Vertragsbedingungen zur Nutzung eines GWH-/ GWA-/ EMT-Zertifikats der DARZ GmbH unterhalb der Smart Metering-PKI

Vertragsbedingungen zur Nutzung eines GWH-/ GWA-/ EMT-Zertifikats der DARZ GmbH unterhalb der Smart Metering-PKI

Inhalt

Vertragsbedingungen zur Nutzung eines GWH-/ GWA-/ EMT-Zertifikats der DARZ GmbH unterhalb der Smart Metering-PKI

1. Dokumenteninformationen

1.1 Bearbeitungsvermerk

	Name und Funktion	Version	Datum	Unterschrift
Erstellt von:	Tiziana Knecht	3.3	01.04.2026	
Geprüft von:	Jürgen Henzler	3.3	01.04.2026	
Genehmigt von:	Raphael Munasypow	3.3	01.04.2026	
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.Req.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

1.3 Gleichstellungshinweis

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

Vertragsbedingungen zur Nutzung eines GWH-/ GWA-/ EMT-Zertifikats der DARZ GmbH unterhalb der Smart Metering-PKI

2. Einleitung

Die volatile Stromerzeugung aus erneuerbaren Energien erfordert es, Netze, Erzeugung und Verbrauch von verschiedenen Energien wie Strom oder Gas effizient und intelligent miteinander zu verknüpfen. Dabei muss die fluktuierende Stromerzeugung aus erneuerbaren Energien und der Stromverbrauch bedarfs- und verbrauchsorientiert durch intelligente Netze und technische Systeme ausbalanciert werden.

Zur Unterstützung dieses Ziels werden intelligente Messsysteme (Smart Metering Systems) eingesetzt, die dem Letztverbraucher eine höhere Transparenz über den eigenen Energieverbrauch bieten und die Basis dafür schaffen, seinen Energieverbrauch an die Verfügbarkeit von Energie anzupassen. Die zentrale Kommunikationseinheit des intelligenten Messsystems stellt das Smart Meter Gateway (SMGW oder im Folgenden auch Gateway genannt) in den Haushalten der Letztverbraucher dar. Diese Einheit trennt das Weitverkehrsnetz (WAN), d. h. das Netz zu den Backendsystemen von Smart Meter Gateway Administratoren (GWA) und externen Marktteilnehmern (EMT), von dem im Haushalt befindlichen Heimnetz (HAN) und den lokal angebundenen Zählern im metrologischen Netz (LMN). Die Hauptaufgaben des SMGW bestehen dabei in der technischen Separierung der angeschlossenen Netze, der sicheren Kommunikation in diese Netze, der Erfassung, Verarbeitung und Speicherung empfangener Messwerte verschiedener Zähler, der sicheren Weiterleitung der Messwerte an die Backend-systeme externer autorisierter Marktteilnehmer im WAN sowie der Verarbeitung von Administrationstätigkeiten durch den jeweiligen GWA.

Zur Absicherung der Kommunikation im WAN ist eine gegenseitige Authentisierung der Kommunikationspartner erforderlich. Die Kommunikation erfolgt dabei stets über einen verschlüsselten und integritätsgesicherten Kanal. Zudem werden Daten vom SMGW vor der Übertragung zur Integritätssicherung signiert und zur Gewährleistung des Datenschutzes für den End-empfänger 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 (TR-3109-4) spezifiziert. Sie wird in die folgenden drei Hierarchiestufen unterteilt:

- Die 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.

Die DARZ GmbH betreibt in diesem Kontext eine Sub-CA, die im Folgenden als DARZ.CA bezeichnet wird. Vor diesem Hintergrund entspricht die in diesem Dokument genannte Sub-CA der DARZ.CA.

Das vorliegende Dokument stellt die Zertifizierungsrichtlinie (CP) inkl. der Erklärung zum Zertifizierungsbetrieb (CPS) der DARZ.CA (Sub-CA der DARZ GmbH) dar und beinhaltet Sicherheitsvorgaben sowie Beschreibungen technischer, organisatorischer und rechtlicher Aspekte.

Die DARZ.CA CP/CPS unterwirft sich der CP-SM-PKI und beschreibt die Vorgaben der DARZ.CA und deren Umsetzung.

Die in der CP verwendeten Inhalte werden dem [RFC 2119] entsprechend mit folgenden deutschen Schlüsselworten beschrieben:

- MUSS bedeutet, dass es sich um eine normative Anforderung handelt.
- DARF NICHT / DARF KEIN bezeichnet den normativen Ausschluss einer Eigenschaft.
- 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 Vertragsbedingungen sind eine Ergänzung zu den Allgemeinen Geschäftsbedingungen (AGB) der DARZ GmbH und spezifizieren zusätzlich die durch den Endnutzer einzuhaltenden Vertragsbedingungen für die Nutzung eines durch die DARZ GmbH ausgestellten Zertifikats sowie die durch den Vertrag zugesicherten Service Leistungen.

3. Vertragsbedingungen zur Nutzung eines GWH-/ GWA-/ EMT- Zertifikats der DARZ GmbH unterhalb der Smart Metering-PKI

Die Vertragsbedingungen zur Nutzung eines GWH-/ GWA-/ EMT- Zertifikats der DARZ GmbH (Kurzform: Vertragsbedingungen) unterhalb der Smart Metering-PKI sind Bestandteil des Angebotes und somit der Beauftragung. Sie müssen gegengezeichnet werden und der Beauftragung beigefügt sein. Die Allgemeinen Geschäftsbedingungen (Kurzform: AGB) sind eben-falls Vertragsbestandteil der Beauftragung.

Änderungen in den Vertragsbedingungen müssen schriftlich in signierter Form an die verantwortliche Person der Vertragsnehmer gesendet werden. Der Vertragsnehmer muss der Veränderung zustimmen. Dies kann mit einer signierten MAIL - Kommunikation erfolgen.

Der Vertragsnehmer kann jederzeit die aktuellen Vertragswerke anfordern.

3.1 Certificate Policy der DARZ.CA

Certificate Policy der DARZ.CA ist Vertragsbestandteil der Vertragsbedingungen zur Nutzung eines GWH-/ GWA-/ EMT- Zertifikats der DARZ GmbH

Die Certificate Policy der DARZ.CA. ist öffentlich (https://www.da-rz.de/de/ueber-darz/unternehmen/pki/sm-pki/). Sie ist Vertragsbestandteil der Vertragsbedingungen. In der Certificate Policy (kurz genannt CP) sind die Rollen und ihre Aufgaben beschrieben. Sollte die DARZ GmbH Veränderungen in der CP vornehmen, werden dem Vertragspartner diese umgehend mitgeteilt. Die DARZ GmbH darf jeder Zeit Anpassungen an der CP vornehmen.

3.2 Zertifikatsnehmer und Zertifikatsnutzer

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.

Zertifikatsnutzer im Sinne dieser DARZ.CA Policy sind alle natürlichen und juristischen Personen bzw. technischen

Komponenten, die Zertifikate aus der SM-PKI, insbesondere auch Zertifikate aus der DARZ.CA, für die Erledigung von Geschäftsprozessen/Aufgaben verwenden.

Zertifikatsnutzer sind Kommunikationspartner (Personen, Organisationen bzw. Systeme), die am zertifikatsbasierten Verfahren zur sicheren E-Mail-Kommunikation mit der DARZ GmbH teilnehmen.

3.3 Erlaubte Verwendung von Zertifikaten

Die im Rahmen der DARZ.CA ausgestellten Zertifikate dürfen innerhalb der SM-PKI für alle Verfahren genutzt werden, die von den im Zertifikat enthaltenen Schlüsselverwendungszwecken ermöglicht werden. Die Anwendungsfälle für den Einsatz der Schlüssel und Zertifikate sind in der (CP-SM-PKI) und (TR-3109-4) beschrieben.

Die DARZ.CA erstellt Zertifikats-Sets (TLS, ENC, SIG) für die SM-PKI Teilnehmer GWA, GWH, SMGW sowie EMT und das DARZ.CA CA-TLS Zertifikat.

Teilnehmer bzw. Zertifikatinhaber sind selbst für die Nutzung in den Anwendungsprogrammen zuständig, sowie für die Prüfung, ob die damit möglichen Anwendungen deren Sicherheitsanforderungen genügen.

Die entsprechenden Technischen Sicherheitsmaßnahmen im Zusammenhang mit den Schlüssel(paaren) und den Zertifikaten sind in Kapitel 6 der CP beschrieben.

3.4 Verbotene Verwendung von Zertifikaten

Die private Verwendung der Zertifikate ist untersagt.

Geschäftspartner dürfen die Zertifikate nicht ohne die Genehmigung der DARZ.CA über die in der Certificate Policy der DARZ.CA Ziffer 1.4.1 beschriebene Verwendung hinaus im Zusammenhang mit Geschäftsangelegenheiten mit Dritten nutzen.

4. Registrierungsverfahren

4.1 Wer kann einen Zertifikatsantrag stellen?

Die Beantragung eines Zertifikates für einen Geschäftspartner erfolgt auf Initiative von Beschäftigten der DARZ GmbH über einen elektronischen Antragsworkflow, der nach Genehmigung durch den direkten Vorgesetzten des Beschäftigten der DARZ GmbH an die DARZ.CA übersendet wird.

Ein im Rahmen des elektronischen Antragsprozesses zu erzeugendem Antragsformular wird dem Geschäftspartner von der DARZ.CA zur Unterschrift übersandt.

4.2 Beantragungsprozess und Zuständigkeiten

Die Beantragung von Zertifikaten erfolgt im Rahmen eines mehrstufigen Registrierungsprozesses der DARZ.CA. Der Onboardingprozess wird in dem Dokument VA_TR-03145 Onboarding PKI erläutert, welches dem Kunden im Zuge des Registrierungsprozesses zur Verfügung gestellt wird.

Der Vertragspartner muss jährlich einen aktuellen Handelsregisterauszug per Mail oder Post an die DARZ.CA senden.

Der Vertragspartner muss jährlich die Registrierung, Antragsdaten und die aktuelle Kommunikationsmatrix per SMIME signierter und verschlüsselter Mail an die DARZ.CA senden und somit bestätigen, dass er weiterhin aktiv ist.

Die DARZ.CA spricht den Kunden proaktiv an und dokumentiert die Durchführung in Confluence unter „Überprüfung der Ansprechpartner Sub.CA“.

4.3 Annahme oder Ablehnung von initialen Zertifikatsanträgen

Trotz Erfüllung der formalen Voraussetzungen besteht kein Anspruch auf Erteilung eines Zertifikats. Die DARZ.CA bleibt in ihrer Vergabeentscheidung frei.

4.4 Fristen für die Bearbeitung von Zertifikatsanträgen

Die Bearbeitungsdauer von Zertifikatsanträgen beträgt grundsätzlich maximal eine Woche.

4.5 Ausgabe von Zertifikaten

Nach der erfolgreichen Bearbeitung eines Zertifikatsantrages wird das Zertifikat DARZ.CA über die Gateway-Software bereitgestellt. Zusätzlich KANN ein Versand per E-Mail an den Zertifikatsnehmer erfolgen. Eine Ausnahme stellen initiale Zertifikate dar welche ausschließlich über die sichere Austauschplattform der DARZ GmbH (Secure Data Space / Kategorisierung der Dateien “streng vertraulich“) und in Ausnahmefällen per signierter und verschlüsselter E-Mail an den Antragsteller versendet werden.

Öffentliche Schlüssel der DARZ.CA finden Sie unter https://www.da-rz.de/de/ueber-darz/unternehmen/pki/sm-pki/

4.6 Benachrichtigung des Zertifikatsnehmers über die Ausgabe des Zertifikats

Nach Erstellung wird das Zertifikat dem Zertifikatsnehmer in geeigneter Weise durch die DARZ.CA sicher übermittelt.

4.7 Annahme von Zertifikaten

Die Annahme des Zertifikates erfolgt mit der Bestätigung des Empfangs bzw. mit der Nutzung des Zertifikats.

4.8 Veröffentlichung des Zertifikats durch die CA

Eine Veröffentlichung der Zertifikate in einem Verzeichnisdienst wird nicht ausgeschlossen.

4.9 Gültigkeitsdauer der Zertifikate

Die ausgestellten Zertifikate haben eine Gültigkeitsdauer entsprechend den geforderten rechtlichen Vorgaben. Ausnahmen bedürfen einer zusätzlichen schriftlichen Vereinbarung.

5. Sperrung von Zertifikaten

Siehe Cerificate Policy der DARZ.CA

5.1 Identifizierung und Authentifizierung von Anträgen auf Sperrung

Die Sperrung eines Zertifikates kann von den folgenden Beteiligten initiiert werden

- Zertifikatsinhaber
- DARZ.CA
- ROOT.CA

5.2 Gründe für eine Zertifikatssperrung

Ein Zertifikat muss gesperrt werden, wenn mindestens einer der folgenden Gründe Eintritt:

- Die im Zertifikat enthaltenen Angaben sind nicht oder nicht mehr gültig.
- Der private Schlüssel wurde kompromittiert.
- Der Zertifikatsnehmer ist nicht mehr berechtigt, das Zertifikat zu nutzen.
- Der Zertifikatsnehmer benötigt das Zertifikat nicht mehr.
- Der Zertifikatsnehmer hält Verpflichtungen gemäß diesen Vertragsbedingungen nicht ein.
- Die DARZ.CA stellt ihren Zertifizierungsbetrieb ein. In diesem Fall werden sämtliche von der DARZ.CA ausgestellten Zertifikate gesperrt.
- Der private Schlüssel der ausstellenden oder einer übergeordneten Root-CA wird kompromittiert. In diesem Fall werden sämtliche von diesen CA's ausgestellte Zertifikate gesperrt.
- Die Algorithmen, die Schlüssellänge oder die Gültigkeitsdauer des Zertifikates bieten keine ausreichende Sicherheit mehr. Die DARZ.CA behält sich vor, die betreffenden Zertifikate zu sperren.

5.3 Schlüsselerneuerung

Den Prozess der Schlüsselerneuerung finden Sie in der aktuellen Certificate Policy der DARZ.CA Kapitel 3.

https://www.da-rz.de/de/ueber-darz/unternehmen/pki/sm-pki/

5.4 Sperrverfahren

Die Sperrung eines Zertifikates kann von einer berechtigten Person des Zertifikatsnehmer beauftragt werden.

Der Benutzer kann die Sperrung seines eigenen Zertifikates jederzeit beantragen, auch wenn keiner oben genannten Gründe vorliegt.

Die Sperrung eines Zertifikates kann wie folgt erfolgen:

- per elektronischer signierter Mail
- telefonisch
- schriftlich

Die DARZ.CA führt die Sperrung des Zertifikates an der entsprechenden CA durch und veröffentlicht die entsprechende Sperrliste. Der Zertifikatsnehmer wird über die Sperrung des Zertifikates unterrichtet.

Jährlich muss der Vertragspartner alle bei der DARZ.CA registrierten Personen schriftlich bestätigen.

5.5 Aktualisierungs- und Prüfungszeiten bei Sperrungen

Die Zertifikatsnehmer sind verpflichtet, bei Bekanntwerden eines Sperrgrundes unverzüglich die Sperrung des Zertifikates zu veranlassen.

Die Sperrung des Zertifikates wird von der DARZ.CA unverzüglich nach Zugang des Sperrantrages durchgeführt.

Sperrinformationen werden mittels Sperrlisten veröffentlicht. Zur Prüfung der Gültigkeit von Zertifikaten muss der Zertifikatsnutzer jeweils die aktuell veröffentlichte Sperrliste verwenden.

CA-Sperrlisten werden laut CP zu Verfügung gestellt. CP Kapitel 2, 4.9,

Wird aufgrund einer Sperrung eines Zertifikates eine neue Sperrliste erstellt, wird diese unverzüglich veröffentlicht und ersetzt die bisher gültige Sperrliste unabhängig von deren ursprünglich angegebener Gültigkeitsdauer.

Eine neue Sperrliste enthält solange die Informationen über gesperrte Zertifikate, bis alle Zertifikate abgelaufen sind.

Die Veröffentlichung von Sperrlisten wird unmittelbar nach deren Erzeugung veranlasst.

6. Beendigung der Teilnahme

Eine Beendigung der Zertifikatsnutzung durch den Zertifikatsinhaber erfolgt entweder durch die Sperrung des Zertifikates oder indem nach Ablauf der Gültigkeit kein neues Zertifikat beantragt wird.

7. Protokollierung und Archivierung von Aufzeichnungen

Die nachfolgenden Ereignisse werden protokolliert und dokumentiert:

- Systeminitialisierung,
- Zertifizierungsanträge,
- Registrierung der Benutzer,
- Schlüsselerzeugung für CA, Root-CA, Benutzer,
- Zertifikatserstellung für CA, Root-CA, Benutzer,
- Datensicherungen für CA, Root-CA
- Zertifikatsveröffentlichung CA, Root-CA
- Auslieferung des privaten Schlüssels und des Zertifikates,
- Sperranträge,
- Sperrung eines Zertifikates,
- Erstellung einer Sperrliste,
- Veröffentlichung einer Sperrliste.
- Identverfahren

Darüber hinaus werden Störfälle und besondere Betriebssituationen erfasst (Incident-Management).

Die Ordnungsmäßigkeit des Zertifizierungsbetriebes wird im Rahmen der risikoorientierten Prüfungen des Bereiches Revision der DARZ GmbH vorgenommen. Bei Verdacht auf Unregelmäßigkeiten wird eine umgehende Prüfung veranlasst.

Sämtliche Daten, die für den Zertifizierungsprozess relevant sind werden archiviert. Die Archivierung wird bei der betriebsverantwortlichen Stelle der DARZ.CA vorgenommen. Die Archive werden gegen Zugriff, Manipulation und Vernichtung geschützt. Die Aufbewahrungszeiten orientieren sich an gesetzlichen Fristen (10 Jahre), den Grundsätzen der Revisionssicherheit sowie weiteren internen Regelungen. Als Mindestaufbewahrungszeiten gelten die Fristen der Root.CA.

Die Protokolldaten werden zusammen mit anderen relevanten Daten einem regelmäßigen Backup unterzogen. Protokolle auf Papier werden in verschließbaren Schränken verwahrt.

Datensicherungen werden arbeitstäglich nach der Durchführung von

- Schlüsselausgaben,
- Sperrungen von Zertifikaten sowie
- der Erstellung von Sperrlisten

durchgeführt. Sie werden als Original- und Backupdatensicherungen vorgenommen und sicher in unterschiedlichen Gebäudebrandabschnitten hinterlegt.

8. Schlüsselwechsel der CA

Ein Schlüsselwechsel der Zertifizierungsstelle erfolgt spätestens dann, wenn die Gültigkeit der auszustellenden Benutzerzertifikate die Restlaufzeit der CA übersteigen würde.

Die Beantragung und Auslieferung eines Folgezertifikates für die Sub-CA durch die Root-CA geschieht über den gesicherten Web-Service „Metering.CA“.

9. Auflösen der Zertifizierungsstelle

Im Fall der Einstellung des Betriebes der DARZ.CA werden die nachfolgenden Maßnahmen ergriffen:

- Abstimmung der Auflösung mit der SM-PKI-Root
- falls mit der SM-PKI-Root vereinbart, werden alle Aufgaben der SubCA an eine Nachfolgeorganisation übertragen (es ist vorzugsweise eine Nachfolgeorganisation zu wählen, welche die gleiche Software nutzt wie die DARZ.CA.
- Information aller Zertifikatsnehmer sowie vertrauenden Parteien mit einer Vorlauffrist von mindestens drei Monaten.
- Sperrung aller Benutzerzertifikate sowie der Zertifikate der Zertifizierungsstellen.
- Vernichtung der privaten Schlüssel der Zertifizierungsstellen.
- Veröffentlichung der entsprechenden CA- und Root-CA-Sperrlisten.

10. Rollenkonzept

Head of CA Operations:	Trägt die umfassende Verantwortung für das gesamte CA-Geschäft
CA Operator:	Generiert Schlüsselpaare, Zertifikate und Sperrlisten
RA Operator:	Verwaltet die Registrierungen, Suspendierungen und Sperrungen
IT Security Officer:	Plant und überwacht die Implementierung von Sicherheitsmaßnahmen die gesamte CA Betreffend, einschließlich aller technischen, organisatorischen und physikalischen Maßnahmen
System Administrator:	Verantwortlich für die Konfiguration und Instandhaltung der IT-Infrastruktur einschließlich der Netzwerke, Datenbanken und Server
Access Manager:	Verwaltet Rollen, technische und organisatorische Zugangsberechtigungen und die befugten Personen
Revisor:	Interner Auditor, zuständig für die regelmäßige Überprüfung von Logdaten, Datenbanken und Papierdokumentationen der CA auf Unregelmäßigkeiten gemäß der internen Auditplanung

Für jede definierte Rolle wurde ein Vertreter ernannt.

11. Weiterführende Informationen, Zeitpunkt und Häufigkeit der Veröffentlichung

Die DARZ GmbH stellt die Informationen zur DARZ.CA auf der Homepage

− unter https://www.da-rz.de/de/ueber-darz/unternehmen/PKI/

sowie im Intranet (Zugriff nur für Beschäftigte der DARZ sowie deren externe Mitarbeiterinnen und Mitarbeiter) zur Verfügung.

Es werden folgende Informationen veröffentlicht:

- CA-Zertifikate mit Fingerprints,
- Root-CA-Zertifikate mit Fingerprints,
- Sperrlisten,
- Erläuterungen zum Sperrverfahren,

- Zertifizierungsrichtlinie (CP) und Regelungen für den Zertifizierungsbetrieb (CPS).

Für die Veröffentlichung von CA-/Root-CA-Zertifikaten, Sperrlisten sowie CP/CPS gelten die folgenden Intervalle:

CA- / Root-CA-Zertifikaten:	Unmittelbar nach Erzeugung
Sperrlisten:	Nach Sperrungen, sonst turnusmäßig
CP / CPS:	Nach Erstellung bzw. Aktualisierung

12. SHA256 Fingerprint

Das DARZ-CA Zertifikat hat den folgenden SHA256 Fingerprint:

https://www.da-rz.de/de/ueber-darz/unternehmen/pki/sm-pki/

13. Ansprechpartner

Organisation	DARZ GmbH
Abteilung	Geschäftsleitung
Person	Jürgen Henzler
Adresse	Julius-Reiber-Straße 11, D-64293 Darmstadt
Telefon	+49 6151 8762-100
E-Mail	j.henzler@da-rz.de
Webseite	www.da-rz.de

14. Schutz personenbezogener Daten

Die Speicherung und Verarbeitung von personenbezogenen Daten richtet sich nach den gesetzlichen Datenschutzbestimmungen. Jegliche Daten über Zertifikatsnehmer und Teilnehmer der DARZ.CA werden vertraulich behandelt. Eine Offenlegung findet gegenüber staatlichen Instanzen nur bei Vorliegen entsprechender Entscheidungen in Übereinstimmung mit den geltenden Gesetzen statt.

Der Zertifikatsinhaber stimmt der Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten durch die DARZ.CA zu, soweit dies zur Leistungserbringung erforderlich ist. Darüber hinaus können alle Informationen veröffentlicht werden, die als nicht vertraulich behandelt werden.

15. Geistiges Eigentumsrecht

Die DARZ GmbH ist Urheber dieses Dokumentes. Das Dokument kann unverändert an Dritte weitergegeben werden.

16. Zusicherungen und Garantien

16.1 Zusicherungen und Garantien der CA

Die DARZ.CA verpflichtet sich, diesen Vertragsbedingungen sowie den Bestimmungen der Zertifizierungsrichtlinie (CP) und den Regelungen für den Zertifizierungsbetrieb (CPS) zu folgen.

16.2 Zusicherungen und Garantien der Zertifikatsnehmer und -nutzer

Die Zertifikatsnehmer und -nutzer sind zur Einhaltung der Bestimmungen der Zertifizierungsrichtlinie (CP) und den Regelungen für den Zertifizierungsbetrieb (CPS) verpflichtet

16.3 Zusicherungen und Garantien anderer PKI-Teilnehmer

Von der DARZ.CA beauftragte Dienstleister (z. B. Betreiber von Verzeichnisdiensten) werden auf die Einhaltung der Zertifizierungsrichtlinie (CP) und den Regelungen für den Zertifizierungsbetrieb (CPS) verpflichtet

16.4 SLA-Verfügbarkeit

Verfügbarkeit 7x24 (Mo-So)

Reaktionszeit Störungen > unmittelbar

Die DARZ gewährleistet eine Verfügbarkeit pro Monat von 99.85 %

Die Service Verfügbarkeitszeit gliedert sich in fixe und variable Zeiten und ist wie folgt definiert:

$$\left[\left(\frac{Betriebszeit - Störung - geplanteWartung}{Betriebszeit - geplanteWartung}\right) * 100\right] \geq Verfügbarkeit(\%)$$

Das bedeutet im Einzelnen:

- Betriebszeit: ist die Verfügbarkeitsperiode (z. B. bei 7x24x365 die Summe aller Stunden pro Jahr) innerhalb derer die Verfügbarkeit vereinbart wird.
- Störung: ist ungeplante Ausfallzeit (z. B. ungeplante Wartung oder sonstiger Stillstand)
- Ausgeschlossene Zeiten sind:
    - Alle geplanten Ausfallzeiten in Abstimmung mit dem Kunden (Wartung)
    - Höhere Gewalt
- Die Verfügbarkeitszeit definiert sich zu:
    - Der Betriebszeit ./. geplante Wartung in Abstimmung mit dem Kunden ./. Nichtverfügbarkeit bedingt durch höhere Gewalt

Als Ausfallzeit gilt die Zeitspanne der Wiederherstellung der Verfügbarkeit während der vereinbarten Service Zeit. Nach Behebung der Störung informiert DARZ den Auftraggeber. Dies definiert die Wiederherstellung der Verfügbarkeit. Der Auftraggeber schließt den Call final und bestätigt, dass die Störung behoben ist.

16.5 Systemumgebung Hardware

Die in der Systemumgebung der SUB-CA eingesetzte Hardware (Server) entspricht den Anforderungen der TR-03145. Sie befindet sich in einem CAT III gesicherten Gebäude mit besonderen Schutz Mechanismen vor unbefugten Zugriff. Als Hardwaresicherheitsmodul (HSM) werden Systeme von Utimaco eingesetzt. Die eingesetzte Software der Firma MTG erfüllt alle Richtlinien der TR-03145.

17. Gewährleistungen

Grundsätzlich wird keine Gewährleistung übernommen. Die DARZ GmbH garantiert nicht die Verfügbarkeit der Leistungen der PKI.

18. Haftungsbeschränkungen

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

Für die Verletzung sonstiger Pflichten haftet die DARZ GmbH nur bei grobem Verschulden. Gegenüber Kaufleuten und öffentlichen Verwaltungen gilt die Haftungsbeschränkung des Absatzes 1 Satz 2 auch bei grober Fahrlässigkeit einfacher Erfüllungsgehilfen.

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 DARZ GmbH nach den gesetzlichen Bestimmungen.

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

19. Schadensersatz

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 ist die DARZ GmbH von der Haftung freigestellt.

20. Gültigkeitsdauer und Beendigung

20.1 Gültigkeitsdauer

Diese Vertragsbedingungen sind Bestandteil der Beauftragung und somit gebunden an die Laufzeit des Initialvertrages.

20.2 Beendigung

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

20.3 Auswirkung der Beendigung und Weiterbestehen

Von den Konsequenzen der Aufhebung dieser Vertragsbedingungen bleibt die Verantwortung zum Schutz vertraulicher Informationen und personenbezogener Daten unberührt.

21. Individuelle Mitteilungen und Absprachen mit Teilnehmern

In diesem Dokument werden keine entsprechenden Regelungen getroffen.

22. Ergänzungen

22.1 Verfahren für Ergänzungen

Änderungen der Vertragsbedingungen werden rechtzeitig vor ihrem Inkrafttreten veröffentlicht.

22.2 Benachrichtigungsmechanismen und -fristen

Die Zertifikatsinhaber werden rechtzeitig vor dem Inkrafttreten auf die Änderung der Vertragsbedingungen per signierter E-Mail hingewiesen.

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

Beschäftigten der DARZ GmbH gegenüber gilt die im Intranet bekannt gemachte jeweils aktuelle Fassung.

23. Verfahren zur Schlichtung von Streitfällen

Alle Streitigkeiten, die sich aus oder im Zusammenhang mit diesen Vertragsbedingungen oder über deren Gültigkeit ergeben, werden nach der Schiedsgerichtsordnung der Deutschen Institution für Schiedsgerichtsbarkeit e.V. (DIS) unter Ausschluss des ordentlichen Rechtsweges endgültig entschieden. Das Schiedsgericht besteht aus einem Einzelschiedsrichter. Der Schiedsort ist Darmstadt. Die Verfahrenssprache ist Deutsch.

24. Zugrunde liegendes Recht

Der Gerichtsstand ist Darmstadt.

25. Einhaltung geltenden Rechts

Es gilt deutsches Recht. Die von der DARZ.CA ausgestellten Zertifikate sind nicht konform zu qualifizierten Zertifikaten gemäß Signaturgesetz

26. Sonstige Bestimmungen

26.1 Vollständigkeitserklärung

Alle Regelungen in diesem Dokument gelten zwischen der DARZ.CA und den Zertifikatsinhabern. Die Ausgabe einer neuen Version ersetzt alle vorherigen Versionen. Mündliche Vereinbarungen bzw. Nebenabreden sind nicht zulässig.

26.2 Abgrenzungen

Eine Abtretung von Rechten ist nicht vorgesehen.

26.3 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.

26.4 Vollstreckung (Anwaltsgebühren und Rechtsmittelverzicht)

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

Erfüllungsort und Gerichtsstand ist Darmstadt.

26.5 Höhere Gewalt

Die DARZ GmbH übernimmt keine Haftung für die Verletzung einer Pflicht sowie für Verzug oder Nichterfüllung im Rahmen der Vertragsbedingungen sofern das zugrundeliegende Ereignis außerhalb ihrer Kontrolle (z. B. höhere Gewalt, Kriegshandlungen, Netzausfälle, Brände, Erdbeben und andere Katastrophen) resultiert.