dem von der **SEN.CA** eingesetzten Kryptografiemodul MUSS durch den Auditor bei dem Audit der Einsatzumgebung geprüft werden, sofern eine Auditierung der Einsatzumgebung erforderlich ist.

Informativ: SMGW

Bei einem SMGW MUSS ein Kryptografiemodul eingesetzt werden, das nach [BSI-CC-PP-0077] zertifiziert ist.

6.3. Andere Aspekte des Managements von Schlüsselpaaren

6.3.1. Archivierung öffentlicher Schlüssel

Die Zertifikate eines Teilnehmers der **SEN.CA** MÜSSEN inklusive der Statusdaten archiviert werden, siehe Anhang B – Archivierung.

6.3.2. Gültigkeitszeitraum von Zertifikaten und Schlüsselpaaren

Der Gültigkeitszeitraum von Zertifikaten und Schlüsseln wird in der BSI TR-03109-4 definiert.

Unabhängig vom Gültigkeitszeitraum MÜSSEN die folgenden Zertifikate spätestens in dem hierzu angegebenen Intervall gewechselt werden.

Instanz	Zertifikat	Intervall
Root-CA Informativ	C(Root)	Alle 3 Jahre
	C _{CRL-S} (Root)	Alle 3 Jahre
	C _{TLS-S} (Root)	Alle 2 Jahre
SEN.CA	C(Sub-CA)	Alle 2 Jahre

Tabelle 13: Intervall Zertifikatswechsel bei einer CA

Sobald die **SEN.CA** über ein neues Zertifikat verfügt, MUSS dieses zum Ausstellen neuer Zertifikate und der zugehörigen Sperrlisten verwendet werden.

 Stadtwerke Saarbrücken	Certificate Policy SEN.CA	Version: 3.0
		Seite: 68/99
SWIT- 1961468859- 1355		Gültig ab: 01.12.2022
Status: Freigegeben	Klassifizierung: Öffentlich	Druckdatum: 01.12.2022

6.4. Aktivierungsdaten

Die Aktivierungsdaten für die Kryptografiemodule der **SEN.CA** MÜSSEN sicher aufbewahrt werden.

6.5. Sicherheitsanforderungen für die Rechneranlagen

Nachfolgend werden die Anforderung an die Rechneranlagen definiert, die von den jeweiligen PKI-Teilnehmern der **SEN.CA** umgesetzt werden MÜSSEN:

- **SEN.CA, GWH, EMT: Netzwerkkontrolle:** Es MÜSSEN entsprechende Maßnahmen umgesetzt werden, um das interne Netzwerk vom externen zu trennen und vor unbefugtem Zugriff zu schützen.
- **SEN.CA, aktive EMT: 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.
- **SEN.CA: System-Härtung:** 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.
- **SEN.CA: System-Konfiguration:** Die Konfigurationsoptionen und -einstellungen DÜRFEN nur die minimal benötigten Funktionalitäten für den CA Betrieb enthalten.
- **SEN.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.
- **SEN.CA: Vertraulichkeit und Integrität:** Die CA MUSS sensitive Daten vor unbefugtem Zugriff oder Veränderung schützen.
- **SEN.CA, GWH und EMT: Logging und Audit-Trails:** Log-Dateien und Audit-Trails MÜSSEN regelmäßig geprüft werden, und automatisierte Benachrichtigungen MÜSSEN auf Abweichung vom vorgesehenen Betrieb hinweisen.
- **SEN.CA: Speicherort von Log-Dateien:** Die Dateien der Audit-Trails SOLLEN NICHT auf dem CA-Server, der für die Verwaltung 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.
- **SEN.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 spezifischen Anforderungen an die Rechneranlagen eines GWA sind Teil der BSI TR-03109-6.

 Stadtwerke Saarbrücken	Certificate Policy SEN.CA	Version: 3.0
		Seite: 69/99
SWIT- 1961468859- 1355		Gültig ab: 01.12.2022
Status: Freigegeben	Klassifizierung: Öffentlich	Druckdatum: 01.12.2022

6.6. Zeitstempel

Keine Anforderungen an Zeitstempel.

6.7. Validierungsmodell

Die Anforderungen an die Zertifikatsvalidierung der **SEN.CA** MÜSSEN eingehalten werden und sind in der TR-03109-4 spezifiziert.

7. Profile für Zertifikate und Sperrlisten

7.1. Profile für Zertifikate und Zertifikatsrequests

Die Profile für die Zertifikate und die Zertifikatsrequests MÜSSEN durch die **SEN.CA** entsprechend den spezifizierten Vorgaben der BSI TR-03109-4 umgesetzt werden.

Das Namensschema zu den Zertifikaten ist in Anhang A – Namensschema definiert.

Die Struktur der Sperrlisten, das Sperrmanagement, z.B. Veröffentlichung, Aktualisierung und Sperrlistenvalidierung, werden in der jeweils aktuellen Fassung der BSI TR-03109-4 definiert und MÜSSEN in der **SEN.CA** angewendet werden.

7.1.1. Zugriffsrechte

Die erlaubte Funktion der Zertifikate wird über die Key-Usage-Extension definiert und MÜSSEN in der **SEN.CA** angewendet werden, siehe BSI TR-03109-4.

7.1.2. Zertifikatserweiterung

Die Certificate Extensions sind in der jeweils aktuellen Fassung der BSI TR-03109-4 definiert und MÜSSEN in der **SEN.CA** angewendet werden.

7.2. Profile für Sperrlisten

Die Anforderungen an die Sperrlisten bzw. CRL-Profile sind in der jeweils aktuellen Fassung der BSI TR-03109-4 definiert und MÜSSEN in der **SEN.CA** angewendet werden..

7.3. Profile für OCSP Dienste

In der **SEN.CA** werden keine OCSP-Dienste eingesetzt.

8. Überprüfung und andere Bewertungen

 Stadtwerke Saarbrücken	Certificate Policy SEN.CA	Version: 3.0
		Seite: 70/99
SWIT- 1961468859- 1355		Gültig ab: 01.12.2022
Status: Freigegeben	Klassifizierung: Öffentlich	Druckdatum: 01.12.2022


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

8.1. Inhalte, Häufigkeit und Methodik

8.1.1. Testbetrieb

Die **SEN.CA** stellt eine Testumgebung gemäß Abschnitt 1.3.1 zur Verfügung welche die Antragsteller der **SEN.CA** zum Test der Funktionalitäten ihrer PKI-Infrastruktur und –Prozesse durchlaufen MÜSSEN, bevor diese Teilnehmer der **SEN.CA** werden, siehe Abschnitt 3.2.

Testumgebung bereitgestellt durch	Nutzer	Zweck	Ergebnis
Root-CA Informativ	SEN.CA	Nachweis der vollständigen und korrekten Funktion der Zertifikatsantragsstellung und Zertifikatsannahme. Basis: Web-Service-Schnittstelle	Nach erfolgreichem Abschluss der Tests erfolgt die signierte Bestätigung der erfolgreichen bestandenen Tests durch die Root-CA
SEN.CA	GWA	Nachweis der vollständigen und korrekten Funktion der Zertifikatsantragsstellung und Zertifikatsannahme. Basis: Web-Service-Schnittstelle	Nach erfolgreichem Abschluss der Tests erfolgt die signierte Bestätigung der erfolgreichen bestandenen Tests durch die SEN.CA
	GWH	Nachweis der vollständigen und korrekten Funktion der Zertifikatsantragsstellung und Zertifikatsannahme. Basis: Web-Service-Schnittstelle	Nach erfolgreichem Abschluss der Tests erfolgt die signierte Bestätigung der erfolgreichen bestandenen Tests durch die SEN.CA
	EMT	Nachweis der Konformität des Zertifikatsrequests	Nach erfolgreicher Prüfung erfolgt die signierte Bestätigung per E-Mail der SEN.CA
	RA-FirstLevel-Instanz	Nachweis der vollständigen und korrekten Prozessschritte zur Identifizierung von Antragstellern	Nach erfolgreichem Abschluss der Tests erfolgt die signierte Bestätigung der erfolgreichen

 Stadtwerke Saarbrücken	Certificate Policy SEN.CA	Version: 3.0
		Seite: 71/99
SWIT- 1961468859- 1355		Gültig ab: 01.12.2022
Status: Freigegeben	Klassifizierung: Öffentlich	Druckdatum: 01.12.2022

		Basis: Support-Portal (ITSM-Portal*)	bestandenem Tests durch die SEN.CA
--	--	--------------------------------------	---

Tabelle 14: Testumgebungen

8.1.2. Beantragung der Teilnahme an der SEN.CA

Folgende Anforderungen **MÜSSEN** bei Beantragung der Teilnahme an der **SEN.CA** erfüllt werden, siehe Tabelle 15. Teilweise sind dazu vorab die in Abschnitt 8.1.1 aufgeführten Nachweise zu erbringen. Detaillierte Informationen sind in Abschnitt 5.1 definiert.

** Das Support Portal der **SEN.CA**, hier auch IT-Service Managementportal (ITSM-Portal) genannt, bietet für alle registrierten Servicenehmer der **SEN.CA** workflowbasierende Unterstützungsprozesse rund um die Services der **SEN.CA** welche im Rahmen der ISO/IEC 27001 Zertifizierung gemäß dem Best Practice nach ITIL Edition 2013 implementiert sind.*

**SWIT-
1961468859-
1355**
Certificate Policy SEN.CA

Gültig ab: 01.12.2022

Status: Freigegeben
Klassifizierung: Öffentlich

Druckdatum: 01.12.2022

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

Tabelle 15: Anforderung für die Teilnahme an der SEN.CA

 Stadtwerke Saarbrücken	Certificate Policy SEN.CA	Version: 3.0
		Seite: 73/99
SWIT- 1961468859- 1355		Gültig ab: 01.12.2022
Status: Freigegeben	Klassifizierung: Öffentlich	Druckdatum: 01.12.2022

8.1.3. Wirkbetrieb

Die vorausgesetzten Nachweise / Zertifizierungen aus Abschnitt 8.1.2 MÜSSEN im Wirkbetrieb auf Basis des jeweiligen Prüf- / Zertifizierungsschemas aufrechterhalten werden.

Sollte eine Zertifizierung nicht mehr gültig sein, MUSS dies der **SEN.CA** umgehend mitgeteilt werden, siehe Abschnitt 3.2.7.

Eine geänderte Version der Certificate Policy der **SEN.CA** MUSS veröffentlicht werden. Bei einer Änderung MUSS die Root hierüber über einen der benannten Ansprechpartner mittels verschlüsselter und signierter E-Mail informiert werden. Die aktuelle Certificate Policy der **SEN.CA** finden sie unter folgender URL: <https://support.sen-cloud.de/SEN-PKI>

8.2. Reaktionen auf identifizierte Vorfälle

Die Reaktionen auf identifizierte Vorfälle sind in Abschnitt 5.2.10 Meldepflichten definiert.

9. Sonstige finanzielle und rechtliche Regelungen

9.1. Preise

Es werden Gebühren zur Nutzung der **SEN.CA** erhoben.

9.1.1. Nutzungsentgelte für Zertifikatsausstellung und -erneuerung

Die Preise und Konditionen, der Service-Katalog und die Angebotsübersicht der Service Level sind im Dokument „Baseline der SEN-Cloud“ beschrieben.

9.1.2. Nutzungsentgelte für Zertifikate

Die Preise und Konditionen, der Service-Katalog und die Angebotsübersicht der Service Level sind im Dokument „Baseline der SEN-Cloud“ beschrieben.

9.1.3. Nutzungsentgelte für Sperr- oder Statusinformationen

Die Preise und Konditionen, der Service-Katalog und die Angebotsübersicht der Service Level sind im Dokument „Baseline der SEN-Cloud“ beschrieben.

9.1.4. Gebühren für andere Dienste

Die Preise und Konditionen, der Service-Katalog und die Angebotsübersicht der Service Level sind im Dokument „Baseline der SEN-Cloud“ beschrieben.

9.1.5. Rückerstattung

Eine Rückerstattung von Gebühren ist nicht vorgesehen.

 Stadtwerke Saarbrücken	Certificate Policy SEN.CA	Version: 3.0
		Seite: 74/99
SWIT- 1961468859- 1355		Gültig ab: 01.12.2022
Status: Freigegeben	Klassifizierung: Öffentlich	Druckdatum: 01.12.2022

9.2. Finanzielle Zuständigkeiten

Der Eigentümer der **SEN.CA** ist die co.met GmbH. Die co.met GmbH gehört als Tochtergesellschaft der Stadtwerke Saarbrücken GmbH mit 100% zum kommunalen Querverbund des Saarbrücker Stadtwerke-Konzerns und damit zur Unternehmensgruppe der Landeshauptstadt Saarbrücken. Der Sponsor und Betreiber der **SEN.CA** ist die Stadtwerke Saarbrücken GmbH. Die Stadtwerke Saarbrücken GmbH ist finanziell eigenständig und unabhängig. Sie sichert einen Betrieb unter den hier beschriebenen Rahmenbedingungen zu und sichert diese entsprechend durch Dritte ab. Sollte der Dienst durch den Betreiber nicht fortgeführt werden können, so wird eine Fortführung des PKI-Betriebs bis zum Auslauf aller Zertifikate zugesichert.

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

9.3. Vertraulichkeit von Geschäftsdaten

9.3.1. Geltungsbereich von vertraulichen Informationen

Alle Informationen und Daten über Zertifikatsnehmer und Teilnehmer der **SEN.CA**, die nicht unter Abschnitt 9.3.2 fallen, werden als vertrauliche Informationen eingestuft.

9.3.2. Informationen, die nicht zu den vertraulichen Informationen gehören

Alle Informationen die nicht als vertraulich definiert wurden, werden als öffentlich betrachtet.

Alle Informationen und Daten die in herausgegebenen Zertifikaten und Sperrlisten, explizit wie z.B. E-Mail-Adressen oder implizit wie z.B. Daten über die Zertifizierung, enthalten sind oder davon abgeleitet werden können, werden als nicht vertraulich eingestuft.

Veröffentlichte Zertifikate, die Certificate Policy der **SEN.CA** und Sperrinformationen gelten als öffentlich.

9.3.3. Zuständigkeit für den Schutz vertraulicher Informationen

Die **SEN.CA** trägt die Verantwortung für Maßnahmen zum Schutz vertraulicher Informationen. Daten dürfen im Rahmen der **SEN.CA** Dienstleistung nur weitergegeben werden, wenn zuvor eine Vertraulichkeitserklärung unterzeichnet wurde und die mit den Aufgaben betrauten Mitarbeiter auf Einhaltung der gesetzlichen Bestimmungen über den Datenschutz verpflichtet wurden.

9.4. Datenschutz und Personendaten

9.4.1. Richtlinie zur Verarbeitung personenbezogener Daten

Die **SEN.CA** MUSS zur Leistungserbringung personenbezogene Daten elektronisch speichern und verarbeiten. Dies MUSS in Übereinstimmung mit dem Datenschutzgesetz geschehen.

 Stadtwerke Saarbrücken	Certificate Policy SEN.CA	Version: 3.0
		Seite: 75/99
SWIT- 1961468859- 1355		Gültig ab: 01.12.2022
Status: Freigegeben	Klassifizierung: Öffentlich	Druckdatum: 01.12.2022

9.4.2. Vertraulich zu behandelnde Daten

Für personenbezogene Daten gelten die Regelungen aus Abschnitt 9.3.1 analog.

9.4.3. Nicht vertraulich zu behandelnde Daten

Für personenbezogene Daten gelten die Regelungen aus Abschnitt 9.3.2 analog.

9.4.4. Verantwortlicher Umgang mit personenbezogenen Daten

Die **SEN.CA** trägt die Verantwortung für Maßnahmen zum Schutz personenbezogener Daten.

9.4.5. Nutzung personenbezogener Daten

Der Zertifikatsnehmer stimmt der Nutzung von personenbezogenen Daten durch die **SEN.CA** zu, soweit dies zur Leistungserbringung erforderlich ist. Darüber hinaus können alle Informationen veröffentlicht werden, die als nicht vertraulich behandelt werden und deren Veröffentlichung nicht widersprochen wurde, siehe Abschnitt 9.3.2.

Dies ist durch **SEN.CA** über die Weitergabe der Geschäftsbedingungen für den PKI Dienst geklärt.

9.4.6. Offenlegung bei gerichtlicher Anordnung oder im Rahmen einer gerichtlichen Beweisführung


Die **SEN.CA** richtet sich bei der Speicherung und Verarbeitung von personenbezogenen Daten nach den gesetzlichen Datenschutzbestimmungen. Alle innerhalb der **SEN.CA** operierenden Teilnehmer unterliegen dem Recht der Bundesrepublik Deutschland und müssen vertrauliche und personenbezogene Informationen an staatliche Organe beim Vorliegen entsprechender Entscheidungen in Übereinstimmung mit den geltenden Gesetzen freigeben. Die Übergabe erfolgt durch bzw. nach Abstimmung mit der Juristischen Abteilung.

9.4.7. Andere Umstände einer Veröffentlichung

Es sind keine weiteren Umstände für eine Veröffentlichung vorgesehen.

9.5. Rechte am geistigen Eigentum

Die Stadtwerke Saarbrücken GmbH ist Urheber dieses Dokumentes. Die co.met GmbH hat als 100% Tochtergesellschaft der SW-GmbH für die Betriebsdauer der **SEN.CA** ein umfängliches Nutzungsrecht. Das Dokument KANN unverändert an Dritte weitergegeben werden.

 Stadtwerke Saarbrücken	Certificate Policy SEN.CA	Version: 3.0
		Seite: 76/99
SWIT- 1961468859- 1355		Gültig ab: 01.12.2022
Status: Freigegeben	Klassifizierung: Öffentlich	Druckdatum: 01.12.2022

9.6. Zusicherungen und Gewährleistungen

9.6.1. Zusicherungen und Gewährleistungen der CA

Die **SEN.CA** verpflichtet sich, den Bestimmungen dieser **SEN.CA** CP sowie der CP der Root-CA (SM-PKI) zu folgen. Weiter werden die Vorgaben aus BSI TR-03109 und TR-03145 umgesetzt und eingehalten.

9.6.2. Zusicherungen und Gewährleistungen der RA

Die **SEN.CA** sowie die in die Registrierung eingebundenen Stellen verpflichten sich, den Bestimmungen dieser **SEN.CA** CP zu folgen.

9.6.3. Zusicherungen und Gewährleistungen der Zertifikatsinhaber

Die Zertifikatsinhaber sichern zu, die in den Abschnitten 1.4 beschriebenen Regelungen einzuhalten.

9.6.4. Zusicherungen und Gewährleistungen der Zertifikatsnutzer

Die Zertifikatsnutzer sichern zu, die in den Abschnitten 1.4 beschriebenen Regelungen einzuhalten.

9.6.5. Zusicherungen und Gewährleistungen für weitere Teilnehmer

Von der **SEN.CA** beauftragte Dienstleister werden auf die Einhaltung dieser **SEN.CA** CP rechtssicher verpflichtet.

9.7. Gewährleistung

Die Stadtwerke Saarbrücken GmbH gewährleisten als Betreiber der **SEN.CA** als Bestandteil der SM-PKI des Bundes den ordnungsgemäßen Betrieb nach dieser Richtlinie und im Rahmen von BSI TR-03109 und TR-03145. Weiter werden die folgenden Verfügbarkeiten für die Dienste garantiert:

Es wird eine Verfügbarkeit gemäß dem vereinbarten SLA für die Betriebsphase gewährleistet.

9.8. Haftungsbeschränkungen

Verletzen die Stadtwerke Saarbrücken GmbH bei der Vertragsdurchführung schuldhaft eine vertragswesentliche Pflicht, die hierfür im Einzelfall von besonderer Bedeutung ist, so haften sie für den dadurch entstehenden Schaden. Bei einfacher Fahrlässigkeit ist die Haftung der Stadtwerke Saarbrücken GmbH auf den vertragstypischen Schaden beschränkt.

Für die Verletzung sonstiger Pflichten haften die Stadtwerke Saarbrücken GmbH nur bei grobem Verschulden. Gegenüber Kaufleuten und öffentlichen Verwaltungen gilt die Haftungsbeschränkung des Absatz 1 Satz 2 auch bei grober Fahrlässigkeit einfacher Erfüllungsgehilfen.

 Stadtwerke Saarbrücken	Certificate Policy SEN.CA	Version: 3.0
		Seite: 77/99
SWIT- 1961468859- 1355		Gültig ab: 01.12.2022
Status: Freigegeben	Klassifizierung: Öffentlich	Druckdatum: 01.12.2022

Vorstehende Haftungsausschlüsse und -begrenzungen finden keine Anwendung auf die Haftung für Schäden aus der Verletzung des Lebens, des Körpers oder der Gesundheit; insofern haftet die Stadtwerke Saarbrücken GmbH nach den gesetzlichen Bestimmungen.

Im Falle einer Haftung der Stadtwerke Saarbrücken GmbH nach den vorstehenden Absätzen bestimmt sich der Haftungsumfang entsprechend § 254 BGB danach, wie das Verschulden der Stadtwerke Saarbrücken GmbH im Verhältnis zu anderen Ursachen an der Entstehung des Schadens mitgewirkt hat.

9.9. Haftungsfreistellung

Bei der unsachgemäßen Verwendung des Zertifikats und dem zugehörigen privaten Schlüssel oder einer Verwendung des Schlüsselmaterials beruhend auf fälschlichen oder fehlerhaften Angaben bei der Beantragung sind die Stadtwerke Saarbrücken GmbH von der Haftung freigestellt.

9.10. Inkrafttreten und Aufhebung

9.10.1. Inkrafttreten

Die **SEN.CA** CP tritt an dem Tag in Kraft, an dem sie gemäß Kapitel 2 veröffentlicht wird. **SEN.CA** CP und **SEN.CA** CPS erhalten ihre Gültigkeit mit der Verabschiedung durch den PKI-Ausschuss. Die Gültigkeit einer **SEN.CA** CP / **SEN.CA** CPS erlischt mit der Verabschiedung und Veröffentlichung einer neuen Version.

9.10.2. Aufhebung

Dieses Dokument ist so lange gültig, bis es durch eine neue Version ersetzt wird oder der Betrieb der **SEN.CA** eingestellt wird.

9.10.3. Konsequenzen der Aufhebung

Von den Konsequenzen der Aufhebung dieser Richtlinie bleibt die Verantwortung zum Schutz vertraulicher Information und personenbezogener Daten unberührt. Alle Teilnehmerverträge bleiben weiterhin bestehen bis die Zertifikate gesperrt oder ausgelaufen sind.

9.11. Individuelle Mitteilungen und Absprachen mit Teilnehmern

9.12. Änderungen

9.12.1. Verfahren bei Änderungen

Änderungen der **SEN.CA** CP werden rechtzeitig vor ihrem Inkrafttreten veröffentlicht. Die **SEN.CA** CP wird jährlich vom PKI Ausschuss geprüft.

 Stadtwerke Saarbrücken	Certificate Policy SEN.CA	Version: 3.0
		Seite: 78/99
SWIT- 1961468859- 1355		Gültig ab: 01.12.2022
Status: Freigegeben	Klassifizierung: Öffentlich	Druckdatum: 01.12.2022

Änderungen werden durch die Veröffentlichung einer aktualisierten Version der **SEN.CA** CP im PKI-Repository kenntlich gemacht. Es bestehen Kontrollen, die gewährleisten, dass die **SEN.CA** CP nicht ohne die vorherige Genehmigung des PKI-Ausschusses veröffentlicht wird.

9.12.2. Benachrichtigungsmethode und -fristen

Die Zertifikatsnehmer werden rechtzeitig vor dem Inkrafttreten auf die Änderung der **SEN.CA** CP per signierter E-Mail hingewiesen. Die jeweils aktuelle vom PKI Ausschuss bestätigte Version ist im PKI Repository unter folgender Adresse veröffentlicht und einzusehen:

<https://support.sen-cloud.de/SEN-PKI>

Das Einverständnis des Ansprechpartners der **SEN.CA** mit den Änderungen gilt als erteilt, wenn der Betreiber bis zum Zeitpunkt des Inkrafttretens keine gegenteilige Erklärung mit signierter E-Mail zugeht. Auf diese Folge wird die **SEN.CA** bei dem Hinweis auf die Änderung besonders aufmerksam machen.

9.12.3. Bedingungen für die Änderung des Richtlinienbezeichners (OID)

Der Richtlinienbezeichner ändert sich bis zum Ende der Gültigkeit der zugehörigen Zertifizierungsinstanz nicht.

9.13. Bestimmungen zur Schlichtung von Streitfällen

Die Anrufung eines Schiedsverfahrens liegt im Ermessen der Stadtwerke Saarbrücken GmbH.

9.14. Gerichtsstand

Der Gerichtsstand ist Saarbrücken.

9.15. Einhaltung geltenden Rechts

Es gilt deutsches Recht. Die von der **SEN.CA** ausgestellten Zertifikate sind nicht konform zu qualifizierten Zertifikaten gemäß eIDAS-Verordnung – Signatur nach EU-Richtlinie.

9.16. Sonstige Bestimmungen

9.16.1. Vollständigkeitserklärung

Alle Regelungen in dieser **SEN.CA** CP gelten zwischen der **SEN.CA** und den Zertifikatsnehmern. Die Ausgabe einer neuen Version ersetzt alle vorherigen Versionen. Mündliche Vereinbarungen bzw. Nebenabreden sind nicht zulässig.

9.16.2. Abtretung der Rechte

Eine Abtretung von Rechten ist nicht vorgesehen.

 Stadtwerke Saarbrücken	Certificate Policy SEN.CA	Version: 3.0
		Seite: 79/99
SWIT- 1961468859- 1355		Gültig ab: 01.12.2022
Status: Freigegeben	Klassifizierung: Öffentlich	Druckdatum: 01.12.2022

9.16.3. Salvatorische Klausel

Sollten einzelne Bestimmungen dieser Zertifizierungsrichtlinie unwirksam sein oder werden, so lässt dies den übrigen Inhalt der Zertifizierungsrichtlinie unberührt. Auch eine Lücke berührt nicht die Wirksamkeit der Zertifizierungsrichtlinie im Übrigen. Anstelle der unwirksamen Bestimmung gilt diejenige wirksame Bestimmung als vereinbart, welche der ursprünglich gewollten am nächsten kommt oder nach Sinn und Zweck der Zertifizierungsrichtlinie geregelt worden wäre, sofern der Punkt bedacht worden wäre.


9.16.4. Rechtliche Auseinandersetzungen / Erfüllungsort

Rechtliche Auseinandersetzungen, die aus dem Betrieb der **SEN.CA** herrühren, obliegen den Gesetzen der Bundesrepublik Deutschland.

Erfüllungsort und Gerichtsstand ist der Sitz des Betreibers - Saarbrücken.

9.17. Andere Regelungen

Nicht zutreffend.

 Stadtwerke Saarbrücken	Certificate Policy SEN.CA	Version: 3.0
		Seite: 80/99
SWIT- 1961468859- 1355		Gültig ab: 01.12.2022
Status: Freigegeben	Klassifizierung: Öffentlich	Druckdatum: 01.12.2022

Anhang A – Namensschema

Die Common Names (CN) der verschiedenen SM-PKI Teilnehmer MÜSSEN folgendem Schema entsprechen:

,<org>.<function>[.<extension>]'

Durch die Registrierungsprozesse MUSS von den CAs sichergestellt werden, dass die PKI-Teilnehmer die Common Names (Funktionskennzeichnung ,<function>') entsprechend ihrer PKI-Rolle zugewiesen bekommen.

Eine **SEN.CA** MUSS sicherstellen, dass ein Common Name in Kombination mit der Sequenznummer unter dem Issuer Common Name der **SEN.CA** bei Endnutzer-Zertifikaten bzw. bei einem Zertifikatstripel ausschließlich einmal vergeben wird, um die Eindeutigkeit dieser Zertifikate in der SM-PKI zu gewährleisten. Des Weiteren MUSS die Root sicherstellen, dass jede Sub-CA einen anderen Common Name erhält.

Tabelle 16 beschreibt die Bestandteile der CN für die Teilnehmer der SM-PKI:

Namensteil	Bedeutung	Länge, Kodierung, Ausnahmen
<org>	Kürzel der Identität / Organisation	Länge max. 48 Zeichen, erstes Zeichen muss ein Buchstabe oder eine Ziffer sein.
<function>	Funktionskennzeichnung innerhalb der SM-PKI	Länge max. 4 Zeichen. Feste Werte: CA, EMT, GWA, GWH oder SMGW.
<extension>	Erweiterung, zusätzliche Informationen	Länge max. 10 Zeichen. Bezeichnung/Kürzel der RA-FirstLevel-Instanz . Zwingend vorgegebene Werte bei CA´s gemäß Tabelle 17(Root-CA) und Tabelle 22(Sub-CA).

Tabelle 16: Namensschema (Kodierung Common Name)

Grundsätzliche Festlegungen:

- Die Länge des CN ist auf 64 Zeichen begrenzt.
- Die Kodierung ist 'Printable String'.
- Die zulässigen Zeichen sind: „0...9“, „a...z“, „A...Z“, „-“ (keine Leerzeichen).
- Der Punkt („.“) ist ausschließlich als Trennzeichen zwischen den Namensteilen zulässig und MUSS bei Vorhandensein im Namen des Zertifikatsinhabers weggelassen oder durch ein „-“ ersetzt werden.
- Die Leserichtung ist von links nach rechts (parsen, z.B. nach dem ersten Punkt immer ,<function>').

**SWIT-
1961468859-
1355**
Certificate Policy SEN.CA

Gültig ab: 01.12.2022

Status: Freigegeben
Klassifizierung: Öffentlich

Druckdatum: 01.12.2022

– Für Endnutzer (GWH, GWA und EMT) SOLL auf Basis der <extension> eine bessere Unterscheidbarkeit der von Ihnen genutzten Zertifikate herbeigeführt werden. In dieser <extension> wird in den durch die **SEN.CA** ausgestellten Zertifikaten, die eindeutige Bezeichnung/Kürzel der **RA-FirstLevel-Instanz** hinterlegt.

Eine Erweiterung des Namensschemas ist möglich durch die Nutzung/Vorgabe weiterer Funktionsbezeichnungen und die Flexibilität der Nutzung der zusätzlichen Informationen in der optionalen Erweiterung.

Das Kürzel der Identität (<org>) wird in der **SEN.CA** durch den Zertifikatsinhaber festgelegt und sollte:

- kurz,
- sprechend (Identität erkennbar) und
- eindeutig

sein. Einen entsprechenden Vorschlag KANN der Zertifikatsinhaber bei der Antragstellung an die **SEN.CA** weiterleiten.

Ausnahmen bzw. Festlegungen für das Kürzel der Identität (<org>):

Root-CA: „SM-Root“

SMGW: Herstellerübergreifende Identifikationsnummer entsprechend [DIN 43863-5] und Codierung gemäß [TR-03109-1].

Die Zertifikate der Wirkumgebung haben das in den folgenden Tabellen angegebene Namensschema.

A.1 Root-CA (informell)

Die Zertifikate der Root-CA haben folgendes Namensschema:

C(Root) und Link-C(Root)

Attribut Typ	Kürzel	Vorgabe	Wert	Erläuterung
common name	CN	mandatory	“SM-Root.CA”	Name der Root-CA
organisation	O	mandatory	“SM-PKI-DE”	Name der PKI
organisational unit	OU	optional	“<Organisationseinheit>”	Name der Organisationseinheit
country	C	mandatory	“DE”	Ländercode
serial number	SERIAL NUMBER	mandatory	“<SN>”	Sequenznummer des Zertifikats im Bereich von 1 bis $2^{31}-1$. Diese wird bei jedem neuen Zertifikat um den Wert 1 hochgezählt.

 Stadtwerke Saarbrücken	Certificate Policy SEN.CA	Version: 3.0
		Seite: 82/99
SWIT- 1961468859- 1355		Gültig ab: 01.12.2022
Status: Freigegeben	Klassifizierung: Öffentlich	Druckdatum: 01.12.2022

Tabelle 17: Namensschema Zertifikat C(Root) und Link-C(Root)

C_{CRL-S}(Root)

Attribut Typ	Kürzel	Vorgabe	Wert	Erläuterung
common name	CN	mandatory	„SM-Root.CA.CRL-S“	Kennzeichnung als CRL-Signer
organisation	O	mandatory	„SM-PKI-DE“	Name der PKI
organisational unit	OU	optional	„<Organisationseinheit>“	Name der Organisationseinheit
country	C	mandatory	„DE“	Ländercode

Tabelle 18: Namensschema Zertifikat C_{CRL-S}(Root)

C_{TLS-S}(Root)

Attribut Typ	Kürzel	Vorgabe	Wert	Erläuterung
common name	CN	mandatory	„SM-Root.CA.TLS-S“	Kennzeichnung als TLS-Signer
organisation	O	mandatory	„SM-PKI-DE“	Name der PKI
organisational unit	OU	optional	„<Organisationseinheit>“	Name der Organisationseinheit
country	C	mandatory	„DE“	Ländercode
serial number	SERIAL NUMBER	mandatory	„<SN>“	Sequenznummer des Zertifikats im Bereich von 1 bis 2 ³¹ -1. Diese wird bei jedem neuen Zertifikat um den Wert 1 hochgezählt.

Tabelle 19: Namensschema Zertifikat C_{TLS-S}(Root)

C_{TLS}(Root)

Attribut Typ	Kürzel	Vorgabe	Wert	Erläuterung
common name	CN	mandatory	„SM-Root.CA.TLS“	Kennzeichnung als TLS-Zertifikat der Root
organisation	O	mandatory	„SM-PKI-DE“	Name der PKI
organisational unit	OU	optional	„<Organisationseinheit>“	Name der Organisationseinheit
country	C	mandatory	„DE“	Ländercode

 Stadtwerke Saarbrücken	Certificate Policy SEN.CA	Version: 3.0
		Seite: 83/99
SWIT- 1961468859- 1355		Gültig ab: 01.12.2022
Status: Freigegeben	Klassifizierung: Öffentlich	Druckdatum: 01.12.2022

serial number	SERIAL NUMBER	mandatory	„<SN>“	Sequenznummer des Zertifikats im Bereich von 1 bis $2^{31}-1$. Diese wird bei jedem neuen Zertifikat um den Wert 1 hochgezählt.
---------------	------------------	-----------	--------	--

Tabelle 20: Namensschema Zertifikat C_{TLS}(Root)

A.2 Sub-CA

Sub-CAs haben folgendes Namensschema:

Attribut Typ	Kürzel	Vorgabe	Wert	Erläuterung
common name	CN	mandatory	„<org>.CA“	Eindeutiger Name der Sub-CA.
organisation	O	mandatory	„SM-PKI-DE“	Name der PKI
organisational unit	OU	optional	„<Organisationseinheit>“	Name der Organisationseinheit
country	C	mandatory	<LC>	Zwei Zeichen Ländercode gemäß [ISO 3116 ALPHA-2]
serial number	SERIAL NUMBER	mandatory	„<SN>“	Sequenznummer des Zertifikats im Bereich von 1 bis $2^{32}-1$. Diese wird bei jedem neuen Zertifikat um den Wert 1 hochgezählt.
street	street	optional	„<Straße>“	Straße der Sub-CA
postal code	postal code	optional	„<PLZ>“	Postleitzahl der Sub-CA
locality	L	optional	„<Ortsname>“	Ortsname des Sub-CA-Inhaberstandortes
state	ST	optional	„<Bundesland>“	Bundesland des Sub-CA-Inhaberstandortes

Tabelle 21: Namensschema der Sub-CA-Zertifikate

Bei den TLS-Zertifikaten der Sub-CA MUSS der „common name“, entsprechend Tabelle 22 definiert und ergänzt werden. Die Unterscheidung, ob das Zertifikat von der Root oder der Sub-CA selbst ausgestellt wurde, erfolgt über den Issuer-DN im Zertifikat.

 Stadtwerke Saarbrücken	Certificate Policy SEN.CA	Version: 3.0
		Seite: 84/99
SWIT- 1961468859- 1355		Gültig ab: 01.12.2022
Status: Freigegeben	Klassifizierung: Öffentlich	Druckdatum: 01.12.2022

Zertifikat	Wert	Erläuterung
C _{TLS,Root} (Sub-CA)	„<org>.CA.TLS“	Kennzeichnung als TLS-Zertifikat der Sub-CA
C _{TLS} (Sub-CA)	„<org>.CA.TLS“	Kennzeichnung als TLS-Zertifikat der Sub CA

Tabelle 22: Erweiterung Common Name: TLS-Zertifikate Sub-CA

A.3 EMT

EMT haben folgendes Namensschema:

Attribut Typ	Kürzel	Vorgabe	Wert	Erläuterung
common name	CN	mandatory	„<org>.EMT.<RA-FirstLevel-Instanz >“	Eindeutiger Name der Organisation
organsiation	O	mandatory	“SM-PKI-DE”	Name der PKI
organisational unit	OU	mandatory	“<Organisationseinheit> = **Haupt-Mandant-Name “	Name der Organisationseinheit des **Haupt-Mandant
country	C	mandatory	<LC>	Zwei Zeichen Ländercode gemäß [ISO 3116 ALPHA-2]
serial number	SERIAL NUMBER	mandatory	“<SN>”	Sequenznummer des Zertifikats im Bereich von 1 bis 2 ³¹ -1. Diese wird bei jedem neuen Zertifikat um den Wert 1 hochgezählt.
street	street	optional	„<Straße>“	Straße des Zertifikatsinhabers
postal code	postal code	optional	„<PLZ>“	Postleitzahl des Zertifikatsinhabers
locality	L	optional	„<Ortsname>“	Ortsname des Zertifikatsinhabers
state	ST	optional	„<Bundesland>“	Bundesland des Zertifikatsinhabers

Tabelle 23: Namensschema der EMT-Zertifikate

****Als Haupt-Mandant (HM) wird in der SEN.CA ein Auftragnehmer (AN) bezeichnet welcher in seiner Funktion diese Dienstleistung für mehrere Mandanten (Zertifikatsnehmer) in einem Konsortium bereitstellt.**

 Stadtwerke Saarbrücken	Certificate Policy SEN.CA	Version: 3.0
		Seite: 85/99
SWIT- 1961468859- 1355		Gültig ab: 01.12.2022
Status: Freigegeben	Klassifizierung: Öffentlich	Druckdatum: 01.12.2022

A.4 GWA

Für GWAs gilt folgendes Namensschema:

Attribut Typ	Kürzel	Vorgabe	Wert	Erläuterung
common name	CN	mandatory	„<org>.GWA.<RA-FirstLevel-Instanz>“	Eindeutiger Name des GWA.
organsiation	O	mandatory	“SM-PKI-DE”	Name der PKI
organisational unit	OU	mandatory	“<Organisationseinheit> = **Haupt-Mandant-Name “	Name der Organisationseinheit des **Haupt-Mandant
country	C	mandatory	<LC>	Zwei Zeichen Ländercode gemäß [ISO 3116 ALPHA-2]
serial number	SERIAL NUMBER	mandatory	“<SN>”	Sequenznummer des Zertifikats im Bereich von 1 bis 2 ³¹ -1. Diese wird bei jedem neuen Zertifikat um den Wert 1 hochgezählt.
street	street	optional	„<Straße>“	Straße des Zertifikatsinhabers
postal code	postal code	optional	„<PLZ>“	Postleitzahl des Zertifikatsinhabers
locality	L	optional	„<Ortsname>“	Ortsname des Zertifikatsinhabers
state	ST	optional	„<Bundesland>“	Bundesland des Zertifikatsinhabers

Tabelle 24: Namensschema der GWA-Zertifikate

***Als Haupt-Mandant (HM) wird in der SEN.CA ein Auftragnehmer (AN) bezeichnet welcher in seiner Funktion diese Dienstleistung für mehrere Mandanten (Zertifikatsnehmer) in einem Konsortium bereitstellt.*

 Stadtwerke Saarbrücken	Certificate Policy SEN.CA	Version: 3.0
		Seite: 86/99
SWIT- 1961468859- 1355		Gültig ab: 01.12.2022
Status: Freigegeben	Klassifizierung: Öffentlich	Druckdatum: 01.12.2022

A.5 GWH

GWHs haben folgendes Namensschema:

Attribut Typ	Kürzel	Vorgabe	Wert	Erläuterung
common name	CN	mandatory	„<org>.GWH[.<RA-FirstLevel-Instanz >]“	Eindeutiger Name des GWH.
organsiation	O	mandatory	“SM-PKI-DE”	Name der PKI
organisational unit	OU	optional	“<Organisationseinheit> = **Haupt-Mandant-Name ”	Name der Organisationseinheit des **Haupt-Mandant
country	C	mandatory	<LC>	Zwei Zeichen Ländercode gemäß [ISO 3116 ALPHA-2]
serial number	SERIAL NUMBER	mandatory	“<SN>”	Sequenznummer des Zertifikats im Bereich von 1 bis 2 ³¹ -1. Diese wird bei jedem neuen Zertifikat um den Wert 1 hochgezählt.
street	street	optional	„<Straße>“	Straße des Zertifikatsinhabers
postal code	postal code	optional	„<PLZ>“	Postleitzahl des Zertifikatsinhabers
locality	L	optional	„<Ortsname>“	Ortsname des Zertifikatsinhabers
state	ST	optional	„<Bundesland>“	Bundesland des Zertifikatsinhabers

Tabelle 25: Namensschema der GWH-Zertifikate

***Als Haupt-Mandant (HM) wird in der SEN.CA ein Auftragnehmer (AN) bezeichnet welcher in seiner Funktion diese Dienstleistung für mehrere Mandanten (Zertifikatsnehmer) in einem Konsortium bereitstellt.*

A.6 SMGW

Bei SMGWs wird zwischen Gütesiegel- und Wirkzertifikaten unterschieden.

SMGW Wirkzertifikate

Das Namensschema für Wirkzertifikate lautet wie folgt:

**SWIT-
1961468859-
1355**
Certificate Policy SEN.CA

Gültig ab: 01.12.2022

Status: Freigegeben
Klassifizierung: Öffentlich

Druckdatum: 01.12.2022

Attribut Typ	Kürzel	Vorgabe	Wert	Erläuterung
common name	CN	mandatory	„<org>.SMGW[.<extension>]“	<org>= Herstellerübergreifende Identifikationsnummer für Messeinrichtungen
organisation	O	mandatory	“SM-PKI-DE”	Name der PKI
organisational unit	OU	optional	“<Organisationseinheit>”	Name des zuständigen GWA
country	C	mandatory	<LC>	Zwei Zeichen Ländercode gemäß [ISO 3116 ALPHA-2]
serial number	SERIAL NUMBER	mandatory	“<SN>”	Sequenznummer des Zertifikats im Bereich von 1 bis 2 ³¹ -1. Diese wird bei jedem neuen Zertifikat um den Wert 1 hochgezählt.

Tabelle 26: Namensschema der SMGW-Zertifikate im Wirkbetrieb
SMGW Gütesiegelzertifikate

Das Namensschema für Gütesiegelzertifikate ist das folgende:

Attribut Typ	Kürzel	Vorgabe	Wert	Erläuterung
common name	CN	mandatory	„<org>.SMGW[.<extension>]“	<org>= Herstellerübergreifende Identifikationsnummer für Messeinrichtungen
organisation	O	mandatory	„SM-PKI-DE“	Name der PKI
organisational unit	OU	optional	„<Organisationseinheit>“	Name des SMGW- Herstellers
country	C	mandatory	<LC>	Zwei Zeichen Ländercode gemäß [ISO 3116 ALPHA-2]
serial number	SERIAL NUMBER	mandatory	„0“	Sequenznummer des Zertifikats, im Gütesiegelzertifikat mit 0 belegt

Tabelle 27: Namensschema der SMGW-Gütesiegelzertifikate

 Stadtwerke Saarbrücken	Certificate Policy SEN.CA	Version: 3.0
		Seite: 88/99
SWIT- 1961468859- 1355		Gültig ab: 01.12.2022
Status: Freigegeben	Klassifizierung: Öffentlich	Druckdatum: 01.12.2022

A.7 Alternativnamen

Die Zertifikatserweiterungen (extensions) SubjectAltNames und IssuerAltName MÜSSEN gemäß Tabelle 28 und Tabelle 29 genutzt werden.

A.7.1 SubjectAltNames

Die Belegung der Extension SubjectAltNames (Extension-ID: 2.5.29.17) ist wie folgt:

Zertifikat	Rfc822Name	dNSName	uniformResourceIdentifizier
C(Root)	eine Kontakt E-Mail-Adresse	Entfällt	Zugehörige Webseite
C _{CRL-S} (Root)		Entfällt	
C _{TLS-S} (Root)		Entfällt	
C _{TLS} (Root)		Domain Name (TLS-Server- Zertifikat)	
C _{TLS,Root} (Root)			
C(Sub-CA)		Entfällt	
C _{TLS} (Sub-CA)		Domain Name (TLS-Server- Zertifikat)	Optional: Zugehörige Webseite
C(GWA) -C _{Enc} (GWA) -C _{Sig} (GWA) -C _{TLS} (GWA)	Domain Name (ausschließlich bei einem TLS-Server- Zertifikat, siehe nachfolgende Anforderungen)		
C(GWH) -C _{Enc} (GWH) -C _{Sig} (GWH) -C _{TLS} (GWH)			
C(EMT) -C _{Enc} (EMT) -C _{Sig} (EMT) -C _{TLS} (EMT)			

Tabelle 28: Belegung Extension SubjectAltNames für CAs und Endnutzer

Bei einem TLS-Server-Zertifikat, welches über die Extension ExtendedKeyUsage mit dem Wert TLS-Web-Server-Authentifikation (1.3.6.1.5.5.7.3.1) gemäß [TR-03109-4] verfügt, MUSS der zugehörige Domain Name in der Extension SubjectAltNames angegeben werden.

Falls notwendig, ist es möglich mehrere Domain Name aufzunehmen, mit einer Obergrenze von 20 Einträgen. Zertifikate DÜRFEN KEINE Wildcards im SubjectAltName enthalten.

 Stadtwerke Saarbrücken	Certificate Policy SEN.CA	Version: 3.0
		Seite: 89/99
SWIT- 1961468859- 1355		Gültig ab: 01.12.2022
Status: Freigegeben	Klassifizierung: Öffentlich	Druckdatum: 01.12.2022

A.7.2 IssuerAltName

Die Belegung der Extension IssuerAltName (Extension-ID) (OID): 2.5.29.18 ist wie folgt:

Zertifikat	Inhalt
C(Root)	Entsprechend der Extension SubjectAltNames in C(Root)
C _{CRL-S} (Root)	
C _{TLS-S} (Root)	
C(Sub-CA)	
C _{TLS} (Root)	Entsprechend der Extension SubjectAltNames in C _{TLS-S} (Root)
C _{TLS,Root} (Root)	
C _{TLS} (Sub-CA)	Entsprechend der Extension SubjectAltNames in C(Sub-CA)
C(GWA)	
- C _{Enc} (GWA)	
- C _{Sig} (GWA)	
- C _{TLS} (GWA)	
C(GWH)	
- C _{Enc} (GWH)	
- C _{Sig} (GWH)	
- C _{TLS} (GWH)	
C(EMT)	Entsprechend der Extension SubjectAltNames in C(Sub-CA)
- C _{Enc} (EMT)	
- C _{Sig} (EMT)	
- C _{TLS} (EMT)	
C(SMGW)	
- C _{Enc} (SMGW)	
- C _{Sig} (SMGW)	
- C _{TLS} (SMGW)	

Tabelle 29: Belegung Extension IssuerAltName für CAs und Endnutzer

Anhang B – Archivierung

 Stadtwerke Saarbrücken	Certificate Policy SEN.CA	Version: 3.0
		Seite: 90/99
SWIT- 1961468859- 1355		Gültig ab: 01.12.2022
Status: Freigegeben	Klassifizierung: Öffentlich	Druckdatum: 01.12.2022

Die folgende Tabelle gibt die Archivierungszeiträume für die unterschiedlichen Zertifikate der **SEN.CA** Teilnehmer wieder. Die Speicherung bzw. auch die Bereitstellung der Zertifikate KANN in dem LDAP-Verzeichnis der **SEN.CA** erfolgen, wobei die anderen Teilnehmer von der eigenverantwortlichen Speicherung der Zertifikate nicht befreit werden.

Teilnehmer	Archivierungsort	Zertifikatstyp	Archivierungsdauer
SEN.CA	Zertifikatsspeicher	C(Sub-CA)	Zertifikatslaufzeit + 10 ½ Jahre
		C _{TLs} (Sub-CA)	
		C _{S/MIME} (ASP-Sub-CA)	
EMT	Zertifikatsspeicher	C _{TLs} (EMT)	Zertifikatslaufzeit + 2 ½ Jahre
		C _{Enc} (EMT)	
		C _{Sig} (EMT)	
		C _{S/MIME} (ASP-EMT)	
GWA	Zertifikatsspeicher	C _{TLs} (GWA)	Zertifikatslaufzeit + 2 ½ Jahre
		C _{Enc} (GWA)	
		C _{Sig} (GWA)	
		C _{S/MIME} (ASP-GWA)	
GWH	Zertifikatsspeicher	C _{TLs} (GWH)	Zertifikatslaufzeit + 2 ½ Jahre
		C _{Enc} (GWH)	
		C _{Sig} (GWH)	
		C _{S/MIME} (ASP-GWH)	
SMGW	Zertifikatsspeicher	C _{TLs} (SMGW)	Zertifikatslaufzeit + 2 ½ Jahre
		C _{Enc} (SMGW)	
		C _{Sig} (SMGW)	

Tabelle 30: Archivierung öffentlicher Schlüssel

 Stadtwerke Saarbrücken	Certificate Policy SEN.CA	Version: 3.0
		Seite: 91/99
SWIT- 1961468859- 1355		Gültig ab: 01.12.2022
Status: Freigegeben	Klassifizierung: Öffentlich	Druckdatum: 01.12.2022

Anhang C – Definitionen

Begriff	Beschreibung
Ansprechpartner	Der Ansprechpartner (auch ASP oder Vertreter genannt) ist im Rahmen der operativen Tätigkeit der Vertreter des Unternehmens in Richtung der CA-Instanz und darf in dessen Namen die Entscheidungen treffen bzw. die Anträge autorisieren.
Antragsteller	Der Antragsteller im Sinne dieses Dokumentes ist das Unternehmen, welches die Zertifikate für den Betrieb der SEN.CA , eines GWH, eines GWA oder eines EMT bei der zuständigen CA-Instanz anfordert.
Gütesiegel-Zertifikat	siehe [TR-03109-4]
Vier-Augen-Prinzip	Parallele Gegenkontrolle durch eine zweite Person bei der Durchführung eines Vorgangs. Die eindeutige Identifikation und Rolle der teilnehmenden Mitarbeiter MUSS protokolliert werden. Das Vier-Augen-Prinzip KANN organisatorisch so umgesetzt werden, dass bei diesem Prozess zwei unterschiedliche Personen beteiligt sein MÜSSEN, die nicht zeitgleich gemeinsam am gleichen Ort agieren MÜSSEN.
Schlüsselmanagement	Verwaltung von Schlüsseln (insbesondere Erzeugung, Speicherung und Löschung bzw. Zerstörung von Schlüsseln)
Hinterlegung von Schlüsseln	Sichere Verwahrung einer Kopie eines Schlüssels an einem Zweitort.
Zerstörung von Schlüsseln	Zerstörung des Schlüssels durch einen sicheren Löschemechanismus im Kryptografiemodul. Dieser wird i.d.R. durch ein Überschreiben mit einem vorgegebenen Wert oder durch das interne dauerhafte Sperren aller Zugriffe auf den Schlüssel realisiert. Verfügt das Kryptografiemodul nicht über einen entsprechenden Löschemechanismus, muss eine unwiederherstellbare mechanische Zerstörung erfolgen.
PKI-Rolle	Die PKI-Rolle beschreibt die Funktionsklasse eines PKI-Teilnehmers in der SM-PKI. Folgende PKI-Rollen sind in der SM-PKI vorhanden: GWA, GWH, EMT, Sub-CA (SEN.CA), SMGW und Root-CA. Ein PKI-Teilnehmer ist eine Instanz seiner PKI-Rolle.
Wirkzertifikat	siehe [TR-03109-4]
Sequenznummer	SERIAL NUMBER des Distinguished Name, siehe Anhang A – Namensschema
Serialnummer	serialNumber Feld des Zertifikats, siehe [TR-03109-4]

Tabelle 31: Definitionen



**SWIT-
1961468859-
1355**

Certificate Policy SEN.CA

Gültig ab: 01.12.2022

Status: Freigegeben

Klassifizierung: Öffentlich

Druckdatum: 01.12.2022

 Stadtwerke Saarbrücken	Certificate Policy SEN.CA	Version: 3.0
		Seite: 93/99
SWIT- 1961468859- 1355		Gültig ab: 01.12.2022
Status: Freigegeben	Klassifizierung: Öffentlich	Druckdatum: 01.12.2022

Anhang D – Literaturverzeichnis

AIS 20	BSI: Anwendungshinweise und Interpretationen zum Schema AIS 20, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren Version 3, Stand 2013
AIS 31	BSI: Anwendungshinweise und Interpretationen zum Schema AIS 20, Funktionalitätsklassen und Evaluationsmethodologie für physikalischer Zufallszahlengeneratoren Version 3, Stand 2013
BSI-CC-PP-0073	BSI: 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, Version 1.3
BSI-CC-PP-0077-V2	BSI: Protection Profile for the Security Module of a Smart Meter Gateway (Security Module PP) Schutzprofil für das Sicherheitsmodul der Kommunikationseinheit eines intelligenten Messsystems für Stoff- und Energiemengen, Version 1.03
DIN 43863-5	DIN: Herstellerübergreifende Identifikationsnummer für Messeinrichtungen, Stand 2012
BSI TR-03109	BSI: Dachdokument, Version 1.0.1
BSI TR-03109-1	BSI: Anforderungen an die Interoperabilität der Kommunikationseinheit eines intelligenten Messsystems, Version 1.0
BSI TR-03109-TS-1	BSI: Testkonzept zu BSI TR-03109- TS-1, Version 00.91
BSI TR-03109-2	BSI: Smart Meter Gateway – Anforderungen an die Funktionalität und Interoperabilität des Sicherheitsmoduls, Version 1.1
BSI TR-03109-3	BSI: Kryptographische Vorgaben für die Infrastruktur von intelligenten Messsystemen, Version 1.1
BSI TR-03116-3	BSI: Kryptographische Vorgaben für Projekte der Bundesregierung, Stand 2017
BSI TR-03116-4	BSI: Technische Richtlinie TR-03116-4, Kryptographische Vorgaben für Projekte der Bundesregierung, Teil 4 Kommunikationsverfahren in Anwendungen, Stand 2017
Certificate Policy der Smart Metering PKI	BSI: Certificate Policy der Smart Metering PKI, Version 1.1.1

 Stadtwerke Saarbrücken	Certificate Policy SEN.CA	Version: 3.0
		Seite: 94/99
SWIT- 1961468859- 1355		Gültig ab: 01.12.2022
Status: Freigegeben	Klassifizierung: Öffentlich	Druckdatum: 01.12.2022

BSI TR-03109-4	BSI: Smart Metering PKI - Public Key Infrastruktur für Smart Meter Gateways, Version 1.2.1
BSI TR-03109-6	BSI: Smart Meter Gateway Administration, Version 1.0
BSI TR-03145-1	BSI: Secure CA operation, Part 1, Generic requirements for Trust Centers instantiating as Certification Authority in a Public-Key Infrastructure with security level 'high', Version 1.1
BSI TR-02102-1	BSI: "Kryptographische Verfahren: Empfehlungen und Schlüssellängen" Version: 2017-01
BSI TR 02102-2	BSI: "Kryptographische Verfahren: Verwendung von Transport Layer Security (TLS)" Version: 2017-01
BSI TR 02102-3	BSI: Kryptographische Verfahren: "Verwendung von Internet Protocol Security (IPsec) und Internet Key Exchange (IKEv2)" Version: 2017-01
BSI TR 02102-4	BSI: "Kryptographische Verfahren: Teil 4 – Verwendung von Secure Shell (SSH) Version: 2017-01
BSI Elliptic Curve Cryptography	BSI: Technical Guideline TR-03111, Version 2.0
BSI Zertifizierung von Produkten	Zertifizierung nach CC, Stand 2016 Bestätigung nach SigG, Stand 2016 Zertifizierung nach TR, Stand 2016
KeyLifecycle	BSI: Key Lifecycle Security Requirements, Version 1.0.1
BMW i – (Messtellenbetriebsgesetz – MsbG)	Gesetz zur Digitalisierung der Energiewende; Stand 2016
GDEW	BMW i: Gesetz zur Digitalisierung der Energiewende, 2016
eIDAS	Verordnung über elektronische Identifizierung und Vertrauensdienste, Stand 2017
BNetzA	Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen), Stand 2015
ISO/IEC 27001:2013	ISO/IEC: ISO/IEC 27001:2013 'Information technology - Security techniques – Information security management systems - Requirements', ISO/IEC JTC1/SC27
ISO/IEC 27005:2011	Information technology — Security techniques — Information security risk management (second edition)

 Stadtwerke Saarbrücken	Certificate Policy SEN.CA	Version: 3.0
SWIT- 1961468859- 1355		Seite: 95/99
Status: Freigegeben	Klassifizierung: Öffentlich	Gültig ab: 01.12.2022 Druckdatum: 01.12.2022

ISO 19005-1	ISO/IEC: Document management – Electronic document file format for longterm preservation – Part 1: User of PDF 1.4 (PDF/A-1),
ISO 3116 ALPHA-2	ISO: Codes for countries and their subdivisions, ALPHA-2 coding,
RFC 2119	IETF: Key words for use in RFCs to indicate requirement levels
RFC 2986	IETF: PKCS #10: Certification Request Syntax Specification
RFC 5280	IETF: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
RFC 6454	IETF: The Web Origin Concept
RFC 3647	IETF: Internet X.509 Public Key Infrastructure, Certificate Policy and Certification Practices Framework

 Stadtwerke Saarbrücken	Certificate Policy SEN.CA	Version: 3.0
		Seite: 96/99
SWIT- 1961468859- 1355		Gültig ab: 01.12.2022
Status: Freigegeben	Klassifizierung: Öffentlich	Druckdatum: 01.12.2022

Glossar

Begriff	Beschreibung
Ansprechpartner	Der Ansprechpartner (auch ASP oder Vertreter genannt) ist im Rahmen der operativen Tätigkeit der Vertreter des Unternehmens in Richtung der CA-Instanz und darf in dessen Namen die Entscheidungen treffen bzw. die Anträge autorisieren.
Antragsteller	Der Antragsteller im Sinne dieses Dokumentes ist das Unternehmen, welches die Zertifikate für einen GWH, einen GWA oder einen EMT bei der zuständigen CA-Instanz anfordert.
Vier-Augen-Prinzip	<p>Parallele Gegenkontrolle durch eine zweite Person bei der Durchführung eines Vorgangs.</p> <p>Die eindeutige Identifikation und Rolle der teilnehmenden Mitarbeiter MUSS protokolliert werden.</p> <p>Das Vier-Augen-Prinzip KANN organisatorisch so umgesetzt werden, dass bei diesem Prozess zwei unterschiedliche Personen beteiligt sein MÜSSEN, die nicht zeitgleich gemeinsam am gleichen Ort agieren MÜSSEN.</p>
Schlüsselmanagement	Verwaltung von Schlüsseln (insbesondere Erzeugung, Speicherung und Löschung bzw. Zerstörung von Schlüsseln)
Hinterlegung von Schlüsseln	Sichere Verwahrung einer Kopie eines Schlüssels an einem Zweitort.
Zerstörung von Schlüsseln	Zerstörung des Schlüssels durch einen sicheren Löschmechanismus im Kryptografiemodul. Dieser wird i.d.R. durch ein Überschreiben mit einem vorgegebenen Wert oder durch das interne dauerhafte Sperren aller Zugriffe auf den Schlüssel realisiert. Verfügt das Kryptografiemodul nicht über einen entsprechenden Löschmechanismus, muss eine unwiederherstellbare mechanische Zerstörung erfolgen.
PKI-Rolle	Die PKI-Rolle beschreibt die Funktionsklasse eines PKI-Teilnehmers in der SM-PKI. Folgende PKI-Rollen sind in der SM-PKI vorhanden: GWA, GWH, EMT, Sub-CA (SEN.CA), SMGW und Root-CA. Ein PKI-Teilnehmer ist eine Instanz seiner PKI-Rolle.

Tabelle 32: Glossar

 Stadtwerke Saarbrücken	Certificate Policy SEN.CA	Version: 3.0
		Seite: 97/99
SWIT- 1961468859- 1355		Gültig ab: 01.12.2022
Status: Freigegeben	Klassifizierung: Öffentlich	Druckdatum: 01.12.2022

Stichwort- und Abkürzungsverzeichnis

Abkürzung	Begriff
ASP	Ansprechpartner (des Unternehmens)
BSI	Bundesamt für Sicherheit in der Informationstechnik
CA	Certificate Authority
CC	Common Criteria
CER	Canonical Encoding Rules (Format zur Zertifikatscodierung)
CLS	controllable local systems
CN	Common Name
CP	Certificate Policy
CPS	Certificate Practise Statement
CRL	Certificate Revocation List (Zertifikatssperrliste)
DRG	(Funktionsklasse für Zufallsgeneratoren)
EMT	Externe Marktteilnehmer
ENC	Encryption / Verschlüsselung
GWA	Gateway Administrator
GWH	Gateway Hersteller
HAN	Home Area Network (Heimnetz)
HSM	Hardware Sicherheitsmodul
ITSM	IT-Service Management
ISMS	Information Security Management System
ISO	International Organization of Standardization
KEK	Key Encyption Key
KM	Krypto Modul
LDAP	Lightweight Directory Access Protocol
LMN	Lokales metrologisches Netzwerk
NTG	hybride deterministische Zufallszahlgeneratoren (Funktionsklasse für Zufallsgeneratoren)
OCSP	Online Certificate Status Protocol
PIN	Personal Identifikation Number
PKI	Public Key Infrastructure
PP	Protection Profile
PTG	hybride physikalische Zufallszahlgeneratoren (Funktionsklasse für Zufallsgeneratoren)
RA	Registration Authority

 Stadtwerke Saarbrücken	Certificate Policy SEN.CA	Version: 3.0
		Seite: 98/99
SWIT- 1961468859- 1355		Gültig ab: 01.12.2022
Status: Freigegeben	Klassifizierung: Öffentlich	Druckdatum: 01.12.2022

SHA	Secure Hash Algorithm
-----	-----------------------

Abkürzung	Begriff
SMGW	Smart Meter Gateway
S/MIME	Secure/Multipurpose Mail Extension
SM-PKI	Smart Metering – Public Key Infrastructure
TLS	Transport Layer Security (Protokoll zur Verschlüsselung einer Datenübertragung)
TR	Technische Richtlinie
WAN	Wide Area Network (Weitverkehrsnetz)
X.509	ITU-T-Standard für eine Public-Key-Infrastruktur

Tabelle 33: Stichwort- und Abkürzungsverzeichnis

 Stadtwerke Saarbrücken	Certificate Policy SEN.CA	Version: 3.0
		Seite: 99/99
SWIT- 1961468859- 1355		Gültig ab: 01.12.2022
Status: Freigegeben	Klassifizierung: Öffentlich	Druckdatum: 01.12.2022

Änderungshistorie

< Versionsnummer > - < Datum der Änderung > - < Autor > - < Beschreibung der Änderung >

- 3.0 - 01.12.2022 - Knauth Julia - Neue Freigabeversion erstellt

- 2.2 - 01.12.2022 - Knauth Julia - Anpassung Lenkungsinformationen

- 2.1 - 24.11.2022 - Knauth Julia - Aufbereitung nach Freigabe-Prozess

- 2.0 - 24.11.2022 - Knauth Julia - Neue Freigabeversion erstellt

- 1.2 - 24.11.2022 - Knauth Julia - Aktualisierung Ansprechpartner

- 1.1 - 08.09.2020 - Klein Thomas - Aufbereitung nach Freigabe-Prozess

- 1.0 - 08.09.2020 - Klein Thomas - Neue Freigabeversion erstellt
