



Vertragsbedingungen
zur Nutzung von Zertifikaten
der DARZ.CA
unterhalb der Smart Metering-PKI

Vertragsbedingungen zur Nutzung von Zertifikaten der DARZ.CA unterhalb der Smart Metering-PKI



Inhalt

1.	Dokumenteninformationen	4
1.1	Bearbeitungsvermerk	4
1.2	Änderungshistorie	4
1.3	Gleichstellungshinweis	4
2.	Geltungsbereich, Vertragsbestandteile und Rangfolge	4
2.1	Gegenstand	4
2.2	Begriffe	5
2.3	Verpflichtung auf die Regelwerke	5
2.4	Rangfolge	5
3.	Zertifikate, Verwendung und Gültigkeit	5
3.1	Zertifikatstypen	5
3.2	Erlaubte und verbotene Verwendung	5
3.3	Gültigkeitszeiträume	5
4.	Registrierung und Zertifikatsantrag	6
4.1	Antragsberechtigung	6
4.2	Registrierungsunterlagen	6
4.3	Testteilnahme	6
4.4	Annahme oder Ablehnung von Anträgen	6
4.5	Bearbeitungsfristen	7
4.6	Ausgabe von Zertifikaten	7
5.	Schlüssel der Teilnehmer	7
6.	Annahme von Zertifikaten und Folgeanträge	8
6.1	Annahme	8
6.2	Folgeanträge	8
7.	Pflichten des Teilnehmers im Betrieb	8
7.1	Sicherheitsnachweise	8
7.2	Änderungen und jährliche Bestätigung	8
7.3	Dienstleister und Mandantenbetrieb	9
7.4	Nutzung des Verzeichnisdienstes	9
7.5	Kommunikation	9
7.6	Meldepflichten	9
8.	Sperrung und Suspendierung	10
8.1	Sperrberechtigte	10
8.2	Sperrgründe	10
8.3	Sperrantrag	10
8.4	Durchführung der Sperrung	10
8.5	Sperrdienst und Sperrlisten der DARZ.CA	11
8.6	Pflichten bei der Sperrlistenprüfung	11
8.7	SMGW: technische Verantwortlichkeit und Suspendierung	11
9.	Leistungen der DARZ.CA	11
9.1	Betrieb	11
9.2	Veröffentlichung	11
9.3	Fehlermeldungen und Rückfragen	12
9.4	Testumgebung	12
9.5	Service Level	12
9.6	Schlüsselwechsel der DARZ.CA	12

Vertragsbedingungen zur Nutzung von Zertifikaten der DARZ.CA unterhalb der Smart Metering-PKI



9.7	Protokollierung und Archivierung	12
9.8	Einstellung des CA-Betriebs	12
10.	Beendigung der Teilnahme	12
11.	Laufzeit und Änderungen	13
12.	Datenschutz und Vertraulichkeit	13
13.	Haftung und Freistellung	13
14.	Schlussbestimmungen	13
14.1	Anwendbares Recht	13
14.2	Gerichtsstand	13
14.3	Höhere Gewalt	13
14.4	Abtretung	13
14.5	Vollständigkeit und Form	14
14.6	Salvatorische Klausel	14
14.7	Geistiges Eigentum	14
15.	Kontakt	14
16.	Referenzdokumente	14

Vertragsbedingungen zur Nutzung von Zertifikaten der DARZ.CA unterhalb der Smart Metering-PKI



1. Dokumenteninformationen

1.1 Bearbeitungsvermerk

	Name und Funktion	Version	Datum	Unterschrift
Erstellt von:	Jürgen Henzler	3.4	08.10.2026	
Geprüft von:	Tiziana Knecht	3.4	08.10.2026	
Genehmigt von:	Raphael Munasypow	3.4	08.10.2026	
Rücknahme durch:				

1.2 Änderungshistorie

Datum	Bearbeiter	Version	Änderungsgrund / Änderungen
21.08.2017	Lisa Weinand	0.1	Initialisierung
13.04.2018	Rüdiger Heusel	2.0	Überprüfung, Schreibfehlerkorrekturen Überprüfung der Konformität zu CP
16.04.2018	Rüdiger Heusel	2.1	Ergänzung 7.6: wiederkehrende Bestätigung -- volle Konformität zu IR.Reg.5
03.12.2019	Jürgen Henzler	2.2	Anpassungen / IR / Verantwortlichkeiten
15.04.2020	Franziska Gimbel	2.3	Anpassungen / IR / Texte
01.11.2020	Franziska Gimbel	2.4	Kontrolle / Anpassungen
03.05.2021	Franziska Gimbel	2.5	Kontrolle / Anpassungen
12.05.2021	Franziska Gimbel	2.6	Anpassungen Kapitel 7 & 9
18.05.2021	Franziska Gimbel	2.7	Ergänzung Kapitel 3.3
12.05.2023	Tiziana Knecht	2.8	Anpassung Kapitel 7
06.05.2024	Tiziana Knecht	2.9	Kontrolle / Anpassungen
14.05.2024	Tiziana Knecht Jürgen Henzler	3.0	Anpassung Kapitel 5.4, 16.4
04.11.2024	Tiziana Knecht Jürgen Henzler	3.1	Anpassung Kapitel 4.2
14.04.2025	Tiziana Knecht Jürgen Henzler	3.2	Position 23 / Schiedsgericht Anforderungen IT Sicherheit
01.04.2026	Tiziana Knecht Jürgen Henzler	3.3	Kontrolle, keine Änderung
08.10.2026	Jürgen Henzler	3.4	Neufassung: Angleichung an BSI-CP SM-PKI v1.1.2, TR-03109-4 und DARZ-CP; neue Gliede- rung

1.3 Gleichstellungshinweis

In diesem Dokument wird für die Beschreibung von Aufgaben, Funktionen oder Rollen aus Vereinfachungsgründen die männliche Schreibweise gewählt. Damit sind alle Geschlechter angesprochen, denen Aufgaben, Funktionen oder Rollen zugeordnet werden, ohne eine Wertung ihres Geschlechts, ihrer physischen oder psychischen Fähigkeiten oder eine sonstige Wertung vorzunehmen.

2. Geltungsbereich, Vertragsbestandteile und Rangfolge

2.1 Gegenstand

(1) Die DARZ GmbH (im Folgenden „DARZ“) betreibt unterhalb der Root-CA der Smart Metering-PKI (SM-PKI) des Bundesamts für Sicherheit in der Informationstechnik (BSI) die Sub-CA „DARZ.CA“ und die Testumgebung „DARZ-Test.CA“.

(2) Diese Vertragsbedingungen regeln die Rechte und Pflichten zwischen DARZ und dem Teilnehmer bei Registrierung, Beantragung, Ausgabe, Nutzung, Sperrung und Suspendierung von Zertifikaten der DARZ.CA. Sie gelten für Gateway-Administratoren

Vertragsbedingungen zur Nutzung von Zertifikaten der DARZ.CA unterhalb der Smart Metering-PKI



(GWA), Gateway-Hersteller (GWH) und externe Marktteilnehmer (EMT) sowie für die von GWA und GWH beantragten Zertifikate für Smart Meter Gateways (SMGW).

(3) Die Vertragsbedingungen sind Bestandteil des Angebots und der Beauftragung. Sie werden vom Teilnehmer gegengezeichnet und der Beauftragung beigelegt.

2.2 Begriffe

- **Teilnehmer:** GWA, GWH oder EMT, dem die DARZ.CA Zertifikate ausstellt (Zertifikatsnehmer). Für Dienstleister des Teilnehmers gilt Ziff. 7.3.
- **Ansprechpartner:** vom Teilnehmer benannte und bei der Registrierung identifizierte natürliche Person, die für den Teilnehmer gegenüber der DARZ.CA handelt.
- **Zertifikatstripel:** TLS-, Verschlüsselungs- und Signaturzertifikat eines Endnutzers mit gleicher Laufzeit.
- **BSI-CP:** Certificate Policy der Smart Metering-PKI des BSI.
- **DARZ-CP:** Certificate Policy der DARZ.CA (OID 1.3.6.1.4.1.51695.1.1).

2.3 Verpflichtung auf die Regelwerke

(1) Der Teilnehmer verpflichtet sich, die BSI-CP, die TR-03109-4 und die DARZ-CP in der jeweils gültigen Fassung einzuhalten. Nur Teilnehmer, die diese Verpflichtung eingegangen sind, nehmen an der SM-PKI teil.

(2) Maßgeblich sind derzeit BSI-CP Version 1.1.2, TR-03109-4 Version 1.2.1 und DARZ-CP.

2.4 Rangfolge

(1) Die Vorgaben der BSI-CP und der Technischen Richtlinien des BSI gehen allen vertraglichen Regelungen vor. Danach gilt die DARZ-CP.

(2) Im Übrigen gilt bei Widersprüchen folgende Rangfolge: Angebot bzw. Leistungsschein, diese Vertragsbedingungen, Service Level Vereinbarung (SLA), Allgemeine Geschäftsbedingungen der DARZ GmbH (AGB).

(3) Widersprechen sich diese Vertragsbedingungen und die DARZ-CP, gilt die DARZ-CP, soweit die BSI-CP nicht Strengeres verlangt.

3. Zertifikate, Verwendung und Gültigkeit

3.1 Zertifikatstypen

(1) Die DARZ.CA stellt für GWA, GWH und EMT jeweils ein Zertifikatstripel aus. Ein Teilnehmer kann bei Bedarf weitere Zertifikatstripel per Folgeantrag beantragen, etwa für Lastverteilung oder Ausfallsicherheit.

(2) Für SMGW stellt die DARZ.CA Gütesiegelzertifikate auf Antrag des GWH und Wirkzertifikate auf Antrag des GWA aus. Das SMGW beantragt selbst keine Zertifikate.

3.2 Erlaubte und verbotene Verwendung

(1) Zertifikate und die zugehörigen privaten Schlüssel dürfen ausschließlich für die Verfahren eingesetzt werden, die der im Zertifikat festgelegte Verwendungszweck ermöglicht. Die Anwendungsfälle ergeben sich aus der BSI-CP, der TR-03109-4 und, für die Marktkommunikation (AS4), aus der DARZ-CP.

(2) Jede darüber hinausgehende Verwendung ist untersagt, insbesondere zu privaten Zwecken.

(3) Der Teilnehmer ist für den Einsatz der Zertifikate in seinen Anwendungen verantwortlich und prüft, ob diese seinen Sicherheitsanforderungen genügen.

3.3 Gültigkeitszeiträume

(1) Es gelten folgende Laufzeiten:

Zertifikat	Gültigkeit
Sub-CA-Zertifikat der DARZ.CA	5 Jahre
TLS-Zertifikate der DARZ.CA	2 Jahre

Vertragsbedingungen zur Nutzung von Zertifikaten der DARZ.CA unterhalb der Smart Metering-PKI



Zertifikat	Gültigkeit
GWA (TLS, Verschlüsselung, Signatur)	3 Jahre
GWH, EMT und SMGW (TLS, Verschlüsselung, Signatur)	2 Jahre

(2) Ein Zertifikat ist nie länger gültig als das ausstellende Sub-CA-Zertifikat. Die Laufzeit kann sich dadurch verkürzen.

(3) Maßgeblich sind die Laufzeiten der TR-03109-4 in der jeweils gültigen Fassung.

4. Registrierung und Zertifikatsantrag

4.1 Antragsberechtigung

(1) Zertifikate dürfen ausschließlich Organisationen beantragen: GWA, GWH und EMT. Anträge natürlicher Personen sind ausgeschlossen.

(2) Der Teilnehmer handelt gegenüber der DARZ.CA ausschließlich über seine benannten Ansprechpartner.

4.2 Registrierungsunterlagen

(1) Für die Registrierung legt der Teilnehmer vor:

- Antragsschreiben mit Firma, Anschrift und Unternehmensnachweis (aktueller Handelsregistrierungsauszug [nicht älter als drei Monate] oder Nachweis der Institution),
- Kontaktdaten der Ansprechpartner mit Vertreterregelung,
- Bestätigung der Geschäftsführung, dass der Vertreter zur Antragstellung und zu verbindlichen Angaben berechtigt ist,
- persönliche S/MIME-Zertifikate der Ansprechpartner einschließlich Zertifikatskette,
- Erklärung zur Einhaltung der Sicherheitsvorgaben und die Nachweise nach Ziff. 7.1,
- SHA-256-Hashwert des initialen Zertifikatsrequest-Pakets mit Angabe des Darstellungsformats, bestätigt durch Unterschrift des Bevollmächtigten und per S/MIME signierter und verschlüsselter E-Mail übermittelt,
- Bestätigung der erfolgreichen Testteilnahme nach Ziff. 4.3.

(2) Zusätzlich gilt je Rolle:

- **GWA und GWH:** Mindestens zwei bevollmächtigte Vertreter werden persönlich bei der Registrierungsstelle der DARZ.CA identifiziert. Den Termin stimmt die DARZ.CA ab.
- **EMT:** Erklärung zur Nutzung des Zertifikats, aus der hervorgeht, ob der EMT als aktiver oder passiver EMT tätig wird.
- **EMT in der Marktkommunikation:** Zuteilungsurkunde des zuständigen Codenummernverzeichnisses (BDEW Energie Codes GmbH für Strom, DVGW Service und Consult GmbH für Gas) für die Aufnahme der Marktpartner-ID.

(3) Beauftragt der Teilnehmer einen Dienstleister mit Beantragung oder Betrieb, legt er zusätzlich eine schriftliche Bestätigung vor, die den Dienstleister berechtigt und dessen autorisierte Ansprechpartner benennt.

(4) Die Registrierungsstelle prüft die Angaben im Zertifikatsrequest gegen die eingereichten Unterlagen. Der Ablauf ist in der DARZ-CP Kap. 4.2 und im Dokument „VA_TR-03145 Onboarding PKI“ beschrieben, das der Teilnehmer bei der Registrierung erhält.

4.3 Testteilnahme

(1) Vor Aufnahme des Wirkbetriebs durchläuft der Teilnehmer Registrierung, Zertifikatsbeantragung, -erneuerung und -sperrung erfolgreich in der DARZ-Test.CA. GWA testen zusätzlich SMGW-Wirkzertifikate, GWH zusätzlich SMGW-Gütesiegelzertifikate.

(2) Die DARZ.CA bestätigt den erfolgreichen Abschluss per S/MIME signierter und verschlüsselter E-Mail.

4.4 Annahme oder Ablehnung von Anträgen

(1) Die Registrierungsstelle prüft die Unterlagen gegen die DARZ-CP. Sind sie unvollständig oder fehlerhaft, fordert sie den Ansprechpartner zur Nachlieferung auf.

Vertragsbedingungen zur Nutzung von Zertifikaten der DARZ.CA unterhalb der Smart Metering-PKI



(2) Die Freigabe teilt die DARZ.CA dem Ansprechpartner per S/MIME signierter und verschlüsselter E-Mail mit. Eine Ablehnung erfolgt formell und mit Begründung auf demselben Weg.

(3) Ein Anspruch auf Ausstellung besteht nicht, solange die Voraussetzungen der BSI-CP und der DARZ-CP nicht erfüllt sind.

4.5 Bearbeitungsfristen

(1) Für die initiale Ausgabe gelten folgende Richtwerte:

Schritt	Tätigkeit	Zeitraumen
1	Start des Antrags durch den Teilnehmer	–
2	Kontaktaufnahme zur Terminvereinbarung durch die DARZ.CA; Termin innerhalb der folgenden 3 Arbeitstage	3 Arbeitstage
3	Übergabe der Unterlagen, ggf. im persönlichen Termin	–
4	Vorprüfung und Rückmeldung an den Teilnehmer	1 Kalenderwoche
5 (optional)	Nachlieferungsfrist für den Teilnehmer	3 Kalenderwochen
6	Prüfung und Rückmeldung an den Teilnehmer	1 Kalenderwoche
7	Ausstellung der Zertifikate	7 Arbeitstage

(2) Die Fristen setzen die fristgerechte und vollständige Mitwirkung des Teilnehmers voraus. Verzögert sich diese, verschieben sich die Fristen entsprechend.

(3) Folgezertifikate über die Web-Service-Schnittstelle stellt die DARZ.CA synchron aus. Für Ersatzzertifikate nach einer Sperrung gelten die Richtwerte nicht.

4.6 Ausgabe von Zertifikaten

(1) Initiale Zertifikate erhält der Ansprechpartner per S/MIME verschlüsselter E-Mail.

(2) Folgezertifikate werden über die Web-Service-Schnittstelle nach TR-03109-4 oder per S/MIME verschlüsselter E-Mail ausgegeben.

(3) SMGW-Zertifikate werden ausschließlich über die Web-Service-Schnittstelle ausgegeben.

5. Schlüssel der Teilnehmer

(1) **Erzeugung:** Der Teilnehmer erzeugt jedes Schlüsselpaar selbst und unmittelbar vor der Beantragung des Zertifikats neu. Für jeden Verwendungszweck des Zertifikatstripels wird ein eigenes Schlüsselpaar verwendet. Bei SMGW erzeugt das Sicherheitsmodul des SMGW die Schlüssel.

(2) **Besitznachweis:** Jeder Zertifikatsrequest enthält eine innere Signatur. Die DARZ.CA prüft damit, dass der Antragsteller im Besitz des privaten Schlüssels ist.

(3) **Keine Hinterlegung:** DARZ erzeugt, erhält und hinterlegt keine privaten Schlüssel der Teilnehmer und kann sie nicht wiederherstellen. Geht ein privater Schlüssel verloren, lässt der Teilnehmer das Zertifikat sperren und beantragt ein neues Zertifikatstripel nach Ziff. 6.2.

(4) **Schlüsselerneuerung:** Für einen bereits zertifizierten öffentlichen Schlüssel wird kein neues Zertifikat ausgestellt. Jede Erneuerung erfordert ein neues Schlüsselpaar.

(5) **Schutz:** Der Teilnehmer erzeugt, speichert und nutzt seine privaten Schlüssel in einem Kryptografiemodul nach den Vorgaben der DARZ-CP Kap. 7.2 und der BSI-CP. Er hält die Anforderungen der BSI „Key Lifecycle Security Requirements“ (KeyLifeSec), Security Level 2, an Lebenszyklus und Einsatzumgebung ein; ausgenommen sind SMGW.

(6) **Aktivierungsdaten:** PIN, Passwörter und vergleichbare Geheimnisse für den Zugriff auf die privaten Schlüssel kennen nur die berechtigten Personen des Teilnehmers.

Vertragsbedingungen zur Nutzung von Zertifikaten der DARZ.CA unterhalb der Smart Metering-PKI



6. Annahme von Zertifikaten und Folgeanträge

6.1 Annahme

- (1) Der Ansprechpartner prüft jedes Zertifikat nach Erhalt auf Korrektheit und Vollständigkeit. Bei SMGW kann der GWH bzw. GWA die Prüfung automatisiert beim Erhalt oder Einbringen durchführen.
- (2) Ein fehlerhaftes Zertifikat weist der Ansprechpartner per S/MIME signierter und verschlüsselter E-Mail an DARZ.CA@da-rz.de zurück. Er nennt den Grund und, soweit möglich, die fehlerhaften Einträge.
- (3) Mit der ersten Nutzung gilt das Zertifikat als angenommen.

6.2 Folgeanträge

- (1) Der Teilnehmer beantragt neue Zertifikate rechtzeitig vor Ablauf, damit er sie ohne Betriebsunterbrechung in seine Systeme einbringen kann. Für SMGW ist der GWA verantwortlich.
- (2) Routinemäßige Folgeanträge stellt der Teilnehmer über die Web-Service-Schnittstelle (TLS nach TR-03116-3) oder per S/MIME signierter und verschlüsselter E-Mail des Ansprechpartners. Das Request-Paket trägt die äußere Signatur des noch gültigen Signaturschlüssels; das verwendete TLS-Zertifikat ist weder gesperrt noch abgelaufen.
- (3) Fehlt eine dieser Absicherungen, gilt das Verfahren für nicht routinemäßige Folgeanträge nach DARZ-CP Kap. 4.3.2. Fehlen beide, ist eine erneute initiale Registrierung erforderlich.
- (4) Nach einer Sperrung beantragt der Teilnehmer stets ein vollständiges neues Zertifikatstripel.
- (5) In der Übergangszeit können altes und neues Zertifikat parallel gültig sein.

7. Pflichten des Teilnehmers im Betrieb

7.1 Sicherheitsnachweise

- (1) Der Teilnehmer erbringt die für seine Rolle geforderten Nachweise und hält sie während der gesamten Teilnahme aufrecht:

Rolle	Nachweis
GWA	Zertifizierung nach TR-03109-6
GWH	Common-Criteria-Zertifikat auf Basis von BSI-CC-PP-0073
Aktiver EMT	ISO/IEC 27001 (nativ oder auf Basis von IT-Grundschutz) oder Nachweis, dass ein so zertifizierter Dritter die Leistung erbringt
Passiver EMT	Sicherheitskonzept, dass die Anforderungen der BSI-CP berücksichtigt

- (2) Die Zertifizierungen unterliegen in der Regel einem jährlichen Überwachungsaudit. Der Teilnehmer legt die Ergebnisse und, soweit ausgestellt, das neue Zertifikat rechtzeitig vor Ablauf der eingereichten Unterlagen vor.
- (3) Verliert der Teilnehmer eine geforderte Zertifizierung, teilt er dies unverzüglich mit. Seine Zertifikate werden gesperrt.
- (4) Änderungen, die eine Erst- oder Re-Zertifizierung erfordern, meldet der Teilnehmer unverzüglich mit den Ergebnissen der Zertifizierung. Beispiele sind der Wechsel vom passiven zum aktiven EMT und der Wechsel des IT-Betriebsstandorts.

7.2 Änderungen und jährliche Bestätigung

- (1) Änderungen der Registrierungsdaten teilt der Teilnehmer der DARZ.CA unverzüglich mit. Mit jedem Folgeantrag bestätigt er, dass die vorliegenden Registrierungsdaten aktuell sind.
- (2) Zusätzlich übermittelt der Teilnehmer jährlich:
 - einen aktuellen Handelsregisterauszug per E-Mail oder Post,
 - die Bestätigung von Registrierung, Antragsdaten und aktueller Kommunikationsmatrix per S/MIME signierter und verschlüsselter E-Mail,
 - die Bestätigung aller bei der DARZ.CA registrierten Personen.

Vertragsbedingungen zur Nutzung von Zertifikaten der DARZ.CA unterhalb der Smart Metering-PKI



Die DARZ.CA fordert diese Bestätigung aktiv an.

(3) Scheidet ein identifizierter Vertreter aus, benennt der Teilnehmer unverzüglich einen Nachfolger. Dieser wird wie bei der Registrierung persönlich identifiziert. Die Geschäftsführung des Teilnehmers bestätigt Benennung und Ausscheiden.

(4) Will ein EMT zwischen aktiver und passiver Rolle wechseln, teilt er dies der DARZ.CA vorab mit, legt die Unterlagen nach Ziff. 4.2 und 7.1 vor und beantragt neue Zertifikate. Aufgaben eines aktiven EMT übernimmt er erst nach Bestätigung der DARZ.CA per S/MIME signierter E-Mail.

(5) Bei einer Umfirmierung (Änderung von Name oder Rechtsform) stellt der Teilnehmer einen neuen initialen Antrag. Das bisherige Zertifikat bleibt bis zum Abschluss des Wechsels gültig, längstens 2 Wochen, und wird danach gesperrt.

7.3 Dienstleister und Mandantenbetrieb

(1) Setzt der Teilnehmer einen Dienstleister ein, etwa für das EMT-Frontend oder den GWA-Betrieb, bleibt er für die Einhaltung dieser Vertragsbedingungen verantwortlich. Er verpflichtet den Dienstleister entsprechend. Der Teilnehmer muss der DARZ.CA die Vollmachten vorlegen.

(2) Die Übermittlung zwischen Dienstleister und Auftraggeber erreicht ein Sicherheitsniveau, das mit den Mechanismen der TR-03116-3 vergleichbar ist.

(3) Betreut der Dienstleister mehrere Auftraggeber, trennt er sie technisch und/oder organisatorisch. Nutzt er je Auftraggeber eigene Zertifikate, liegen deren Schlüssel in getrennten Verwaltungsbereichen des Kryptografiemoduls, die jeweils durch ein eigenes Geheimnis geschützt sind.

(4) Werden Teile eines GWA durch Dienstleister erbracht, ist dies im ISMS des GWA und des Auftraggebers abzubilden und muss der TR-03109-6 entsprechen.

7.4 Nutzung des Verzeichnisdienstes

(1) Der Teilnehmer greift auf den Verzeichnisdienst der DARZ.CA nur mit seinem TLS-Zertifikat aus der SM-PKI zu.

(2) Der Verzeichnisdienst dient ausschließlich der Aktualisierung angefragter Zertifikate. Ein Massenabruf ist untersagt. Die DARZ.CA begrenzt die Anzahl der Suchergebnisse.

7.5 Kommunikation

(1) Für den formalen Informationsaustausch akzeptiert die DARZ.CA ausschließlich S/MIME signierte und verschlüsselte E-Mails, soweit diese Vertragsbedingungen nichts anderes bestimmen. Nachrichten ohne sicherheitskritischen Inhalt dürfen unsigniert und unverschlüsselt an zentrale Postfächer gesendet werden.

(2) Ansprechpartner nutzen persönliche S/MIME-Zertifikate. Funktionspostfächer sind nur zum Empfang zulässig und verfügen über ein eigenes Verschlüsselungszertifikat.

(3) Vor Ablauf seines S/MIME-Zertifikats übermittelt der Ansprechpartner das neue Zertifikat per E-Mail, die mit dem alten, noch gültigen Zertifikat signiert ist.

(4) Die Vertragssprache ist Deutsch. Mitteilungen, Dokumente und Korrespondenz sind in deutscher Sprache zu verfassen.

7.6 Meldepflichten

(1) Eine Kompromittierung des privaten Schlüssels und andere sicherheitsrelevante Vorfälle meldet der Teilnehmer unverzüglich an die DARZ.CA. Die Meldung enthält mindestens:

- was betroffen ist,
- wann das Ereignis eingetreten ist bzw. bemerkt wurde,
- wer es festgestellt hat,
- wo es aufgetreten ist,
- wie es vermutlich abgelaufen ist,
- welche Maßnahmen bereits eingeleitet wurden.

(2) Ein EMT informiert den zuständigen GWA, wenn er Anomalien in den Daten eines SMGW feststellt, die auf eine Fehlfunktion oder Kompromittierung hindeuten, oder wenn gesperrte SMGW wiederholt Kommunikationsversuche unternehmen.

(3) Kompromittiertes Schlüsselmaterial nutzt der Teilnehmer nicht weiter. Er veranlasst die Sperrung nach Ziff. 8.

Vertragsbedingungen zur Nutzung von Zertifikaten der DARZ.CA unterhalb der Smart Metering-PKI



8. Sperrung und Suspendierung

8.1 Sperrberechtigte

(1) Die Sperrung eines Zertifikats können veranlassen: der Teilnehmer über seine benannten Ansprechpartner, die DARZ.CA und die SM-PKI-Root.

(2) Für SMGW-Gütesiegelzertifikate ist der GWH sperrberechtigt, nach Übertragung der technischen Verantwortlichkeit allein der GWA. Für SMGW-Wirkzertifikate ist der GWA sperrberechtigt.

8.2 Sperrgründe

(1) Ein Zertifikat wird gesperrt, wenn mindestens einer der folgenden Gründe vorliegt:

- Die Angaben im Zertifikat sind nicht oder nicht mehr zutreffend, etwa nach einer Umfirmierung.
- Der private Schlüssel ist kompromittiert, oder es besteht ein begründeter Verdacht darauf.
- Der Teilnehmer ist nicht mehr berechtigt, das Zertifikat zu nutzen, oder benötigt es nicht mehr.
- Der Teilnehmer verliert eine nach Ziff. 7.1 geforderte Zertifizierung.
- Der Teilnehmer verstößt gegen Pflichten aus diesen Vertragsbedingungen, der DARZ-CP oder der BSI-CP.
- Algorithmen, Schlüssellänge oder Gültigkeitsdauer bieten keine ausreichende Sicherheit mehr.
- Der private Schlüssel der DARZ.CA oder der SM-PKI-Root ist kompromittiert. Dann werden alle betroffenen Zertifikate gesperrt.
- Die DARZ.CA stellt ihren Zertifizierungsbetrieb ein. Dann werden alle von ihr ausgestellten Zertifikate gesperrt.

(2) Der Teilnehmer kann die Sperrung seiner Zertifikate jederzeit auch ohne Grund beantragen.

(3) Der Teilnehmer veranlasst die Sperrung unverzüglich, sobald ihm ein Sperrgrund bekannt wird.

(4) Eine Sperrung kann nicht zurückgenommen werden. Ausnahme ist die Suspendierung nach Ziff. 8.7.

8.3 Sperrantrag

(1) Sperranträge sind auf folgenden Wegen möglich:

- per S/MIME signierter und verschlüsselter E-Mail des benannten Ansprechpartners an DARZ.CA@da-rz.de,
- über die Web-Service-Schnittstelle der DARZ.CA. Für SMGW-Zertifikate ist dieser Weg verpflichtend; gesperrt wird stets das vollständige Zertifikatstripel als Paket. Nur wenn der Web-Service nicht verfügbar ist, ist eine S/MIME signierte und verschlüsselte E-Mail zulässig,
- telefonisch über die Sperrhotline aus der Kommunikationsmatrix, erreichbar 24x7 oder per verschlüsselter Mail von berechtigten Personen.

(2) Jeder Sperrantrag enthält:

- den Zertifikatstyp (GWA, GWH, EMT, SMGW-Gütesiegel- oder -Wirkzertifikat),
- die ausstellende CA,
- die Seriennummern des Zertifikatstripels,
- den Distinguished Name (CN, O, OU, C, Serial Number),
- den Sperrgrund,
- den Zeitpunkt, ab dem das Zertifikat als unsicher gilt, sofern bekannt.

8.4 Durchführung der Sperrung

(1) Die DARZ.CA prüft jeden Sperrantrag unverzüglich und setzt valide Anträge unverzüglich um.

(2) Sperrungen von GWA-Zertifikaten und anderen Zertifikaten mit systemrelevanter Bedeutung erfolgen gemäß DARZ-CP in Abstimmung mit der SM-PKI-Root.

(3) Bei einer Kompromittierung eines privaten Schlüssels stimmt die DARZ.CA das weitere Vorgehen unverzüglich mit der SM-PKI-Root ab. Ordnet die SM-PKI-Root eine sofortige Sperrung an, setzt die DARZ.CA diese unverzüglich um.

(4) Die DARZ.CA informiert den Teilnehmer über den Abschluss der Sperrung per S/MIME signierter und verschlüsselter E-Mail.

Vertragsbedingungen zur Nutzung von Zertifikaten der DARZ.CA unterhalb der Smart Metering-PKI



8.5 Sperrdienst und Sperrlisten der DARZ.CA

- (1) Die DARZ.CA nimmt Sperranträge 24 Stunden an 7 Tagen der Woche entgegen.
- (2) Die Sperrliste wird regulär innerhalb von 24 Stunden und nach jeder Sperrung unverzüglich aktualisiert. Ihre Gültigkeit überschreitet das Aktualisierungsintervall um höchstens 3 Tage.
- (3) Die Sperrlisten sind ohne Authentifizierung frei abrufbar. Für ihre Verfügbarkeit gilt Ziff. 9.5.
- (4) Nach Ablauf der Gültigkeit eines Zertifikats wird sein Eintrag aus der Sperrliste entfernt.
- (5) Einen OCSP-Dienst bietet die DARZ.CA nicht an. Der Sperrstatus wird über die Sperrliste geprüft.

8.6 Pflichten bei der Sperrlistenprüfung

- (1) Der Teilnehmer ruft die Sperrliste täglich ab und prüft Zertifikate bei jeder Verwendung auf Sperrung. Für SMGW übernimmt dies der GWA täglich und anlassbezogen.
- (2) Bei Erstinbetriebnahme und auf Aufforderung einer CA ruft der Teilnehmer die Sperrliste zusätzlich anlassbezogen ab.
- (3) Ist eine Sperrliste nicht verfügbar, prüft der Teilnehmer mit der zuletzt bekannten Sperrliste weiter und informiert die DARZ.CA unverzüglich. Die DARZ.CA stellt die aktuelle Sperrliste dann auf anderem Weg bereit und informiert nach 3 Tagen ohne Abhilfe die SM-PKI-Root.
- (4) Suspendierte Zertifikate behandelt der Teilnehmer wie gesperrte Zertifikate.

8.7 SMGW: technische Verantwortlichkeit und Suspendierung

- (1) Der GWH überträgt die technische Verantwortlichkeit für Gütesiegelzertifikate an den GWA mit dem Formular der DARZ.CA per S/MIME signierter und verschlüsselter E-Mail oder mit einem mit CSig(GWH) signierten Datensatz über die Web-Service-Schnittstelle. Die Übertragung ist je SMGW einmalig und wird rechtssicher dokumentiert. Die DARZ.CA informiert den GWA über den Abschluss.
- (2) Suspendiert werden können nur SMGW-Wirkzertifikate. Der GWA beantragt die Suspendierung über die Web-Service-Schnittstelle, ausnahmsweise per S/MIME signierter und verschlüsselter E-Mail, stets für das vollständige Zertifikatstripel und mit Begründung.
- (3) Der GWA meldet jede von ihm veranlasste Suspendierung als Sicherheitsvorfall mit Begründung per S/MIME signierter E-Mail. Fehlt die Begründung nach 7 Kalendertagen, erinnert die DARZ.CA den GWA. Geht sie innerhalb weiterer 3 Arbeitstage nicht ein, meldet die DARZ.CA den Vorgang als Sicherheitsvorfall an die SM-PKI-Root.
- (4) Eine Suspendierung dauert höchstens 30 Tage. Danach sperrt die DARZ.CA die Zertifikate endgültig. Eine Rücknahme der Suspendierung dient ausschließlich der Beantragung neuer Zertifikate; nach deren Installation lässt der GWA die alten Zertifikate endgültig sperren und dokumentiert seine Entscheidung nachvollziehbar.
- (5) Die DARZ.CA informiert den GWA über den Abschluss der Suspendierung per S/MIME signierter E-Mail.
- (6) Bei Außerbetriebnahme eines SMGW lässt der GWA dessen Zertifikate über die Web-Service-Schnittstelle sperren.

9. Leistungen der DARZ.CA

9.1 Betrieb

- (1) DARZ betreibt die DARZ.CA gemäß BSI-CP, TR-03109-4, TR-03145 und DARZ-CP. DARZ ist nach ISO/IEC 27001 und nach TR-03145 zertifiziert und hält diese Zertifizierungen nachweislich aufrecht.
- (2) Die DARZ.CA verpflichtet von ihr beauftragte Dienstleister, etwa Betreiber von Verzeichnisdiensten, auf die BSI-CP und die DARZ-CP.

9.2 Veröffentlichung

- (1) Alle ausgestellten Zertifikate werden unmittelbar nach der Ausstellung im Verzeichnisdienst (LDAPS) der DARZ.CA veröffentlicht.
- (2) Unter <https://da-rz.de/de/sm-pki-darz/> veröffentlicht die DARZ.CA:
 - ihre Kontaktdaten,
 - die CA-Zertifikate mit SHA-256-Fingerprint und Angabe des Formats,
 - je Sub-CA-Zertifikat die Parameter für den Zugriff auf Verzeichnisdienst und Sperrliste,
 - die DARZ-CP und diese Vertragsbedingungen,

Vertragsbedingungen zur Nutzung von Zertifikaten der DARZ.CA unterhalb der Smart Metering-PKI



- Erläuterungen zum Sperrverfahren.

(3) Neue CA-Zertifikate veröffentlicht die DARZ.CA unmittelbar nach ihrer Erzeugung. Vor der ersten Nutzung eines CA-Zertifikats gleicht der Teilnehmer dessen SHA-256-Fingerprint mit dem veröffentlichten Wert ab.

9.3 Fehlermeldungen und Rückfragen

Die DARZ.CA nimmt Fehlermeldungen zu Zertifikaten, Zurückweisungen und Rückfragen unter DARZ.CA@da-rz.de entgegen.

9.4 Testumgebung

(1) Die DARZ.CA stellt die DARZ-Test.CA bereit. Sie ist technisch von der Wirkumgebung getrennt und verwendet eigene Schlüssel. Sie dient der Erstregistrierung und dem Test systemkritischer Vorgänge, etwa des Wechsels des Vertrauensankers.

(2) Zertifikate der DARZ-Test.CA dürfen nicht im Wirkbetrieb verwendet werden.

9.5 Service Level

(1) Die DARZ.CA sagt für die Web-Service-Schnittstelle, den Verzeichnisdienst, den Sperrdienst und die Sperrlisten eine Verfügbarkeit von 99,98 % zu. Messzeitraum, Reaktionszeiten und Gutschriften regelt das SLA.

(2) Geplante Wartungen stimmt die DARZ.CA mit dem Teilnehmer ab.

9.6 Schlüsselwechsel der DARZ.CA

(1) Die DARZ.CA wechselt ihren Schlüssel spätestens, bevor die Laufzeit auszustellender Teilnehmerzertifikate die Restlaufzeit ihres Sub-CA-Zertifikats übersteigen würde. Das Folgezertifikat beantragt sie über die gesicherte Web-Service-Schnittstelle der SM-PKI-Root.

(2) Der Teilnehmer bindet neue CA-Zertifikate rechtzeitig in seine Systeme ein.

9.7 Protokollierung und Archivierung

Die DARZ.CA protokolliert und archiviert alle für den Zertifizierungsbetrieb relevanten Vorgänge nach DARZ-CP Kap. 6.2.4 und 6.2.5. Die Aufbewahrung beträgt mindestens zehn Jahre; längere Fristen der SM-PKI-Root gehen vor.

9.8 Einstellung des CA-Betriebs

(1) Stellt die DARZ.CA ihren Betrieb ein, stimmt sie dies mit der SM-PKI-Root ab. Sie informiert alle Teilnehmer und vertrauenden Parteien mit mindestens drei Monaten Vorlauf.

(2) Soweit mit der SM-PKI-Root vereinbart, gehen ihre Aufgaben auf eine Nachfolgeorganisation über. Andernfalls erfüllt die DARZ.CA ihre Aufgaben für die Restlaufzeit der Zertifikate.

(3) Mit Einstellung des Betriebs werden alle ausgestellten Zertifikate gesperrt, die privaten CA-Schlüssel vernichtet und die Sperrlisten veröffentlicht.

(4) Für einen Wechsel zu einer anderen Sub-CA gilt die „DARZ.CA Wechsel- und Exit-Information“ in der jeweils unter <https://darz.de/de/sm-pki-darz/> veröffentlichten Fassung.

10. Beendigung der Teilnahme

(1) Die Beendigung der Teilnahme kann der Teilnehmer oder die DARZ.CA einleiten. Die Beendigung der Teilnahme an der SM-PKI ist von der Kündigung des Vertrags zu unterscheiden.

(2) Die Beendigung erfolgt in drei Schritten:

1. Der Teilnehmer informiert alle Unternehmen (EMT, GWH, GWA), mit denen er im Rahmen der Nutzung seiner Zertifikate in Kontakt stand.
2. Die betroffenen Zertifikate werden so ausgetauscht, dass ein kontinuierlicher Betrieb möglich bleibt. Den Zeitrahmen stimmen die Beteiligten ab. Ausgenommen sind Sperrungen wegen einer Gefahr für den sicheren Betrieb der DARZ.CA oder der SM-PKI.
3. Alle Zertifikate des Teilnehmers werden gesperrt. Die S/MIME-Zertifikate seiner Ansprechpartner werden bei der DARZ.CA so gekennzeichnet, dass sie nicht mehr für die vertrauliche Kommunikation genutzt werden.

(3) Läuft ein Zertifikat ab, ohne dass ein Folgezertifikat beantragt wird, endet die Nutzung dieses Zertifikats mit Ablauf seiner Gültigkeit.

Vertragsbedingungen zur Nutzung von Zertifikaten der DARZ.CA unterhalb der Smart Metering-PKI



11. Laufzeit und Änderungen

- (1) Diese Vertragsbedingungen gelten für die Laufzeit der Beauftragung. Die Pflichten zum Schutz vertraulicher Informationen und personenbezogener Daten bestehen über das Vertragsende hinaus fort.
- (2) Änderungen, die zwingend aus Vorgaben des BSI, der SM-PKI-Root oder aus geltendem Recht folgen, werden mit Inkrafttreten der jeweiligen Vorgabe wirksam. Die DARZ.CA kündigt sie per S/MIME signierter E-Mail an, soweit möglich mit angemessenem Vorlauf.
- (3) Sonstige Änderungen teilt die DARZ.CA mindestens sechs Wochen vor ihrem Inkrafttreten per S/MIME signierter E-Mail mit. Sie werden nur mit Zustimmung des Teilnehmers in Textform wirksam; eine S/MIME signierte E-Mail genügt. Stimmt der Teilnehmer nicht zu, gilt die bisherige Fassung fort.
- (4) Ändern sich die Pflichten des Teilnehmers durch eine Änderung nach Abs. 2 wesentlich, kann er den Vertrag außerordentlich mit einer Frist von drei Monaten kündigen.
- (5) Diese Regelung gilt entsprechend für Änderungen der DARZ-CP.
- (6) Der Teilnehmer kann die aktuellen Vertragsdokumente jederzeit anfordern. Sie sind zudem unter <https://da-rz.de/de/sm-pki-darz/> veröffentlicht.

12. Datenschutz und Vertraulichkeit

- (1) DARZ verarbeitet personenbezogene Daten der Ansprechpartner und Vertreter, soweit dies für Registrierung, Zertifikatsbetrieb und die Erfüllung rechtlicher Pflichten erforderlich ist. Rechtsgrundlagen sind Art. 6 Abs. 1 lit. b, c und f DSGVO. Einzelheiten enthält die Datenschutzerklärung der DARZ GmbH.
- (2) Zertifikatsinhalte und Sperrinformationen sind nicht vertraulich. Zertifikate stehen den Teilnehmern der SM-PKI im Verzeichnisdienst zur Verfügung, Sperrlisten sind öffentlich abrufbar. Alle übrigen Informationen über den Teilnehmer behandelt DARZ vertraulich.
- (3) Gegenüber der SM-PKI-Root übermittelt die DARZ.CA Informationen, soweit die BSI-CP dies vorsieht, etwa bei Sicherheitsvorfällen oder Sperrungen systemrelevanter Zertifikate. Gegenüber anderen Behörden legt DARZ Informationen nur offen, soweit sie rechtlich dazu verpflichtet ist.

13. Haftung und Freistellung

- (1) Die Haftung der DARZ richtet sich nach den AGB der DARZ GmbH in der jeweils vereinbarten Fassung.
- (2) Der Teilnehmer stellt DARZ von Ansprüchen Dritter frei, die darauf beruhen, dass er oder sein Dienstleister schuldhaft
 - Zertifikate oder private Schlüssel entgegen Ziff. 3.2 oder Ziff. 5 verwendet,
 - bei Registrierung oder Beantragung unrichtige Angaben macht oder
 - eine Kompromittierung oder einen Sperrgrund nicht unverzüglich meldet.
- (3) Führt die DARZ.CA eine Sperrung auf einen nach Ziff. 8.3 authentisierten Sperrantrag ordnungsgemäß durch, haftet sie nicht für deren Folgen.

14. Schlussbestimmungen

14.1 Anwendbares Recht

Es gilt deutsches Recht. Die Zertifikate der DARZ.CA sind keine qualifizierten Zertifikate im Sinne der Verordnung (EU) Nr. 910/2014 (eIDAS-VO).

14.2 Gerichtsstand

Erfüllungsort und ausschließlicher Gerichtsstand für alle Streitigkeiten aus oder im Zusammenhang mit diesen Vertragsbedingungen ist Darmstadt, soweit der Teilnehmer Kaufmann, juristische Person des öffentlichen Rechts oder öffentlich-rechtliches Sondervermögen ist. Ein Schiedsverfahren findet nicht statt.

14.3 Höhere Gewalt

Für Fälle höherer Gewalt gelten die AGB.

14.4 Abtretung

Rechte aus diesen Vertragsbedingungen kann der Teilnehmer nur mit Zustimmung der DARZ abtreten.

Vertragsbedingungen zur Nutzung von Zertifikaten der DARZ.CA unterhalb der Smart Metering-PKI



14.5 Vollständigkeit und Form

- (1) Diese Fassung ersetzt alle vorherigen Fassungen der Vertragsbedingungen. Mündliche Nebenabreden bestehen nicht.
(2) Änderungen und Ergänzungen bedürfen der Textform, soweit Ziff. 11 nichts anderes bestimmt.

14.6 Salvatorische Klausel

Sollten einzelne Bestimmungen dieser Vertragsbedingungen unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt. An die Stelle der unwirksamen Bestimmung tritt die wirksame Regelung, die deren Sinn und Zweck am nächsten kommt. Gleiches gilt für Lücken.

14.7 Geistiges Eigentum

Die DARZ GmbH ist Urheber dieses Dokuments. Es darf unverändert an Dritte weitergegeben werden.

15. Kontakt

Zweck	Kontakt
Registrierungsstelle, Anträge, Fehlermeldungen	DARZ.CA@da-rz.de (S/MIME signiert und verschlüsselt)
Sperranträge	DARZ.CA@da-rz.de, Web-Service-Schnittstelle, Sperrhotline laut Kommunikationsmatrix
Zentrale	+49 6151 8762-100
Veröffentlichungen	https://da-rz.de/de/sm-pki-darz/
Verantwortlich für die DARZ.CA	DARZ GmbH, Geschäftsführung, Jürgen Henzler, Julius-Reiber-Straße 11, 64293 Darmstadt

16. Referenzdokumente

Dokument	Version	Herausgeber
Certificate Policy der Smart Metering-PKI	1.1.2	BSI
TR-03109-4 Smart Metering PKI	1.2.1	BSI
TR-03109-6 Smart-Meter-Gateway-Administration	jeweils gültige Fassung	BSI
TR-03116-3 Kryptographische Vorgaben, Teil 3: Intelligente Messsysteme	jeweils gültige Fassung	BSI
TR-03145-1 Secure Certification Authority operation	jeweils gültige Fassung	BSI
BSI-CC-PP-0073 Protection Profile Smart Meter Gateway	jeweils gültige Fassung	BSI
Key Lifecycle Security Requirements	1.0.3	BSI
Certificate Policy der DARZ.CA	jeweils gültige Fassung	DARZ GmbH
Service Level Vereinbarung	jeweils gültige Fassung	DARZ GmbH
AGB der DARZ GmbH	jeweils vereinbarte Fassung	DARZ GmbH

Vertragsbedingungen zur Nutzung von Zertifikaten der DARZ.CA unterhalb der Smart Metering-PKI



Dokument	Version	Herausgeber
VA_TR-03145 Onboarding PKI	jeweils gültige Fassung	DARZ GmbH
DARZ.CA Wechsel- und Exit-Information	jeweils veröffentlichte Fassung	DARZ GmbH