TSE-PKI Certificate Policy der DARZ-TSE-PKI

Inhalt

Dokumenteninformationen 6

1.1 Bearbeitungsvermerk ... 6
1.2 Änderungshistorie ... 6
1.3 Gleichstellungshinweis ... 6

2. Einleitung 7

2.1 Überblick ... 8
2.2 Name und Identifizierung des Dokuments ... 8
2.3 PKI-Teilnehmer ... 8
2.3.1 Zertifizierungsstellen ... 8
(a) Root-CA ... 8
(b) Sub-CA ... 8
2.3.2 Registrierungsstellen ... 8
2.3.3 TSE ... 8
2.3.4 Zertifikatsnutzer ... 9
2.3.5 Verwendung von Zertifikaten ... 9
(a) Erlaubte Verwendung von Zertifikaten ... 9
(b) Verbotene Verwendung von Zertifikaten ... 9
2.4 Administration der Policy ... 9
2.4.1 Pflege der Policy ... 9
2.4.2 Zuständigkeit für das Dokument ... 9
2.4.3 Ansprechpartner/Kontaktperson ... 9
2.4.4 Zuständiger für die Anerkennung eines CPS ... 10
2.4.5 CPS-Aufnahmeverfahren ... 10

3. Verantwortlichkeit für Veröffentlichungen und Verzeichnisse 11

3.1 Verzeichnisse ... 11
3.2 Veröffentlichung von Informationen zur Zertifikatserstellung ... 11
3.3 Zeitpunkt und Häufigkeit der Veröffentlichungen ... 11
3.4 Zugriffskontrollen auf Verzeichnisse ... 11

4. Identifizierung und Authentifizierung 11

4.1 Regeln für die Namensgebung ... 11
4.1.1 Arten von Namen ... 11
4.1.2 Notwendigkeit für aussagefähige Namen ... 11
4.1.3 Anonymität oder Pseudonymität von Zertifikatsnehmern ... 11
4.1.4 Eindeutigkeit von Namen ... 11
4.1.5 Anerkennung, Authentifizierung und die Rolle von Markennamen ... 12
4.2 Initiale Überprüfung zur Teilnahme ... 12
4.2.1 Methoden zur Überprüfung bzgl. Besitz des privaten Schlüssels ... 12
4.2.2 Authentifizierung von Organisationszugehörigkeiten ... 12
(a) Sub-CA ... 12
(b) TSE-Hersteller ... 12
(c) TSE ... 13
4.2.3 Anforderungen zur Identifizierung und Authentifizierung des Zertifikats-Antragstellers ... 13
4.2.4 Ungeprüfte Zertifikatsnehmerangaben ... 14
4.2.5 Prüfung der Berechtigung zur Antragstellung ... 14
4.2.6 Kriterien für den Einsatz interoperierender Systeme/Einheiten ... 14
4.2.7 Aktualisierung/Anpassung der Zertifizierungsinformationen der Teilnehmer ... 14
4.2.8 Aktualisierung/Anpassung der Registrierungsinformationen der Teilnehmer ... 14
4.3 Identifizierung und Authentifizierung von Anträgen auf Schlüsselerneuerung ... 14
4.3.1 Schlüsselerneuerung der Root-CA ... 14
4.3.2 Schlüssleerneuerung der Sub-CA ... 14
4.3.3 Schlüsselerneuerung des TSE-Signaturzertifikates ... 14

4.3.4 Schlüssleerneuerung des TLS-Client-Zertifikates des TSE-Betreibers ... 15
4.4 Identifizierung und Authentifizierung von Anträgen auf Sperrung ... 15
4.4.1 Initiative des Zertifikatsinhabers ... 15
(a) Verantwortlichkeit für die Sperrung einer TSE ... 16
4.4.2 Initiative der Certificate Authority ... 16

5. Betriebsanforderungen für den Zertifikatslebenszyklus 17

5.1 Zertifikatsantrag ... 17
5.1.1 Wer kann einen Zertifikatsantrag stellen? ... 17
5.1.2 Beantragungsprozess und Zuständigkeiten ... 17
5.2 Verarbeitung von Zertifikatsanträgen ... 17
5.2.1 Durchführung der Identifizierung und Authentifizierung ... 17
5.2.2 Annahme oder Ablehnung von Zertifikatsanträgen ... 18
(a) Sub-CA Zertifikate ... 18
(b) TSE-Betreiber-Zertifikate (Webservice) ... 18
5.2.3 Fristen für die Bearbeitung von Zertifikatsanträgen ... 18
5.2.4 Ausgabe von Zertifikaten ... 18
(a) TSE-Zertifikate ... 18
(b) TSE-Betreiber-Zertifikate ... 18
(c) Sub-CA-Zertifikate ... 18
5.2.5 Benachrichtigung des Zertifikatsnehmers über die Ausgabe des Zertifikats ... 18
5.3 Annahme von Zertifikaten ... 19
5.3.1 Veröffentlichung von Zertifikaten durch die CA ... 19
5.4 Verwendung von Schlüsselpaar und Zertifikat ... 19
5.4.1 Verwendung des privaten Schlüssels und des Zertifikats durch den Zertifikatsnehmer ... 19
5.4.2 Verwendung des öffentlichen Schlüssels und des Zertifikats durch Zertifikatsnutzer ... 19
5.5 Zertifikatserneuerung ... 19
5.6 Zertifizierung nach Schlüsselerneuerung ... 19
5.6.1 Bedingungen der Zertifizierung nach Schlüsselerneuerung ... 19
5.7 Änderungen am Zertifikat ... 19
5.8 Sperrung und Suspendierung von Zertifikaten ... 19
5.8.1 Sperrung ... 20
5.8.2 Suspendierung ... 20
5.8.3 Aktualisierungs- und Prüfungszeiten bei Sperrungen ... 20
5.9 Service zur Statusabfrage von Zertifikaten ... 20
5.10 Beendigung der Teilnahme ... 20
5.11 Hinterlegung und Wiederherstellung von Schlüsseln ... 20

6. Organisatorische, betriebliche & physikalische Sicherheitsanforderungen 21

6.1 Generelle Sicherheitsanforderungen ... 21
6.1.1 Erforderliche Zertifizierungen der PKI-Teilnehmer ... 21
6.1.2 Anforderungen an die Zertifizierung gemäß ISO/IEC 27001 ... 21
6.2 Erweiterte Sicherheitsanforderungen ... 21
6.2.1 Betriebsumgebung und Betriebsabläufe ... **Fehler! Textmarke nicht definiert.**
6.2.2 Verfahrensanweisungen ... 22
6.2.3 Personal ... 22
6.2.4 Monitoring ... 23
6.2.5 Archivierung von Aufzeichnungen ... 23
6.2.6 Schlüsselwechsel der DARZ-TSE-PKI ... 24
6.2.7 Auflösen der Zertifizierungsstelle ... 24
6.2.8 Aufbewahrung der privaten Schlüssel ... 24
6.2.9 Behandlung von Vorfällen und Kompromittierungen ... 24
6.2.10 Meldepflichten ... 25
6.3 Notfall-Management ... 25

7. Technische Sicherheitsmaßnahmen 26

7.1 Erzeugung und Installation von Schlüsselpaaren ... 26

7.1.1 Generierung von Schlüsselpaaren für die Zertifikate ... 26
7.1.2 Lieferung privater Schlüssel ... 26
7.1.3 Lieferung öffentlicher Zertifikate ... 26
7.1.4 Schlüssellängen und kryptografische Algorithmen ... 26
7.1.5 Festlegung der Parameter der öffentlichen Schlüssel und Qualitätskontrolle ... 26
7.1.6 Verwendungszweck der Schlüssel ... 26
7.2 Sicherung des privaten Schlüssels und Anforderungen an kryptografische Module ... 26
7.2.1 Mehrpersonen-Zugriffssicherung zu privaten Schlüsseln ... 26
7.2.2 Ablage privater Schlüssel ... 26
7.2.3 Backup privater Schlüssel ... 26
7.2.4 Archivierung privater Schlüssel ... 27
7.2.5 Transfer privater Schlüssel in oder aus kryptografischen Modulen ... 27
7.2.6 Speicherung privater Schlüssel in kryptografischen Modulen ... 27
7.2.7 Aktivierung privater Schlüssel ... 27
7.2.8 Deaktivierung privater Schlüssel ... 27
7.2.9 Zerstörung privater Schlüssel ... 27
7.2.10 Beurteilung kryptographischer Module ... 27
(a) RootCA und SubCA ... 27
(b) TSE ... 27
7.3 Andere Aspekte des Managements von Schlüsselpaaren ... 27
7.3.1 Archivierung öffentlicher Schlüssel ... 27
7.3.2 Gültigkeitsperioden von Zertifikaten und Schlüsselpaaren ... 28
7.4 Aktivierungsdaten ... 28
7.5 Umgesetzte Sicherheitsanforderungen für die Rechneranlagen ... 28
7.6 Zeitstempel ... 28
7.7 Validierungsmodell ... 29

8. Profile für Zertifikate und Sperrlisten 30

8.1 Profile für Zertifikate und Zertifikatsrequests ... 30
8.1.1 Zugriffsrechte ... 30
8.1.2 Zertifikatserweiterung ... 30
8.2 Profile für Sperrlisten ... 30
8.3 Profile für OCSP Dienste ... 30

9. Überprüfungen der CA und andere Bewertungen 31

9.1 Inhalte, Häufigkeit und Methodik ... 31
9.2 Reaktionen auf identifizierte Vorfälle ... 31

10. Sonstige finanzielle und rechtliche Angelegenheiten 32

10.1 Preise ... 32
10.2 Finanzielle Zuständigkeiten ... 32

11. Vertraulichkeitsgrad von Geschäftsdaten 33

11.1.1 Definition von vertraulichen Informationen ... 33
11.1.2 Informationen, die nicht zu den vertraulichen Informationen gehören ... 33
11.1.3 Zuständigkeiten für den Schutz vertraulicher Informationen ... 33
11.2 Schutz personenbezogener Daten ... 33
11.2.1 Datenschutzkonzept ... 33
11.2.2 Als persönlich behandelte Daten ... 33
11.2.3 Daten, die nicht als persönlich behandelt werden ... 33
11.2.4 Zuständigkeiten für den Datenschutz ... 33
11.2.5 Hinweis und Einwilligung zur Nutzung persönlicher Daten ... 33
11.2.6 Auskunft gemäß rechtlicher oder staatlicher Vorschriften ... 33
11.2.7 Andere Bedingungen für Auskünfte ... 33
11.3 Geistiges Eigentumsrecht ... 33
11.4 Zusicherungen und Garantien ... 34
11.4.1 Zusicherungen und Garantien der CA ... 34

11.4.2 Zusicherungen und Garantien der RA ... 34
11.4.3 Zusicherungen und Garantien der Zertifikatsnehmer ... 34
11.4.4 Zusicherungen und Garantien der Zertifikatsnutzer ... 34
11.4.5 Zusicherungen und Garantien anderer PKI-Teilnehmer ... 34
11.5 Gewährleistungen ... 34
11.6 Haftungsbeschränkungen ... 34
11.7 Schadensersatz ... 34
11.8 Gültigkeitsdauer und Beendigung ... 35
11.8.1 Gültigkeitsdauer ... 35
11.8.2 Beendigung ... 35
11.8.3 Auswirkung der Beendigung und Weiterbestehen ... 35
11.9 Individuelle Mitteilungen und Absprachen mit Teilnehmern ... 35
11.10 Ergänzungen ... 35
11.10.1 Verfahren für Ergänzungen ... 35
11.10.2 Benachrichtigungsmechanismen und –fristen ... 35
11.10.3 Bedingungen für OID Änderungen ... 35
11.11 Verfahren zur Schlichtung von Streitfällen ... 35
11.12 Zugrunde liegendes Recht ... 35
11.13 Einhaltung geltenden Rechts ... 36
11.14 Sonstige Bestimmungen ... 36
11.14.1 Vollständigkeitserklärung ... 36
11.14.2 Abgrenzungen ... 36
11.14.3 Salvatorische Klausel ... 36
11.14.4 Vollstreckung (Anwaltsgebühren und Rechtsmittelverzicht) ... 36
11.14.5 Höhere Gewalt ... 36

12. Abkürzungen 37

13. Literaturverweise 38

14. Anhänge 39

14.1 Zertifikatsprofile ... 39
14.2 Allgemeine Struktur ... 39
14.2.1 Root-CA-Zertifikat ... 40
14.2.2 Sub-CA-Zertifikat ... 40
14.2.3 TSE-Signaturzertifikat ... 41
14.3 Namensschemata ... 41
14.4 Extensions ... 42

Dokumenteninformationen

1.1 Bearbeitungsvermerk

	Name und Funktion	Version	Datum	Unterschrift
Erstellt von:	Tiziana Knecht	1.6	13.06.2023	
Geprüft von:	ppa. Raphael Munasypow	1.6	13.06.2023	
Genehmigt von:	Jürgen Henzler	1.6	13.06.2023	
Rücknahme durch:				

1.2 Änderungshistorie

Datum	Bearbeiter	Version	Änderungsgrund / Änderungen
03.08.2020	Franziska Gimbel	1.0	
09.09.2020	Franziska Gimbel	1.1	Anpassungen, Update
20.10.2020	Alexander Waltinger	1.2	OID Eintrag
30.03.2021	Franziska Gimbel	1.3	Anpassung
13.04.2021	Franziska Gimbel	1.4	Anpassung
06.04.2023	Franziska Gimbel	1.5	Anpassung in 5.2.4
13.06.2023	Jürgen Henzler Tiziana Knecht	1.6	Anpassungen 5.2.1, 5.8.3 und 5.2.4

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.

2. Einleitung

Die auf dem Gesetz zum Schutz vor Manipulationen an digitalen Grundaufzeichnungen [KassenG] basierende Kassensicherungsverordnung [KassenSichV] präzisiert die Anforderungen des § 146a der Abgabenordung [AO]. Sie regelt, wie elektronische Aufzeichnungssysteme (Electronic Record-keeping Systems, ERS) wie zum Beispiel elektronische Kassensysteme oder Registrierkassen Geschäftsvorfälle protokollieren und speichern müssen. Sie gibt vor, dass elektronische Aufzeichnungssysteme mit einer Technischen Sicherheitseinrichtung (TSE) ausgerüstet sein müssen, so dass der Schutz der digitalen Aufzeichnungen vor Manipulationen gewährleistet ist.

Die Mindestanforderungen an die Technische Sicherheitseinrichtung werden vom Bundesamt für Sicherheit in der Informationstechnik (BSI) in der Technischen Richtlinie (TR) [BSI TR-03153] sowie mehreren Schutzprofilen (Protection Profiles, PP), darunter [BSI PP-SMAERS] und [BSI PP-CSP] bzw. [BSI PP-CSPL] festgelegt. Zum Zweck der Interoperabilität muss die TSE über eine einheitliche Einbindungsschnittstelle und eine einheitliche Exportschnittstelle verfügen. Letztere kann zum Beispiel von Finanzbeamten verwendet werden, um die aufgezeichneten Daten im Rahmen einer Steuerprüfung abzurufen. Die Sicherheitsfunktionalität der TSE ist in einem Sicherheitsmodul gekapselt. Das Sicherheitsmodul beinhaltet die Security Module Application for Electronic Record-keeping Systems (SMAERS) und den Cryptographic Service Provider (CSP). Es kann über die Secure Element API nach [BSI TR-03151] angesprochen werden. Kryptographische Vorgaben für Anwendungen der Secure Element API sind in [BSI TR-03116-5] zu finden.

Im Allgemeinen ist das Sicherheitsmodul für die Absicherung der digitalen Aufzeichnungen durch die Berechnung von Prüfwerten zuständig. Bei den Prüfwerten handelt es sich um digitale Signaturen, so dass Integrität und Authentizität der Aufzeichnungen sichergestellt werden. Die Signaturen werden mithilfe des privaten Schlüssels der TSE erstellt. Dieser darf nur im Sicherheitsmodul der TSE vorliegen. Die Prüfwertverifikation ist mit dem zugehörigen öffentlichen Schlüssel möglich. Der TSE-Betreiber ist verpflichtet, dem Steuerpflichtigen ein Zertifikat über den zur genutzten TSE zugehörigen öffentlichen Schlüssel bereitzustellen. Um die Authentizität der öffentlichen Schlüssel und damit auch die Authentizität der Prüfwerte zu gewährleisten, lässt der TSE-Betreiber eine Public-Key-Infrastruktur (TSE-PKI) betreiben.

Die TSE-PKI ist hierarchisch aufgebaut. An ihrer Spitze steht eine Stammzertifizierungsstelle (Root-CA), die den Vertrauensanker darstellt. Sie stellt den ihr untergeordneten Sub-CAs CA-Zertifikate aus und autorisiert sie damit zur Ausstellung von EE-Zertifikaten. Die Zertifizierungsstellen unterhalten Zertifikatssperrlisten (Certificate Revocation Lists, CRLs), auf denen vor Laufzeitende gesperrte oder widerrufene Zertifikate veröffentlicht werden.

Root-CA und Sub-CAs verfügen über eine Zertifizierung nach [ISO/IEC 27001] und [BSI TR-03145]. Sie erfüllen die Anforderungen des Standards für den sicheren Betrieb einer CA mit Sicherheitslevel „hoch“ nachweislich.

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

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.

Informative Kapitel werden explizit am Anfang als solche gekennzeichnet.

2.1 Überblick

Das Dokument richtet sich an alle Nutzer der DARZ-TSE-PKI.

Die Gliederung erfolgt nach dem Muster des Standards RFC 3647.

Die Verantwortlichkeit für die DARZ-TSE-PKI obliegt der DARZ GmbH.

2.2 Name und Identifizierung des Dokuments

Identifikator	Wert
Titel	Certificate Policy und Certificate Practice Statement der DARZ-TSE-PKI (Sub-CA der DARZ GmbH)
Version	1.6
Datum	13.06.2023
OID	1.3.6.1.4.1.51695.1.3

2.3 PKI-Teilnehmer

2.3.1 Zertifizierungsstellen

Der Betreiber der DARZ-TSE-PKI ist die DARZ GmbH, Julius-Reiber-Strasse 11, 64293 Darmstadt.

(a) Root-CA

Die Root-CA stellt den Übergeordneten Vertrauensanker der TSE-PKI dar.

(b) Sub-CA

Die Sub-CA stellt Zertifikate für Zertifikatsnutzer aus.

2.3.2 Registrierungsstellen

Die DARZ-TSE-PKI verfügt über eine Registrierungsstelle (RA). Die Registrierungsstelle ist für die zweifelsfreie Identifizierung des Zertifikatsnehmers vor der Ausstellung des Zertifikats durch die Zertifizierungsstelle zuständig. Sie authentifiziert den Antragsteller und die Antragsdaten.

Die Registrierungsstelle der Root-CA bearbeitet die Registrierungen der Sub-CAs. Die Sub-CAs verfügen über eigene Registrierungsstellen, die für die Bearbeitung der Registrierungen der Endentitäten zuständig sind. Zu den Endentitäten gehört auch die TSE. Vor der Ausstellung eines EE-Zertifikats für die TSE prüft die Sub-CA RA die Echtheit des Sicherheitsmoduls der TSE.

Der TSE-Betreiber betreibt ebenfalls eine Registrierungsstelle: die Betreiber-RA. Sie kommuniziert mit der Sub-CA RA und ist für die Vorabprüfung der Antragsdaten zuständig.

2.3.3 TSE

Die TSE-Signaturzertifikate sind nicht zur Ausstellung weiterer Zertifikate autorisiert, es handelt sich hierbei also um Endentitäten (End Entities, EEs), bzw Endentität-Zertifikate.

Die Signatur-Zertifikate der TSEs werden durch die vom TSE-Betreiber gestellte Betreiber-RA über eine technische Schnittstelle bei der Sub-CA RA beantragt. Der TSE-Betreiber erhält nach seiner erfolgreichen Registrierung bei der Sub-CA RA ein Endentität-Zertifikat, das nicht Teil der TSE-PKI ist. Es wird von einer internen Verwaltungs-PKI des Sub-CA-Betreibers ausgestellt. Die Betreiber-RA verwendet dieses Zertifikat zur Authentisierung gegenüber der Sub-CA RA und zum Signieren der Zertifikatsanträge für die TSE-Zertifikate. Es wird entsprechend seines Verwendungszwecks als RA-Zertifikat bezeichnet.

2.3.4 Zertifikatsnutzer

Zu den Zertifikatsnutzern gehören Steuerpflichtige und Finanzbeamte. Sie können das TSE-Zertifikat zur Prüfwertverifikation verwenden. Sie können die Gültigkeit des TSE-Zertifikats verifizieren, indem sie die Zertifikatskette prüfen sowie die Zertifikatssperrliste der ausstellenden Sub-CA prüfen.

2.3.5 Verwendung von Zertifikaten

(a) Erlaubte Verwendung von Zertifikaten

Die im Rahmen der DARZ-TSE-PKI ausgestellten Zertifikate dürfen 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 (TR-03153) beschrieben.

(b) Verbotene Verwendung von Zertifikaten

Die private Verwendung der Zertifikate ist untersagt.
Geschäftspartner dürfen die Zertifikate nicht ohne die Genehmigung der DARZ-TSE-PKI über die in Ziffer 2.3.5 beschriebene Verwendung hinaus im Zusammenhang mit Geschäftsangelegenheiten mit Dritten nutzen.

2.4 Administration der Policy

2.4.1 Pflege der Policy

Die für dieses Dokument verantwortliche Organisation ist die DARZ GmbH. Die DARZ GmbH kann über folgende Adresse kontaktiert werden:

Organisation	DARZ GmbH
Abteilung	IT-Services
Adresse	Julius-Reiber-Straße 11, D-64293 Darmstadt
Telefon	+49 6151 8762-100
E-Mail	info@da-rz.de
Webseite	www.da-rz.de

Diese CP wird im Intranet und auf der Homepage der DARZ GmbH veröffentlicht.
Eine Weitergabe an andere Organisationen ist vorgesehen, damit eine unabhängige Überprüfung der Arbeitsweise der DARZ-TSE-PKI möglich ist.

2.4.2 Zuständigkeit für das Dokument

Die Verwaltung dieses Dokuments erfolgt durch die DARZ GmbH. Jede aktualisierte Version des Dokuments wird den Anwendern unverzüglich über die angegebene Internetseite (siehe 2.4) zur Verfügung gestellt.

2.4.3 Ansprechpartner/Kontaktperson

Organisation	DARZ GmbH
Abteilung	IT-Services
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

2.4.4 Zuständiger für die Anerkennung eines CPS

Diese CP wird durch die verantwortliche Organisation (s. Kap. 2.4.1) überprüft und ist Bestandteil der Betriebsdokumentation der DARZ-TSE-PKI.

2.4.5 CPS-Aufnahmeverfahren

Entfällt.

3. Verantwortlichkeit für Veröffentlichungen und Verzeichnisse

3.1 Verzeichnisse

Die DARZ GmbH stellt die Informationen zur DARZ-TSE-PKI auf der Homepage − unter https://www.da-rz.de/de/ueber-darz/unternehmen/PKI/ sowie im Intranet (Zugriff nur für Beschäftigte der DARZ GmbH sowie deren externe Mitarbeiterinnen und Mitarbeiter) zur Verfügung.

3.2 Veröffentlichung von Informationen zur Zertifikatserstellung

Die DARZ GmbH veröffentlicht folgende Informationen:

- Kontaktdaten der DARZ-TSE-PKI
- DARZ-TSE-PKI -Zertifikate mit Hash (SHA 256)
- Parameter zur Einrichtung eines Zugriffs auf die Sperrliste bzw. das LDAP-Verzeichnis
- Formulare
- Erläuterungen zum Sperrverfahren
- Zertifizierungsrichtlinie (CP)

3.3 Zeitpunkt und Häufigkeit der Veröffentlichungen

Für die Veröffentlichung von DARZ-TSE-PKI-Zertifikaten, Sperrlisten sowie CP gelten die folgenden Intervalle:

Alle von der DARZ-TSE-PKI ausgestellten Zertifikate	Unmittelbar nach Ausstellung
Sperrlisten	Nach Suspendierungen/Sperrungen, sonst turnusmäßig
CP	Nach Erstellung bzw. Aktualisierung

3.4 Zugriffskontrollen auf Verzeichnisse

Der lesende Zugriff auf die unter den Ziffern 3.1 und 3.2 aufgeführten Informationen ist nicht eingeschränkt. Der schreibende Zugriff liegt im Verantwortungsbereich der DARZ-TSE-PKI.

4. Identifizierung und Authentifizierung

4.1 Regeln für die Namensgebung

4.1.1 Arten von Namen

Der Name der ausgestellten Zertifikate (Distinguished Name = DN) richtet sich nach den Vorgaben des Standards X.509 und dem Namensschema gemäß Anhang 14.3.

4.1.2 Notwendigkeit für aussagefähige Namen

Die Angaben der Zertifikatsinhaber werden gemäß den Anforderungen aus Kapitel 4.1 der CP-SM-PKI in die Zertifikate aufgenommen.

4.1.3 Anonymität oder Pseudonymität von Zertifikatsnehmern

Anonymität oder Pseudonymität in Namen von Zertifikaten ist nicht erlaubt.

4.1.4 Eindeutigkeit von Namen

Die Angaben der Zertifikatsinhaber werden gemäß den Anforderungen aus 4.2.2(b) in die Zertifikate der DARZ-TSE-PKI aufgenommen. Eine Namensgleichheit (gleicher CN bei unterschiedlichem Zertifikatsnehmer) wird durch die DARZ-TSE-PKI verhindert, entsprechend vergibt die DARZ-TSE-PKI einen CN nicht mehrfach. Sollten zwei oder mehr Zertifikatsnehmer der DARZ-TSE-PKI den gleichen CN wünschen, wird dieser Konflikt gelöst. Es behält der Teilnehmer seinen CN, der zuerst sein initiales

Zertifikat mit diesem CN von der DARZ-TSE-PKI erhalten hat. Der oder die anderen Zertifikatsnehmer lassen sich ein Zertifikat mit einem anderen CN ausstellen, um an der DARZ-TSE-PKI teilnehmen zu dürfen.

4.1.5 Anerkennung, Authentifizierung und die Rolle von Markennamen

Im Rahmen der Beantragung von Zertifikaten für Geschäftspartner dürfen nur solche Marken oder Warenzeichen als Teil des Zertifikatseintrags für die im Antrag anzugebende Firma bzw. Behörde verwendet werden, zu deren Verwendung diese berechtigt sind. Diese Berechtigung wird jedoch bei der Registrierung nicht geprüft.
Die DARZ-TSE-PKI bietet insbesondere keine Prozeduren zur Auflösung von Markenstreitigkeiten an. Diese sind zwischen den daran beteiligten Unternehmen ggf. durch markenrechtliche oder wettbewerbsrechtliche Maßnahmen im Zivilrechtsweg zu lösen. Falls der DARZ-TSE-PKI ein rechtskräftiges Urteil vorgelegt wird, das die Unrechtmäßigkeit der Verwendung einer Marke oder eines Warenzeichens feststellt, wird das Zertifikat gesperrt.

4.2 Initiale Überprüfung zur Teilnahme

4.2.1 Methoden zur Überprüfung bzgl. Besitz des privaten Schlüssels

Zum Nachweis des Besitzes des privaten Schlüssels beinhaltet ein Zertifikatsrequest eine sogenannte innere Signatur.

Hierdurch wird bei der Antragsprüfung durch Verifikation der inneren Signatur mit dem im Zertifikatsrequest enthaltenen zugehörigen öffentlichen Schlüssel durch die DARZ-TSE-PKI geprüft, dass der Antragsteller im Besitz des privaten Schlüssels ist.

4.2.2 Authentifizierung von Organisationszugehörigkeiten

(a) Sub-CA

Die SubCAs der DARZ-TSE-PKI werden durch die DARZ GmbH selbst betrieben. Eine Authentifizierung oder Registrierung ist nicht notwendig.
Die Erzeugung einer neuen Sub-CA unterliegt den im ISMS der DARZ definierten Zugriffsrechten, Prozessen und Verantwortlichkeiten für derartige Changes.

(b) TSE-Hersteller

Zur Anbindung eines neuen TSE-Betreibers in die DARZ-TSE-PKI muss das Unternehmen authentifiziert und mindestens ein bevollmächtigter Vertreter des TSE bei dem Betreiber der ausgewählten Sub-CA identifiziert und authentifiziert werden.
Notwendige Unterlagen und Daten für die Registrierung sind:

- Antragsschreiben zur Ausgabe eines Zertifikates für einen TSE_Betreiber 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 eines gesetzlichen Vertreters des Unternehmens bzw. der Leitung der Institution, in der der Vertreter des Betreibers berechtigt wird, den Antrag für den TSE-Betreiber zu stellen und in der Sache dazu verbindliche Aussagen und Angaben zu machen.
    - Informationen zu geplanten Antrags- und Zertifikatsdaten für die TSE-Endentität-Zertifikate, zur Unterstützung der späteren Antragsprüfung. Die Sub-CA fordert die einzureichenden Informationen im Rahmen der Registrierung an. Hierzu können bspw. zählen:
        - Öffentlicher Schlüssel des Attestation Keys
        - Geplanter Wert für SubjectDN.Organization
        - Geplanter Wert für SubjectDN.Country
        - Geplante Werte für SubjectDN.dnQualifier (Certification ID, durch BSI vergeben)

- Persönliche/individuelle Zertifikate für die gesicherte E-Mail-Kommunikation der benannten Ansprechpartner inklusive der zur Verifikation erforderlichen Zertifikatskette

- Der TSE-Betreiber muss eine Erklärung zur Einhaltung der Sicherheitsvorgaben aus dieser TSE-PKI CP/CPS für die Teilnahme an der TSE-PKI (Siehe Abschnitt 6) vorlegen.

Sollte ein Dienstleister für den Betrieb eines TSE-Betreiber beauftragt werden, muss zusätzlich zu den genannten Unterlagen eine schriftliche Bestätigung durch den Auftraggeber mit Benennung der autorisierten Ansprechpartner vorgelegt werden.

Eine Sub-CA muss Anträge und Zertifikatsdaten unterschiedlicher TSE-Betreiber diesen individuell zuordnen können. Zu diesem Zweck wird von der Sub-CA für jeden TSE-Betreiber ein individueller Mandant angelegt.
Der Sub-CA-Betreiber stellt dem TSE-Betreiber einen Webservice zur Verfügung, den er zur Beantragung von TSE-Endentität-Zertifikaten verwenden muss und zur Sperrung verwenden kann. Die durchführbaren Aktionen wie Sperrung oder Beantragung werden durch Rollenzuweisungen auf CA-Seite reglementiert. Der Sub-CA-Betreiber übergibt dem TSE-Betreiber die technische Dokumentation dieser Schnittstelle spätestens nach erfolgreichem Abschluss der Registrierung.
Zur Nutzung des Webservices stellt der Sub-CA-Betreiber dem TSE-Betreiber mindestens ein Zertifikat aus, welches von einer internen Verwaltungs-PKI des Sub-CA-Betreibers signiert ist. Das Schlüsselmaterial für dieses Zertifikat wird vom Sub-CA-Betreiber generiert. Die Übergabe an den TSE-Betreiber erfolgt im PKCS#12-Format. Der Keystore und das zugehörige Zertifikat müssen dem TSE-Betreiber in getrennten, S/MIME verschlüsselten e-Mails zugesandt werden.
Der TSE-Betreiber erhält ferner den öffentlichen Schlüssel der Webservice-Schnittstelle. Er ist verpflichtet, diesen bei einem Verbindungsaufbau mit der Webschnittstelle zu validieren.

(c) TSE

Eine TSE kann selbst keine Zertifikate beantragen. Entsprechend beantragt ein berechtigter Antragsteller des TSE-Betreibers als dritte Partei stellvertretend die Signaturzertifikate für die TSE unter Verwendung der vom Sub-CA-Betreiber bereitgestellten technischen Schnittstelle.

Grundvoraussetzung für das Aufbringen von TSE-Zertifikaten ist, dass der TSE-Betreiber bei einer Sub-CA der TSE-PKI registriert ist (Kapitel_ 2.3.2) und dass der von ihm benannte Antragsteller über ein gültiges Zertifikat zur Client-Authentisierung an der Webservice-Schnittstelle der Sub-CA hat, sowie über den zugehörigen privaten Schlüssel verfügt.

Der TSE-Betreiber ist für die Einhaltung der Rahmenbedingungen verantwortlich und muss den Prozess gemäß den Vorgaben nachvollziehbar dokumentieren.

Der Antragsteller muss die Echtheit des Sicherheitsmoduls der TSE, für die er das Zertifikat beantragt, gegenüber der Sub-CA RA unter Beweis stellen. Es muss sichergestellt werden, dass der zur Prüfwertberechnung verwendete private Schlüssel tatsächlich und ausschließlich im Sicherheitsmodul der TSE vorliegt.

Der CSP-Light-Server implementiert dazu ein Key-Attestation-Verfahren, welches im Zuge der Zertifikatsbeantragung durchgeführt werden muss. Als Eingabe für das Key-Attestation-Verfahren muss dabei eine von der RA generierte Zufallszahl (Nonce) verwendet werden, die von der Betreiber-RA an den CSP-Light-Server (Antragsteller) weitergeleitet wird. Die Ausgabe des Verfahrens ist eine vom CSP-Light-Server signierte Datenstruktur, die sich Attestation Response nennt. Nach Erhalt der Nonce generiert der CSP-Light-Server ein neues TSE-Schlüsselpaar. Anschließend generiert er die Attestation Response und signiert sie mit seinem privaten Attestation Key. Neben der Nonce enthält die Attestation Response den neu generierten, zu zertifizierenden öffentlichen Schlüssel der TSE und weitere Metadaten. Über die Nonce wird die Aktualität (Freshness) der Attestation Response sichergestellt und somit ein Schutz vor Replay-Attacken gewährleistet.

Die Betreiber-RA generiert einen Zertifikatsantrag im Certificate Request Message Format (CRMF) nach [RFC 4211], in den sie die Attestation Response einbettet. Die Betreiber-RA autorisiert den Zertifikatsantrag, indem sie ihn mit dem privaten Schlüssel ihres RA-Zertifikats signiert. Damit erklärt die Betreiber-RA die Korrektheit der Antragsdaten, die Legitimität des Antrags und die Verantwortlichkeit für den Antrag. Der signierte Zertifikatsantrag hat die Datenstruktur CmsSignedData gemäß Cryptographic Message Syntax (CMS) [RFC 5652]. Zur Kennzeichnung des Inhalts wird diese Datenstruktur wiederum in eine ContentInfo-Struktur (ebenfalls gemäß Cryptographic Message Syntax) eingebettet. Anschließend übermittelt die Betreiber-RA diese ContentInfo-Struktur an die Sub-CA RA.

Die Sub-CA muss die äußere Signatur des Zertifikatsrequests prüfen und sicherstellen, dass sie mit demselben Schlüssel erzeugt wurde, der für die TLS-Client-Authentifizierung verwendet wurde. Die Sub-CA MUSS Gültigkeit und Sperrstatus des verwendeten CSIG/TLS(TH) überprüfen.
Die Sub-CA MUSS den Zertifikatsantrag hinsichtlich ordnungsgemäßer Struktur und korrektem Inhalt überprüfen.
Die von der Sub-CA produzierten Zertifikate werden von dem TSE-Betreiber geprüft und in die TSE eingebracht.

4.2.3 Anforderungen zur Identifizierung und Authentifizierung des Zertifikats-Antragstellers

Ein Zertifikatsrequest darf nicht von einer Einzelperson (natürliche Person), sondern muss von einer Organisation (juristische Person) gestellt werden.

4.2.4 Ungeprüfte Zertifikatsnehmerangaben

Die Registrierungsstelle überprüft die Angaben zum Zertifikatsnehmer im Zertifikatsrequest gegen die eingereichten Unterlagen auf Korrektheit (vergl. Kapitel 4.2.2).

4.2.5 Prüfung der Berechtigung zur Antragstellung

Siehe Kapitel 3.2

4.2.6 Kriterien für den Einsatz interoperierender Systeme/Einheiten

Nicht zutreffend.

4.2.7 Aktualisierung/Anpassung der Zertifizierungsinformationen der Teilnehmer

Die für die Teilnehmer an der DARZ-TSE-PKI geforderten Zertifizierungen (siehe Abschnitt 6.1.1) ggf. einem Überwachungszyklus, für das z.B. ein Audit positiv abgeschlossen werden muss.

Die DARZ-TSE-PKI 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, so wird das Zertifikat bzw. werden die Zertifikate aus der DARZ-TSE-PKI gesperrt. Informationen über relevante Änderungen, die beispielsweise 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 der DARZ-TSE-PKI zur Verfügung stellen.

Die DARZ-TSE-PKI aktualisiert anschließend die entsprechenden Registrierungsdaten.

4.2.8 Aktualisierung/Anpassung der Registrierungsinformationen der Teilnehmer

Änderungen der Registrierungsinformationen sind der DARZ-TSE-PKI unverzüglich mitzuteilen.

4.3 Identifizierung und Authentifizierung von Anträgen auf Schlüsselerneuerung

4.3.1 Schlüsselerneuerung der Root-CA

Das Schlüsselmaterial der Root-CA wird ohne formale Beantragung auf interne Veranlassung des Betreibers der Root-CA erneuert.

4.3.2 Schlüssleerneuerung der Sub-CA

Die Schlüsselerneuerung der SubCA muss bei der Registration Authority der Root-CA beantragt werden. Die Ausstellung neuer Sub-CA-Zertifikate erfolgt ausschließlich im Auftrag der Root-RA. Die Beantragung erfolgt innerhalb der Organisation des Betreibers durch die für den Sub-CA-Betrieb Verantwortlichen.

Der Antrag muss in Form eines auf einem neuen Schlüsselpaar basierten PKCS#10-Requests an die Root-CA gesendet werden. Die zu Grunde liegenden Schlüssel müssen auf dem von der Sub-CA verwendeten HSM generiert werden.
Wird die betreffende Sub-CA für eine andere Organisation betrieben, so muss die Root-RA aktuelle Unterlagen vom registrierten Ansprechpartner der auftraggebenden Organisation anfordern, um den Erneuerungsantrag prüfen zu können.
Der SubjectDN des neuen Sub-CA-zertifikates wird von der Root-RA festgelegt. Hierzu wird der SubjectDN des vorherigen Zertifikates wiederverwendet und die darin enthaltene SerialNumber um 1 erhöht. Für sonstige Änderungen am SubjectDN muss der Zertifikatsnehmer ein neues Sub-CA-Zertifikat beantragen.

Im Falle einer Genehmigung des Antrags wird der Antrag in der Root-CA weiterverarbeitet; hierbei erfolgt zunächst eine Prüfung der PKCS#10-Signatur. Das Zertifikat wird mit dem Schlüssel aus dem PKCS#10-Request und mit dem von der Root-RA festgelegten SubjectDN ausgestellt. Anschließend wird es organisationsintern an die Sub-CA übergeben. Dort wird das Zertifikat auf Korrektheit geprüft, importiert und mit dem privaten Schlüssel des PKCS#10-Requests zusammengeführt.

4.3.3 Schlüsselerneuerung des TSE-Signaturzertifikates

Eine Schlüsselerneuerung wird auf demselben Wege durchgeführt, wie unter 4.2.2(c) beschrieben. Die Erneuerung muss unter Verwendung eines neuen Schlüsselpaares erfolgen, wobei der Subject-DN identisch zum bisherigen sein muss.

4.3.4 Schlüssleerneuerung des TLS-Client-Zertifikates des TSE-Betreibers

Die RA der Sub-CA überwacht die ausgestellten Zertifikate der internen Verwaltungs-PKI. Sie veranlasst eine Rechtzeitige Erneuerung der Zertifikate unter Beibehaltung des bisherigen Subject-DN. Die Zertifikate werden dann wie in 4.2.2(b) dargestellt an die TSE-Betreiber übermittelt.

4.4 Identifizierung und Authentifizierung von Anträgen auf Sperrung

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

- dem Zertifikatsinhaber oder einem Bevollmächtigtem
- der DARZ-TSE-PKI (Jeweils der Aussteller – Sub-CA oder Root-CA)

Der TSE-Betreiber hat dazu folgende Möglichkeiten:

- Sperrung über einen Webservice
  - Im Falle des TSE-Signaturzertifikates kann die Sperrung durch den TSE-Betreiber erfolgen, sofern dieser die Rolle eines Sperrberechtigten einnimmt.
  - Der TSE-Betreiber kann die Sperrung über den Webservice unter Verwendung des Sperrpasswortes veranlassen, sofern dieser von der Sub-CA die Rolle eines Sperr-Operators zugewiesen bekommen hat.
  - Das Sperrpasswort wird von der Sub-CA bei jeder Zertifikatsausstellung individuell generiert und zusammen mit dem ausgestellten Zertifikat an den TSE-Betreiber übergeben. Der TSE-Betreiber kann das Sperrpasswort an eine dritte Person weitergeben, womit diese zur Sperrung des jeweiligen Zertifikates autorisiert wird.

- Sperrung über den Sperrservice der Sub-CA
  - Bei einer Sperrung eines TSE-Signaturzertifikates durch den TSE-Betreiber über den Sperrservice der Sub-CA muss eine mit S/MIME signierte E-Mail zur Übermittlung des Sperrauftrags verwendet werden. Alternative, gleichwertig abgesicherte Kommunikationskanäle können ebenfalls verwendet werden.
  - Das Sperrpasswort zum TSE-Signaturzertifikat wird im Falle einer Signierten Nachricht nicht benötigt.
  - Wird ein Sperrauftrag über einen Kanal übermittelt, bei dem die Sub-CA eine Überprüfung des Antragsstellers nicht mittels digitaler Signatur überprüfen kann, so muss das Sperrpasswort mit übermittelt werden. Die Kenntnis des Sperrpasswortes weist den Sperrantragsteller als berechtigte Person aus.
  - Falls eine Sperrmöglichkeit durch Dritte vom TSE-Betreiber nicht gewünscht ist, muss er dies der Sub-CA in einer signierten E-Mail schriftlich mitteilen und muss die von der CA generierten Sperrpassworte nach Erhalt verwerfen. Die Sub-CA darf in diesem Fall keine mit Passwort legitimierten Sperraufträge für die TSE-Signaturzertifikate dieses TSE-Betreibers entgegennehmen.

Die Sub-CA muss vollständige und korrekte Sperraufträge für TSE-Signaturzertifikate über die oben genannten Sperrservices entgegennehmen und ausführen.

Bei einer Sperrung von des Sub-CA Zertifikates durch den Betreiber der Sub-CA muss eine mit S/MIME signierte E-Mail oder ein vergleichbar abgesicherter Kommunikationskanal zur Übermittlung des Sperrauftrags an die Root-CA verwendet werden.

Ein vollständiger Sperrauftrag muss folgende Informationen enthalten:

- Organisation, Name, Anschrift und E-Mail-Adresse des Absenders
- Zertifikatstyp
- Ausstellende Sub-CA bzw. Root-CA („IssuerDN“ des Zertifikats, siehe [RFC 5280])
- Zertifikats-Seriennummer („SerialNumber“ des Zertifikats, siehe [RFC 5280]; *nicht* SubjectDN.SN)
- Sperrgrund (siehe auch Kapitel 4.8)
- Zeitpunkt, ab dem das Zertifikat als unsicher/gesperrt einzustufen ist (optional, nur wenn genauer Zeitpunkt bekannt ist)

4.4.1 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.

Der Zertifikatsinhaber nutzt diesem Fall eine der unter 4.4. genannten Möglichkeiten zur Sperrung des Zertifikates.

Die Sperrung des jeweiligen Zertifikats wird über die Sperrliste der DARZ-TSE-PKI veröffentlicht, und der Zertifikatsinhaber wird über den abgeschlossenen Sperrprozess per signierter E-Mail informiert.

(a) Verantwortlichkeit für die Sperrung einer TSE

Für die Sperrung einer TSE und für die zusätzliche Erteilung von TSE-Sperrberechtigungen an Dritte ist der TSE-Betreiber verantwortlich. Sofern Sperrpassworte genutzt werden, hat der TSE-Betreiber dafür Sorge zu tragen, das Sperrpasswort in geeigneter Form an die Parteien weitergegeben werden, die eine legitime Sperrberechtigung haben. Der TSE-Betreiber muss die sperrberechtigte Partei über die sichere Handhabung und Speicherung der Sperrpasswörter informieren. Der TSE-Betreibe muss zur Weitergabe der Sperrpasswörter geeignete Maß-nahmen wie z.B. einen abgesicherten und integren Kommunikationskanal über eine verschlüsselte und signierte E-Mail verwenden.

4.4.2 Initiative der Certificate Authority

Die Darz-TSE-PKI hat die Aufgabe, bei erkannten Schwachstellen alle Tätigkeiten durchzuführen, welche die Integrität und Sicherheit der PKI sicherstellen. Die Schwachstellen werden direkt nach Bekanntwerden der Root gemeldet. Die Einleitung weiterer Schritte wird ggf. in Absprache mit der Root vorgenommen. Mögliche Gründe sind beispielsweise

- ein erkannter Verstoß gegen Betriebsauflagen (insbesondere gegen die Anforderungen für die Teilnahme an der DARZ-TSE-PKI (siehe 6),
- erkannte (erhebliche) Schwächen in der eingesetzten Kryptographie oder Kryptoimplementierung,
- Änderungen in den zentralen Vorgaben (z.B. der (TR-03153)),
- 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 (das Sub-CA Zertifikat der DARZ-TSE-PKI selbst) erfolgen in Abstimmung mit der Root-CA. Die Zertifikate einer TSE können in der eigenen Verantwortung durch die DARZ-TSE-PKI gesperrt werden. Sollten nach Ansicht des Betreibers der DARZ-TSE-PKI Sperrungen dieser Zertifikate systemrelevante Auswirkungen haben, so informiert die DARZ-TSE-PKI die Zertifikatsinhaber.

Eine Sperrung des jeweiligen Zertifikats wird über die Sperrliste der DARZ-TSE-PKI veröffentlicht. Der Zertifikatsinhaber sowie die Root werden über den abgeschlossenen Sperrprozess informiert.

5. Betriebsanforderungen für den Zertifikatslebenszyklus

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

- Zertifikatsbeantragung,
- Verarbeitung von Zertifikatsanträgen und
- Zertifikatsausstellung.

Innerhalb der Prozesse des Zertifikatslebenszyklus der DARZ-TSE-PKI muss die relevante personenbezogene Kommunikation verschlüsselt und signiert erfolgen, wofür individuelle/ personenbezogene Zertifikate eingesetzt werden. Für alle beteiligten Personen wird der Besitz von individuellen/personenbezogenen S/MIME-Zertifikaten vorausgesetzt.

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

5.1 Zertifikatsantrag

In den folgenden Unterkapiteln wird definiert, wer ein Zertifikat bei der DARZ-TSE-PKI beantragen darf und welche Organisationseinheit für die Bearbeitung des Zertifikatsantrags verantwortlich ist.

5.1.1 Wer kann einen Zertifikatsantrag stellen?

Ein Zertifikatsantrag darf ausschließlich von einer Organisation gestellt werden. Befugte Organisationen sind TSE-Betreiber und der Sub-CA-Betreiber, die sich gemäß Abschnitt 4.3 an der DARZ-TSE-PKI identifiziert haben müssen.

Betreibt ein TSE-Betreiber mehrere Instanzen des Clients für die Sub-CA-Schnittstelle, so kann er sich entsprechend mehrere TLS-Zertifikate von der Sub-CA ausstellen lassen, um jeden Client mit einem eigenen Zertifikat auszustatten.

Der Zertifikatsrequest für ein TSE-Signaturzertifikat muss unter Nutzung der Zertifikate für den Zugriff auf den Webservice bei der Sub-CA gestellt werden. Der Request ist mit dem TSE-Betreiber-Zertifikat zu signieren.
Die Zertifikate müssen eindeutig gekennzeichnet werden (siehe14.3).

5.1.2 Beantragungsprozess und Zuständigkeiten

Für die Bearbeitung eines Zertifikatsantrags ist die Registration Authority (RA) der DARZ-TSE-PKI verantwortlich.

Die Kontaktadresse zur Koordinierung lautet wie folgt:
DARZ GmbH
Julius-Reiber-Strasse 11
64293 Darmstadt
FIXME@da-rz.de

5.2 Verarbeitung von Zertifikatsanträgen

5.2.1 Durchführung der Identifizierung und Authentifizierung

Der Zertifikatsnehmer übergibt durch seinen benannten Ansprechpartner, je nach Definition im Abschnitt 4.2, die Unterlagen und Nachweise für die Zertifikatsbeantragung an die SubCA-RA der DARZ-TSE-PKI.

Die RA-Mitarbeiter der DARZ-TSE-PKI prüfen die eingereichten Dokumente / Nachweise. Sollten die Unterlagen / Nachweise nicht vollständig oder fehlerhaft sein, informieren diese den ASP des Zertifikatsnehmers und fordern ihn zur Nachlieferung auf.

Sollte einer der benannten und identifizierten Mitarbeiter ausscheiden und damit die erforderliche Anzahl von mindestens zwei Ansprechpartnern unterschritten werden, muss mindestens ein neuer Vertreter benannt werden (vergleichbar dem im Abschnitt 4.2 beschriebenen Prozess). Die Benennung des neuen Vertreters bzw. der neuen Vertreter sowie das Ausscheidens des bisherigen Vertreters muss vom Geschäftsführer analog zu Abschnitt 4.2 des Teilnehmers bestätigt werden.

Für die TSEs werden keine direkten Ansprechpartner benannt, da diese Aufgaben von den TSE-Betreibern bzw. deren Betreiber-RA übernommen werden.

Bei allen Prozessen der Beantragung, Ausgabe und Verwaltung der Zertifikate wird seitens der DARZ-TSE-PKI hinsichtlich der eingesetzten Kryptografie immer die aktuelle Version der (TR-03116-3) bei der Nutzung des Webservice bzw. wird die (TR-03116-4) zur Absicherung der E-Mail-Kommunikation via S/MIME berücksichtigt.

5.2.2 Annahme oder Ablehnung von Zertifikatsanträgen

Die vorliegenden bzw. nachgelieferten Unterlagen / Nachweise werden von den RA-Mitarbeitern gegen die Vorgaben dieser CP/CPS der DARZ-TSE-PKI geprüft.

(a) Sub-CA Zertifikate

Durch die Root-RA muss im Rahmen der Prüfung auch der vorliegende Zertifikatsrequest für Sub-CA Zertifikate formal überprüft werden.

Im Positivfall wird der Zertifikatsantrag formell freigegeben.

Durch die RA werden im Rahmen der Prüfung auch der vorliegende Zertifikatsrequest für die initialen Zertifikate formal und die Übereinstimmung der gedruckten Hashwerte in den Unterlagen mit denen der Zertifikatsrequests überprüft.

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

(b) TSE-Betreiber-Zertifikate (Webservice)

Für die TSE-Betreiber Zertifikate ist kein formaler Beantragungsprozess durch den TSE-Betreiber vorgesehen. Die Zertifikate werden bei der initialen Registrierung durch den DARZ-TSE-PKI Sub-CA-RA bei der zuständigen RA der internen Verwaltungs-PKI beantragt.

Im Positivfall wird der Zertifikatsantrag formell freigegeben und der die Sub-CA-RA per signierter E-Mail darüber informiert.

Im Negativfall wird der Zertifikatsantrag formell abgelehnt und die die Sub-CA-RA per signierter E-Mail über die Ablehnung (inkl. entsprechender Begründung) informiert. Der Beantragungsprozess ist mit diesem Schritt beendet und muss durch
Die Sub-CA-RA ggf. neu initiiert werden.

5.2.3 Fristen für die Bearbeitung von Zertifikatsanträgen

Zertifikatsanträge sollten so schnell wie möglich bearbeitet werden.

5.2.4 Ausgabe von Zertifikaten

(a) TSE-Zertifikate

TSE-Zertifikate müssen über den Webservice beantragt werden. Die Parameter des Requests werden von der Sub-CA geprüft und auf dieser Basis automatisiert genehmigt. Im Positivfall erhält der beantragende TSE-Betreiber das signierte Zertifikat sofort zurück. Wenn ein Zertifikat nicht innerhalb von 12 Stunden freigeschaltet wurde, wird dieses automatisch gesperrt.

(b) TSE-Betreiber-Zertifikate

TSE-Betreiber Zertifikate werden wie unter 4.2.2(b) beschrieben ausgestellt.

(c) Sub-CA-Zertifikate

Sub-CA-Zertifikate werden wie unter 4.2.2(a) beschrieben ausgestellt.

5.2.5 Benachrichtigung des Zertifikatsnehmers über die Ausgabe des Zertifikats

Der Ansprechpartner wird nach der Ausstellung eines Zertifikats der DARZ-TSE-PKI - außer TSE-Zertifikate - per signierter und verschlüsselter E-Mail (S/MIME) hierüber informiert.

5.3 Annahme von Zertifikaten

Bei den Endentity-Zertifikaten prüft die Betreiber-RA des TSE-Betreibers nach Erhalt die Angaben im Zertifikat auf Korrektheit und Vollständigkeit. Um ein Zertifikat zurückzuweisen, schickt der Die Betreiber-RA des TSE-Betreibers eine signierte und verschlüsselte Email-Nachricht an die DARZ-TSE-PKI. 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. Die DARZ-TSE-PKI nimmt Fehlermeldungen unter der Mailadresse RA-DARZ-TSE-PKI@da-rz.de entgegen.
Bei einer TSE kann diese Prüfung durch den TSE-Betreibers automatisiert z.B. bei dem Erhalt oder der Einbringung der Zertifikate erfolgen.

Der Sub-CA Betreiber muss eine Kommunikationsschnittstelle für Fehlermeldungen bereitstellen. Die entsprechende Kommunikationsschnittstelle MUSS von der Sub-CA in der Sub-CA Policy definiert werden. Bei der Root-CA wird die Kontaktadresse auf der Web-Seite der Root-CA angegeben.

5.3.1 Veröffentlichung von Zertifikaten durch die CA

Alle ausgestellten TSE-Zertifikate werden direkt nach der Ausstellung in dem Verzeichnisdienst der DARZ-TSE-PKI veröffentlicht.

Root- und Sub-CA-Zertifikate und deren Hash-Werte werden auf der Website des CA-Betreibers veröffentlicht.

5.4 Verwendung von Schlüsselpaar und Zertifikat

5.4.1 Verwendung des privaten Schlüssels und des Zertifikats durch den Zertifikatsnehmer

TSE-Zertifikate und die zugehörigen privaten Schlüssel müssen gemäß ihrem Verwendungszweck eingesetzt werden, d.h. im Rahmen der vorgeschriebenen Nutzung in der TSE gemäß [BSI-TR-03153].

Die privaten Schlüssel der CA-Zertifikate dürfen ausschließlich zur Signatur der ausgegebenen Zertifikate gemäß Kap.4.2.2(c) und zur Signatur von ARL/CRL verwendet werden.

Der TSE-Betreiber darf sein TSE-Betreiber-Zertifikat ausschließlich zur Signatur von Zertifikatsrequests für TSE-Zertifikate und für den TLS-Verbindungsaufbau mit der zuständigen Sub-CA verwenden. Er muss den privaten Schlüssel geheim halten und vor unbefugtem Zugriff angemessen schützen.

5.4.2 Verwendung des öffentlichen Schlüssels und des Zertifikats durch Zertifikatsnutzer

Die Verwendung des öffentlichen Schlüssels und des Zertifikats erfolgt gemäß [TR-03151].

5.5 Zertifikatserneuerung

Eine Zertifikatserneuerung auf Basis des bestehenden Schlüsselpaares ist nicht zugelassen.

5.6 Zertifizierung nach Schlüsselerneuerung

5.6.1 Bedingungen der Zertifizierung nach Schlüsselerneuerung

Es gelten die Anforderungen aus Kapitel 4.3.

5.7 Änderungen am Zertifikat

Änderungen an gültigen Zertifikatsinhalten, abgesehen vom individuellen privaten Schlüsselmaterial, sind nicht zulässig. Sollte sich Änderungsbedarf ergeben, z.B. durch eine Umfirmierung eines Zertifikatsnehmers (d.h. die Änderung des Firmennamens oder der Gesellschaftsform), muss ein neues Zertifikat gemäß Abschnitt 4.2 beauftragt und das alte Zertifikat gesperrt werden.

5.8 Sperrung und Suspendierung von Zertifikaten

Zu den Verantwortlichkeiten siehe 4.2.

5.8.1 Sperrung

Alle Zertifikate werden über die von der Root- bzw. Sub-CA bereitgestellten Schnittstellen/Prozesse gesperrt. Eine Sperrung kann nicht zurückgenommen werden.
Alle Sperrungen müssen ereignisgesteuert nach Durchführung einer Sperrung umgesetzt werden.
Ist dem Sperrenden der genaue Zeitpunkt für den Eintritt des Sperrgrundes bekannt, so muss dieser bei der Sperrung angegebenen werden, ansonsten erfolgt der Eintrag in die Sperrliste ohne diesen Parameter.

5.8.2 Suspendierung

Eine Suspendierung von Zertifikaten wird nicht unterstützt.

5.8.3 Aktualisierungs- und Prüfungszeiten bei Sperrungen

In der folgenden Tabelle sind die minimal erforderlichen Aktualisierungs- und Prüfungszeiten der Sperrlisten für die einzelnen DARZ-TSE-PKI Teilnehmer 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 DARZ-TSE-PKI wie in 2 definiert erreichbar ist.

PKI-Teilnehmer	Regelmäßige Aktualisierung der Sperrliste	Erreichbarkeit für Sperrungen	Anlassbezogene Aktualisierung der Sperrliste	Abruf der Sperrliste	Prüfung der Zertifikate auf Sperrung
Root-CA	Innerhalb von 24 Stunden	Täglich	Unverzüglich	Täglich	Täglich
Sub-CA	Innerhalb von 24 Stunden	Täglich	Unverzüglich	Täglich	Bei jeder Verwendung

TABELLE 1: ZEITLICHE ANFORDERUNGEN BEI SPERRUNGEN

5.9 Service zur Statusabfrage von Zertifikaten

Die DARZ-TSE-PKI unterhält derzeit keinen Dienst zur Statusabfrage von Zertifikaten. Die Bereitstellung von Sperrlisten ist in Kapitel 3 geregelt.

5.10 Beendigung der Teilnahme

Die Beendigung der Teilnahme eines Zertifikatsnehmers kann durch diesen selbst oder die zugehörige CA eingeleitet werden.
Bei der Außerbetriebnahme einer TSE kann das Zertifikat der TSE gesperrt werden

5.11 Hinterlegung und Wiederherstellung von Schlüsseln

Eine Schlüsselhinterlegung und Wiederherstellung der DARZ-TSE-PKI ist vorgesehen. Eine Schlüsselhinterlegung und Wiederherstellung durch die DARZ-TSE-PKI wird für PKI-Teilnehmer unterhalb der DARZ-TSE-PKI nicht angeboten.

6. Organisatorische, betriebliche & physikalische Sicherheitsanforderungen

6.1 Generelle Sicherheitsanforderungen

DARZ GmbH besitzt eine gültige ISO27001-Zertifizierung und erfüllt alle aufgelisteten Sicherheitsanforderungen. DARZ GmbH als Betreiber der DARZ-TSE-PKI hat zusätzlich eine Zertifizierung nach TR-03145.

6.1.1 Erforderliche Zertifizierungen der PKI-Teilnehmer

Die Zertifizierung nach ISO/IEC 27001 sowie eine Zertifizierung nach TR-03145 gelten für den Betrieb der DARZ-TSE-PKI mit. Zertifizierungen weiterer PKI-Teilnehmer werden durch die DARZ-TSE-PKI überprüft.

- TSE-Betreiber : Zertifikat auf Basis von [BSI-TR-03153], Common-Criteria-Zertifikat auf Basis von [BSI-CC-PP-0111-2019]
- TSE : Zertifikat auf Basis von [BSI-TR-03153], Common-Criteria-Zertifikat auf Basis von [BSI-CC-PP-0111-2019]

6.1.2 Anforderungen an die Zertifizierung gemäß ISO/IEC 27001

Die Zertifizierung gemäß ISO/IEC 27001 umfasst alle Geschäftsprozesse und IT-Systeme des Registrierungs- und Zertifizierungsbetriebs der betreffenden PKI-Infrastruktur. Es wurde von einem hohen Schutzbedarf ausgegangen. Die Überprüfung der Anforderungen aus TR-03145 ist vor Inbetriebnahme erfolgt.

6.2 Erweiterte Sicherheitsanforderungen

6.2.1 Betriebsumgebung und Betriebsabläufe

Lage und Gebäude

Die DARZ.CA wird innerhalb eines zutrittsgesicherten Bereiches mit einem weiteren separaten Sicherheitsbereich betrieben. Sie unterhält darüber hinaus verschiedene Sicherheitsanlagen zur Hinterlegung von Produktiv- und Backup-Systemen und –Medien. Der Sicherheitsbereich sowie die Sicherheitsanlagen sind an die zentrale Alarmleitstelle des Gebäudes angebunden. Zudem ist der Sicherheitsbereich an ein lokales optisches und akustisches Alarmsystem angeschlossen.

Zutritt

Der räumliche Zutritt erfolgt über ein mehrstufiges Zutrittskontrollsystem. Zu dem Sicherheitsbereich der DARZ.CA ist ausschließlich das dort produktiv tätige PKI-Betriebspersonal zutrittsberechtigt. Es wird ein ausweisbezogenes Login mit biometrischer Bestätigung durchgeführt.

Strom, Heizung und Klimaanlage

Die Installation zur Stromversorgung entspricht den erforderlichen Normen. Eine Notstromversorgung über Dieselgeneratoren ist vorhanden. Eine Klimatisierung des Sicherheitsbereiches ist vorhanden.

Gefährdung durch Wasser

Die Räume verfügen über einen angemessenen Schutz vor Wasserschäden.

Brandschutz

Die Richtlinien für den Brandschutz werden eingehalten. Die Räume sind über Rauchmelder an die Brandmeldeanlage angeschlossen und enthalten eine automatische Löschanlage. Handfeuerlöscher sind in angemessener Anzahl vorhanden.

Aufbewahrung von Datenträgern

Sämtliche Datenträger mit Software sowie tagesaktuelle Sicherungen werden in mehrfachen Ausfertigungen als Original- und Backup-Versionen vorgehalten und in unterschiedlichen Gebäudeabschnitten (Gebäude/Orte) sicher aufbewahrt. Darüber hinaus werden der Gesamtbestand außer Kraft gesetzter Software sowie alte Datensicherungen in einem Archiv hinterlegt.

Sämtliche Datenträger werden mehrstufig in anwendungsbezogenen Stahlkassetten, die sich in Tresorschränken, welche sich wiederum in Tresoranlagen befinden, sicher hinterlegt.

Datenvernichtung

Elektronische Datenträger werden vor Ort sachgerecht zerstört und entsorgt. Papierdatenträger werden vor Ort mittels Aktenvernichten sachgerecht zerstört und entsorgt.

Desaster Backup

Eine externe Sicherung von Daten, außerhalb der DARZ.CA, bei anderen Dienstleistern findet nicht statt.

6.2.2 Verfahrensanweisungen

Es wird im Rahmen eines Rollenkonzeptes sichergestellt, dass Verantwortungsbereiche klar definiert sind, dass einzelne Personen nicht unbemerkt Veränderungen an sicherheitskritischen Komponenten der DARZ-TSE-PKI vornehmen können und private Schlüssel einsehen, generieren oder manipulieren können. Die Namen der am Prozess der Generierung sowie Auslieferung von Schlüsseln und Zertifikaten beteiligten Personen werden protokolliert.

Rollenbeschreibungen

Head of CA operations	Trägt die umfassende Verantwortung für das gesamte CA-Geschäft
CA Operator (SubCA)	Generiert Schlüsselpaare, Zertifikate und Sperrlisten
RA Operator (SubCA)	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. Der aktuelle Ansprechpartner wird wie unter Kapitel 3 beschrieben im Internet veröffentlicht. Die interne Vertretung wird nur im Intranet der DARZ GmbH veröffentlicht.

Die DARZ-TSE-PKI setzt im Produktionsbetrieb für den Umgang mit hochsicherheitskritischen Zugangsmedien und kryptographischen Schlüsselmaterialien und Zertifikaten ein durchgängiges Vier-Augen-Prinzip ein.

Das Konzept sieht vor, dass die Hinterlegung, der Zugriff und der Einsatz der hochsicheren Zugangsmedien stets vom PKI-Betriebspersonal im Vier-Augen-Prinzip wahrgenommen werden. Darüber hinaus wird der gesamte Prozess der Generierung von kryptographischem Schlüsselmaterial und Zertifikaten bis zur Weitergabe im Vier-Augen-Prinzip durchgeführt. Das durchgängige Vier-Augen-Prinzip setzt die Dokumentation der Rollenverteilung der am Generierungsprozess beteiligten Personen in verschiedenen zu erstellenden sowie systembedingt erzeugten Protokollen voraus.

Identifizierung und Authentifizierung jeder Rolle

Das Rollenkonzept wird durch technische und organisatorische Maßnahmen umgesetzt. Die Identifizierung und Authentifizierung der Rollen erfolgt

- beim Zutritt zu Sicherheitsbereichen und Tresoren bzw.
- beim Zugriff auf Wertschränke oder sicherheitskritische Systeme und Anwendungen

mit Hilfe von SmartCards, Hardwaretoken, Benutzerkennungen und Passwörtern. Die Rollenverteilung wird in verschiedenen zu erstellenden sowie systembedingt erzeugten Protokollen dokumentiert.

Das Rollenkonzept stellt die Trennung von bestimmten Rollen und Aufgaben sicher, um zu verhindern, dass eine Person allein einen Schlüssel erzeugen oder ein Zertifikat ausstellen und weitergeben kann.

6.2.3 Personal

Die DARZ-TSE-PKI setzt im Betrieb erfahrenes Personal ein, das über die erforderlichen IT-Kenntnisse und spezifischen Kenntnisse des CA-Betriebs verfügt.

Von allen Mitarbeitern des Betreibers der DARZ-TSE-PKI (DARZ GmbH) liegt ein polizeiliches Führungszeugnis, ohne Einträge, welche eine Eignung für die Tätigkeit in Frage stellen, vor.

Das mit dem Betrieb der DARZ-TSE-PKI betraute Personal wird regelmäßig und anlassbezogen geschult. Es ist hinsichtlich der Sicherheitsrelevanz seiner Arbeit sensibilisiert.

Schulungen und Fortbildungen werden insbesondere bei der Einführung neuer Richtlinien, IT-Systeme und IT-Verfahren durchgeführt.

Das PKI-Betriebspersonal wird in allen Bereichen des CA-Betriebes eingesetzt.

Unerlaubte Handlungen, die die Sicherheit der DARZ-TSE-PKI gefährden oder gegen Datenschutzbestimmungen verstoßen, werden über die Personalstellen disziplinarisch geahndet bzw. strafrechtlich verfolgt.

Dem Personal des Betreibers der DARZ-TSE-PKI stehen zum ordnungsgemäßen Betrieb der PKI folgende Dokumente zur Verfügung:

- Certificate Policy (CP) inkl. Certification Practice Statement (CPS) (mit diesem Dokument)
- Betriebshandbücher
- Benutzeranleitungen
- Dienstvorschriften und –anweisungen
- Relevante ISO27001-Dokumente
- Aktive Betreiberverträge und mögliche Zusatzdokumente welche die Zusammenarbeit definieren und abgrenzen

6.2.4 Monitoring

Die nachfolgenden Ereignisse werden protokolliert und dokumentiert:

- Systeminitialisierung
- Zertifizierungsanträge
- Registrierung der Benutzer
- Schlüsselerzeugung für CA
- Zertifikatserstellung für CA
- Datensicherungen für CA
- Zertifikatsveröffentlichung CA
- Nutzung des privaten Schlüssels und des Zertifikates
- Sperranträge
- Sperrung eines Zertifikates
- Erstellung einer Sperrliste
- Veröffentlichung einer Sperrliste
- Notfall-Management Protokolle

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

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

6.2.5 Archivierung von Aufzeichnungen

Sämtliche Daten, die für den Zertifizierungsprozess relevant sind werden archiviert. Die Archivierung wird bei der betriebsverantwortlichen Stelle der DARZ-TSE-PKI vorgenommen. Die Archive werden gegen Zugriff, Manipulation und Vernichtung geschützt. Die Aufbewahrungszeiten orientieren sich an gesetzlichen Fristen, den Grundsätzen der Revisionssicherheit sowie weiteren internen Regelungen.

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
- der Erstellung von Sperrlisten

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

6.2.6 Schlüsselwechsel der DARZ-TSE-PKI

Der Schlüsselwechsel der DARZ-TSE-PKI kann einerseits geplant und andererseits ungeplant erfolgen:

- Geplanter Schlüsselwechsel: Im Fall eines planbaren Schlüsselwechsels werden die beschriebene Verfahren berücksichtigt und entsprechend der vorhanden Prozesse abgearbeitet.
- Ungeplanter Schlüsselwechsel: Für den Fall, dass ein unvorhergesehener Schlüsselwechsel der DARZ-TSE-PKI notwendig ist, sind entsprechende Verfahren im Notfallmanagement, welches Bestandteil der Betriebsdokumentation ist, definiert.
- Sowohl ein geplanter als auch ein ungeplanter Schlüsselwechsel der DARZ-TSE-PKI erfolgt gemäß dem Vier-Augen-Prinzip.

6.2.7 Auflösen der Zertifizierungsstelle

Im Fall der Einstellung des Betriebes der DARZ-TSE-PKI werden die nachfolgenden Maßnahmen ergriffen:

- Information aller Zertifikatsnehmer sowie vertrauenden Parteien mit einer Vorlauffrist von mindestens drei Monaten.
- Vernichtung der privaten Schlüssel der Zertifizierungsstellen nach Einstellung der Tätigkeiten.
- Veröffentlichung der entsprechenden CA- und Root-CA-Sperrlisten.

6.2.8 Aufbewahrung der privaten Schlüssel

Kryptografiemodule	Die Schlüssel sind in vertrauenswürdigen Kryptografie-Modulen gespeichert.
Schutz der Speichermedien	siehe Kapitel **Fehler! Verweisquelle konnte nicht gefunden werden.** Betriebsumgebung.
Schlüsselaufbewahrung	die Speichermedien befinden sich im physisch und durch technisch-organisatorische Maßnahmen hochgesicherten Bereich, der Zutritt ist auf eine klar definierte Zahl von Personen beschränkt.
Vertrauenswürdiges Personal	der private Schlüssel wird durch vertrauenswürdiges Personal erzeugt, gespeichert und verwendet
Abfallbeseitigung	es ist sichergestellt, dass Abfälle nicht unberechtigt genutzt und vertrauliche Informationen nicht veröffentlicht werden können
Gehärtete IT-Systeme	eine Zertifizierung auf Basis ISO27001 liegt vor

Der CSP innerhalb der TSE muss die Anforderungen gemäß [BSI-CC-PP-0104-2019] oder [BSI-CC-PP-0111-2019], ergänzt mit den Anforderungen aus [BSI-CC-PP-0107-2019] optional ergänzt mit [BSI-CC-PP-0108-2019] erfüllen.

6.2.9 Behandlung von Vorfällen und Kompromittierungen

Das Verfahren zur Behandlung von Sicherheitsvorfällen und Kompromittierungen von privaten Schlüsseln wird von der zuständigen Stelle für IT-Sicherheitsvorfälle festgelegt.

Werden innerhalb der Zertifizierungsstelle fehlerhafte oder manipulierte Rechner, Software und/oder Daten festgestellt, die Auswirkungen auf die Prozesse der Zertifizierungsstelle haben, wird der Betrieb des entsprechenden Systems unverzüglich eingestellt.

Das System wird unter Verwendung der Software sowie der Datensicherungen neu aufgesetzt und nach Überprüfung in einem sicheren Zustand in Betrieb genommen. Das fehlerhafte oder modifizierte System wird analysiert. Bei Verdacht einer vorsätzlichen Handlung werden gegebenenfalls rechtliche Schritte eingeleitet.

Falls Zertifikate mit fehlerhaften Angaben generiert wurden, wird der Zertifikatsinhaber unverzüglich informiert und das Zertifikat von der Zertifizierungsstelle gesperrt.

Bei Kompromittierung oder einem begründeten Verdacht auf Kompromittierung eines privaten Schlüssels ist das jeweilige Zertifikat unverzüglich zu sperren. Bei systemkritischen Zertifikaten ist die SM-PKI Root zu beteiligen. Alle betroffenen Zertifikatsinhaber werden umgehend benachrichtigt.

6.2.10 Meldepflichten

Bei Kompromittierung oder anderweitigen sicherheitsrelevanten Vorfällen muss eine Meldung aufbereitet und an die DARZ-TSE-PKI kommuniziert werden. Die Meldepflicht liegt auf Seiten des Zertifikatsnehmers.

Folgende Vorkommnisse sind Beispiele für eine Meldepflicht:

- Kompromittierung des privaten Schlüsselmaterials
- Verstoß gegen relevante Betriebsauflagen
- Betreiber der CA ist nicht mehr aktiv (Bsp.: Insolvenz)
- Aufforderung zur Sperrung oder Suspendierung eines Zertifikates

Folgende Angaben müssen der Meldung mindestens beigefügt werden:

- Was wurde kompromittiert bzw. was wurde betroffen?
- Wann ist das Vorkommnis passiert bzw. wann wurde der Vorfall bemerkt?
- 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?

Bei Eintreten von sicherheitskritischen Ereignissen unterrichtet die DARZ-TSE-PKI die zuständige Stelle für IT-Sicherheitsvorfälle der DARZ GmbH.

6.3 Notfall-Management

Eine Wiederaufnahme des Zertifizierungsbetriebes nach einer Katastrophe ist Bestandteil der Notfallplanung und kann innerhalb kurzer Zeit erfolgen, sofern die Sicherheit des Betriebes der DARZ-TSE-PKI gegeben ist.

7. Technische Sicherheitsmaßnahmen

7.1 Erzeugung und Installation von Schlüsselpaaren

7.1.1 Generierung von Schlüsselpaaren für die Zertifikate

Die Schlüsselpaare der DARZ-TSE-PKI als Zertifikatsnehmer werden zentral im Sicherheitsbereich der DARZ-TSE-PKI auf Hardware-Security-Modulen im Vier-Augen-Prinzip erstellt.

7.1.2 Lieferung privater Schlüssel

Die Erstellung der privaten Schlüssel der TSE-Zertifikate erfolgt dezentral durch die Zertifikatsnehmer der DARZ-TSE-PKI. Daher erfolgt keine Lieferung der privaten Schlüssel.

7.1.3 Lieferung öffentlicher Zertifikate

Alle Zertifikate werden nach der Erstellung sofort im Verzeichnis der DARZ-TSE-PKI abgelegt und sind somit für alle PKI-Teilnehmer zugänglich.

7.1.4 Schlüssellängen und kryptografische Algorithmen

Die CA-Schlüssel der DARZ-TSE-PKI sind konform zu den Anforderungen aus [BSI-TR-03116-5]. Ebenso werden die zum jeweiligen Zeitpunkt konkret zu verwendenden kryptografischen Algorithmen und Schlüssellängen durch die [BSI-TR-03116-5] bestimmt.

7.1.5 Festlegung der Parameter der öffentlichen Schlüssel und Qualitätskontrolle

Es gelten die Vorgaben aus der Certificate Policy der SM-PKI Root.

7.1.6 Verwendungszweck der Schlüssel

Die Schlüssel werden ausschließlich für die in Kapitel 4.2 beschrieben Verwendungszwecke eingesetzt.

7.2 Sicherung des privaten Schlüssels und Anforderungen an kryptografische Module

Die Teilnehmer der DARZ-TSE-PKI verwenden Kryptografiemodule zur Generierung, Speicherung und Nutzung ihrer privaten Schlüssel zu ihren Zertifikaten aus der DARZ-TSE-PKI. Die Sicherheitsanforderungen an Kryptografiemodule zum Schutz der privaten Schlüssel zu den Zertifikaten werden in Kapitel 7.2 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 (KeyLifeSec) – Security Level 2 eingehalten werden.

7.2.1 Mehrpersonen-Zugriffssicherung zu privaten Schlüsseln

Die privaten Schlüssel einer CA sind durch ein Vier-Augen-Prinzip geschützt.

7.2.2 Ablage privater Schlüssel

Es ist sichergestellt, dass die Daten der privaten Schlüssel nach den Anforderungen aus Kapitel 6.2.8 zur sicheren Handhabung und Lagerung von Schlüsselmaterial gespeichert werden.

7.2.3 Backup privater Schlüssel

Es liegt ein kryptographisch gesichertes Backup der privaten CA-Schlüssel vor. Der Zugriff erfolgt im Vier-Augen-Prinzip.

7.2.4 Archivierung privater Schlüssel

Es wird keine Archivierung gesperrter oder abgelaufener privater Schlüssel durchgeführt. Diese privaten Schlüssel werden unter Beachtung der Einschränkungen aus Kapitel 7.2.9 zerstört.

7.2.5 Transfer privater Schlüssel in oder aus kryptografischen Modulen

Ein Transfer privater CA-Schlüssel erfolgt nur zu Backup- oder Wiederherstellungszwecken in verschlüsselter Form und im Vier-Augen-Prinzip.

7.2.6 Speicherung privater Schlüssel in kryptografischen Modulen

Grundsätzlich werden die privaten Schlüssel der DARZ-TSE-PKI auf einem Kryptografiemodul gespeichert.

- Die einzige Ausnahme bilden die client- und serverseitigen TLS-Schlüssel der DARZ-TSE-PKI, die zur TLS-Authentisierung an der Web-Service-Schnittelle verwendet werden.

7.2.7 Aktivierung privater Schlüssel

Die Aktivierung eines privaten CA-Schlüssels ist nur im Vier-Augen-Prinzip möglich.

7.2.8 Deaktivierung privater Schlüssel

Es ist technisch sichergestellt, dass deaktivierte Schlüssel nicht genutzt werden können.

7.2.9 Zerstörung privater Schlüssel

Die privaten Schlüssel der DARZ-TSE-PKI werden in folgenden Fällen sicher und unwiederherstellbar zerstört:

- Der Gültigkeitszeitraum eines DARZ-TSE-PKI-Schlüssels ist abgelaufen
- Der Schlüssel einer DARZ-TSE-PKI-Komponente wurde gesperrt.

Die Backups der Schlüssel werden ebenfalls berücksichtigt.

Die Zerstörung der privaten Schlüssel erfolgt durch einen sicheren Lösch-Mechanismus im Kryptografiemodul. Für diesen Prozess gelten die Anforderungen aus (KeyLifeSec).

7.2.10 Beurteilung kryptographischer Module

(a) RootCA und SubCA

Die Root-CA bzw. Sub-CA muss sicherheitsüberprüfte oder zertifizierte Hardware-Sicherheitsmodule (HSM) oder Chipkarten einsetzen.

(b) TSE

Bei einem TSE muss ein Kryptografiemodul eingesetzt werden, dass nach [BSI-CC-PP-0104-2019] bzw. [BSI-CC-PP-0111-2019] zertifiziert ist. Der TSE-Betreiber benötigt für sein Kryptografiemodul eine Bestätigung bzw. eine Sicherheitsaussage des Herstellers, dass diese Nachweise durch eine entsprechende Prüfstelle erbracht wurden.
Das Vorhandensein der Bestätigung zu dem vom PKI-Teilnehmer eingesetzten Kryptografiemodul muss vom TSE-Betreiber bei der Einrichtung technische Service-Schnittstelle gegenüber der Sub-CA nachgewiesen werden.

7.3 Andere Aspekte des Managements von Schlüsselpaaren

7.3.1 Archivierung öffentlicher Schlüssel

Sämtliche von der DARZ-TSE-PKI erstellten öffentlichen Schlüssel werden inklusive der Statusdaten in der Datenbank der Zertifizierungsstelle archiviert.

7.3.2 Gültigkeitsperioden von Zertifikaten und Schlüsselpaaren

- Root-CA 13 Jahre.
- SubCa 10 Jahre.
- TSE-Betreiber-Zertifikate: 8 Jahre
- TSE-Signatur-Zertifikate 8 Jahre

7.4 Aktivierungsdaten

Im Rahmen der DARZ-TSE-PKI ist der Zugriff auf die privaten Schlüssel der Zertifizierungsstelle kryptografisch und durch ein Vier-Augen-Prinzip geschützt.

Die Aktivierungsdaten für die Kryptografiemodule werden sicher aufbewahrt.

7.5 Umgesetzte Sicherheitsanforderungen für die Rechneranlagen

- Es werden entsprechende Maßnahmen umgesetzt, um das interne Netzwerk vom externen zu trennen und vor unbefugtem Zugriff zu schützen.
- Der Einsatz von Intrusion-Detection- Systemen (IDS) im gesicherten Netzsegment wird berücksichtigt. Die Log-Dateien des IDS mussen regelmäßig kontrolliert werden.
- Die CA-Server, die zur Erstellung von Zertifikaten verwendet werden, werden gehärtet. Dies umfasst die Konfiguration und Einstellung der verwendeten Hardware- und Software-Komponenten.
- Die Konfigurationsoptionen und -einstellungen enthalten nur die minimal benötigten Funktionalitäten für den CA Betrieb.
- Die Netzwerke, in denen sich die CA-Server befinden, werden durch geeignete Maßnahmen geschützt.
- Software-Updates werden bei sicherheitsrelevanten Änderungen schnellstmöglich eingespielt, andere Updates werden regelmäßig aktualisiert.
- Die CA schützt sensitive Daten vor unbefugtem Zugriff oder Veränderung.
- Log-Dateien und Audit-Trails werden regelmäßig geprüft, und automatisierte Benachrichtigungen weisen auf Abweichung vom vorgesehenen Betrieb hin.
- Die Dateien der Audit-Trails werden auf dem CA-Server, der für die Verwaltung von Zertifikaten verwendet wird, gespeichert. Der Speicherort für Log-Dateien kann temporär der CA-Server sein. Die Log-Dateien werden dann regelmäßig auf einen anderen Speicherort ausgelagert.
- Das System verfügt über eine angemessene Benutzerverwaltung.
- Die CA begrenzt den Zugriff auf die benötigten Systemfunktionen und Hilfsprogramme.
- Die Integrität der System-Komponenten und Informationen wird gegen Viren, Schadsoftware sowie nicht zugelassene Programme geschützt.

7.6 Zeitstempel

Ein Zeitstempeldienst wird nicht angeboten.

7.7 Validierungsmodell

Bei der Verifikation digitaler Signaturen von Log-Nachrichten und Sperrlisten innerhalb der TSE-PKI gilt das Hybridmodell. Alle im Zertifizierungspfad enthaltenen Zertifikate müssen zum Zeitpunkt der Signaturerzeugung gültig gewesen sein. Bei der Verifikation von Zertifikatssignaturen gilt hingegen das Schalenmodell. Ist im Sperrlisteneintrag eines gesperrten Zertifikats ein InvalidityDate verzeichnet, so ist die Signatur auch dann als ungültig zu betrachten, wenn sie im Zeitraum zwischen diesem InvalidityDate und dem Sperrzeitpunkt erstellt wurde. Um eine Verifikation digitaler Signaturen für einen Zeitraum von mindestens zehn Jahren zu gewährleisten, verbleiben Sperrlisteneinträge mindestens für bis zu zehn Jahre nach dem Ende des Gültigkeitszeitraums des gesperrten Zertifikates in der Sperrliste. Ebenso werden die Sperrlisteninformationen jeweils entsprechend lang publiziert.

8. Profile für Zertifikate und Sperrlisten

8.1 Profile für Zertifikate und Zertifikatsrequests

Die Profile für die Zertifikate und die Zertifikatsrequests sind in 14.1spezifiziert. Das Namensschema zu den Zertifikaten ist in Anhang 14.3 definiert.

8.1.1 Zugriffsrechte

Die erlaubte Funktion der Zertifikate wird über die Key-Usage-Extension definiert.

8.1.2 Zertifikatserweiterung

Die Certificate Extensions werden in Anhang 14.4 definiert.

8.2 Profile für Sperrlisten

Die DARZ-TSE-PKI veröffentlicht Zertifikatssperrlisten gemäß des Standards X.509 Version 3. Die Root CA und Sub CA der TSE-PKI stellen Sperrlisten bereit. Die Verteilpunkte von Sperrlisten wird in der entsprechenden Erweiterung in ausgestellten Zertifikaten aufgenommen.

8.3 Profile für OCSP Dienste

OCSP wird durch DARZ-TSE-PKI nicht unterstützt.

9. Überprüfungen der CA und andere Bewertungen

9.1 Inhalte, Häufigkeit und Methodik

Die Arbeitsprozesse der Zertifizierungsstelle sowie der an der Registrierung beteiligten Stellen werden regelmäßig bzw. anlassbezogen überprüft.
Die Audits des technischen Aufbaus der PKI und der operativen Abläufe werden in regelmäßigen Abständen durch die interne Revision nach den in der DARZ GmbH für solche Vorgänge festgelegten Regeln durchgeführt. Die Ergebnisse der Audits werden nicht veröffentlicht. Grundsätzlich werden interne Audits und Prüfungen in regelmäßigen Abständen vorgenommen.

Die internen Prüfungen werden durch den Zentralbereich Revision der DARZ GmbH, sowie die Leitung der DARZ-TSE-PKI vorgenommen. Die Prüfer verfügen über das Know-how sowie die notwendigen Kenntnisse auf dem Gebiet Public Key Infrastructure (PKI), um die Prüfungen vornehmen zu können.

Der Prüfer darf nicht in den Produktionsprozess der DARZ-TSE-PKI eingebunden sein. Eine Selbstüberprüfung ist nicht erlaubt.

Es können alle für die PKI relevanten Bereiche überprüft werden. Die Prüfungsinhalte obliegen dem Prüfer.

9.2 Reaktionen auf identifizierte Vorfälle

Festgestellte Mängel müssen in Abstimmung zwischen Zertifizierungsstelle und Prüfer zeitnah beseitigt werden (siehe Kapitel 6.2.10). Der Prüfer wird über die Beseitigung der Mängel informiert.

10. Sonstige finanzielle und rechtliche Angelegenheiten

10.1 Preise

Preise für TSE/SubCA Dienstleistungen werden auf Anfrage zur Verfügung gestellt.

10.2 Finanzielle Zuständigkeiten

Der Angebotswunsch zur Teilnahme und Fragen zu den finanziellen Konditionen können wir Ihnen auf Anfrage gerne zur Verfügung stellen.

11. Vertraulichkeitsgrad von Geschäftsdaten

11.1.1 Definition von vertraulichen Informationen

Alle Informationen und Daten über Zertifikatsinhaber und Teilnehmer der DARZ-TSE-PKI, die nicht unter Ziffer 11.1.2 fallen, werden als vertrauliche Informationen eingestuft.

11.1.2 Informationen, die nicht zu den vertraulichen Informationen gehören

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

11.1.3 Zuständigkeiten für den Schutz vertraulicher Informationen

Die DARZ-TSE-PKI trägt die Verantwortung für Maßnahmen zum Schutz vertraulicher Informationen.

11.2 Schutz personenbezogener Daten

11.2.1 Datenschutzkonzept

Die Speicherung und Verarbeitung von personenbezogenen Daten richtet sich nach den gesetzlichen Datenschutzbestimmungen.

11.2.2 Als persönlich behandelte Daten

Jegliche Daten über Zertifikatsnehmer und Teilnehmer der DARZ-TSE-PKI werden vertraulich behandelt.

11.2.3 Daten, die nicht als persönlich behandelt werden

Es gelten die Bestimmungen in Ziffer 11.1.2.

11.2.4 Zuständigkeiten für den Datenschutz

Die DARZ-TSE-PKI trägt die Verantwortung für Maßnahmen zum Schutz personenbezogener Daten.

11.2.5 Hinweis und Einwilligung zur Nutzung persönlicher Daten

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

11.2.6 Auskunft gemäß rechtlicher oder staatlicher Vorschriften

Die DARZ-TSE-PKI richtet sich bei der Speicherung und Verarbeitung von personenbezogenen Daten nach den gesetzlichen Datenschutzbestimmungen. Eine Offenlegung findet gegenüber staatlichen Instanzen nur bei Vorliegen entsprechender Entscheidungen in Übereinstimmung mit den geltenden Gesetzen statt.

11.2.7 Andere Bedingungen für Auskünfte

Es sind keine weiteren Umstände für eine Veröffentlichung vorgesehen.

11.3 Geistiges Eigentumsrecht

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

11.4 Zusicherungen und Garantien

11.4.1 Zusicherungen und Garantien der CA

Die DARZ-TSE-PKI verpflichtet sich, den Bestimmungen der Zertifizierungsrichtlinie (CP) und den Regelungen für den Zertifizierungsbetrieb (CPS) zu folgen.

11.4.2 Zusicherungen und Garantien der RA

Die DARZ-TSE-PKI verpflichtet sich, den Bestimmungen der Zertifizierungsrichtlinie (CP) und den Regelungen für den Zertifizierungsbetrieb (CPS) zu folgen.

11.4.3 Zusicherungen und Garantien der Zertifikatsnehmer

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

11.4.4 Zusicherungen und Garantien der Zertifikatsnutzer

Die Zertifikatsnutzer sind zur Einhaltung der Bestimmungen der Zertifizierungsrichtlinie (CP) und den Regelungen für den Zertifizierungsbetrieb (CPS) verpflichtet.

11.4.5 Zusicherungen und Garantien anderer PKI-Teilnehmer

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

11.5 Gewährleistungen

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

11.6 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.

11.7 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.

11.8 Gültigkeitsdauer und Beendigung

11.8.1 Gültigkeitsdauer

Diese Zertifizierungsrichtlinie (CP) und die Regelungen für den Zertifizierungsbetrieb (CPS) treten an dem Tag in Kraft, an dem sie veröffentlicht werden.

11.8.2 Beendigung

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

11.8.3 Auswirkung der Beendigung und Weiterbestehen

Von den Konsequenzen der Aufhebung dieser Zertifizierungsrichtlinie (CP) und den Regelungen für den Zertifizierungsbetrieb (CPS) bleibt die Verantwortung zum Schutz vertraulicher Informationen und personenbezogener Daten unberührt.

11.9 Individuelle Mitteilungen und Absprachen mit Teilnehmern

In dieser Zertifizierungsrichtlinie werden keine entsprechenden Regelungen getroffen.

11.10 Ergänzungen

11.10.1 Verfahren für Ergänzungen

Änderungen der Zertifizierungsrichtlinie (CP) und den Regelungen für den Zertifizierungsbetrieb (CPS) werden rechtzeitig vor ihrem Inkrafttreten veröffentlicht.

11.10.2 Benachrichtigungsmechanismen und –fristen

Die Zertifikatsinhaber werden rechtzeitig vor dem Inkrafttreten auf die Änderung der Zertifizierungsrichtlinie (CP) und den Regelungen für den Zertifizierungsbetrieb (CPS) per signierter E-Mail hingewiesen.
Das Einverständnis von Geschäftspartnern mit den Änderungen gilt als erteilt, wenn der DARZ-TSE-PKI bis zum Zeitpunkt des Inkrafttretens keine gegenteilige Erklärung mit signierter E-Mail zugeht. Auf diese Folge wird die DARZ-TSE-PKI bei dem Hinweis auf die Änderung besonders aufmerksam machen. Sollte ein Geschäftspartner den Änderungen vor dem Zeitpunkt des Inkrafttretens in Form einer signierten E-Mail widersprechen, kommt es zu einem Klärungsgespräch zwischen dem Geschäftspartner und der DARZ GmbH. Sollte der Kunde die aktualisierte CP weiterhin nicht akzeptieren, wird die Sperrung aller Kundenzertifikate entsprechend Kap. 5.8 eingeleitet.
Beschäftigten der DARZ GmbH gegenüber gilt die im Intranet bekannt gemachte jeweils aktuelle Fassung.

11.10.3 Bedingungen für OID Änderungen

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

11.11 Verfahren zur Schlichtung von Streitfällen

Die Anrufung eines Schiedsverfahrens liegt im Ermessen der DARZ GmbH.

11.12 Zugrunde liegendes Recht

Der Gerichtsstand ist Darmstadt.

11.13 Einhaltung geltenden Rechts

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

11.14 Sonstige Bestimmungen

11.14.1 Vollständigkeitserklärung

Alle Regelungen in dieser Zertifizierungsrichtlinie (CP) und Regelungen für den Zertifizierungsbetrieb (CPS) gelten zwischen der DARZ-TSE-PKI und den Zertifikatsinhabern. Die Ausgabe einer neuen Version ersetzt alle vorherigen Versionen. Mündliche Vereinbarungen bzw. Nebenabreden sind nicht zulässig.

11.14.2 Abgrenzungen

Eine Abtretung von Rechten ist nicht vorgesehen.

11.14.3 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.

11.14.4 Vollstreckung (Anwaltsgebühren und Rechtsmittelverzicht)

Rechtliche Auseinandersetzungen, die aus dem Betrieb der DARZ-TSE-PKI herrühren, obliegen den Gesetzen der Bundesrepublik Deutschland.
Erfüllungsort und Gerichtsstand ist Darmstadt.

11.14.5 Höhere Gewalt

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

12. Abkürzungen

BSI	Bundesamt für Sicherheit in der Informationstechnologie
CA	Certification Authority, Zertifizierungsinstanz
CN	Common Name (Bestandteil des Distinguished Name)
CP	Certificate Policy; Zertifizierungsrichtlinie einer PKI
CPS	Certification Practice Statement, Regelungen für den Zertifizierungsbetrieb
CRL	Certificate Revocation List, Sperrliste
DN	Distinguished Name
EMAIL	Email address (Bestandteil des Distinguished Name)
Hardwaretoken	Hardware zur Speicherung von privaten Schlüsseln
LDAP	Light Directory Access Protocol, Verzeichnisdienst
O	Organization (Bestandteil des Distinguished Name)
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OU	Organizational Unit (Bestandteil des Distinguished Name)
PKI	Public Key Infrastructure
RFC	Request for Comment, Dokumente für weltweite Standardisierungen
RFC 3647	Dieser RFC dient der Beschreibung von Dokumenten, die den Betrieb einer PKI beschreiben
Root-CA	oberste Zertifizierungsinstanz einer PKI
SHA 256	Secure Hash Algorithm No.2 Version
S/MIME	Secure Multipurpose Internet Mail Extensions, Standard für sichere E-Mail
Sperrliste	signierte Liste einer CA, die gesperrte Zertifikate enthält
TLS	Transport Layer Security (Protokoll zur Verschlüsselung einer Datenübertragung)
x.509v1	Zertifizierungsstandard
Zertifikat	sichere Zuordnung von öffentlichen Schlüsseln zu einem Teilnehmer

13. Literaturverweise

ISO/IEC 27001 (2015)	*IT-Sicherheitsverfahren – Informationssicherheits-Managementsysteme – Anforderungen. DIN.*
TR-03116-3 (2019)	*Kryptographische Vorgaben für Projekte der Bundesregierung; Teil 3: Intelligente Messsysteme. Stand 2019 (11.01.2019) Bonn: BSI.*
TR-03145 (2017)	*Secure Certification Authority operation. Version 1.1 (27.03.2017) Bonn: BSI.*
BSI PP-CSP	*Common Criteria Protection Profile: Cryptographic Service Provider, BSI-CC-PP-0104-2019*
BSI PP-CSPL	*Common Criteria Protection Profile: Cryptographic Service Provider Light, BSI-CC-PP-0111-2019*
BSI PP-SMAERS	*Common Criteria Protection Profile: Security Module Application for Electronic Record-keeping Systems, BSI-CC-PP-0105-2019 & BSI-CC-PP-0105-2020*
BSI TR-02102-2	*Technische Richtlinie BSI TR-02102, Kryptographische Verfahren: Empfehlungen und Schlüssellängen Teil 2: Verwendung von Transport Layer Security (TLS), Version: 2020-1*
BSI TR-03116-5	*Technische Richtlinie BSI TR-03116, Kryptographische Vorgaben für Projekte der Bundesregierung Teil 5: Anwendungen der Secure Element API, Stand 2020 (27.01.2020)*
BSI TR-03145-1	*Technical Guideline BSI TR-03145, Secure CA operation Part 1. Generic requirements for Trust Centers instantiating as Certification Authority (CA) in a Public-Key Infrastructure (PKI) with security level 'high', Version 1.1 (27.03.2017)*
BSI TR-03151	*Technical Guideline BSI TR-03151, Secure Element API (SE API), Version 1.0.1 (20.12.2018)*
ISO 3116 ALPHA-2	*ISO: Codes for countries and their subdivisions, ALPHA-2 coding*
ISO/IEC 27001	*ISO/IEC 27001:2013. Information technology - Security techniques -Information security management systems requirements specification*
KassenG	*Gesetz zum Schutz vor Manipulationen an digitalen Grundaufzeichnungen, BGBl. I S. 3152*
KassenSichV	*Kassensicherungsverordnung: Verordnung zur Bestimmung der technischen Anforderungen an elektronische Aufzeichnungs- und Sicherungssysteme im Geschäftsverkehr, BGBl. I S. 3515 (26.09.2017)*
RFC 4211	*IETF RFC 4211, J. Schaad, Internet X.509 Public Key Infrastructure Certificate Request Message Format (CRMF), 2005*
RFC 4511	*IETF RFC 4511, J. Sermersheim, Lightweight Directory Access Protocol (LDAP): The Protocol, 2006*
RFC 5280	*IETF RFC 5280, D. Cooper et al., Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, 2008*
RFC 5652	*IETF RFC 5652, R. Housley, Cryptographic Message Syntax (CMS), 2009*

14. Anhänge

14.1 Zertifikatsprofile

In der TSE-PKI werden X.503-Zertifikate der Version 3 verwendet. Ein X.509-Zertifikat besteht gemäß [RFC 5280] aus den folgenden drei Feldern:

1. **TBSCertificate**
2. **SignatureAlgorithm**
3. **SignatureValue**

Das Feld „TBSCertificate“ enthält den Zertifikatsinhalt, der vom Zertifikatsaussteller signiert wird. Der Zertifikatsaussteller verwendet dazu den im Feld „SignatureAlgorithm“ angegebenen Signatur-algorithmus. Die Signatur steht im Feld „SignatureValue“.

In Anhang 14.2 ist die Struktur des TBSCertificate für die verschiedenen Zertifikatstypen der TSE-PKI beschrieben. Die jeweils im TBSCertificate enthaltenen Extensions sind getrennt davon in Anhang 14.4 aufgelistet.

Für die Zertifikate der TSE-PKI gelten die kryptographischen Vorgaben aus [BSI TR-03116-5]. Für die Signatur von Zertifikaten zulässige Signaturverfahren sind ECDSA und ECSDSA, zulässige Hashfunktionen sind SHA-2 und SHA-3 mit einer minimalen Outputlänge von 384 Bit. Die Domain-Parameter des im Zertifikat enthaltenen EC-Schlüssels sollen als Named Curve angegeben werden. In den CA-Zertifikaten dürfen die Domain-Parameter BrainpoolP384r1, BrainpoolP512r1, NIST P-384 und NIST P-521 verwendet werden. In den TSE-Signaturzertifikaten sind zusätzlich auch BrainpoolP256r1 und NIST P-256 erlaubt. Die EC-Punkte müssen im Uncompressed Encoding angegeben werden.

TBSCertificate

In Anhang 14.2 ist die allgemeine Struktur des TBSCertificate zu finden. In den anschließenden Anhangs-Kapiteln 14.3 wird das TBSCertificate für die verschiedenen Zertifikatstypen der TSE-PKI im Detail beschrieben.

14.2 Allgemeine Struktur

Ein TBSCertificate der X.509-Version 3 enthält die folgenden Felder:

1. **Version**
   - „v3“
2. **SerialNumber**
   - von der Aussteller-CA vergebene Seriennummer des Zertifikats
3. **Signature**
   - Signaturalgorithmus des Zertifikats; entspricht Wert im Feld „SignatureAlgorithm“
4. **Issuer**
   - eindeutiger Name des Zertifikatsausstellers
5. **Validity**
   - Gültigkeitszeitraum des Zertifikats, definiert durch Gültigkeitsbeginn und Gültigkeitsende

6. **Subject**
   - eindeutiger Name des Zertifikatsinhabers
7. **SubjectPublicKeyInfo**
   - öffentlicher Schlüssel des Zertifikatsinhabers und zugehörige Schlüsselinformationen (Schlüsselalgorithmus, Schlüsselparameter)
8. **Extensions**
   - zusätzliche Zertifikatsattribute; detaillierte Beschreibung in Anhang **Fehler! Verweisquelle konnte nicht gefunden werden.**

Issuer und Subject werden als Distinguished Name (DN) angegeben. Ein DN besteht aus mehreren Relative Distinguished Names (RDNs). In 14.3 sind die Namensschemata für die verschiedenen Zertifikatstypen zu finden.

14.2.1 Root-CA-Zertifikat

1. **Version**
   - „v3“
2. **SerialNumber**
   - zufällig gewählt, 126 Bit Entropie
3. **Signature**
   - ECDSAwithSHA384 (1.2.840.10045.4.3.3)
4. **Issuer**
   - entspricht Subject
5. **Validity**
   - Gültigkeitsdauer: 13 Jahre
6. **Subject**
   - Der Subject-DN des Root-CA-Zertifikats setzt sich aus den in Tabelle 2 enthaltenen RDNs zusammen.
7. **SubjectPublicKeyInfo**
   - Named Curve: brainpoolP384r1 (1.3.36.3.3.2.8.1.1.11)

14.2.2 Sub-CA-Zertifikat

1. **Version**
   - „v3“
2. **SerialNumber**
   - zufällig gewählt, 126 Bit Entropie
3. **Signature**
   - ECDSAwithSHA384 (1.2.840.10045.4.3.3)
4. **Issuer**

- entspricht Subject des Root-CA-Zertifikats

5. **Validity**
   - Gültigkeitsdauer: 10 Jahre (vgl. Kapitel)
6. **Subject**
   - Der Subject-DN des Sub-CA-Zertifikats setzt sich aus den in Tabelle 3 enthaltenen RDNs zusammen.
7. **SubjectPublicKeyInfo**
   - Named Curve: brainpoolP384r1 (1.3.36.3.3.2.8.1.1.11)

14.2.3 TSE-Signaturzertifikat

1. **Version**
   - „v3“
2. **SerialNumber**
   - zufällig gewählt, 126 Bit Entropie
3. **Signature**
   - ECDSAwithSHA384 (1.2.840.10045.4.3.3)
4. **Issuer**
   - entspricht Subject des Sub-CA-Zertifikats
5. **Validity**
   - Gültigkeitsdauer: 8 Jahre (vgl. Kapitel)
6. **Subject**
   - Der Subject-DN des TSE-Signaturzertifikats setzt sich aus den in Tabelle 4 enthaltenen RDNs zusammen.
7. **SubjectPublicKeyInfo**
   - Named Curve: brainpoolP256r1 (1.3.36.3.3.2.8.1.1.7) oder NIST P-256 (1.2.840.10045.3.1.7)

14.3 Namensschemata

Die nachfolgenden Tabellen enthalten die Namenschemata für die verschiedenen Zertifikate der TSE-PKI. Der Subject-DN der Zertifikate setzt sich aus den angegebenen RDNs zusammen.

Tabelle 2: Namensschema des Root-CA-Zertifikats

RDN	Abkürzung	Beschreibung	Wert	Verwendung
Common Name	CN	Name der Root-CA		Pflicht
Organization	O	Name der Organisation		Pflicht
Organizational Unit	OU	Name der Organisationseinheit	<OU>	optional
Country	C	Ländercode gemäß [ISO 3116 ALPHA-2]	DE	Pflicht
Serial Number	SERIALNUMBER	Sequenznummer des Zertifikats; wird bei jedem neuen Zertifikat um 1 hochgezählt	<SN>	Pflicht

Tabelle 3: Namensschema des Sub-CA-Zertifikats

RDN	Abkürzung	Beschreibung	Wert	Verwendung
Common Name	CN	Name der Sub-CA		Pflicht
Organization	O	Name der Organisation		Pflicht

Organizational Unit	OU	Name der Organisationseinheit	<OU>	optional
Street	STREET	Straße der Sub-CA	<Straße>	optional
Postal Code	postalcode	Postleitzahl der Sub-CA	<PLZ>	optional
Locality	L	Ort des Sub-CA-Inhaberstandortes	<Ort>	optional
State	ST	Bundesland des Sub-CA-Inhaberstandortes	<Bundesland>	Optional
Country	C	Ländercode gemäß [ISO 3116 ALPHA-2]	DE	Pflicht
Serial Number	SERIALNUMBER	Sequenznummer des Zertifikats; wird bei jedem neuen Zertifikat um 1 hochgezählt	<SN>	Pflicht

***Tabelle 4**: Namensschema des TSE-Signaturzertifikats*

RDN	Abkürzung	Beschreibung	Wert	Verwendung
Common Name	CN	eindeutige Exemplar-ID Devices (max. 64 Zeichen gemäß RFC 5280!)	<Zertifizierungs-ID CSP>_ <Zertifizierungs-ID SMAERS>_<virtuelle SMAERS-ID>	Pflicht
Organization	O	Name der Betreiber-Organisation	Exakt wie in RA für den Betreiber/PKI-Client hinterlegt	Pflicht
DN Qualifier	DN	Zertifizierungs-ID	<Zertifizierungs-ID> (wie im CN enthalten)	Pflicht
Serial Number	SERIALNUMBER	Seriennummer der TSE	SHA256-Hash über den Public Key gemäß TR-03151	Pflicht
Country	C	Ländercode gemäß [ISO 3116 ALPHA-2]	DE	Pflicht

14.4 Extensions

Tabelle 5 enthält eine Übersicht der verwendeten Zertifikats-Extensions. Sie sind in [RFC 5280] definiert. Die Verwendung der Extensions ist abhängig vom Zertifikatstyp. Mit 'x' markierte Extensions sind im jeweiligen Zertifikat vorhanden.

Tabelle 5: Zertifikats-Extensions

Nr.	Bezeichnung	C(Root-CA)	C(Sub-CA)	C_{SIG}(TSE)
1	AuthorityKeyIdentifier		x	x
2	SubjectKeyIdentifier	x	x	
3	KeyUsage	x	x	x
4	CertificatePolicies	x	x	x
5	SubjectAltName	x	x	
6	IssuerAltName	x	x	x
7	BasicConstraints	x	x	x
8	CRLDistributionPoints		x	x
9	AuthorityInfoAccess	x	x	x

Eine Beschreibung der einzelnen Extensions ist im Folgenden zu finden.

1. **AuthorityKeyIdentifier**
   - OID: 2.5.29.35
   - Kritisch: nein
   - Beschreibung: Der AuthorityKeyIdentifier dient der Unterscheidung verschiedener öffentlicher Schlüssel desselben Zertifikatsausstellers.
   - Wert: SHA-1 Hash des öffentlichen Schlüssels des Zertifikatsausstellers
2. **SubjectKeyIdentifier**
   - OID: 2.5.29.14
   - Kritisch: nein
   - Beschreibung: Der SubjectKeyIdentifier dient der Identifikation eines Zertifikats mit einem bestimmten öffentlichen Schlüssel.

- Wert: SHA-1 Hash des öffentlichen Schlüssels des Zertifikatsinhabers

3. **KeyUsage**
   - OID: 2.5.29.15
   - Kritisch: ja
   - Beschreibung: Die KeyUsage-Extension spezifiziert, wofür der zum zertifizierten öffentlichen Schlüssel zugehörige private Schlüssel verwendet werden darf.
   - Wert: Der Wert ist abhängig vom Zertifikatstyp. In Tabelle 6 sind die Werte für die verschiedenen Zertifikatstypen zusammengefasst.

TABELLE 6: KEYUSAGE-EXTENSION

Zertifikat	C(Root-CA)	C(Sub-CA)	C_{SIG}(TSE)
Gesetzte Bits	keyCertSign, cRLSign,	keyCertSign, cRLSign,	digitalSignature

4. **CertificatePolicies**
   - OID: 2.5.29.32
   - Kritisch: nein
   - Beschreibung: Die CertificatePolicies-Extension verweist auf die Certificate Policy (CP), nach der das Zertifikat ausgestellt wurde.
   - Wert: OID der CP, nach der das Zertifikat ausgestellt wurde (policyIdentifier) und Bezugspunkt der CP (policyQualifiers: PolicyQualifierInfo mit CPSUri)
5. **SubjectAltName**
   - OID: 2.5.29.17
   - Kritisch: nein
   - Beschreibung: Die SubjectAltName-Extension enthält weitergehende Informationen zum Zertifikatsinhaber.
   - Wert: Alternativname des Zertifikatsinhabers, z. B. Kontakt-E-Mail-Adresse (rfc822Name) oder URL der Webseite (uniformResourceIdentifier)
6. **IssuerAltName**
   - OID: 2.5.29.35
   - Kritisch: nein
   - Beschreibung: Die IssuerAltName-Extension enthält weitergehende Informationen zum Zertifikatsaussteller.
   - Wert: Alternativname des Zertifikatsausstellers entsprechend der SubjectAltName-Extension des Aussteller-Zertifikats
7. **BasicConstraints**
   - OID: 2.5.29.19
   - Kritisch: ja
   - Beschreibung: Die BasicConstraints-Extension legt fest, ob es sich um ein CA- oder ein EE-Zertifikat handelt. Bei CA-Zertifikaten gibt sie zusätzlich an, wie viele Intermediate-Zertifikate auf das CA-Zertifikat in einem Zertifizierungspfades folgen dürfen.
   - Wert: Der Wert ist abhängig vom Zertifikatstyp. In Tabelle 7 sind die Werte für die verschiedenen Zertifikatstypen zusammengefasst.

TABELLE 7: BASICCONSTRAINTS-EXTENSION

Zertifikat	C(Root-CA)	C(Sub-CA)	C_{SIG}(TSE)
cA	true	true	false
pathLenConstraint	1	0	/

8. **CRLDistributionPoints**
   - OID: 2.5.29.31
   - Kritisch: nein

- Beschreibung: Die CRLDistributionPoints-Extension spezifiziert ein- oder mehrere Bezugspunkte für die CRL der Aussteller-CA. Wenn eine CRL nicht von der CA selbst herausgegeben wird, enthält die Extension den CRL-Herausgeber.
- Wert: HTTP/LDAP Download URL auf Anfrage

9. **AuthorityInfoAccess**
    - OID: 1.3.6.1.5.5.7.1.1
    - Kritisch: nein
    - Beschreibung: Die AuthorityInfoAccess-Extension enthält Bezugspunkte für weitere Informationen, die von der Aussteller-CA bereitgestellt werden.
    - Wert: Download-URL des Aussteller-Zertifikats (caIssuers)