

# Telekom Security HBA SM(C)-B

## [HPC105] Erklärung zum Zertifizierungsbetrieb (CP/CPS)

Deutsche Telekom Security GmbH  
Trust Center & ID Security

öffentlich

Version: 14.00  
Status: freigegeben

Gültig ab: 30.04.2026  
Letztes Review: 24.04.2026

Mit Veröffentlichung dieses Dokumentes verlieren alle bisherigen Versionen ihre Gültigkeit!

# Impressum

<b>Herausgeber</b>	Deutsche Telekom Security GmbH Trust Center & ID Security	
<b>Dateiname</b>	<b>Gültig ab</b>	<b>Titel</b>
HPC105 CPS HBA SMC-B V14.00.docx	30.04.2026	Telekom Security HBA SM(C)-B [HPC105] Erklärung zum Zertifizierungsbetrieb (CP/CPS)
<b>Version</b>	<b>Letztes Review</b>	<b>Status</b>
14.00	24.04.2026	freigegeben
<b>Autor</b>	<b>Inhaltlich geprüft von</b>	<b>Freigegeben von</b>
Telekom Security	Telekom Security	Telekom Security
<b>Ansprechpartner</b>	<b>Telefon</b>	<b>E-Mail</b>
Deutsche Telekom Security GmbH – Trust Center & ID Security		trustcenter.gematik@telekom.de
<b>Kurzbeschreibung</b>	Certification Practice Statement Deutsche Telekom Security GmbH HBA gemäß RFC3647	

Tabelle 1: Impressum

Copyright © 2026 by Deutsche Telekom Security GmbH, Bonn

Alle Rechte, auch die des auszugsweisen Nachdrucks, der fotomechanischen Wiedergabe (einschließlich Mikrokopie) sowie der Auswertung durch Datenbanken oder ähnliche Einrichtungen, vorbehalten.

## Änderungen

Version	Stand	Bearbeiter	Änderungen / Kommentar
01.00	30.06.2017	T-Systems International GmbH	erste freigegebene Version HBA
02.00	28.02.2018	T-Systems International GmbH	Aufnahme SMC-B Anpassung der Zertifikatshierarchien
03.00	15.08.2018	T-Systems International GmbH	Überarbeitung nach ETSI-Audit
04.00	05.11.2019	T-Systems International GmbH	Zusammenführung paralleler Versionen, Verwendung von Feldern und Variablen
05.00	10.06.2020	Telekom Security	Anpassungen aufgrund Ausgliederung der Telekom Security
06.00	10.10.2020	Telekom Security	Aktualisierung POSTIDENT
07.00	12.02.2021	Telekom Security	Überarbeitung nach ETSI-Audit
08.00	04.06.2021	Telekom Security	Aufnahme SM-B, Herausnahme CVC G1
09.00	30.05.2022	Telekom Security	Neues Identifizierungsverfahren „VDA Ident“
10.00	15.06.2023	Telekom Security	Neues Identifizierungsverfahren „PostIdent eID“
11.00	25.03.2024	Telekom Security	Neue Kartengeneration G2.1 und vertrauenswürdige Rollen überarbeitet
12.00	08.01.2025	Telekom Security	Ausweiskopie wird nicht mehr benötigt
12.01	19.01.2026	Telekom Security	Akzeptanz Zertifikat 4.4.1
13.00	30.01.2026	Telekom Security	Freigabe neue Version
14.00	30.04.2026	Telekom Security	Überarbeitung nach ETSI-Audit

Tabelle 2: Änderungshistorie

# Inhaltsverzeichnis

<b>1</b>	<b>Einleitung.....</b>	<b>13</b>
1.1	Überblick .....	13
1.2	Dokumentenidentifikation .....	15
1.3	PKI-Beteiligte .....	15
1.3.1	Zertifizierungsstelle .....	15
1.3.2	Registrierungsstellen.....	16
1.3.3	Antragsteller .....	16
1.3.4	Vertrauende Dritte .....	17
1.3.5	Weitere Beteiligte .....	17
1.4	Anwendung von Zertifikaten .....	18
1.4.1	Zulässige Verwendung von Zertifikaten.....	18
1.4.2	Unzulässige Verwendung von Zertifikaten.....	18
1.4.3	Testzertifikate.....	18
1.5	Verwaltung des Dokuments.....	19
1.5.1	Zuständigkeit für das Dokument .....	19
1.5.2	Kontaktinformationen .....	19
1.5.3	Stelle, die über die Vereinbarkeit dieser Richtlinien mit der CP entscheidet ...	19
1.5.4	Genehmigungsverfahren dieses Dokuments .....	19
1.6	Definitionen und Abkürzungen.....	20
1.6.1	Definitionen .....	20
1.6.2	Abkürzungen.....	23
<b>2</b>	<b>Veröffentlichung und Verzeichnisdienste .....</b>	<b>25</b>
2.1	Verzeichnisdienste .....	25
2.2	Veröffentlichung von Zertifikatsinformationen .....	25
2.3	Zeitpunkt oder Frequenz der Veröffentlichung.....	26
2.4	Zugangsbeschränken zu den Verzeichnisdiensten.....	26
<b>3</b>	<b>Identifizierung und Authentifizierung .....</b>	<b>27</b>
3.1	Namensgebung.....	27
3.1.1	Namensformen.....	27
3.1.2	Aussagekraft von Namen .....	28
3.1.3	Anonymität bzw. Pseudonyme der Zertifikatsinhaber .....	28
3.1.4	Regeln zur Interpretation verschiedener Namensformen.....	28
3.1.5	Eindeutigkeit von Namen.....	28
3.1.6	Erkennung, Authentifizierung und Rolle von Markennamen .....	28
3.2	Erstmalige Registrierung .....	28

3.2.1	Methoden zum Besitznachweis des privaten Schlüssels .....	28
3.2.2	Identitätsprüfung einer Organisation.....	29
3.2.3	Identitätsprüfung einer natürlichen Person .....	29
3.2.4	Nicht überprüfte Teilnehmerangaben .....	31
3.2.5	Überprüfung der Berechtigung .....	31
3.2.6	Kriterien für Interoperabilität .....	31
3.3	Identifizierung und Authentifizierung bei Zertifikatserneuerung.....	31
3.3.1	Identifizierung und Authentifizierung für routinemäßige Schlüsselerneuerung.....	31
3.3.2	Identifizierung und Authentifizierung bei Schlüsselerneuerung nach Zertifikatssperrung.....	32
3.4	Identifizierung und Authentifizierung bei Sperranträgen .....	32
3.4.1	Sperrung von Karten durch die Antragsteller .....	32
3.4.2	Sperrung von Karten durch den Kartenherausgeber .....	32
<b>4</b>	<b>Anforderung an den Lebenszyklus der Zertifikate.....</b>	<b>33</b>
4.1	Antragstellung .....	35
4.1.1	Wer kann eine Karte beantragen?.....	35
4.1.2	Antragsstellungsverfahren und Pflichten .....	35
4.2	Antragsbearbeitung .....	36
4.2.1	Durchführung der Identifikation und Authentifizierung .....	36
4.2.2	Genehmigung oder Ablehnung von Zertifikatsaufträgen.....	37
4.2.3	Bearbeitungszeit von Anträgen.....	38
4.3	Zertifikatserstellung .....	38
4.3.1	Maßnahmen der CA während der Ausstellung von Zertifikaten .....	38
4.3.2	Benachrichtigung von Antragstellern über die Ausstellung der Zertifikate.....	39
4.4	Zertifikatsübergabe und -annahme.....	39
4.4.1	Akzeptanz durch den Zertifikatsinhaber.....	39
4.4.2	Veröffentlichung des Zertifikats durch die CA.....	39
4.4.3	Benachrichtigung anderer Stellen über die Zertifikatsausstellung durch die CA.....	40
4.5	Verwendung von Schlüsselpaar und Zertifikat.....	40
4.5.1	Nutzung des privaten Schlüssels und des Zertifikats durch den Zertifikatsinhaber.....	40
4.5.2	Nutzung von öffentlichen Schlüsseln und Zertifikaten durch Vertrauende Dritte (Relying Parties) .....	40
4.6	Zertifikatserneuerung .....	40
4.6.1	Bedingungen für eine Zertifikatserneuerung .....	41
4.6.2	Wer darf eine Zertifikatserneuerung beantragen?.....	41
4.6.3	Bearbeitung von Zertifikatserneuerungen.....	41

4.6.4	Benachrichtigung des Zertifikatsnehmers über die Ausstellung eines neuen Zertifikats.....	41
4.6.5	Annahme einer Zertifikatserneuerung.....	41
4.6.6	Veröffentlichung einer Zertifikatserneuerung durch die CA.....	41
4.6.7	Benachrichtigung weiterer Stellen über eine Zertifikatserneuerung durch die CA .....	41
4.7	Zertifikatserneuerung mit Schlüsselwechsel .....	41
4.7.1	Bedingungen für eine Schlüsselerneuerung .....	41
4.7.2	Wer darf die Zertifizierung eines neuen öffentlichen Schlüssels beantragen? .....	42
4.7.3	Bearbeitung von Schlüsselerneuerungsaufträgen .....	42
4.7.4	Benachrichtigung des Zertifikatsnehmers über die Zertifikatsausstellung .....	42
4.7.5	Annahme einer Zertifikatserneuerung mit neuem Schlüsselmaterial .....	42
4.7.6	Veröffentlichung eines Zertifikats mit neuem Schlüsselmaterial durch die Zertifizierungsstelle .....	42
4.7.7	Benachrichtigung weiterer Stellen über eine Zertifikatserstellung durch die Zertifizierungsstelle .....	42
4.8	Änderung von Zertifikatsdaten.....	42
4.8.1	Bedingungen für eine Zertifikatsänderung .....	42
4.8.2	Wer darf eine Zertifikatsänderung beantragen?.....	43
4.8.3	Bearbeitung von Zertifikatsänderungen .....	43
4.8.4	Benachrichtigung des Zertifikatsnehmers über die Ausstellung eines Zertifikats .....	43
4.8.5	Annahme einer Zertifikatsänderung.....	43
4.8.6	Veröffentlichung eines Zertifikats mit geänderten Daten durch die CA .....	43
4.8.7	Benachrichtigung weiterer Stellen durch die CA über eine Zertifikatsausstellung.....	43
4.9	Sperrung und Suspendierung von Zertifikaten.....	43
4.9.1	Gründe für eine Sperrung.....	43
4.9.2	Wer kann eine Sperrung beantragen? .....	44
4.9.3	Ablauf einer Sperrung .....	45
4.9.4	Fristen für einen Sperrantrag.....	46
4.9.5	Fristen für die Bearbeitung eines Sperrantrags durch die CA .....	46
4.9.6	Überprüfungsmethoden für Vertrauende Dritte .....	46
4.9.7	Frequenz der Veröffentlichung von Sperrlisten .....	47
4.9.8	Maximale Latenzzeit von Sperrlisten .....	47
4.9.9	Online- Verfügbarkeit von Sperr-/Statusinformationen.....	47
4.9.10	Anforderungen an Online-Überprüfungsverfahren .....	47
4.9.11	Andere verfügbare Formen der Bekanntmachung von Sperrinformationen ....	47

4.9.12	Besondere Anforderungen bezüglich der Kompromittierung privater Schlüssel.....	47
4.9.13	Suspendierung von Zertifikaten .....	48
4.9.14	Wer kann eine Suspendierung beauftragen?.....	48
4.9.15	Verfahren der Suspendierung.....	48
4.9.16	Beschränkung des Suspendierungszeitraums .....	48
4.10	Auskunftsdienste über den Zertifikatsstatus .....	48
4.10.1	Betriebsbedingte Eigenschaften .....	48
4.10.2	Verfügbarkeit der Dienste.....	49
4.10.3	Weitere Merkmale .....	49
4.11	Kündigung des Zertifizierungsdienstes .....	49
4.12	Schlüsselhinterlegung und Wiederherstellung .....	49
4.12.1	Richtlinien und Praktiken zur Schlüsselhinterlegung und -wiederherstellung .....	49
4.12.2	Richtlinien und Praktiken zum Schutz und Wiederherstellung von Sitzungsschlüsseln.....	49
<b>5</b>	<b>Physikalische, organisatorische und personelle Sicherheitsmaßnahmen .....</b>	<b>50</b>
5.1	Physikalische Sicherheitsmaßnahmen .....	50
5.1.1	Standort und bauliche Maßnahmen.....	50
5.1.2	Zutritt.....	51
5.1.3	Stromversorgung und Klimatisierung im RZ .....	51
5.1.4	Wassergefährdung des RZ.....	51
5.1.5	Brandschutz im RZ.....	51
5.1.6	Aufbewahrung von Datenträgern.....	52
5.1.7	Entsorgung.....	52
5.1.8	Externe Sicherung.....	52
5.2	Organisatorische Sicherheitsmaßnahmen .....	52
5.2.1	Vertrauenswürdige Rollen .....	53
5.2.2	Anzahl der für eine Aufgabe erforderlichen Personen .....	54
5.2.3	Identifizierung und Authentifizierung für jede Rolle .....	54
5.2.4	Rollen, die eine Aufgabentrennung erfordern .....	54
5.3	Personelle Sicherheitsmaßnahmen .....	55
5.3.1	Anforderungen an Qualifikation, Erfahrung und Sicherheitsüberprüfung .....	55
5.3.2	Sicherheitsüberprüfung .....	55
5.3.3	Schulungs- und Fortbildungsanforderungen .....	56
5.3.4	Nachschulungsintervalle und -anforderungen.....	56
5.3.5	Häufigkeit und Abfolge der Arbeitsplatzrotation .....	56

5.3.6	Sanktionen bei unbefugten Handlungen.....	56
5.3.7	Anforderungen an unabhängige Auftragnehmer .....	57
5.3.8	Dokumentation für das Personal .....	57
5.4	Aufzeichnung und Protokollierung wichtiger Ereignisse.....	57
5.4.1	Art der aufgezeichneten Ereignisse .....	57
5.4.2	Bearbeitungsintervall der Protokolle .....	58
5.4.3	Aufbewahrungszeitraum für Audit-Protokolle .....	58
5.4.4	Schutz der Audit-Protokolle .....	58
5.4.5	Sicherungsverfahren für Audit-Protokolle .....	58
5.4.6	Audit-Erfassungssystem (intern vs. extern) .....	58
5.4.7	Benachrichtigung des Ereignis-auslösenden Subjekts .....	58
5.4.8	Schwachstellenbewertung.....	59
5.5	Archivierung von Daten .....	59
5.5.1	Art der archivierten Datensätze .....	59
5.5.2	Aufbewahrungszeitraum für archivierte Daten .....	59
5.5.3	Schutz von Archiven.....	60
5.5.4	Sicherungsverfahren für Archive .....	60
5.5.5	Anforderungen an Zeitstempel von Datensätzen.....	60
5.5.6	Archiverfassungssystem (intern oder extern).....	60
5.5.7	Verfahren zur Beschaffung und Überprüfung von Archivinformationen.....	60
5.6	Schlüsselwechsel der Zertifizierungsstelle .....	60
5.7	Kompromittierung und Wiederanlauf nach einem Notfall .....	61
5.7.1	Umgang mit Störungen und Kompromittierungen .....	61
5.7.2	Beschädigung von EDV-Geräten, Software oder Daten .....	61
5.7.3	Verfahren bei Kompromittierung von privaten Schlüsseln von Zertifizierungsstellen .....	61
5.7.4	Geschäftskontinuität nach einem Notfall.....	61
5.8	Einstellung der Zertifizierungsdienste .....	62
<b>6</b>	<b>Technische Sicherheitsaspekte .....</b>	<b>64</b>
6.1	Erzeugung und Installation von Schlüsselpaaren .....	64
6.1.1	Generierung von Schlüsselpaaren .....	64
6.1.2	Zustellung privater Schlüssel an Endteilnehmer .....	66
6.1.3	Zustellung öffentlicher Schlüssel an Zertifikatsaussteller .....	66
6.1.4	Zustellung öffentlicher CA-Schlüssel an Vertrauende Dritte .....	66
6.1.5	Schlüssellängen .....	66
6.1.6	Generierung der Parameter von öffentlichen Schlüsseln und Qualitätskontrolle.....	66
6.1.7	Schlüsselverwendungen.....	67



6.2	Schutz der privaten Schlüssel und der kryptografischen Module .....	67
6.2.1	Standards und Kontrollen für kryptografische Module .....	67
6.2.2	Mehrpersonenkontrolle (m von n) bei privaten Schlüsseln.....	67
6.2.3	Hinterlegung von privaten Schlüsseln.....	67
6.2.4	Sicherung von privaten Schlüsseln.....	67
6.2.5	Archivierung von privaten Schlüsseln .....	68
6.2.6	Übertragung privater Schlüssel in oder von einem kryptografischen Modul ....	68
6.2.7	Speicherung privater Schlüssel auf kryptografischen Modulen .....	68
6.2.8	Methode zur Aktivierung privater Schlüssel .....	68
6.2.9	Methode zur Deaktivierung privater Schlüssel .....	69
6.2.10	Methode zur Vernichtung privater Schlüssel.....	69
6.2.11	Bewertung kryptografischer Module .....	69
6.3	Weitere Aspekte der Schlüsselverwaltung.....	69
6.3.1	Archivierung öffentlicher Schlüssel .....	69
6.3.2	Gültigkeitsdauer von Zertifikaten und Schlüsselpaaren .....	69
6.4	Aktivierungsdaten.....	70
6.4.1	Generierung und Installation von Aktivierungsdaten .....	70
6.4.2	Schutz von Aktivierungsdaten .....	70
6.4.3	Weitere Aspekte von Aktivierungsdaten .....	70
6.5	Sicherheitsbestimmungen für Computer.....	71
6.5.1	Spezifische technische Anforderungen an die Computersicherheit .....	71
6.5.2	Bewertung der Computersicherheit .....	72
6.6	Technische Kontrollen des Lebenszyklus.....	72
6.6.1	Systementwicklungskontrollen.....	72
6.6.2	Sicherheitsverwaltungskontrollen .....	72
6.6.3	Sicherheitskontrollen des Lebenszyklus .....	73
6.7	Maßnahmen zur Netzwerksicherheit .....	73
6.8	Zeitstempel.....	74
<b>7</b>	<b>Zertifikats-, Sperrlisten- und OCSP-Profil.....</b>	<b>75</b>
7.1	Zertifikatsprofile .....	75
7.1.1	Versionsnummer .....	75
7.1.2	Zertifikatserweiterungen .....	75
7.1.3	OIDs der Algorithmen .....	76
7.1.4	Namensformen.....	76
7.1.5	Namensbeschränkungen.....	76
7.1.6	OIDs der Zertifizierungsrichtlinien.....	77
7.1.7	Nutzung der Erweiterung der Policy-Beschränkungen.....	77

7.1.8	Syntax und Semantik der Policy-Qualifier.....	77
7.1.9	Verarbeitungssemantik für die Erweiterung der Zertifizierungsrichtlinien .....	77
7.2	Sperrlistenprofile .....	77
7.2.1	Versionsnummer .....	77
7.2.2	Sperrlisten und Sperrlisteneintragserweiterungen. ....	77
7.3	OCSP-Profile.....	78
7.3.1	Versionsnummer .....	78
7.3.2	OCSP-Erweiterungen.....	78
<b>8</b>	<b>Compliance-Audits und andere Prüfungen .....</b>	<b>79</b>
8.1	Intervall und Grund von Prüfungen.....	79
8.2	Identität/Qualifikation des Prüfers.....	79
8.3	Beziehung des Prüfers zur prüfenden Stelle.....	79
8.4	Abgedeckte Bereiche der Prüfung.....	79
8.5	Maßnahmen zur Beseitigung von Mängeln oder Defiziten.....	80
8.6	Mitteilung der Ergebnisse .....	80
<b>9</b>	<b>Weitere rechtliche Regelungen .....</b>	<b>81</b>
9.1	Gebühren .....	81
9.1.1	Entgelte für die Ausstellung oder Erneuerung von Zertifikaten .....	81
9.1.2	Entgelte für den Zugriff auf Zertifikate.....	81
9.1.3	Entgelte für den Zugriff auf Sperr- oder Statusinformationen.....	81
9.1.4	Entgelte für andere Leistungen.....	81
9.1.5	Erstattung von Entgelten .....	81
9.2	Finanzielle Verantwortung, Versicherungsschutz .....	81
9.2.1	Versicherungsschutz .....	81
9.2.2	Sonstige finanzielle Mittel .....	82
9.2.3	Versicherungs- oder Gewährleistungsschutz für Endteilnehmer.....	82
9.3	Vertraulichkeit betrieblicher Informationen.....	82
9.3.1	Umfang von vertraulichen Informationen .....	82
9.3.2	Umfang von nicht vertraulichen Informationen.....	82
9.3.3	Verantwortung zum Schutz vertraulicher Informationen.....	82
9.4	Datenschutz .....	82
9.4.1	Datenschutzkonzept.....	82
9.4.2	Vertraulich zu behandelnde Daten .....	83
9.4.3	Nicht vertraulich zu behandelnde Daten .....	83
9.4.4	Verantwortung für den Schutz vertraulicher Daten .....	83
9.4.5	Mitteilung und Zustimmung zur Nutzung vertraulicher Daten.....	83
9.4.6	Offenlegung gemäß gerichtlicher oder verwaltungsmäßiger Prozesse .....	83

9.4.7	Andere Umstände zur Offenlegung von Daten .....	83
9.5	Rechte des geistigen Eigentums (Urheberrecht) .....	83
9.6	Zusicherungen und Gewährleistungen .....	84
9.6.1	Zusicherungen und Gewährleistungen der Zertifizierungsstelle .....	84
9.6.2	Zusicherungen und Gewährleistungen der Registrierungsstelle (RA).....	84
9.6.3	Zusicherungen und Gewährleistungen des Endteilnehmers .....	84
9.6.4	Zusicherungen und Gewährleistungen von Vertrauenden Dritten.....	86
9.6.5	Zusicherungen und Gewährleistungen anderer Teilnehmer .....	86
9.7	Haftungsausschluss .....	86
9.8	Haftungsbeschränkungen.....	86
9.9	Schadensersatz .....	86
9.10	Laufzeit und Beendigung.....	86
9.10.1	Laufzeit .....	86
9.10.2	Beendigung .....	86
9.10.3	Wirkung der Beendigung und Fortbestand .....	87
9.11	Individuelle Mitteilungen und Kommunikation mit Teilnehmern.....	87
9.12	Änderungen.....	87
9.12.1	Verfahren für Änderungen .....	87
9.12.2	Benachrichtigungsverfahren und -zeitraum .....	87
9.12.3	Umstände, die zu einer Änderung der OID führen .....	87
9.13	Bestimmungen zur Beilegung von Streitigkeiten.....	87
9.14	Geltendes Recht .....	88
9.15	Einhaltung geltenden Rechts.....	88
9.16	Verschiedene Bestimmungen.....	88
9.16.1	Vollständiger Vertrag.....	88
9.16.2	Abtretung .....	88
9.16.3	Salvatorische Klausel .....	88
9.16.4	Vollstreckung (Rechtsanwaltsgebühren und Rechtsverzicht) .....	89
9.16.5	Höhere Gewalt .....	89
9.17	Sonstige Bestimmungen.....	89
<b>A</b>	<b>Referenzen.....</b>	<b>90</b>

## Abbildungsverzeichnis

Abbildung 1: Integration der TSP in übergeordnete PKIn .....	14
Abbildung 2: Kartenherausgeber .....	17
Abbildung 3: Verzeichnisse zum Abruf der Zertifikate und Statusinformationen.....	25
Abbildung 4: Übersicht: Beantragungs- und Ausgabeprozess HBA oder SMC-B.....	34
Abbildung 5: Übersicht: Beantragungs- und Ausgabeprozess SM-B-Zertifikate.....	34

## Tabellenverzeichnis

Tabelle 1: Impressum .....	2
Tabelle 2: Änderungshistorie .....	3
Tabelle 3: Glossar .....	23
Tabelle 4: Abkürzungen.....	24
Tabelle 5: Referenzen und mitgeltende Unterlagen .....	91

# 1 Einleitung

Die Deutsche Telekom Security GmbH (nachfolgend „Telekom Security“ genannt) betreibt im Rahmen der Produktion des „Heilberufsausweises“ (HBA), der „Security Modul Cards des Typ B“ (SMC-B) sowie der virtuellen Karten („SM-B“) Zertifizierungsdienste zur Herausgabe von Zertifikaten für den HBA und die SM(C)-B.

Hinweis zur Nomenklatur: Die Bezeichnung „Karte“ gilt übergreifend für beide Kartentypen und wird nachfolgend verwendet, wenn Aussagen sowohl für HBA als auch für SMC-B gelten.

Dieses Dokument beschreibt die Sicherheitsleitlinien des Zertifizierungsdienstes. Es gibt darüber hinaus aber auch weitergehende Informationen über das Zertifikatsmanagement und vereint damit die „Certificate Policy“ (CP) und das „Certification Practice Statement“ (CPS) in einem Dokument.

Das Dokument ist gemäß Kapitel 4 des RFC 3647, dem internationalen Standard für CP und CPS, strukturiert.

Hinweise zur Kennzeichnung von Aussagen:

Da in diesem Dokument sowohl HBA als auch SM(C)-B betrachtet werden, welche sich aber in einigen technischen Merkmalen und organisatorischen Prozessabläufen unterscheiden, gelten folgende Vereinbarungen:

- Aussagen, die nur für HBA gelten werden mit einem vorangestellten [HBA] gekennzeichnet,
- Aussagen, die nur für SMC-B gelten werden mit einem vorangestellten [SMC-B] gekennzeichnet,
- Aussagen, die nur für SM-B gelten, werden mit einem vorangestellten [SM-B] gekennzeichnet,
- Aussagen, die sowohl für SMC-B als auch SM-B gelten, werden mit einem vorangestellten [SM(C)-B] gekennzeichnet
- Wenn die o.g. Kennzeichnungen über einem Textblock stehen, so gelten diese für den gesamten nachfolgenden Text,
- Wenn die o.g. Kennzeichnungen zu Beginn eines Absatzes oder Satzes stehen, so gelten diese nur für diesen Absatz oder Satz,
- Aussagen, welche keine vorangestellte Kennzeichnung haben gelten für beide Kartentypen.

## 1.1 Überblick

Die Zertifizierungsdienste zur Herausgabe von HBA und SM(C)-B bestehen aus mehreren „Trust Service Providern“ (TSP) zur Herausgabe von qualifizierten und nicht-qualifizierten Zertifikaten:

- [HBA] TSP X.509 QES HBA: Zertifizierungsinstanz zur Ausgabe qualifizierter X509-Zertifikate,
- TSP X.509 nonQES HBA und TSP X.509 nonQES SM(C)-B: Zertifizierungsinstanzen zur Ausgabe nicht-qualifizierter X509-Zertifikate.
- TSP CVC: Zertifizierungsinstanz zur Ausgabe von Card Verifiable Certificates (CVC). Der TSP CVC stellt Zertifikate für die Kartengeneration G2.1 aus

[HBA] Für jeden HBA werden folgende Zertifikate ausgestellt:

- Je zwei nicht qualifizierte X509-Zertifikate für Verschlüsselung und Authentisierung (ENC, AUT), ausgestellt durch den TSP X.509 nonQES HBA, jeweils einmal mit RSA und ECC-Schlüsselpaar (G2.1 Standard).
- Zwei qualifizierte X509-Zertifikate für die Erstellung qualifizierter Elektronischer Signaturen (QES), ausgestellt durch den TSP X.509 QES HBA, jeweils einmal mit RSA und ECC-Schlüsselpaar (G2.1 Standard).
- zwei CV-Zertifikate der Generation 2, ausgestellt durch den TSP CVC.

[SM(C)-B] Für jede SM(C)-B werden folgende Zertifikate ausgestellt:

- Drei nicht qualifizierte X509-Zertifikate für Signatur, Verschlüsselung und Authentisierung (OSIG, ENC, AUT), ausgestellt durch den TSP X.509 nonQES SMC-B, jeweils einmal mit RSA und ECC-Schlüsselpaar (G2.1 Standard).
- zwei CV-Zertifikate der Generation 2, ausgestellt durch den TSP CVC.

Die folgende Grafik zeigt die von den TSP ausgestellten Zertifikate sowie deren Integration in die übergeordnete PKIn:

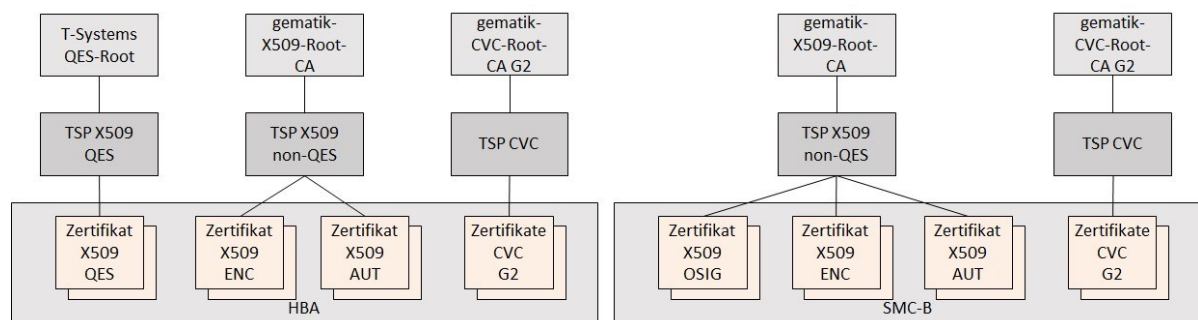


Abbildung 1: Integration der TSP in übergeordnete PKIn

Aufgrund der Integration in die übergeordneten PKI sind für die TSP folgende übergeordnete Policies bindend:

- gematik: Certificate Policy, gemeinsame Zertifizierungsrichtlinie für Teilnehmer der gematik-TSL [gemRL\_TSL\_SP\_CP].
- [HBA] Bundesapothekerkammer, Bundesärztekammer, Bundespsychotherapeutenkammer, Bundeszahnärztekammer und Kassenzahnärztliche Bundesvereinigung: Gemeinsame Policy für die Ausgabe der HPC – Zertifikatsrichtlinie HPC [CP-HPC].

[HBA]

Für die Ausgabe der qualifizierten Zertifikate gelten darüber hinaus die Anforderungen der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates („eIDAS“, electronic IDentification, Authentication and trust Services)

Zur Gewährleistung der eIDAS-Konformität des TSP X.509 QES HBA erfüllt der Zertifizierungsdienst die Anforderungen aus

- [ETSI EN 319 401]: General Policy Requirements for TSPs
- [ETSI EN 319 411-1]: General Policy and security requirements for TSPs
- [ETSI EN 319 411-2]: Requirements for TSPs issuing EU qualified certificates
- [ETSI EN 319 412-2]: Certificate profile for certificates issued to natural persons
- [ETSI EN 319 412-5]: Certificate Profiles: QCStatements

Die Erfüllung der o.g. Anforderungen zur Erlangung und zur Aufrechterhaltung des Status eines „Qualifizierten Vertrauensdiensteanbieters“ gemäß Art. 3 Nr. 20 eIDAS lässt der TSP mindestens jährlich eine Konformitätsbewertung durch eine akkreditierte Zertifizierungsstelle für Produkte, Prozesse und Dienstleistungen im Bereich „qualifizierte Vertrauensdiensteanbieter und die von ihnen erbrachten qualifizierten Vertrauensdienste im Anwendungsbereich der eIDAS“ vornehmen.

Telekom Security ist dafür verantwortlich, dass die beschriebenen Abläufe, Tätigkeiten, Systeme, Rollen und Sicherheitsmaßnahmen auch für den Fall durchgesetzt werden, dass diese ausgelagert wurden. Zur Erbringung des Vertrauensdienstes greift der TSP auf Dienstleistungen Dritter zurück, z.B. zur Identifizierung von Antragstellern sowie zur Bestätigung berufsbezogener Attribute (siehe Kap. 3.2.3). Die Nutzung der Dienstleistungen sind im Sicherheitskonzept berücksichtigt und die Pflichten der Dienstleister in Verträgen definiert. Unbeschadet dessen verbleibt die Gesamtverantwortung bei dem TSP.

## 1.2 Dokumentenidentifikation

Dieses Dokument trägt den Policy-Identifizier „1.3.6.1.4.1.7879.13.35“.

Diese CPS und das PDS stehen im Internet zum Download zur Verfügung unter:

[www.telesec.de](http://www.telesec.de) ("Root Programm" > "Support" > "PKI Repository")

Die AGB (Allgemeine Geschäftsbedingungen) sind zu finden unter:

[www.telesec.de](http://www.telesec.de) ("Service" > "Downloads" > "Allgemeine Geschäftsbedingungen")

Weitere spezifische Informationen zu SMC-B und HBA sind an folgender Stelle zu finden:

[www.telesec.de](http://www.telesec.de) ("Branchen & Eco-Systeme" > "Gesundheitswesen" > "Details Heilberufsausweis (HBA)")

bzw.

[www.telesec.de](http://www.telesec.de) ("Branchen & Eco-Systeme" > "Gesundheitswesen" > "Details Praxisausweis (SMC-B)")

Die genannten Downloadpunkte auf [www.telesec.de](http://www.telesec.de) stehen rund um die Uhr an 7 Tagen der Woche zur Verfügung. Die maximale Downtime beträgt drei Stunden.

## 1.3 PKI-Beteiligte

### 1.3.1 Zertifizierungsstelle

Die Zertifizierungsstelle (CA Certification Authority) ist der Teil einer Public Key Infrastruktur, der Zertifikate ausstellt, verteilt und Prüfmöglichkeiten zur Verfügung stellt.

Die bei der Ausgabe der Zertifikate involvierten CAs gliedern sich in zwei Ebenen:

- Root-CAs: Die Zertifikate werden von folgenden Root-CAs abgeleitet:
  - gematik X509-Root-CA: Diese Root-CA wird im Auftrag der gematik von der Firma arvato betrieben und stellt für die TSP X509 nonQES der Telekom Security folgende Zertifikate aus:

- CA-Zertifikate für die nonQES-Zertifikate:  
„TSYSI.HBA-CA<sup>1</sup>“ bzw. „TSYSI.SMCB-CA“,
- gematik-Root-CA CVC G2.1: Diese Root-CA wird im Auftrag der gematik von der Firma Atos betrieben und stellt für den TSP CVC der Telekom Security folgende Zertifikate aus:
  - CA-Zertifikate für CV-Zertifikate der Generation 2.1.
- [HBA] Telekom-Security-QES-Root-CA: Diese Root-CA wird von Telekom Security betrieben und stellt folgende Zertifikate für den TSP X509 QES der Telekom Security aus:
  - CA-Zertifikate für die QES-Zertifikate: „TSYSI.HBA-qCA“,
- Sub-CAs: Alle CAs der zweiten Ebene werden durch Telekom Security selbst betrieben:
  - CAs für die X509 QES- und nonQES-Zertifikate,
  - CAs für CV-Zertifikate der Generation 2.1.

Alle aufgeführten CAs der zweiten Ebene stellen ausschließlich Zertifikate für die (virtuellen) Karten sowie für die OCSP-Signer aus, es werden keine weiteren Sub-CA-Zertifikate von Ihnen ausgestellt.

### 1.3.2 Registrierungsstellen

Eine Registrierungsstelle (RA) ist eine Stelle, welche die Identifizierung und Authentifizierung von Antragstellern durchführt und Zertifikatsanträge und Sperranträge bearbeitet.

Grundsätzlich muss eine Registrierungsstelle gewährleisten, dass keine unberechtigte Person in den Besitz eines Zertifikats gelangt.

Die Trust-Center-Registrierungsstelle der Telekom Security hat insbesondere folgende Aufgaben:

- [HBA] Entgegennahme von Aufträgen und Prüfung der Identifikationsunterlagen,
- [HBA] Prüfen der Dokumente auf Echtheit und Vollständigkeit,
- [HBA] Identitätsprüfung
- Genehmigung der Zertifikatsausstellung,
- Sperren von Zertifikaten, wenn Sperrgründe vorliegen.

[HBA] Zur Registrierung von HBA-Anträgen sind keine Registrierungsstellen Dritter (externe RA) zugelassen, jedoch wird die Identifizierung der Antragsteller ausgelagert, siehe Kap. 1.3.5.1.

[SM(C)-B] Die Registrierung der SMC-B-Antragsteller und Institutionen erfolgt durch die zuständigen Kartenherausgeber unabhängig von der Beantragung einer SM(C)-B im Vorfeld.

### 1.3.3 Antragsteller

[HBA] Antragsteller sind Ärzte, Zahnärzte, Apotheker und Psychotherapeuten, welche einer zuständigen Kammer angehören.

---

<sup>1</sup> nn: Zähler im Namen der Zertifikate



[SM(C)-B] Antragsteller sind Inhaber oder Mitarbeiter von Institutionen im Gesundheitswesen (Arzt-, Zahnarzt- oder Psychotherapeuten-Praxis, Krankenhäuser, Apotheken, Krankenkassen).

[HBA] [SMC-B] Mit Ausgabe der Karten nach der Antragsbearbeitung sind die Antragsteller die Inhaber der Karten.

[SM-B] Mit Ausgabe der Zertifikate nach der Antragsbearbeitung sind die Antragsteller die Inhaber der Zertifikate.

Hinweis: Zur besseren Lesbarkeit dieses Dokumentes wird nachfolgend im Dokument der Begriff „Antragsteller“ verwendet, womit bei entsprechendem Antrags- bzw. Kartenstatus auch der „Inhaber einer Karte“ gemeint ist.

### 1.3.4 Vertrauende Dritte

Vertrauende Dritte sind natürliche Personen oder Subjekte, die sich auf die Vertrauenswürdigkeit der ausgestellten Zertifikate verlassen, z.B. andere Teilnehmer der Telematik-Infrastruktur. Zur Nutzung und Verifikation der Zertifikate durch Dritte z.B. zur Verschlüsselung, Authentisierung oder Signaturprüfung stehen die Zertifikate und Sperrinformationen zum Abruf in den Verzeichnissen bereit.

### 1.3.5 Weitere Beteiligte

#### 1.3.5.1 Identitätsprüfer

[HBA]

Im Fall des Verfahrens PostIdent Filiale sind die Identitätsprüfer Mitarbeiter der Deutschen Post, im Fall von VDA-Ident sind die Identitätsprüfer Mitarbeiter des Telekom-Konzerns sowie ggfs. externe Registrierungs-/Identifizierungsstellen.

Im Fall des Verfahrens PostIdent eID wird die Identität mittels Online-Ausweisfunktion eines entsprechenden Ausweisdokumentes nachgewiesen.

#### 1.3.5.2 Kartenherausgeber

Die folgende Abbildung stellt die Leistungserbringerorganisationen (LEO) und Kostenträger im Gesundheitswesen dar, d.h. die Sektoren, deren Spitzenorganisationen und die zugeordneten Kartenherausgeber.

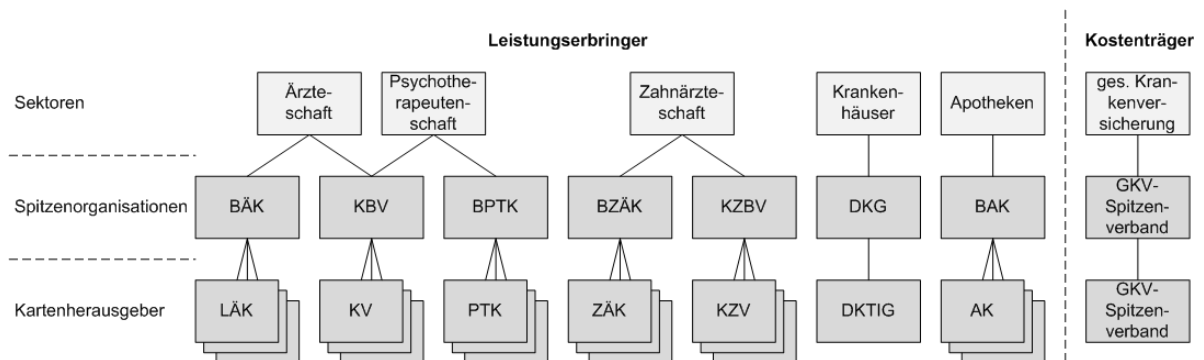


Abbildung 2: Kartenherausgeber

Ein Sektor repräsentiert eine Berufsgruppe wie z.B. Ärzte, Psychotherapeuten oder Zahnärzte. Zu einem Sektor gehören mehrere Kartenherausgeber, die HBAs herausgeben

Die Kartenherausgeber sind verantwortlich für die Ausgabe der Karten in ihrem Zuständigkeitsbereich.

[HBA] Die nachfolgend aufgeführten Kartenherausgeber bestätigen die Attribute zur beruflichen Zulassung ihrer Kammermitglieder und erteilen die Freigabe zur Produktion der HBAs:

- Landes- oder Bezirksärztekammern,
- Apothekerkammern,
- Psychotherapeutenkammern und
- Zahnärztekammern.

[SM(C)-B] Die nachfolgend aufgeführten Kartenherausgeber bestätigen die Art der Institution ihrer Mitglieder und erteilen die Freigabe zur Produktion der SMC-Bs:

- Kassenärztliche Vereinigungen (KVn),
- Kassenzahnärztliche Vereinigungen (KZVn),
- Kassenzahnärztliche Bundesvereinigung (KZBV),
- Deutsche Krankenhaus und Trust Center Informationsgesellschaft (DKTIG),
- Spitzenverband der gesetzlichen Krankenversicherungen (GKVS)
- Apothekerkammern.

## 1.4 Anwendung von Zertifikaten

### 1.4.1 Zulässige Verwendung von Zertifikaten

Die Zertifikate sind im Rahmen der von den Kartenherausgebern vorgesehenen Nutzung innerhalb der Telematik-Infrastruktur zu verwenden.

Sie können darüber hinaus auch zu anderen Zwecken außerhalb der Telematik-Infrastruktur verwendet werden, z.B. das QES-Zertifikat für die rechtsverbindliche Signatur von Dokumenten, sofern im jeweiligen QES-Zertifikat keine Einschränkung definiert ist.

### 1.4.2 Unzulässige Verwendung von Zertifikaten

Die Zertifikate dürfen nur für den zugelassenen Verwendungszweck und nicht als Zertifizierungsstelle (Sub-CA) oder Stammzertifizierungsstelle (Root-CA) eingesetzt werden.

### 1.4.3 Testzertifikate

Neben der Produktivumgebung betreibt der TSP auch eine Testumgebung zur Ausstellung von Testzertifikaten für eigene Testzwecke oder auch Testzwecke Dritter.

Die Zertifikatsmanagement-Prozesse der Testumgebung laufen prinzipiell analog zur Produktivumgebung ab, um vergleichbare Bedingungen sicherzustellen.

Die Testumgebung ist strikt getrennt von der Produktivumgebung aufgebaut. Es kommen in der Testumgebung ausschließlich als Testzertifikate gekennzeichnete CA-, OCSP-, und CRL-Signer-Zertifikate zu Einsatz.

Alle ausgegebenen X509-End-Entity-Zertifikate sind durch die Ergänzungen „TEST-ONLY“ im commonName und „NOT-VALID“ im organizationName (sofern dieser gesetzt ist) eindeutig als Testzertifikate gekennzeichnet.

## 1.5 Verwaltung des Dokuments

### 1.5.1 Zuständigkeit für das Dokument

Das Dokument wurde von der Deutsche Telekom Security GmbH erstellt, welche auch für dessen Fortschreibung verantwortlich ist.

### 1.5.2 Kontaktinformationen

Deutsche Telekom Security GmbH, Trust Center & ID Security,  
Koblenzer Str. 87-93  
57072 Siegen  
Deutschland  
Telefon: 0271/708-1699  
E-Mail: [Trust\\_Center\\_gematik@telekom.de](mailto:Trust_Center_gematik@telekom.de)  
Internet: <https://www.telesec.de>

### 1.5.3 Stelle, die über die Vereinbarkeit dieser Richtlinien mit der CP entscheidet

Telekom Security als zuständige Stelle für dieses Dokument (siehe Kap. 1.5.1) ist verantwortlich dafür, dass Dokumente, die dieses Dokument ergänzen oder untergeordnet sind, mit der Zertifizierungsrichtlinie (Certificate Policy, CP) vereinbar sind.

### 1.5.4 Genehmigungsverfahren dieses Dokuments

Dieses Dokument wird durch den im Betriebsleitfaden des Trust Centers definierten Qualitätssicherungs- und Freigabeprozesses behandelt. Dieser sieht ein bei Anpassungen eine Qualitätssicherung mit anschließender Freigabe durch den Leiter des Trust Centers vor.

Eine neue Version des Dokuments wird erst nach erfolgter Freigabe veröffentlicht.

Die vorliegende CP/CPS wird unabhängig von weiteren Änderungen einem jährlichen Review unterzogen. Das jährliche Review ist in der Änderungshistorie des CP/CPS zu vermerken. Dies gilt auch für den Fall, dass keine inhaltlichen Änderungen vorgenommen werden.

## 1.6 Definitionen und Abkürzungen

### 1.6.1 Definitionen

<b>Begriff</b>	<b>Definition</b>
Authority Revocation List (ARL)	Liste, in der gesperrte digitale Zertifikate von Zertifizierungsstellen (CA- und Root-CA) aufgeführt sind. Vor der Verwendung eines digitalen Zertifikats einer Zertifizierungsstelle sollte anhand der ARL überprüft werden, ob dieses noch verwendet werden darf.
Certificate Policy (CP)	Legt die Richtlinien für die Generierung und Verwaltung von Zertifikaten eines bestimmten Typs fest.
Certificate Revocation List (CRL)	Siehe Sperrliste.
Certification Authority	Siehe Zertifizierungsstelle.
Certification Practice Statement (CPS)	Erklärungen für den Betrieb einer Zertifizierungsstelle. Insbesondere setzt das CPS die Vorgaben und Richtlinien der CP einer Zertifizierungsstelle um.
Digitale Signatur	Mit einem speziellen mathematischen Verfahren erstellte Prüfsumme. Sichert die Authentizität des Signierenden und die Integrität der Daten.
Digitales Zertifikat	Datensatz, der den Namen einer Person oder eines Systems, deren öffentlichen Schlüssel, gegebenenfalls einige andere Angaben und eine Signatur einer Zertifizierungsstelle enthält.
Distinguished Name	Format, mit dem gemäß dem X.500-Standard eindeutige Namen angegeben werden können. In einem digitalen Zertifikat muss ein DN enthalten sein.
Elektronische Signatur	Siehe digitale Signatur.
Endteilnehmer	Siehe auch Zertifikatsnehmer. Der Begriff Endteilnehmer wird überwiegend im Umfeld X.509 verwendet.
Hardware Security Modul (HSM)	Hardwarebox zur sicheren Erzeugung und Speicherung privater Schlüssel.
Hashwert	In diesem Zusammenhang eine kryptografische Prüfsumme fester Länge (die korrekte Bezeichnung wäre kryptografischer Hashwert). Es soll möglichst unwahrscheinlich sein, aus dem Hashwert die Eingabe berechnen oder mehrere mögliche Eingaben zu dem gleichen Hashwert finden zu können (Hashwert wird synonym zu Fingerprint verwendet). Statt einem gesamten digitalen Dokument wird meist nur ein Hashwert signiert.
Kompromittierung	Ein privater Schlüssel ist kompromittiert, wenn er Unbefugten bekannt geworden ist oder von diesen genutzt werden kann. Eine Kompromittierung kann etwa die Folge eines kriminellen Angriffs sein.
Kryptografie	Wissenschaft, die sich mit der Verschlüsselung von Daten und verwandten Themen beschäftigt (etwa digitale Signatur).
Latenzzeit	Zeitraum zwischen einer Aktion und dem Eintreten einer verzögerten Reaktion (Verzögerungszeitraum). Bei der Latenzzeit

erfolgt die Aktion im Verborgenen und wird erst durch die Reaktion festgestellt.

Lightweight Directory Access Protocol (LDAP)	Protokoll zur Abfrage von Verzeichnissen, welches das deutlich kompliziertere Directory Access Protocol (DAP) in vielen Bereichen verdrängt hat. LDAP bietet mehr Möglichkeiten als HTTP und FTP (etwa das Einrichten eines Kontexts, der über mehrere Anfragen aufrechterhalten werden kann). LDAP wird insbesondere zur Abfrage von digitalen Zertifikaten und Sperrlisten innerhalb von Public-Key-Infrastrukturen verwendet.
Online Certificate Status Protocol (OCSP)	Das Online Certificate Status Protocol ermöglicht die Online-Abfrage der Gültigkeit von Zertifikaten.
Public Key Infrastructure X.509 (PKIX)	Standard der IETF, der alle relevanten Bestandteile einer PKI standardisiert.
Public Key Service (PKS)	Service des Trust Centers zur Ausstellung und Verwaltung signaturgesetzkonformer Zertifikate.
Policy	Richtlinien, die das Sicherheitsniveau für die Erzeugung und Verwendung von Zertifikaten festlegen. Es wird zwischen Certificate Policy (CP) und Certification Practice Statement (CPS) unterschieden.
Public Key Infrastruktur	Gesamtheit der Komponenten, Prozesse und Konzepte, die zur Verwendung von Public-Key-Verfahren verwendet werden. Typischerweise besteht eine Public-Key-Infrastruktur aus zentralen Komponenten wie einer Zertifizierungsstelle und einem Verzeichnisdienst und verschiedenen Client-Komponenten.
Registration Authority (RA)	Siehe Registrierungsstelle.
Registrierungsstelle	Komponente, mit der eine Person oder ein System kommunizieren muss, um ein digitales Zertifikat zu erhalten.
Request	Engl. Begriff für Auftrag. In diesem Zusammenhang ist der Zertifikatsauftrag zu verstehen.
Rivest Shamir Adleman (RSA)	Verfahren zur Verschlüsselung, zur digitalen Signatur und zur sicheren Übertragung von Schlüsseln, das nach den drei Kryptografen Rivest, Shamir und Adleman benannt ist.
Root-CA	Siehe Wurzelzertifizierungsstelle.
Schlüssel	Ein Schlüssel bezeichnet in der Kryptografie eine geheime Information (privater Schlüssel) oder ein öffentliches Gegenstück dazu (öffentlicher Schlüssel). Es gibt Verfahren, bei denen jeweils mit dem gleichen privaten Schlüssel ver- und entschlüsselt wird sowie Verfahren bei denen ein öffentlicher Schlüssel zum Verschlüsseln und ein privater zum Entschlüsseln verwendet wird.
Secure Socket Layer (SSL)	Krypto-Protokoll zur Absicherung von Ende-zu-Ende-Verbindungen im Internet, mittlerweile durch das neuere Verfahren TLS abgelöst.
Signatur	Siehe digitale Signatur.

Smartcard	Chipkarte mit Rechenfunktionalität, die für kryptografische Zwecke verwendet werden kann.
Simple Object Access Protocol (SOAP)	Simple Object Access Protocol: SOAP stellt einen einfachen Mechanismus zum Austausch von strukturierter Information zwischen Anwendungen in einer dezentralisierten, verteilten Umgebung zur Verfügung.
Sperrinstanz	Komponente, die Zertifikatssperrungen durchführt.
Sperrliste	Liste, in der gesperrte digitale Zertifikate aufgeführt sind. Vor der Verwendung eines digitalen Zertifikats sollte anhand einer Sperrliste überprüft werden, ob dieses noch verwendet werden darf. Wird auch als Certificate Revocation List (CRL) bezeichnet.
Subject- Distinguished Name (Subject-DN)	Subject = engl. Subject (Person oder Maschine). Format, mit dem gemäß dem X.500- und dem LDAP-Standard eindeutige Namen angegeben werden können. Der Subject-DN bezeichnet eindeutig den Zertifikatsinhaber.
Suspendierung	Im Zusammenhang von PKI ist unter Suspendierung die vorläufige bzw. temporäre Sperrung zu verstehen. Das Zertifikat erscheint zunächst in der Zertifikatssperrliste kann aber durch den Sub-Registrator wieder aktiv geschaltet werden.
Transport-Layer Security (TLS)	Krypto-Protokoll zur Absicherung von Ende-zu-Ende-Verbindungen im Internet.
Validierung	Im Zusammenhang von PKI ist unter Validierung die Gültigkeitsprüfung von Zertifikaten zu verstehen. Im Allgemeinen wird der Gültigkeitszeitraum auf Basis der PC-Systemzeit, der Sperrstatus (auf Basis Sperrliste oder OCSP und die Zertifikats-Hierarchie (ausstellende CA) geprüft.
Vertrauende Dritte (Relying Parties)	Eine natürliche oder juristische Person (z.B. Firma, Organisation) die im Vertrauen auf die Funktion eines Zertifikats handelt.
Verzeichnisdienst	Datenspeicher, der den Abruf von Zertifikaten und Informationen über Zertifikate (insbesondere Sperrlisten) ermöglicht.
Wurzelzertifizierungsstelle	Oberste Zertifizierungsstelle einer CA-Hierarchie, deren Zertifikat somit nicht von einer anderen Zertifizierungsstelle ausgestellt wurde, sondern selbstsigniert ist. Dieses Zertifikat stellt den „vertrauenswürdigen Anker“ innerhalb der Anwendung dar.
X.509	Standard, dessen wichtigster Bestandteil ein Format für digitale Zertifikate ist. Zertifikate der Version X.509v3 werden in allen gängigen Public-Key-Infrastrukturen unterstützt.
Zertifikat	Siehe digitales Zertifikat.
Zertifizierungsstelle	Komponente, die digitale Zertifikate ausstellt, indem sie einen Datensatz bestehend aus öffentlichem Schlüssel, Name und verschiedenen anderen Daten digital signiert. Ebenso werden von der Zertifizierungsstelle Sperrinformationen herausgegeben.
Zertifikatsnehmer	Natürliche oder juristische Person, die ein Zertifikat und den dazu gehörenden privaten Schlüssel verwendet.

## 1.6.2 Abkürzungen

<b>Abkürzung</b>	<b>Erklärung</b>
ARL	Authority Revocation List
BAK	Bundesapothekerkammer
BÄK	Bundesärztekammer
BPtK	Bundespsychotherapeutenkammer
BZÄK	Bundeszahnärztekammer
CA	Certification Authority
CP	Certificate Policy
CPS	Certification Practice Statement
CN	Common Name
CRL	Certificate Revocation List
CVC	Card Verifiable Certificate
CV CA	Card Verifiable Certification Authority
DIN	Deutsches Institut für Normung eV
DKTIG	Deutsche Krankenhaus Trust Center Informationsgesellschaft
DN	Distinguished Name
eGBR	Elektronisches Gesundheitsberuferegister
eIDAS	electronic IDentification, Authentication and trust Services
GKVS	Spitzenverband der gesetzlichen Krankenversicherungen
HBA	Heilberufsausweis
HSM	Hardware Security Modul
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IETF	Internet Engineering Task Force
ICCSN	Integrated Circuit Card Serial Number (Kartenummer des HBA)
ISMS	Informationssicherheits-Managementsystem
ISO	International Organization for Standardization
KBV	Kassenärztliche Bundesvereinigung
KV	Kassenärztliche Vereinigung
KZBV	Kassenzahnärztliche Bundesvereinigung
KZV	Kassenzahnärztliche Vereinigung
LDAP	Lightweight Directory Access Protocol
LEO	Leistungserbringerorganisation
MoD	Manager on Duty

OCS	Online Certificate Status Protocol
OID	Object Identifier
PDS	Policy Disclosure Statement
PIN	Personal Identification Number
PKI	Public Key Infrastruktur
PKIX	Public Key Infrastructure X.509
PN	Kennzeichner für Pseudonym
QES	Qualifizierte Elektronische Signatur
QCSD	Qualified Signature Creation Device
RA	Registration Authority
RFC	Requests for Comments
RSA	Rivest Shamir Adleman
SMC-B	Security Module Card, Typ B
SM-B	Security Module, Typ B ("virtuelle SMC-B")
SOAP	Simple Object Access Protocol
SSL	Secure Socket Layer
TCOP	Trust Center Operator
TI	Telematik-Infrastruktur
TLS	Transport Layer Security
TSP	Trust Service Provider
TSL	Trusted Service List
URL	Uniform Resource Locator
USV	Unterbrechungsfreie Stromversorgung
UTC	Universal Time Coordinated
VDS	Vertrauensdienstegesetz
VZD	Verzeichnisdienst

Tabelle 4: Abkürzungen



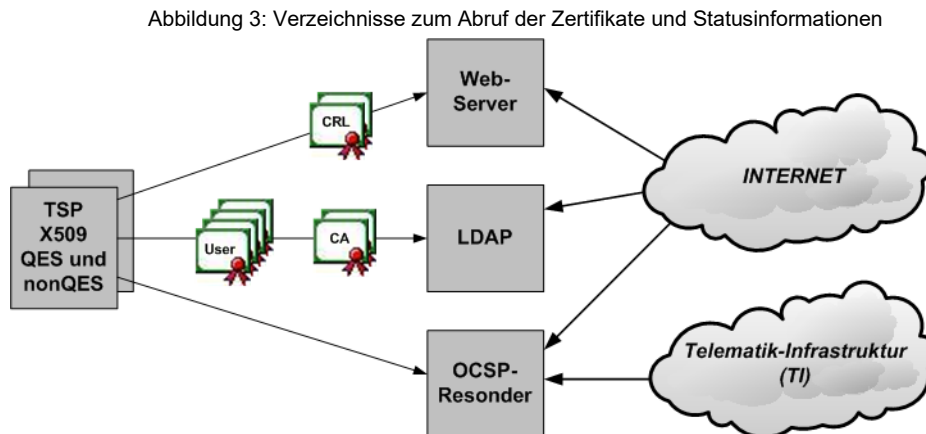
## 2 Veröffentlichung und Verzeichnisdienste

### 2.1 Verzeichnisdienste

Die Zertifikate werden im Verzeichnisdienst (VZD) der gematik veröffentlicht und darüber hinaus in einem LDAP-Verzeichnisdienst der Telekom Security.

### 2.2 Veröffentlichung von Zertifikatsinformationen

Telekom Security veröffentlicht die Zertifikate wie nachfolgend dargestellt in einem LDAP-Verzeichnis im Internet. Die Zertifikatsstatusinformationen werden wie folgt veröffentlicht:



Die Sperrlisten der nonQES-X509-Zertifikate sind im Internet wie folgt erreichbar:

[SM(C)-B] <http://crl.smcg.telesec.de/rl/<CN des CA-Zertifikats>.crl>

[HBA] <http://crl.hba.telesec.de/rl/<CN des CA-Zertifikats>.crl>

Die OCSP-Responder sind im Internet wie folgt erreichbar:

- [SM(C)-B] nonQES-OCSP-Responder: <http://ocsp.smcg.telesec.de/ocspr>
- [HBA] nonQES-OCSP-Responder: <http://ocsp.hba.telesec.de/ocspr>
- [HBA] QES-OCSP-Responder: <http://qocsp.hba.telesec.de/ocspr>

Die OCSP-Responder sind darüber hinaus in der TI erreichbar, die Zieladresse ist in der Trusted Service List (TSL) der gematik hinterlegt und muss bei der Prüfung dort abgefragt werden.

Hinweis: Testzertifikate aus der Testumgebung werden standardmäßig nicht veröffentlicht, können jedoch analog zu den Zertifikaten aus der Produktivumgebung über OCSP oder Sperrlisten geprüft werden. Für die Testumgebung gelten andere URLs für OCSP-Responder und Sperrlisten-Download, welche Dritten auf Anfrage bekannt gegeben werden.

## 2.3 Zeitpunkt oder Frequenz der Veröffentlichung

Telekom Security veröffentlicht die Zertifikate und Sperrlisten wie folgt:

- CA-Zertifikate werden mit Inbetriebnahme veröffentlicht,
- Sperrlisten werden regelmäßig, mindestens einmal täglich veröffentlicht,
- Die X509-Zertifikate werden erst nach Freischaltung durch den Antragsteller und nur bei Zustimmung zur Veröffentlichung durch den Antragsteller veröffentlicht.

## 2.4 Zugangsbeschränken zu den Verzeichnisdiensten

Der Abruf der Zertifikate und Sperrlisten erfolgt anonym über LDAPv3, der Zugriff auf die OCSP-Responder erfolgt per http. Alle Zugriffe unterliegen keiner Zugriffsbeschränkung.

Die Integrität und Authentizität der Sperrlisten und OCSP-Auskünfte wird durch die Signatur mit vertrauenswürdigen Signern aus der jeweils gleichen PKI gewährleistet.

## 3 Identifizierung und Authentifizierung

Die Identifizierung und Authentifizierung der Antragsteller sind die Grundlage zur Gewährleistung der Vertrauensstufe einer PKI.

[HBA] Für die Herausgabe des HBA ist festgelegt, dass alle Antragsteller persönlich identifiziert und deren kompletten Antragsdaten überprüft werden. Darüber hinaus müssen die Kartenherausgeber bestätigen, dass die Antragsteller berechtigt sind, HBAs mit entsprechenden berufsrechtlichen Attributen zu beantragen.

[SM(C)-B] Für die Herausgabe der SMC-B ist festgelegt, dass diese nur an registrierte Institutionen des Gesundheitswesens ausgegeben werden. Die Identifizierung der Vertreter der Institutionen und Antragsteller obliegt den Kartenherausgebern, welche auch gegenüber dem TSP die Art und Berechtigung der Institution bestätigen und die Produktionsfreigabe erteilen.

Die Identifizierung und Authentifizierung der berechtigten Mitarbeiter der Kartenherausgeber als Attribut bestätigende Stelle erfolgt durch die Leitung der jeweiligen Kartenherausgeber. Die berechtigten Mitarbeiter und deren Rollen werden dem TSP schriftlich mitgeteilt.

### 3.1 Namensgebung

Es sind die Namensregeln der X509-Zertifikate aus [gemSpec\_PKI] verbindlich.

[HBA] Für die HBA sind darüber hinaus die Vorgaben aus [ETSI EN 319 412-2] verbindlich.

#### 3.1.1 Namensformen

[HBA]

Für alle auszustellenden Zertifikate wird die Identität des Zertifikatnehmers geprüft. Die entsprechenden Informationen werden in das Zertifikat übernommen. Der Subject-DN der X509-Zertifikate der HBA beinhaltet mindestens folgende Attribute:

- Country: Land, beim HBA immer DE
- givenName: Vorname(n) des Inhabers
- surname: Nachname(n) des Inhabers
- serialNumber: Eindeutige Nummer (in allen X509-Zertifikaten einer Karte gleich, beinhaltet unter anderem die ICCSN der Karte)
- CommonName = Vor- und Nachname(n) des Inhabers (bei Überlänge ggf. gekürzt)

Die zuständige Kammer sowie das Attribut der berufsrechtlichen Zulassung werden in der Zertifikatserweiterung „Admission“ aufgeführt. Weitere Details zu den Zertifikatsinhalten siehe Kap. 7.1.

[SM(C)-B]

Für die auszustellenden Zertifikate werden die Namen der Zertifikats-Inhaber durch die Kartenherausgeber festgelegt, die Inhalte sind Sektor-spezifisch vorgegeben. In allen SM(C)-B werden die Art der Institution und ggf. (optional, Sektor-spezifisch) der bestätigende Kartenherausgeber in der Zertifikatserweiterung „Admission“ aufgeführt. Weitere Details zu den Zertifikatsinhalten siehe Kap. 7.1.

### 3.1.2 Aussagekraft von Namen

[HBA] Da HBA nur für natürliche Personen ausgestellt werden, muss der Name im Zertifikat (givenName, surname und commonName im Subject-DN) dem Namen des Zertifikatsinhabers entsprechen. Bei Namen mit einer Länge von mehr als 64 Zeichen kann der Name gekürzt werden.

[SM(C)-B] Da SMC-B nur für Institutionen des Gesundheitswesens ausgestellt werden, muss der Name im Zertifikat (commonName im Subject-DN) die Institution widerspiegeln. Bei Namen mit einer Länge von mehr als 64 Zeichen kann der Name im Subject-DN gekürzt werden, je nach Sektor kann der vollständige Name zusätzlich in die Erweiterung „subjectAltName“ aufgenommen werden

### 3.1.3 Anonymität bzw. Pseudonyme der Zertifikatsinhaber

Zertifikate mit Pseudonymen oder anonyme Zertifikate werden nicht ausgestellt.

### 3.1.4 Regeln zur Interpretation verschiedener Namensformen

Keine Regelungen.

### 3.1.5 Eindeutigkeit von Namen

Telekom Security stellt sicher, dass Zertifikate mit gleichem Namen durch die Vergabe einer Seriennummer im Subject-DN unterschieden werden. Ein Antragsteller kann mehrere Zertifikate mit demselben eindeutigen Subject DN besitzen. Diese unterscheiden sich durch die Zertifikatsseriennummer.

### 3.1.6 Erkennung, Authentifizierung und Rolle von Markennamen

Nicht anwendbar, da Zertifikate nur für natürliche Personen und Institutionen des Gesundheitswesens ausgestellt werden, welche im Subject-DN den Namen der Person oder der Institution enthalten.

## 3.2 Erstmalige Registrierung

### 3.2.1 Methoden zum Besitznachweis des privaten Schlüssels

[HBA] [SMC-B] Die Schlüssel der Karten werden durch einen Schlüsselgenerator in der Karte selbst erzeugt und können nicht exportiert werden, Mit Übergabe einer Karte an den Inhaber ist somit der alleinige Besitz des Schlüssels sichergestellt.

[SM-B] Die Schlüssel werden in HSM der Antragsteller generiert und mittels PKCS#10-Request übergeben. Durch die Signatur eines PKCS#10-Requests mittels des korrespondierenden privaten Schlüssels wird der Besitz des privaten Schlüssels nachgewiesen.

## 3.2.2 Identitätsprüfung einer Organisation

[SM(C)-B] Die Identitätsprüfung einer Institution obliegt dem zuständigen Kartenherausgeber.

[HBA] Nicht anwendbar, da Zertifikate nur für natürliche Personen ausgestellt werden.

## 3.2.3 Identitätsprüfung einer natürlichen Person

### 3.2.3.1 Registrierung der Antragsteller

[HBA]

Alle Antragsteller werden persönlich anhand eines amtlichen Ausweisdokumentes (Personalausweis, Reisepass zusammen mit Meldebescheinigung, Elektronischer Aufenthaltstitel (EAT) etc.) identifiziert, dabei gelten folgende Bedingungen:

- Der Antragsteller muss je nach Identifizierungsverfahren persönlich beim Identifizierer vorstellig werden.
- Als Identifizierungsvarianten kommen im Regelprozess nur PostIdent Filiale, PostIdent eID und VDA Ident zum Einsatz. PostIdent ist ein Identifizierungsverfahren der Deutschen Post, VDA Ident ein Identifizierungsverfahren des Trust Centers.
- Für die Identifizierung können nur Ausweisdokumente verwendet werden, die für die angebotenen Identifizierungsverfahren zulässig sind.
- Die Art des Ausweisdokumentes sowie die Ausweisnummer und die Gültigkeitsdaten des Ausweises werden auf dem Antragsformular aufgeführt und in der Datenbank gespeichert.
- Als Identifizierungsdaten werden u. a. Name, Meldeanschrift, Geburtsdatum und Geburtsort des Antragstellers erfasst und somit eine eindeutige Identifizierung gewährleistet.
- Die Bestätigung der berufsrechtlichen Zulassung eines Antragstellers erfolgt durch die zuständige Kammer.

Alle Daten, die ins Zertifikat übernommen werden, werden durch die Registrierungsstelle des Trust Centers im Vier-Augen-Prinzip überprüft.

Hinweis zum Datenschutz: Es werden nur die Daten erfasst, die zur Ausstellung der Zertifikate und Karten inkl. Versand und Rechnungslegung benötigt werden. Die Daten werden ausschließlich für diese Zwecke erhoben.

[SMC-B]

Die Identifizierung und Registrierung der Antragsteller obliegt dem Kartenherausgeber. Dieser kann die Daten im Vorfeld oder im Rahmen der Freigabe erfassen und prüfen.

Hinweis zum Datenschutz: Es werden nur die Daten erfasst, die zur Ausstellung der Zertifikate und Karten inkl. Versand und Rechnungslegung benötigt werden. Die Daten werden ausschließlich für diese Zwecke erhoben.

[SM-B]

Die Identifizierung und Registrierung der Antragsteller obliegt aufgrund der hierarchischen Benutzerkonten-Aufbaus teilweise dem TSP und teilweise der antragstellenden Organisation:

- Der TSP identifiziert die primären User jeder antragstellenden Organisation über die unterschiedlichen PostIdent-Verfahren.
- Die primären User der antragstellenden Organisationen identifizieren die weiteren User ihrer Organisation nach einem geeigneten Verfahren, welches den Anforderungen an das Authentifizierungsniveau „hoch“ gemäß der technischen Richtlinie [TR-03107-1] des BSI genügt.

### 3.2.3.2 Registrierung der Mitarbeiter der Kartenherausgeber

Die Kartenherausgeber sind verantwortlich für die Attributbestätigung und Ausgabe der Karten in ihrem Zuständigkeitsbereich. Damit verbunden ist auch die Sperrberichtigung für die ausgegebenen Karten. Der Ablauf zur Ausgabe der Karten ist in Kap. 4 dargestellt.

Im Regelfall erfolgt die Attributbestätigung elektronisch über die TSP-Schnittstelle, d.h. über das Freigabeportal oder die Web-Service-Schnittstellen, siehe Kap. 4.2.2.2.

Für die Nutzung der TSP-Schnittstelle für Kartenherausgeber zur elektronischen Bearbeitung der Anträge existieren vier getrennte Berechtigungen:

- Berechtigung zur Vorbefüllung,
- Berechtigung zur Freigabe,
- Berechtigung zur Sperrung und
- Berechtigung zum Monitoring.

[HBA] [SMC-B] Der TSP führt die Registrierung berechtigter Mitarbeiter der Kartenherausgeber für die Attributbestätigung und der daraus resultierenden Aktivitäten auf Basis der schriftlichen Nachweise der Kartenherausgeber durch. Jedem registrierten Mitarbeiter werden gemäß der Festlegung des Kartenherausgebers eine oder mehrere dieser o.g. Berechtigungen zugeordnet. Die Registrierung der Antragsteller erfolgt ausschließlich durch fachkundige und zuverlässige Trust Center Operatoren (TCOP) des Trust Centers der Telekom Security. Für jeden Mitarbeiter werden die Authentifizierungsdaten zur Authentifizierung gegenüber dem Freigabeportal oder den Web-Service-Schnittstellen hinterlegt.

[SM-B]

Die Identifizierung und Registrierung der Antragsteller obliegt aufgrund der hierarchischen Benutzerkonten-Aufbaus teilweise dem TSP und teilweise dem Kartenherausgeber:

- Der TSP identifiziert die primären User der Kartenherausgeber über die unterschiedlichen PostIdent-Verfahren.
- Die primären User der Kartenherausgeber identifizieren die weiteren User ihrer Organisation nach einem geeigneten Verfahren, welches den Anforderungen an das Authentifizierungsniveau „hoch“ gemäß der technischen Richtlinie [TR-03107-1] des BSI genügt.

### 3.2.4 Nicht überprüfte Teilnehmerangaben

[HBA] Die HBA-Zertifikate beinhalten keine vom TSP ungeprüften Informationen, mit Ausnahme der E-Mail-Adresse, welche in die nicht qualifizierten Zertifikate des elektronischen Arztausweises aufgenommen werden kann.

[SM(C)-B] Die SM(C)-B-Zertifikate enthalten keine vom Kartenherausgeber ungeprüften Informationen, der TSP prüft die Informationen nicht.

### 3.2.5 Überprüfung der Berechtigung

Die Karten dürfen nur durch berechtigte Antragsteller (siehe Kap. 1.3.3) beantragt werden. Deren Berechtigung wird vor Zertifikatserstellung durch den zuständigen Kartenherausgeber gegenüber dem TSP im Rahmen der Attributbestätigung und Produktionsfreigabe bestätigt.

### 3.2.6 Kriterien für Interoperabilität

Die Interoperabilität wird durch die Einhaltung der Vorgaben und Spezifikation der gematik sowie im Falle des HBA darüber hinaus durch die aufgeführten ETSI-Normen gewährleistet.

## 3.3 Identifizierung und Authentifizierung bei Zertifikatserneuerung

### 3.3.1 Identifizierung und Authentifizierung für routinemäßige Schlüsselerneuerung

[HBA] [SMC-B]

Eine Zertifikatserneuerung ist nur in Verbindung mit der Neu-Ausstellung einer Karte möglich, d.h. es werden keine neuen Zertifikate für bereits ausgegebene Karten oder deren Schlüssel erstellt.

Im Rahmen der Zertifikatserneuerung können folgende Karten ausgestellt werden:

- **Austauschausweise:** Austauschausweise sind Karten, die nach Ausgabe einer Karte ausgestellt werden können, wenn der Inhaber die Karte z.B. verloren, zerstört oder durch falsche PIN-Eingabe unbrauchbar gemacht hat. Hierzu muss der Originalausweis bei Beantragung des Austauschausweises noch mindestens 30 Tage gültig sein. In diesem Fall kann auf Antrag ohne erneute Identifizierung und ohne erneute Bestätigung durch den Kartenherausgeber eine neue Karte beantragt werden. Im Falle eines Austauschausweises für einen HBA muss der Antrag schriftlich erfolgen. Die ursprüngliche Gültigkeit des Originalausweises wird auf den Austauschausweis übernommen.
- **Folgekarte:** Folgekarten sind Karten, die rechtzeitig vor dem Ablauf einer Karte beantragt werden können. Mit der Beantragung ist eine erneute Bestätigung und Freigabe des Kartenherausgebers erforderlich. Es muss also der gleiche Identifizierungsprozess wie bei Neukunden durchlaufen werden. Solange ein ablaufender HBA noch gültig ist, kann mit diesem ein elektronischer Antrag, qualifiziert signiert werden, so dass eine erneute Identifizierung nicht erforderlich ist.

[SM-B]

Eine Zertifikatserneuerung ist für SM-B nicht vorgesehen.

### 3.3.2 Identifizierung und Authentifizierung bei Schlüsselerneuerung nach Zertifikatssperrung

[HBA] [SMC-B] Die Ausstellung eines Austauschausweises oder einer Folgekarte nach Sperrung durch den Kartenherausgeber oder Ablauf der Gültigkeit einer Karte ist nicht vorgesehen, in diesen Fällen ist eine neue Karte wie bei Erstbeantragung zu beantragen.

[SM-B] Eine Zertifikatserneuerung ist für SM-B nicht vorgesehen.

## 3.4 Identifizierung und Authentifizierung bei Sperranträgen

### 3.4.1 Sperrung von Karten durch die Antragsteller

[HBA] [SMC-B] Bei Beantragung einer Sperrung der Zertifikate einer Karte muss sich der Antragsteller gegenüber der Zertifizierungsstelle oder der von ihr beauftragten Sperr-Hotline, authentifizieren. Die Authentifizierung gegenüber der Sperr-Hotline erfolgt ausschließlich über ein bei Beantragung der Karte vereinbartes Sperrkennwort. Die Authentifizierung gegenüber der Zertifizierungsstelle kann ebenso mittels des Sperrkennwortes erfolgen. Darüber hinaus kann der Antragsteller die Sperrung schriftlich (formlos) bei der Zertifizierungsstelle veranlassen.

[HBA] Im Fall einer schriftlichen Beantragung einer Sperrung erfolgt die Authentisierung über einen Abgleich der Unterschrift auf dem Sperrantrag mit der Unterschrift auf dem ursprünglichen Antrag.

[SM-B] Die Antragsteller können ihre Zertifikate 7x24 Stunden über das Antragsportal im Vier-Augen-Prinzip sperren lassen oder schriftlich eine Sperrung beantragen, eine telefonische Sperrung ist nicht möglich.

### 3.4.2 Sperrung von Karten durch den Kartenherausgeber

Die Authentisierung der Kartenherausgeber als Sperrberechtigte erfolgt bei elektronischer Sperrung über die TSP-Schnittstelle über die im Rahmen der Registrierung der berechtigten Mitarbeiter (siehe Kap.3.2.3.2) vereinbarten Authentisierungsmechanismen.

[HBA] Im Falle der Sperrung von HBA über die TSP-Schnittstelle muss der Sperrantrag mit einem im Rahmen der Registrierung der berechtigten Mitarbeiter hinterlegten qualifizierten Signaturzertifikat erfolgen.

Darüber hinaus kann ein Kartenherausgeber die Sperrung schriftlich (formlos) bei der Zertifizierungsstelle veranlassen. In diesem Fall erfolgt die Authentisierung über einen Abgleich der Unterschrift auf dem Sperrantrag mit der Unterschrift des Mitarbeiters auf den Registrierungsformularen, die im Rahmen der Registrierung der berechtigten Mitarbeiter der Kartenherausgeber (siehe Kap. 3.2.3.2) übermittelt wurden.



## 4 Anforderung an den Lebenszyklus der Zertifikate

Die Prozesse zur Ausgabe der Karten bzw. der Zertifikate für die SM-B erfolgen über die TSP-Schnittstelle, welche aus folgenden Komponenten besteht:

- **Vorbefüllungsportal:**

Über das Vorbefüllungsportal können die Kartenherausgeber Antragsdaten vorbefüllen, so dass der Antragsteller den Antrag auf Basis der voreingestellten Daten stellen kann. Da die Vorbefüllung optional und der eigentlichen Antragstellung vorgelagert ist, der Antragsprozess aber nur auf Basis der vom Antragsteller gestellten Anträge erfolgt, wird die Vorbefüllung nachfolgend nicht weiter betrachtet.

- **Antragsportal:**

Über das Antragsportal können die Antragsteller Karten bzw. SM-B Zertifikate beantragen, die Zertifikate freischalten und bei Bedarf sperren.

- **Freigabeportal:**

Über das Freigabeportal können die Kartenherausgeber Attribute bestätigen und Karten bzw. SM-B-Zertifikate zur Produktion freigeben, bei Bedarf sperren, Antrags-/Karten-Zertifikatsstatus prüfen, weitere Funktionen abrufen (Statistiken, Monitoring, Exporte, etc.).

- **Web-Service-Schnittstellen:**

[HBA] [SMC-B] Über die Web-Service-Schnittstellen (SOAP) können die Kartenherausgeber die gleichen Funktionen wie über das Vorbefüllungs- und Freigabeportal abrufen. Da auch über die Web-Service-Schnittstellen die gleichen Mechanismen (z.B. qualifiziert signierte Produktions-Freigaben oder Sperrungen) zugrunde liegen, wird die Web-Service-Schnittstelle nachfolgend nicht weiter betrachtet.

[SM-B] Die Nutzung der Web-Service-Schnittstellen (SOAP) ist im Ausgabeprozess der SM-B nicht vorgesehen.

[HBA] [SMC-B] Der Beantragungs- und Ausgabeprozess einer Karte läuft wie folgt dargestellt ab:

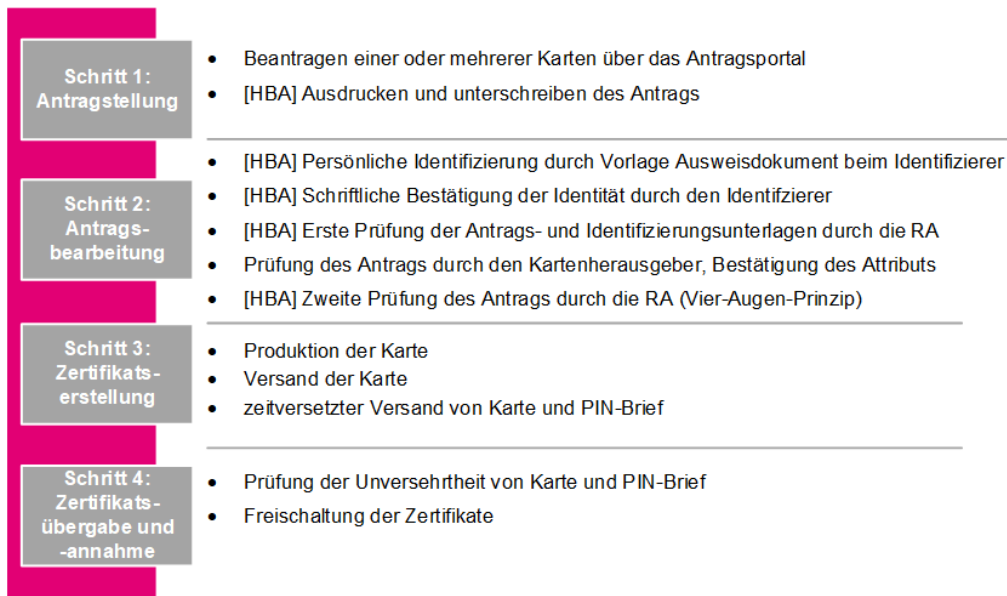


Abbildung 4: Übersicht: Beantragungs- und Ausgabeprozess HBA oder SMC-B

[SM-B] Der Beantragungs- und Ausgabeprozess von Zertifikaten einer SM-B läuft wie folgt dargestellt ab:



Abbildung 5: Übersicht: Beantragungs- und Ausgabeprozess SM-B-Zertifikate

Die einzelnen Schritte werden in den nachfolgenden Kapiteln beschrieben.

## 4.1 Antragstellung

### 4.1.1 Wer kann eine Karte beantragen?

[HBA] HBA dürfen nur durch Ärzte, Zahnärzte, Apotheker und Psychotherapeuten beantragt werden.

[SM(C)-B] SM(C)-B dürfen nur durch Inhaber, Gesellschafter oder berechtigte Mitarbeiter medizinischer Institutionen sowie Krankenkassen beantragt werden,

### 4.1.2 Antragsstellungsverfahren und Pflichten

Der Antragsteller beantragt eine oder mehrere Karten bzw. ein Zertifikatsbündel einer SM-B über das Antragsportal. Nach dem Absenden des Antrags wird dem Antragsteller der Antrag als PDF zum Download angeboten.

[HBA] Der Antragsteller druckt die Antragsunterlagen aus und unterschreibt diese. Die Antragsunterlagen umfassen auch Unterlagen zum anschließend durchzuführenden Identifizierungsverfahren.

Mit dem Antragsformular werden dem Antragsteller die Nutzungsbedingungen (siehe dazu auch Kap. 4.1.2.2) zur Verfügung gestellt und auf den Download der CPS und der PDS verwiesen.

Diese CP/CPS, die Nutzungsbedingungen sowie die in den entsprechenden Handbüchern beschriebenen Anforderungen sind bindend für alle Antragsteller und die betroffenen Kartenherausgeber. Bei Beantragung einer Karte müssen die Antragsteller bestätigen, dass Sie diese CP/CPS zur Kenntnis nehmen und beachten. Darüber hinaus gelten für die Kartenherausgeber und Antragsteller die nachfolgend beschriebenen Anforderungen.

Weitere Parteien (Dritte) sind in diesem Verfahren nicht eingebunden.

#### 4.1.2.1 Anforderungen an die Kartenherausgeber

Die Kartenherausgeber sind verpflichtet, ihre Mitarbeiter für die Tätigkeiten im Rahmen der Attributbestätigung zu schulen und dieses dem TSP nachzuweisen. Die Mitarbeiter müssen gemäß Kap. 3.2.3.2 registriert werden. Im Rahmen der Registrierung werden Schulungsnachweise und Berechtigungen geprüft.

Darüber hinaus sind auch die Kartenherausgeber durch die Übernahme von Tätigkeiten im Rahmen der Freigabe und Attributbestätigung verpflichtet, vertrauliche Informationen entsprechend zu behandeln, siehe Kap. 9.3

#### 4.1.2.2 Anforderungen an die Antragsteller

Die Antragsteller müssen die an Sie gestellten Anforderungen kennen. Dazu werden ihnen verständliche Unterlagen und Hilfestellungen im Antragsportal zur Verfügung gestellt. Die Teilnehmer erhalten Informationen über:

- [HBA] [SM(C)-B] den Schutz der Karte sowie der zugehörigen PINs und PUKs,
- die Gründe und Vorgehensweise bei Zertifikatssperrung,
- die Gültigkeitsprüfung von Zertifikaten,
- die Rezertifizierung,

- die Vorgehensweise bei Änderung von Daten, die im Zertifikat enthalten sind.

Die Antragsteller verpflichten sich bei Beantragung eines Zertifikats, die in Kap.9.6.3 aufgeführten Nutzungsbedingungen zu beachten.

[HBA] Die Bestätigung der Beachtung der Nutzungsbedingungen erfolgt im Falle von HBA zusätzlich mittels Unterschrift auf dem Zertifikatsantrag

## 4.2 Antragsbearbeitung

Die Antragsbearbeitung besteht aus dem Prozess der Identifizierung und Authentifizierung sowie dem Prozess der Genehmigung oder Ablehnung von Zertifikatsanträgen, welcher sich wiederum in die Prüfungen durch die RA und die Freigabe/Attributbestätigung durch den Kartenherausgeber aufteilt.

### 4.2.1 Durchführung der Identifikation und Authentifizierung

[HBA]

Als Identifizierungsvarianten sind im Regelprozess derzeit PostIdent Filiale, PostIdent eID und VDA Ident erlaubt.

#### **PostIdent Filiale**

Mit dem gültigen Ausweisdokument geht der Antragsteller persönlich zum Identifizierer. Der Antragsteller muss eine Filiale der Deutschen Post aufsuchen und lässt sich unter Vorlage des gültigen Ausweisdokuments identifizieren. Der Identifizierer prüft und bestätigt die Identität des Antragstellers, es erfolgt weiterhin eine Unterschriftenprobe des Antragstellers.

Es werden alle relevanten Daten sowie die Unterschrift elektronisch erfasst und dem TSP elektronisch zur Verfügung gestellt.

#### **PostIdent eID**

Voraussetzung ist ein deutscher Personalausweis oder ein elektronischer Aufenthaltstitel (eAT) mit aktivierter Online-Ausweisfunktion und der zugehörigen PIN. Der Prozess ist mobil möglich und rein digital und wird über die PostIdent App der Deutschen Post durchgeführt.

Es werden alle relevanten Daten sowie die Unterschrift digital erfasst und dem TSP elektronisch zur Verfügung gestellt.

#### **VDA Ident**

Im Falle von VDA Ident bei VDA Ident können sich Identifizierungsmitarbeiter und Antragsteller an einem frei wählbaren Ort treffen. Auf einem Identifizierungsformular des TSP dokumentiert der Identifizierer die Daten des vorliegenden Ausweises.

Das Identifizierungsformular wird anschließend dem Trust Center übergeben.

[SMC-B]

Die Identifizierung und Authentifizierung der Antragsteller obliegt dem Kartenherausgeber und kann entweder im Vorfeld oder im Rahmen der Freigabe erfolgen.

[SM-B]

Die Identifizierung und Registrierung der Antragsteller obliegt aufgrund der hierarchischen Benutzerkonten-Aufbaus teilweise dem TSP und teilweise der antragstellenden Organisation:

- Der TSP identifiziert die primären User jeder antragstellenden Organisation über das PostIdent-Verfahren,
- Die primären User der antragstellenden Organisationen identifizieren die weiteren User ihrer Organisation nach einem geeigneten Verfahren, welches den Anforderungen an das Authentifizierungsniveau „hoch“ gemäß der technischen Richtlinie [TR-03107-1] des BSI genügt.

## 4.2.2 Genehmigung oder Ablehnung von Zertifikatsaufträgen

### 4.2.2.1 Registrierung/erste Prüfung durch die RA

[HBA]

Nach Eingang des Antrags und der Identifizierungsunterlagen im Trust Center überprüft ein Trust Center Operator (TCOP) die Unterlagen und gleicht die Daten mit den elektronisch über das Antragsportal übergebenen Daten ab.

Bei erfolgreicher Prüfung stellt der TCOP den Antrag zu Freigabe, siehe nachfolgender Schritt.

Bei nicht erfolgreicher Prüfung wird zunächst versucht, mit dem Antragsteller eine Klärung herbeizuführen und die Möglichkeit der Nachbesserung eingeräumt. Wenn keine Klärung herbeigeführt werden kann, wird der Antrag abgelehnt.

[SM(C)-B]

Die Registrierung und Antragsprüfung obliegt dem Kartenherausgeber und erfolgt im Rahmen der Freigabe (siehe Kap. 4.2.2.2). Es erfolgt keine Antragsprüfung durch den TSP.

### 4.2.2.2 Freigabe/Attributbestätigung durch den Kartenherausgeber

Zur Prüfung des Antrags erhält der zuständige Kartenherausgeber die Information, dass der Antrag zur Freigabe bereitsteht (E-Mail) und kann daraufhin im Freigabeportal den Antrag aufrufen, prüfen und ggf. wie folgt überarbeiten:

- [HBA] Der Kartenherausgeber kann nur die Druckdaten für die optische Personalisierung überarbeiten, jedoch nicht für Zertifikats- und Identifizierungsrelevante Daten.
- [SM(C)-B] Der Kartenherausgeber kann die Zertifikatsinhalte der X509-Zertifikate, insbesondere den commonName der Zertifikate überarbeiten.

Nach erfolgreicher Prüfung bestätigt der Mitarbeiter des Kartenherausgebers das Attribut und erteilt dem TSP wie folgt die Freigabe zur Produktion der Karte.

- [HBA] Der Kartenherausgeber signiert die Freigabe/Bestätigung mittels QES. Zur Erzeugung der QES muss das bei der Registrierung hinterlegte Signaturzertifikat (siehe Kap. 3.2.3.2) genutzt werden.
- [SM(C)-B] Der Kartenherausgeber kann die Freigabe signiert (analog zu HBA, s.o.) oder unsigniert erteilen, die zu nutzende Variante wird Sektor spezifisch festgelegt.

Bei nicht erfolgreicher Prüfung stellt der Mitarbeiter des Kartenherausgebers die Freigabe zurück. Es wird dann zunächst versucht, mit dem Antragsteller eine Klärung herbeizuführen und die Möglichkeit der Nachbesserung eingeräumt. Wenn keine Klärung herbeigeführt werden kann, wird der Antrag abgelehnt.

### 4.2.2.3 Zweite Prüfung durch die RA

[HBA]

Nach Freigabe und Attributbestätigung überprüft zur Gewährleistung des Vier-Augen-Prinzips ein weiterer TCOP (d.h. nicht der TCOP der ersten Prüfung, siehe Kap. 4.2.2.1) die Freigabe/Attributbestätigung des Kartenherausgebers durch Prüfung der QES des Freigabeformulars.

Bei erfolgreicher Prüfung wird der Antrag durch den TCOP zur Produktion frei gegeben, siehe nachfolgenden Schritt.

Bei nicht erfolgreicher Prüfung wird zunächst versucht, mit dem Antragsteller oder dem Kartenherausgeber eine Klärung herbeizuführen und die Möglichkeit der Nachbesserung eingeräumt. Wenn keine Klärung herbeigeführt werden kann, wird der Antrag abgelehnt.

[SMC-B]

Nach nicht-signierter Freigabe durch den Kartenherausgeber wird der Antrag automatisiert zur Produktion freigegeben, es erfolgt keine weitere Prüfung des Antrags durch den TSP.

Im Falle einer qualifiziert signierten Freigabe wird die QES der Freigabe durch den TSP geprüft.

Bei erfolgreicher Prüfung wird der Antrag durch den TCOP zur Produktion frei gegeben, siehe nachfolgenden Schritt.

Bei nicht erfolgreicher Prüfung wird zunächst versucht, mit dem Antragsteller oder dem Kartenherausgeber eine Klärung herbeizuführen und die Möglichkeit der Nachbesserung eingeräumt. Wenn keine Klärung herbeigeführt werden kann, wird der Antrag abgelehnt.

[SM-B]

Es erfolgt keine weitere Prüfung nach Freigabe durch den Kartenherausgeber.

### 4.2.3 Bearbeitungszeit von Anträgen

[HBA] [SMC-B] Die Bearbeitung der Anträge inkl. der Produktion der Karte erfolgt in der Regel innerhalb von zwei Wochen nach Freigabe durch den Kartenherausgeber.

[SM-B] Nicht anwendbar.

## 4.3 Zertifikatserstellung

### 4.3.1 Maßnahmen der CA während der Ausstellung von Zertifikaten

[HBA] [SMC-B] Die TCOPs prüfen regelmäßig die zur Produktion freigegebenen Anträge und erstellen daraus einen Produktionsjob, so dass die Karten produziert werden. Nach Produktion der Karten wird der zuständige Kartenherausgeber und der Antragsteller über die Produktion per E-Mail informiert.

[SM-B] Die Zertifikate einer SM-B werden unmittelbar nach Freigabe durch den Kartenherausgeber automatisiert ausgestellt.

Zu Gewährleistung der Eindeutigkeit des Namens wird in die Zertifikate immer eine Seriennummer im Subject-DN aufgenommen.

[HBA] [SMC-B] Zur Gewährleistung der Schlüsselqualität und der Sicherstellung des alleinigen Zugriffs auf die privaten Schlüssel werden die Schlüssel im Rahmen der Kartenpersonalisierung in der jeweiligen Karte selbst erzeugt. Die Karten verfügen dazu über einen integrierten Schlüsselgenerator. Die geheimen Schlüssel verbleiben im Zugriffsgeschützten Bereich der jeweiligen Karte, d.h. sie verlassen diese niemals. Die Zertifikate werden ausschließlich im Rahmen der Produktion auf die Karte aufgebracht, bevor diese ausgegeben werden. Durch die Verknüpfung der eindeutigen Referenznummern der einzelnen Anträge mit den zugehörigen Karten (die Referenznummer ist Teil der ICCSN) wird sichergestellt, dass jede Karte eindeutig einer Identität zugeordnet ist. Dadurch wird auch sichergestellt, dass ein Schlüssel nicht zwei verschiedenen Identitäten zugewiesen werden kann.

[SM-B] Zur Gewährleistung der Schlüsselqualität und der Sicherstellung des alleinigen Zugriffs auf die privaten Schlüssel werden die Schlüssel durch die Antragsteller generiert und integritätsgeschützt in Form von PKCS#10-Requests übergeben. Durch die Verknüpfung der eindeutigen Referenznummern der einzelnen Anträge mit den zugehörigen SM-B als virtuelle Karten (die Referenznummer ist Teil der ICCSN) wird sichergestellt, dass jede SM-B eindeutig einer Identität zugeordnet ist. Dadurch wird auch sichergestellt, dass ein Schlüssel nicht zwei verschiedenen Identitäten zugewiesen werden kann.

### 4.3.2 Benachrichtigung von Antragstellern über die Ausstellung der Zertifikate

Der Antragsteller erhält über die Ausstellung der Karte bzw. der Zertifikate eine Benachrichtigung per E-Mail mit allen relevanten Informationen.

## 4.4 Zertifikatsübergabe und -annahme

[HBA] [SMC-B] Die produzierten Karten und PIN-Briefe werden zeitversetzt (mind. 3 Tage) an die vom Antragsteller angegebene Adresse per Einschreiben Einwurf versendet. Hinweis: In Ausnahmefällen können die Karten auch durch einen berechtigten Mitarbeiter des Trust Centers persönlich übergeben werden.

[SM-B] Die produzierten Zertifikate werden als Zertifikatsbündel einer SM-B durch einen autorisierten Antragsteller im Antragsportal heruntergeladen.

### 4.4.1 Akzeptanz durch den Zertifikatsinhaber

[HBA] [SMC-B] Der Antragsteller bestätigt den unversehrten Empfang der Karte und des PIN-Briefs sowie die Korrektheit der Zertifikate über das Antragsportal.

Bei falschen Angaben im Zertifikat verpflichtet sich der Antragsteller diese unverzüglich zu melden. Wenn keine entsprechende Meldung innerhalb von 14 Tagen nach Ausstellung des Zertifikats erfolgt, gilt das Zertifikat als akzeptiert.

[SM-B] Der Antragsteller bestätigt den Download sowie die Korrektheit der Zertifikate über das Antragsportal.

### 4.4.2 Veröffentlichung des Zertifikats durch die CA

Die Zertifikate werden nach erfolgter Akzeptanzbestätigung des Antragstellers (siehe Kap. 4.4.1) freigeschaltet und in den Verzeichnisdiensten veröffentlicht, falls der Antragsteller der Veröffentlichung zugestimmt hat.

### 4.4.3 Benachrichtigung anderer Stellen über die Zertifikatsausstellung durch die CA

Die Kartenherausgeber erhalten über die Ausstellung der Karten bzw. Zertifikate in ihrem Zuständigkeitsbereich eine Benachrichtigung per E-Mail mit allen relevanten Informationen.

## 4.5 Verwendung von Schlüsselpaar und Zertifikat

### 4.5.1 Nutzung des privaten Schlüssels und des Zertifikats durch den Zertifikatsinhaber

Das Zertifikat und der zugehörige private Schlüssel dürfen nur entsprechend der vorgesehenen Verwendung genutzt werden, siehe Kap. 9.6.3

[HBA] [SMC-B] Die Inhaber der Karten müssen die PINs und PUKs zur Nutzung ihrer privaten Schlüssel vor unbefugtem Gebrauch schützen und dürfen die Karte und damit die privaten Schlüssel nach Ablauf des Gültigkeitszeitraums oder Sperrung des Zertifikats nicht mehr benutzen, außer zur Entschlüsselung.

Darüber hinaus gelten die Nutzungsbedingungen gemäß Kap.9.6.3.

### 4.5.2 Nutzung von öffentlichen Schlüsseln und Zertifikaten durch Vertrauende Dritte (Relying Parties)

Jeder Vertrauende Dritte, der ein Zertifikat einsetzt, sollte

- vor der Nutzung des Zertifikats dessen Gültigkeit überprüfen, in dem er unter anderem die gesamte Zertifikatskette bis zum Wurzelzertifikat validiert (Zertifizierungshierarchie) sowie den Gültigkeitszeitraum und die Stauts- bzw. Sperrinformationen (CRL (nur bei nonQES), OCSP) des Zertifikats überprüft,
- das Zertifikat ausschließlich für autorisierte Zwecke einzusetzen,
- die technischen Verwendungszwecke prüfen, die durch die im Zertifikat angegebenen Attribute „Schlüsselverwendung“ und „erweiterte Schlüsselverwendung“ festgelegt sind.

Vertrauende Dritte müssen geeignete Software und/oder Hardware zur Überprüfung von Zertifikaten (Validierung) und den damit verbundenen kryptografischen Verfahren verwenden.

## 4.6 Zertifikatserneuerung

[HBA] [SMC-B] Jede Erneuerung von Zertifikaten ist mit einem Kartenwechsel und somit mit einem Schlüsselwechsel verbunden, eine Erneuerung von Zertifikaten ohne Schlüsselwechsel ist ausgeschlossen. Eine Rezertifizierung von vorhandenem Schlüsselmaterial findet also nicht statt. Der Kunde wird über die aktuell gültigen Vertragsdokumente unterrichtet und erkennt diese an.

[SM-B] Eine Zertifikatserneuerung ist für SM-B nicht vorgesehen, die nachfolgenden Beschreibungen gelten daher nur für HBA und SMC-B.



#### 4.6.1 Bedingungen für eine Zertifikatserneuerung

[HBA] [SMC-B] Es gelten die Regelungen gemäß Kap. 3.3.1. Darüber hinaus werden bei Beantragung einer Zertifikatserneuerung dem Antragsteller die aktuellen Nutzungsbedingungen zur Verfügung gestellt, dessen Zurkenntnisnahme der Antragsteller bestätigen muss.

#### 4.6.2 Wer darf eine Zertifikatserneuerung beantragen?

[HBA] [SMC-B] Eine Zertifikatserneuerung darf nur durch den Inhaber einer noch gültigen und nicht gesperrten Karte beantragt werden.

#### 4.6.3 Bearbeitung von Zertifikatserneuerungen

[HBA] [SMC-B] Es gelten die Regelungen gemäß Kap. 3.3.1.

#### 4.6.4 Benachrichtigung des Zertifikatsnehmers über die Ausstellung eines neuen Zertifikats

[HBA] [SMC-B] Es gelten die Regelungen gemäß Kap. 4.3.2.

#### 4.6.5 Annahme einer Zertifikatserneuerung

[HBA] [SMC-B] Es gelten die Regelungen gemäß Kap. 4.4.1.

#### 4.6.6 Veröffentlichung einer Zertifikatserneuerung durch die CA

[HBA] [SMC-B] Es gelten die Regelungen gemäß Kap. 4.4.2.

#### 4.6.7 Benachrichtigung weiterer Stellen über eine Zertifikatserneuerung durch die CA

[HBA] [SMC-B] Es gelten die Regelungen gemäß Kap. 4.4.3.

### 4.7 Zertifikatserneuerung mit Schlüsselwechsel

[SM-B] Eine Zertifikatserneuerung ist für SM-B nicht vorgesehen, die nachfolgenden Beschreibungen gelten daher nur für HBA und SMC-B.

#### 4.7.1 Bedingungen für eine Schlüsselerneuerung

[HBA] [SMC-B] Es gelten die Regelungen gemäß Kap. 3.3.1. Darüber hinaus werden bei Beantragung einer Zertifikatserneuerung dem Antragsteller die aktuellen Nutzungsbedingungen zur Verfügung gestellt, dessen Zurkenntnisnahme der Antragsteller bestätigen muss.

#### 4.7.2 Wer darf die Zertifizierung eines neuen öffentlichen Schlüssels beantragen?

[HBA] [SMC-B] Es gelten die Regelungen gemäß Kap. 4.6.2.

#### 4.7.3 Bearbeitung von Schlüsselerneuerungsaufträgen

[HBA] [SMC-B] Es gelten die Regelungen gemäß Kap. 3.3.1.

#### 4.7.4 Benachrichtigung des Zertifikatsnehmers über die Zertifikatsausstellung

[HBA] [SMC-B] Es gelten die Regelungen gemäß Kap. 4.3.2.

#### 4.7.5 Annahme einer Zertifikatserneuerung mit neuem Schlüsselmaterial

[HBA] [SMC-B] Es gelten die Regelungen gemäß Kap. 4.4.1.

#### 4.7.6 Veröffentlichung eines Zertifikats mit neuem Schlüsselmaterial durch die Zertifizierungsstelle

[HBA] [SMC-B] Es gelten die Regelungen gemäß Kap. 4.4.2.

#### 4.7.7 Benachrichtigung weiterer Stellen über eine Zertifikatserstellung durch die Zertifizierungsstelle

[HBA] [SMC-B] Es gelten die Regelungen gemäß Kap. 4.4.3.

### 4.8 Änderung von Zertifikatsdaten

Die Beantragung eines neuen Zertifikats mit geänderten Daten ist notwendig, wenn sich die im Zertifikat eingetragenen Daten geändert haben.

[HBA] Die Zertifikatserneuerung mit Datenanpassung ist beim HBA insbesondere bei Namensänderung erforderlich. Bei einer Namensänderung sollte kurzfristig nach Ausstellung eines neuen Identifikationsdokumentes ein neuer HBA beantragt werden, eine erneute Identifizierung mit dem neuen Identifikationsdokument ist dabei erforderlich.

#### 4.8.1 Bedingungen für eine Zertifikatsänderung

Das Ausstellen eines neuen Zertifikats ist zwingend erforderlich, wenn sich Zertifikatsinhalte ändern bzw. geändert haben.

## 4.8.2 Wer darf eine Zertifikatsänderung beantragen?

Es gelten die Regelungen gemäß Kap. 4.1.1.

## 4.8.3 Bearbeitung von Zertifikatsänderungen

Eine Zertifikatsänderung entspricht einer Neubeantragung, es gelten daher die Regelungen gemäß Kap. 4.2.

## 4.8.4 Benachrichtigung des Zertifikatsnehmers über die Ausstellung eines Zertifikats

Es gelten die Regelungen gemäß Kap. 4.3.2.

## 4.8.5 Annahme einer Zertifikatsänderung

Es gelten die Regelungen gemäß Kap. 4.4.1.

## 4.8.6 Veröffentlichung eines Zertifikats mit geänderten Daten durch die CA

Es gelten die Regelungen gemäß Kap. 4.4.2.

## 4.8.7 Benachrichtigung weiterer Stellen durch die CA über eine Zertifikatsausstellung

Es gelten die Regelungen gemäß Kap. 4.4.3.

## 4.9 Sperrung und Suspendierung von Zertifikaten

Es sind folgende Möglichkeiten der Sperrung von Zertifikaten gegeben:

- Es sind nur endgültige Sperrungen der X509-Zertifikate möglich.
  - Zertifikatssuspendierungen, d.h. temporäre Sperrungen sind grundsätzlich für alle Zertifikate nicht zulässig.
  - Zertifikatssperrungen sind für CV-Zertifikate nicht vorgesehen, es werden hierfür keine Sperrlisten und OCSP-Auskünfte erzeugt.
- Es können immer nur alle X.509 Zertifikate einer Karte bzw. einer SM-B gemeinsam gesperrt werden, eine Sperrung eines einzelnen X.509 Zertifikats ist nicht möglich.

### 4.9.1 Gründe für eine Sperrung

Die folgenden Gründe erfordern die Zertifikatssperrung durch den Zertifikatsinhaber:

- der private Schlüssel wurde kompromittiert, verloren, gestohlen oder offengelegt oder es besteht ein dringender Verdacht, dass dies geschehen ist,

- die Angaben im Zertifikat sind nicht mehr aktuell, ungültig oder falsch,
- der zertifizierte Schlüssel oder die damit verwendeten kryptografischen Algorithmen und Parameter entsprechen nicht mehr den aktuellen Anforderungen,
- es liegt ein Missbrauch oder Verdacht auf Missbrauch durch zur Nutzung des Schlüssels durch unberechtigte Personen vor,
- gesetzliche Vorschriften oder richterliche Urteile,
- das Zertifikat wird nicht mehr benötigt bzw. der Antragsteller verlangt ausdrücklich die Sperrung des Zertifikats,
- Verlust der berufsrechtlichen Zulassung.

Des Weiteren kann der Antragsteller ohne Angabe von Gründen das Zertifikat jederzeit sperren lassen.

Die Zertifizierungsstelle sperrt ein Zertifikat, wenn mindestens einer der folgenden Gründe vorliegt:

- Der Antragsteller oder der zuständige Kartenherausgeber reicht den Antrag zur Sperrung ein.  
[HBA] Der Antrag muss schriftlich oder elektronisch mit QES versehen erfolgen.
- es wird bekannt, dass das Zertifikat nicht in Übereinstimmung mit dem zum jeweiligen Zeitpunkt gültigen Version des vorliegenden CPS,
- es wird das Abhandenkommens des privaten Schlüssels (z.B. Verlust, Diebstahl, Weitergabe an eine nicht autorisierte Person) bekannt,
- es liegt eine Kompromittierung oder der Verdacht auf eine Kompromittierung des privaten Schlüssels vor,
- es liegt ein über die im Vertrag vereinbarten Zahlungsfristen hinausgehender, erheblicher Zahlungsverzug vor,
- es werden Umstände bekannt, aufgrund derer der Zertifikatsinhaber nicht länger berechtigt ist, eines der im Zertifikat aufgeführten Attribute zu verwenden,
- Wesentliche Angaben im Zertifikat sind nicht mehr korrekt oder irreführend,
- es liegt ein Missbrauch oder Verdacht auf Missbrauch des Zertifikats durch den Zertifikatsnehmer oder andere zur Nutzung des Schlüssels berechnigte Personen vor,
- es erfolgt eine Verwendung und Handhabung des Zertifikats im Widerspruch zu den Nutzungsbedingungen oder des CPS,
- der technische Inhalt, das Format oder die verwendeten Algorithmen entsprechen nicht mehr den aktuellen Anforderungen, bilden ein nicht akzeptables Risiko oder werden von relevanten Stellen missbilligt oder untersagt.
- es wird festgestellt, dass eine wesentliche Voraussetzung für die Ausstellung des Zertifikats nicht erfüllt war,
- die Zertifizierungsstelle stellt den Betrieb ein,
- Gesetzliche Vorschriften oder richterliche Urteile,
- die Berechtigung der Zertifizierungsstelle zur Ausstellung von Zertifikaten läuft ohne Verlängerung aus, wird beendet oder wird entzogen,
- der Zertifikatsnehmer verfügt nicht mehr über die Berechtigung, das Zertifikat zu nutzen.

#### 4.9.2 Wer kann eine Sperrung beantragen?

Sperrberechtigt sind die Antragsteller (siehe Kap. 3.4.1).

Bei Verlust der berufsrechtlichen Zulassung und ggf. auch bei Wechsel der Zugehörigkeit zu einem Kartenherausgeber sind auch die zuständigen Kartenherausgeber sperrberechtigt (siehe Kap. 3.4.2).

[HBA] Die Bundesnetzagentur kann die Sperrung eines Zertifikates aufgrund gesetzlicher Vorschriften anweisen.

Darüber hinaus kann die Zertifizierungsstelle von ihr ausgestellte Zertifikate aus den in Kap. 4.9.1 aufgeführten Gründen sperren.

### 4.9.3 Ablauf einer Sperrung

Zur Sperrung eines Zertifikats gibt es verschiedene Möglichkeiten:

- [HBA] [SMC-B] Der Antragsteller sperrt die Zertifikate seiner Karte selbst über das Antragsportal. Zur Sperrung muss die Referenznummer des Antrags und das zugehörige Sperrkennwort angegeben werden. Die Sperrung erfolgt in diesem Fall automatisch sofort nach Bestätigung des Sperrwunsches.
- [HBA] [SMC-B] Der Antragsteller sperrt die Zertifikate seiner Karte selbst telefonisch unter Angabe der Referenznummer und des Sperrkennwortes über die Sperr-Hotline der Zertifizierungsstelle (7x24 Stunden erreichbar). Die Sperrung erfolgt in diesem Fall automatisch sofort nach Bestätigung des Sperrwunsches.
- [SM-B] Die Antragsteller sperren die Zertifikate selbst über das Antragsportal im Vier-Augen-Prinzip, die Sperrung erfolgt in diesem Fall automatisch sofort nach Bestätigung des Sperrwunsches.
- Der Antragsteller beantragt die Sperrung der Zertifikate seiner Karte schriftlich bei der Zertifizierungsstelle. Die Sperrung erfolgt in diesem Fall nach Posteingang des Sperrantrags bei der Zertifizierungsstelle am gleichen Arbeitstag.
- [HBA] [SMC-B] Der Kartenherausgeber beantragt die Sperrung der Zertifikate aller Karten des Antragstellers z.B. im Falle des Verlusts der berufsrechtlichen Zulassung, ggf. bei einer Praxisauflösung sowie im Todesfalle. In diesem Fall kann die Sperrung über zwei Wege erfolgen:
  - Der Kartenherausgeber beantragt die Sperrung im Freigabeportal

[HBA] Der Beantragung einer Sperrung erfolgt durch einen elektronischen QES signierten Sperrantrag eines registrierten Mitarbeiters. Nach Eingang des Sperrantrags wird der Sperrantrag durch einen TCOP geprüft. Bei erfolgreicher Prüfung erfolgt die Sperrung der Zertifikate der HBA am gleichen Arbeitstag.

[SMC-B] Die Beantragung einer Sperrung kann signiert (analog zu HBA, s.o.) oder nicht-signiert erfolgen. Nach nicht-signiertem Sperrantrag durch den Kartenherausgeber werden die Zertifikate automatisiert gesperrt, es erfolgt keine weitere Prüfung des Sperrantrags durch den TSP. Im Falle einer qualifiziert signierten Sperrung wird die QES des Sperrantrags durch den TSP geprüft, erst nach erfolgreicher Prüfung der Signatur erfolgt die Sperrung der Zertifikate.

[SM-B] Die Beantragung einer Sperrung erfolgt ohne Signatur des Antrags durch den Kartenherausgeber, die Zertifikate werden daraufhin umgehend automatisiert gesperrt, es erfolgt keine weitere Prüfung des Sperrantrags durch den TSP
  - Der Kartenherausgeber beantragt schriftlich bei der Zertifizierungsstelle die Sperrung. Die Sperrung erfolgt in diesem Fall nach Posteingang des Sperrantrags bei der Zertifizierungsstelle am gleichen Arbeitstag.

Hinweis: Bei einigen Sektoren ist auch eine Kartenherausgeber-übergreifende Sperrung möglich, wenn z.B. der Leistungserbringer durch Umzug in einen anderen Kammerbereich gewechselt ist.

Unabhängig von dem Weg der Sperrung werden unmittelbar nach der Sperrung der Antragsteller und der zuständige Kartenherausgeber über die Sperrung der Zertifikate per E-Mail informiert.

Die Sperrung eines Zertifikats wird unmittelbar nach Sperrung im OCSP-Responder wirksam. Bei Nutzung von Sperrlisten (nur für nonQES-Zertifikate) wird eine Sperrung mit der Ausstellung der nächsten Sperrliste wirksam.

#### 4.9.4 Fristen für einen Sperrantrag

Sobald ein Sperrgrund gemäß Kapitel 4.9.1 vorliegt, muss der Sperrantrag so schnell wie möglich gestellt werden.

#### 4.9.5 Fristen für die Bearbeitung eines Sperrantrags durch die CA

Die Sperrung aufgrund eines Sperrantrags durch den Zertifikatsnehmer über das Antragsportal oder über die Sperrhotline erfolgt unverzüglich.

Die Sperrung aufgrund eines nicht-signierten Sperrantrags durch den Kartenherausgeber über das Freigabeportal erfolgt unverzüglich.

Die Sperrung aufgrund eines schriftlichen oder per QES signiertem elektronischen Sperrantrags des Zertifikatsnehmers oder des zuständigen Kartenherausgebers erfolgt so schnell wie möglich während der Arbeitszeit der TCOP, spätestens jedoch innerhalb des nächsten Arbeitstages.

Bei Eingang einer Problemmeldung zu einem Zertifikat werden innerhalb von 24 Stunden die Fakten und Umstände untersucht und es werden dem Zertifikatsnehmer sowie der meldenden Person eine erste Rückmeldung zu den bis dahin vorliegenden Erkenntnissen gegeben. Anschließend werden mit dem Zertifikatsnehmer und der meldenden Person die Analyseergebnisse besprochen und es wird entschieden, ob eine Sperrung erforderlich ist. Falls eine Sperrung erforderlich ist, wird unter Beachtung der zeitlichen Vorgaben aus Kap. 4.9.1 und Berücksichtigung der folgenden Aspekte der Zeitpunkt der Sperrung festgelegt:

- Art des mutmaßlichen Problems (Umfang, Kontext, Schweregrad, Ausmaß, Schadensrisiko)
- Auswirkungen einer Sperrung (direkte und kollaterale Auswirkungen auf Endteilnehmer vertrauende Dritte)
- Anzahl der erhaltenen Problemmeldungen zu einem Zertifikat oder Zertifikatsnehmer
- Meldende Entität
- Einschlägige Rechtsvorschriften

Wenn Zertifikate nicht innerhalb der vorgegebenen Frist gesperrt werden können, wird die nicht fristgerechte Sperrung als Sicherheitsvorfall behandelt und es wird ein Revocation Delay Bug in Bugzilla gemäß der CCADB-Policy gemeldet.

#### 4.9.6 Überprüfungsmethoden für Vertrauende Dritte

Vertrauende Dritte müssen die Möglichkeit erhalten, den Status von Zertifikaten überprüfen zu können, denen sie vertrauen möchten. Dazu werden Sperrlisten (CRL) und Online-Statusabfragen (OCSP) wie folgt angeboten:

- Die gesperrten X509 non-QES Zertifikate werden in die Sperrliste (CRL) aufgenommen, für QES-Zertifikate werden keine Sperrlisten bereitgestellt.
- Alle gesperrten X509-Zertifikate, d.h. sowohl die QES- als auch die nonQES-Zertifikate erhalten unverzüglich nach Sperrung im OCSP-Responder den Status „revoked“.

Hinweis: Für CV-Zertifikate werden keine Sperrinformationen angeboten, da CV-Zertifikate nicht gesperrt werden können.

#### 4.9.7 Frequenz der Veröffentlichung von Sperrlisten

Die Sperrlisten werden periodisch mindestens täglich erstellt und unverzüglich gemäß Kap. 2 veröffentlicht.

#### 4.9.8 Maximale Latenzzeit von Sperrlisten

Die Latenzzeit der Zertifikatssperrliste (CRL) nach automatischer Generierung beträgt wenige Minuten.

#### 4.9.9 Online- Verfügbarkeit von Sperr-/Statusinformationen

Die Zertifizierungsstelle stellt Online-Informationen zum Zertifikatsstatus 7x24 Stunden monatlich via OCSP bereit. Die OCSP-Responder weisen zur Hauptzeit (Montag bis Freitag von 6 bis 22 Uhr sowie Samstag und Sonntag von 6 bis 20 Uhr) eine Verfügbarkeit von mindestens 99,9% und außerhalb der Hauptzeit eine Verfügbarkeit von mindestens 99% auf. Die Einhaltung dieser Vorgaben wird durch die gematik überwacht.

Die URL des OCSP-Responders ist im Zertifikat in der Erweiterung „Zugriff auf Stelleninformation (Authority Information Access)“ aufgeführt.

#### 4.9.10 Anforderungen an Online-Überprüfungsverfahren

Vertrauende Dritte müssen den Status eines Zertifikats überprüfen, um Informationen darüber zu erhalten, ob ein Zertifikat, dem sie vertrauen möchten, vertrauenswürdig ist. Für den Abruf aktueller Statusinformationen steht der OCSP-Responder zur Verfügung. Eine weitere Möglichkeit der Statusabfrage liefert die aktuelle Zertifikatssperrliste (nur für nonQES-Zertifikate).

#### 4.9.11 Andere verfügbare Formen der Bekanntmachung von Sperrinformationen

Der Zertifikatsinhaber und der zuständige Kartenherausgeber werden per E-Mail über die Sperrung des Zertifikats benachrichtigt (revoke notification), in der die relevanten Zertifikatsinformationen enthalten sind.

#### 4.9.12 Besondere Anforderungen bezüglich der Kompromittierung privater Schlüssel

Bei einer Kompromittierung eines privaten Schlüssels ist das entsprechende Zertifikat unverzüglich zu sperren.

### 4.9.13 Suspendierung von Zertifikaten

Eine Suspendierung (temporäre Sperrung) von Zertifikaten ist nicht zulässig und nicht möglich.

### 4.9.14 Wer kann eine Suspendierung beauftragen?

Nicht anwendbar, da keine Suspendierung möglich ist, siehe Kap. 4.9.13.

### 4.9.15 Verfahren der Suspendierung

Nicht anwendbar, da keine Suspendierung möglich ist, siehe Kap. 4.9.13.

### 4.9.16 Beschränkung des Suspendierungszeitraums

Nicht anwendbar, da keine Suspendierung möglich ist, siehe Kap. 4.9.13.

## 4.10 Auskunftsdienste über den Zertifikatsstatus

Telekom Security bietet zur Auskunft über den Zertifikatsstatus der Zertifikate sowohl Sperrlisten für die X509 nonQES-Zertifikate als auch OCSP-Auskünfte für alle X509-Zertifikate an, Details dazu siehe Kap.2.

Über die gesamte Dauer des Betriebs werden sowohl von den CAs signierte Sperrlisten als auch von delegierten OCSP-Signern signierte OCSP-Auskünfte bereitgestellt.

### 4.10.1 Betriebsbedingte Eigenschaften

OCSP-Antworten für Zertifikate entsprechen den Vorgaben aus RFC6960 und werden wie folgt signiert:

- OCSP-Antworten für QES-Zertifikate werden von einem von der QES-CA ausgestellten OCSP-Signer-Zertifikat signiert,
- OCSP-Antworten für nonQES-Zertifikate werden von einem von der nonQES-CA ausgestellten OCSP-Signer-Zertifikat signiert.

CRLs werden von einem von der nonQES-CA ausgestellten CRL-Signer-Zertifikat signiert.

#### 4.10.1.1 Betriebliche Vorgaben für die Bereitstellung der OCSP-Responder

Die OCSP-Responder werden konform zum [RFC6960] betrieben. Anfragen zu Zertifikaten mit unbekanntem Zertifikatsseriennummern werden mit dem Status „unknown“ beantwortet. OCSP-Anfragen und -Antworten werden generell geloggt und überwacht.

OCSP-Antworten werden auf Anfrage generiert und erhalten einen Wert im nextUpdate-Feld, der 5 Tage nach dem thisUpdate-Wert liegt, werden jedoch maximal für 2 Stunden für weitere Anfragen wiederverwendet.



## 4.10.2 Verfügbarkeit der Dienste

Die Zertifikatsstatus-Dienste stehen 7x24 Stunden zur Verfügung.

## 4.10.3 Weitere Merkmale

Die OCSP-Responder unterstützen die Anforderungen gemäß [Common-PKI].

## 4.11 Kündigung des Zertifizierungsdienstes

Die Kündigung/Abschaltung des Zertifizierungsdienstes hat die Sperrung aller ausgestellten Zertifikate zur Folge. Weitere Details sind im Beendigungsplan festgelegt.

Bei einer vorzeitigen Beendigung der Zertifikatsnutzung einer Karte vor Ablauf der Gültigkeit durch den Antragsteller muss die Karte durch den Inhaber gesperrt werden.

## 4.12 Schlüsselhinterlegung und Wiederherstellung

### 4.12.1 Richtlinien und Praktiken zur Schlüsselhinterlegung und -wiederherstellung

Eine Schlüsselhinterlegung bei Dritten (z.B. Treuhänder, Notar) ist für alle Zertifikate nicht realisiert.

Für die CA-Zertifikate werden die Schlüsselpaare auf einem sicherheitsüberprüften Hardware Security Module (HSM) hinterlegt und in sicherer Umgebung abgelegt. Die Speicherung des Schlüsselmaterials auf weiteren HSM erfolgt ausschließlich zur Schlüsselhinterlegung (Back-Up) und dient zu Wiederherstellung und Aufrechterhaltung des Dienstes durch qualifiziertes Personal (Trusted Role) des Trust Centers.

[HBA] [SMC-B] Für die Karten-Zertifikate werden Schlüsselpaare auf Smartcards verwendet, ein Backup dieser Schlüssel ist nicht vorgesehen und nicht möglich.

[SM-B] Für die Zertifikate der SM-B werden Schlüsselpaare auf HSM der antragstellenden Organisation verwendet, ein evtl. Backup dieser Schlüssel obliegt den antragstellenden Organisationen selbst.

### 4.12.2 Richtlinien und Praktiken zum Schutz und Wiederherstellung von Sitzungsschlüsseln

Nicht anwendbar.

## 5 Physikalische, organisatorische und personelle Sicherheitsmaßnahmen

Das Trust Center ist in einem speziell geschützten Gebäude untergebracht und wird von fachkundigem Personal betrieben. Alle Prozesse für die Generierung und Verwaltung von Zertifikaten der dort betriebenen Zertifizierungsstellen sind genau definiert. Alle technischen Sicherheitsmaßnahmen sind dokumentiert.

Die angewendeten physikalischen, organisatorischen und personellen Sicherheitsmaßnahmen sind in einem Sicherheitskonzept nach IT-Grundschutz festgelegt, deren Wirksamkeit ist auf Basis einer Bedrohungsanalyse nachgewiesen.

Die für den operativen Betrieb notwendigen Sicherheitsmaßnahmen sind in dem Service- und Organisations-Handbuch sowie dem Betriebsleitfaden des Trust Centers beschrieben.

Die Anforderungen aus [ETSI EN 319 401] sind umgesetzt, d.h. es sind Festlegungen

- zur Risikobewertung im Rahmen des ISMS,
- zu den Richtlinien zur Informationssicherheit,
- zum Asset-Management
- zur Informationssicherheit in der Lieferkette Supply Chain Policy

beschrieben.

### 5.1 Physikalische Sicherheitsmaßnahmen

Der Betrieb der Zertifizierungsstelle erfolgt im Trust Center der Telekom Security. Das Trust Center ist eIDAS-konform und erfüllt somit sehr hohe Ansprüche an die physikalische Sicherheit. Die Maßnahmen sind detailliert im Sicherheitskonzept beschrieben. Die Anforderungen aus [ETSI EN 319 401] Kap. 7.6 sind umgesetzt.

#### 5.1.1 Standort und bauliche Maßnahmen

Telekom Security betreibt die Zertifizierungsstelle in einem Rechenzentrum, welches aus zwei voll redundant ausgelegten Hälften, zwei getrennt arbeitenden Energietrakten (Elektro, Klima, Wasser) mit Gebäudemanagementsystem und Notstromaggregaten sowie einem Verwaltungstrakt besteht.

Die Errichtung und der Betrieb des Trust Centers bzw. des Rechenzentrums erfolgt unter Beachtung der entsprechenden Richtlinien des Bundesamtes für Sicherheit in der Informationstechnik (BSI), des Gesamtverbands der Deutschen Versicherungswirtschaft (GDV), der einschlägigen DIN-Normen zu Brandschutz, Rauchschutz und Angriffshemmung. Das Trust Center ist sicherheitstechnisch vom GDV abgenommen.

Die technischen Maßnahmen werden durch organisatorische Elemente ergänzt, die die Handhabung der sicherheitsrelevanten Techniken und Regelungen über den Zutritt zu Sicherheitszonen für Mitarbeiter und Dritte (Besucher, Fremd- und Reinigungspersonal), die Anlieferung von Material (Hardware, Zubehör, Betriebsmittel) und Ordnung am Arbeitsplatz sowie in Rechnerräumen beinhalten.

Die Antragsbearbeitung und Personalisierung der Karten erfolgt nicht in den Räumlichkeiten des Rechenzentrums, sondern an anderen (Büro-) Standorten der Telekom Security, welche ebenso in Sicherheitskonzepten betrachtet sind und in den Audits gemäß Kap. 8 geprüft werden.

### 5.1.2 Zutritt

Im Trust Center gelten Zutrittsregelungen, welche die die Zutrittsrechte für Mitarbeiter, Mitarbeiter von Fremdfirmen und Gästen in den einzelnen Sicherheitszonen regelt. Der kontrollierte Zutritt zu den verschiedenen Sicherheitsbereichen ist mit einem rechnergesteuerten Zutrittskontrollsystem geschützt. Gäste werden nur nach vorheriger Anmeldung empfangen. Hier gelten besondere Sicherheitsvorschriften.

### 5.1.3 Stromversorgung und Klimatisierung im RZ

Die Ansaugöffnungen für die Außenluft sind so angeordnet, dass keine Schadstoffe wie Staub und Schmutz, ätzende, giftige oder leicht brennbare Gase eindringen können. Die Systeme werden mit einem sehr geringen Außenluftanteil betrieben. Die erforderlichen Zu- und Abluftöffnungen sind zugangsgeschützt. Zum Schutz gegen Luftverunreinigung durch schwebende Partikel sind Filter installiert. Die Frischluftansaugung wird ständig auf aggressive Gase überwacht. Im Notfall (z.B. Brand in der Umgebung) wird die Außenluftansaugung automatisch durch Luftklappen verschlossen.

Zum Ausfallschutz der Energieversorgung ist eine unabhängige Wechselspannungsversorgung entsprechend VDE-Vorschriften installiert. Sie bietet Schutz gegen Spannungsschwankungen, unterbrechungsfreie Kurzzeitüberbrückung, eine Langzeitüberbrückung mit zwei getrennten, ortsfesten Notstromaggregaten mit einer Leistung, die der Volllast des Rechenzentrums entspricht.

### 5.1.4 Wassergefährdung des RZ

Das Rechenzentrum liegt in einer geschützten Lage, d.h. es liegt nicht in der Nähe von Gewässern und Niederungen (Hochwassergefahr). Die Brandbekämpfung erfolgt mit inertem Gas.

### 5.1.5 Brandschutz im RZ

Die geltenden Brandschutzbestimmungen (z.B. DIN 4102, Auflagen der örtlichen Feuerwehr, Vorschriften über Feuerresistenz, VDE-gerechte Elektroinstallation) werden eingehalten. Alle Brandschutztüren besitzen automatische Schließeinrichtungen. In Absprache mit der Feuerwehr wird nur in äußersten Notfällen mit Wasser gelöscht.

Brandabschnitte sind durch feuerbeständige Bauteile gesichert. Durchgänge durch Brandschutzwände sind mit selbsttätig schließenden Brandschutztüren ausgestattet

In Bereichen mit Doppelböden sowie abgehängten Decken sind Brandschutzwände durchgehend bis zum Geschoßboden bzw. zur Geschoßdecke ausgeführt.

In allen Systemräumen, Systemoperatorräumen, Archivräumen, USV-Räumen sowie weiteren ausgewählten Räumen sind Brandfrühsterkennungssysteme (Ansaugsysteme) installiert. Überwacht wird die Zu- bzw. Abluft der Klimageräte der einzelnen Räume. In den weiteren Räumen sind Brandmelder verbaut.

## 5.1.6 Aufbewahrung von Datenträgern

Datenträger, die Produktionssoftware und -daten, Audit-, Archiv- oder Sicherungsinformationen enthalten, werden in Räumen gelagert, die mit den entsprechenden physischen Zutrittskontrollen versehen sind und Schutz vor Unfallschäden (z.B. Wasser-, Brand- und elektromagnetische Schäden) bieten.

## 5.1.7 Entsorgung

Vertrauliche Dokumente und Materialien werden vor ihrer Entsorgung physisch zerstört. Datenträger, die vertraulichen Informationen enthalten, werden vor ihrer Entsorgung derart behandelt, dass diese Daten nicht auslesbar oder wieder herstellbar sind. Kryptografische Geräte werden vor ihrer Entsorgung gemäß den Richtlinien des Herstellers physisch vernichtet. Andere Abfälle werden gemäß den regulären Entsorgungsrichtlinien der Telekom Security entsorgt.

## 5.1.8 Externe Sicherung

Telekom Security führt routinemäßige Sicherungen von kritischen Systemdaten, Audit-Protokolldaten und anderen vertraulichen Informationen durch. Die Sicherungskopien werden räumlich getrennt von den Ursprungsdaten gelagert. Die Sicherungen werden von vertrauenswürdigen Rolleninhabern durchgeführt (siehe dazu Kapitel 5.2.1).

## 5.2 Organisatorische Sicherheitsmaßnahmen

Die organisatorischen Maßnahmen sind im Sicherheitskonzept niedergelegt und werden durch das Betriebskonzept des Trust Centers umgesetzt. Die relevanten Anforderungen aus [ETSI EN 319 401] Kap. 7.4 b, c, d, e sind umgesetzt und werden regelmäßig von einer Konformitätsbewertungsstelle gemäß eIDAS überprüft.

Die nachfolgende Aufzählung nennt einen Teil der organisatorischen Maßnahmen, aus unterschiedlichen Quellen, die zur Wahrung der Sicherheit getroffen wurden:

- Maßnahmen zur Ermittlung, Bewertung und regelmäßigen Überprüfung von Restrisiken sind im Sicherheitskonzept des Public Key Service enthalten.
- Die Bestimmungen zur Einbindung von externen Dienstleistern ist entsprechend den gültigen Gesetzen und Verordnungen in den Verträgen umgesetzt, so dass die Einhaltung von Sicherheitsmaßnahmen jederzeit vom Trust Center oder von externen Auditoren überprüft werden kann.
- Alle Mitarbeiter des Trust Centers sind verpflichtet die strengen internen Datenschutz- und Sicherheitsrichtlinien des Konzerns Deutsche Telekom AG einzuhalten.
- Die Systeme des Trust Centers werden regelmäßig auf sicherheitsrelevante Veränderungen untersucht. Alle sicherheitsrelevanten Veränderungen müssen vor Inbetriebnahme durch das Change Advisory Board des Trust Centers freigegeben werden.

## 5.2.1 Vertrauenswürdige Rollen

Zur Gewährleistung eines sicheren Betriebs verfügt der TSP über eine geeignete Organisation, in der die folgenden vertrauenswürdigen Rollen abgebildet sind:

- Leiter Trust Center: trägt die gesamte Verantwortung für alle Trust Services und berichtet an die Geschäftsführung der Telekom Security
- Leiter VDA: ist Ansprechpartner und Auskunftsperson für die nationalen Aufsichtsbehörden für die qualifizierten Vertrauensdienste
- Solution Manager: verantwortet und verwaltet einen Trust Service
- Trust Center Information Security Officer: hat die übergreifende Verantwortung für die Informationssicherheitsrichtlinie des Trust Center sowie die Implementierung von Sicherheitsmaßnahmen und berichtet an den Leiter Trust Center
- Trust Center Operator: prüft und bearbeitet Anträge zur Zertifikatsausstellung, -suspension, -sperrung oder -erneuerung
- System-Administrator, -Operator: installiert, konfiguriert und wartet die Systeme, kann Daten-Sicherungen und -Rücksicherungen durchführen
- interner Auditor: prüft regelmäßig sowie bei Unstimmigkeiten z.B. Protokolldaten, Datenbanken und papierbasierte Dokumentationen der Trust Services
- Compliance-Manager: prüft regelmäßig die den Trust Services zugrunde liegenden Anforderungen, stimmt diese mit den Solution Managern ab und koordiniert die erforderlichen Prüfungen durch externe Auditoren.

Vertrauenswürdige Personen sind alle Personen (Mitarbeiter, Auftragnehmer, und Berater) mit Zugang zu oder Kontrolle über Authentifizierungs- oder Kryptografische Abläufe, die erhebliche Auswirkungen auf Folgendes haben können:

- die Validierung von Informationen in Zertifikatsaufträgen,
- die Annahme, Ablehnung oder sonstige Bearbeitung von Zertifikatsaufträgen, Sperraufträgen oder Erneuerungsaufträgen,
- die Vergabe oder den Widerruf von Zertifikaten, einschließlich Personal, das Zugang und Zugriff auf die Datenbanksysteme hat,
- den Umgang mit Informationen von Antragstellern und Kartenherausgebern.

Vertrauenswürdige Personen sind insbesondere:

- Mitarbeiter des Trust Centers (z.B. Systemadministration),
- Mitarbeiter kryptografischer Abteilungen,
- Sicherheitspersonal,
- zuständiges technisches Personal und
- für die Verwaltung der vertrauenswürdigen Infrastruktur zuständige leitende Angestellte.

Dabei werden folgende Aufgaben zurzeit ganz oder teilweise durch Auftragnehmer oder unabhängige Dritte durchgeführt:

- Betrieb des Rechenzentrums (maximal bis auf Betriebssystemebene der IT-Systeme)
- Archivierung von Dokumenten in entsprechenden Hochsicherheitsarchiven

Die oben genannten vertrauenswürdigen Personen müssen die in diesem CP/CPS festgelegten Anforderungen erfüllen. Durch eine schriftliche Bestätigung (z. B. per E-Mail) akzeptieren diese Personen ihre zugewiesene(n) Rolle(n).

Ebenfalls müssen diese vertrauenswürdigen Personen frei von Interessenskonflikten gestellt werden, damit die ausgeübten Rollen unbefangen und vorurteilsfrei ausgeübt werden können. Das ISMS des Trust Centers ist verantwortlich für die Initiierung, Durchführung und Kontrolle der Methoden, Prozesse und Verfahren, die in den Sicherheitskonzepten und dem CP/CPS der vom Trust Center betriebenen Zertifizierungsstellen dargestellt werden.

## 5.2.2 Anzahl der für eine Aufgabe erforderlichen Personen

Die Aufrechterhaltung des Betriebs der Zertifizierungsstelle und des Verzeichnisdienstes (Administration, Sicherung, Wiederherstellung) wird von fachkundigen und vertrauenswürdigen Mitarbeitern wahrgenommen.

Arbeiten an hochsensitiven Komponenten (z.B. Schlüsselerstellungssystem, HSM) sind durch besondere interne Kontrollverfahren geregelt und werden von mindestens zwei Mitarbeitern durchgeführt. Der Kreis der Personen, die diese Tätigkeiten ausführen dürfen, ist auf ein Minimum reduziert. Das betrifft insbesondere alle Tätigkeiten mit Bezug zu privaten CA-Schlüsseln.

## 5.2.3 Identifizierung und Authentifizierung für jede Rolle

Mitarbeiter, die als besonders vertrauenswürdige Personen eingestuft sind und besonders vertrauenswürdige Tätigkeiten wahrnehmen, unterliegen einer internen Sicherheitsüberprüfung (siehe Kapitel 5.3.2).

Telekom Security stellt sicher, dass Mitarbeiter einen vertrauenswürdigen Status erlangt haben und die Zustimmung der Abteilung erteilt wurde, bevor diese Mitarbeiter:

- Zugangsgeräte und Zugang zu den erforderlichen Einrichtungen erhalten,
- die elektronische Berechtigung zum Zugriff auf die IT-Systeme erhalten,
- zur Durchführung bestimmter Aufgaben im Zusammenhang mit diesen Systemen zugelassen werden.

Die Mitarbeiter des Trust Centers werden nach positiver Prüfung formell vom Leiter des Trust Centers ernannt.

Die Vergabe der erforderlichen Berechtigungen erfolgt nach dem „Least Privilege“-Prinzip, d.h. alle Berechtigungen sind auf das erforderliche Minimum beschränkt.

Nach Beendigung des Arbeitsverhältnisses oder Wechsel der Tätigkeit eines Mitarbeiters in einer vertrauenswürdigen Rolle werden dessen Zugriffsberechtigungen innerhalb von 24 Stunden entzogen.

## 5.2.4 Rollen, die eine Aufgabentrennung erfordern

Die folgenden Rollen erfordern eine Aufgabentrennung und werden daher von verschiedenen Mitarbeitern begleitet:

- Antragsvalidierung und Antragsfreigabe,
- Sicherung und Rücksicherung von Datenbanken und HSMs,
- Key Lifecycle Management von CA- und Root-CA-Zertifikaten.

## 5.3 Personelle Sicherheitsmaßnahmen

Telekom Security setzt umfassende personelle Sicherheitsmaßnahmen um, die einen hohen Schutz ihrer Einrichtungen und der Zertifizierungsdienste gewährleisten. Im Trust Center ist der Einsatz von qualifiziertem geschultem Personal obligatorisch, die personellen Maßnahmen sind im Sicherheitskonzept niedergelegt.

Die Anforderungen aus [ETSI EN 319 401] Kap. 7.2 sind umgesetzt und werden sowohl in internen als auch in externen Audits geprüft. Das Personal unterliegt keinem Kostendruck oder Mengengerüst oder sonstigen Zwängen deren Einhaltung möglicherweise mit den Qualitätsanforderungen bei der Prüfung von Antragsunterlagen konkurrieren würde.

### 5.3.1 Anforderungen an Qualifikation, Erfahrung und Sicherheitsüberprüfung

Telekom Security verlangt von seinen Mitarbeitern, die eine vertrauenswürdige Rolle einnehmen sollen, entsprechende Nachweise über Qualifizierung und Erfahrung, die dazu notwendig sind, ihre voraussichtlichen beruflichen Pflichten kompetent und zufriedenstellend zu erfüllen.

In regelmäßigen Abständen sind ein neues Führungszeugnis sowie Schulungsnachweise der Telekom Security vorzulegen.

### 5.3.2 Sicherheitsüberprüfung

Vor dem Beginn der Beschäftigung in einer vertrauenswürdigen Rolle führt Telekom Security eine Sicherheitsüberprüfung mit folgendem Inhalt durch:

- Überprüfung und Bestätigung der bisherigen Beschäftigungsverhältnisse,
- Überprüfung von Arbeitszeugnissen,
- Bestätigung des höchsten oder maßgebenden Schul-/Berufsabschlusses,
- polizeiliches Führungszeugnis.

Sofern die in diesem Abschnitt festgelegten Anforderungen nicht erfüllt werden können, macht Telekom Security ersatzweise Gebrauch von einer gesetzlich zulässigen Ermittlungsmethode, die im Wesentlichen die gleichen Informationen liefert.

Ergebnisse einer Sicherheitsüberprüfung, die zu einer Ablehnung eines Anwärters für eine vertrauenswürdige Person führt, können beispielsweise sein

- falsche Angaben seitens des Anwärters oder der vertrauenswürdigen Person,
- besonders negative oder unzuverlässige berufliche Referenzen, und
- gewisse Vorstrafen.

Berichte, die solche Informationen enthalten, werden durch Mitarbeiter der Personalabteilung und Sicherheitspersonal bewertet, die das weitere angemessene Vorgehen festlegen. Das weitere Vorgehen kann Maßnahmen bis einschließlich zur Rücknahme des Einstellungsangebots an Anwärter für vertrauenswürdige Positionen führen oder der Kündigung von vertrauenswürdigen Personen beinhalten.

Die Verwendung von in einer Sicherheitsüberprüfung ermittelten Informationen zur Ergreifung solcher Maßnahmen unterliegt geltendem Recht.

### 5.3.3 Schulungs- und Fortbildungsanforderungen

Das Personal des Trust Centers besucht Fortbildungsmaßnahmen die zur kompetenten und zufriedenstellenden Erfüllung ihrer beruflichen Pflichten erforderlich sind. Telekom Security führt Unterlagen über diese Schulungsmaßnahmen.

Die Schulungsprogramme sind auf die individuellen Tätigkeitsbereiche abgestimmt und beinhalten u.a.:

- fortgeschrittene PKI-Kenntnisse,
- Verfahrensweisen nach ITIL,
- Datenschutz,
- Daten- und Fernmeldegeheimnis,
- Informationsschutz,
- Zutrittsschutz,
- Antikorruption,
- Sicherheits- und Betriebsrichtlinien und -verfahren der Telekom Security,
- Verwendung und Betrieb eingesetzter Hardware und Software,
- Meldung von und Umgang mit Störungen und Kompromittierungen und
- Verfahren für die Schadensbehebung im Notfall (Disaster Recovery) und Geschäftskontinuität (Business Continuity).

Mitarbeiter, welche mit der Validierung von Zertifikatsaufträgen befasst sind, erhalten zusätzlich Schulungen in den folgenden Bereichen:

- Richtlinien, Verfahren und aktuelle Entwicklungen zu Validierungsmethoden,
- Inhalte und insbesondere relevante Änderungen des vorliegenden CPS,
- Relevante Anforderungen und Vorgaben aus den Zertifizierungsnormen,
- Allgemeine Bedrohungs- und Angriffsszenarien bzgl. der Validierungsmethoden (z.B. Social Engineering)

### 5.3.4 Nachschulungsintervalle und -anforderungen

Das Personal der Telekom Security erhält im erforderlichen Umfang und spätestens nach Ablauf von 12 Monaten Auffrischungsschulungen und Fortbildungslehrgänge.

### 5.3.5 Häufigkeit und Abfolge der Arbeitsplatzrotation

Nicht anwendbar.

### 5.3.6 Sanktionen bei unbefugten Handlungen

Telekom Security behält sich vor, unbefugte Handlungen oder andere Verstöße gegen dieses CP/CPS und der daraus abgeleiteten Verfahren zu ahnden und entsprechende Disziplinarmaßnahmen einzuleiten. Diese Disziplinarmaßnahmen können Maßnahmen bis einschließlich der Kündigung beinhalten und richten sich nach der Häufigkeit und Schwere der unbefugten Handlungen.



### 5.3.7 Anforderungen an unabhängige Auftragnehmer

Telekom Security behält sich vor, unabhängige Auftragnehmer oder Berater zur Besetzung vertrauenswürdiger Positionen einzusetzen. Diese Personen unterliegen denselben Funktions- und Sicherheitskriterien wie Mitarbeiter der Telekom Security in vergleichbarer Position.

Diesem Personenkreis, der die in Kapitel 5.3.2 beschriebene Sicherheitsüberprüfung noch nicht abgeschlossen oder nicht erfolgreich durchlaufen hat, wird der Zugang zu den gesicherten Einrichtungen von Telekom Security nur unter der Bedingung gestattet, dass sie stets von vertrauenswürdigen Personen begleitet und unmittelbar beaufsichtigt werden.

### 5.3.8 Dokumentation für das Personal

Um die beruflichen Pflichten angemessen erfüllen zu können, stellt Telekom Security seinen Mitarbeitern alle dafür erforderliche Dokumente (Schulungsunterlagen, Verfahrensanweisungen) und Hilfsmittel zur Verfügung.

## 5.4 Aufzeichnung und Protokollierung wichtiger Ereignisse

Es ist im Loggingkonzept sowie im Installationshandbuch festgelegt, welche Daten und Ereignisse in welchen Abständen von wem aufgezeichnet werden. Darüber hinaus wird geregelt, wie lange die Protokolldaten gespeichert werden und wie sie vor Verlust und unbefugtem Zugriff geschützt werden. Es werden dabei die Anforderungen aus [ETSI EN 319 401] Kap. 7.10 umgesetzt.

Bei der Aufzeichnung und ggf. Auswertung der geloggtten Daten wird die Sensibilität der Daten berücksichtigt.

### 5.4.1 Art der aufgezeichneten Ereignisse

Generell enthalten alle Protokolleinträge mindestens das Datum und die Uhrzeit des Eintrags, einen Verweis auf die Person oder das System, welches den Eintrag generiert hat sowie eine Beschreibung des Ereignisses.

In der Zertifikatshistorie werden alle relevanten Ereignisse von der Antragstellung über die Registrierung, die Freigaben durch den Kartenherausgeber (Attributbestätigung), die Prüfungen durch den TSP, die Produktion, den Versand der Karten und PIN-Briefe bis zur Freischaltung durch den Antragsteller und ggf. der Sperrung erfasst und Integritätsgeschützt abgelegt.

Die Beantragung und Implementierung der CA-Zertifikate sowie OCSP- und CRL-Signer wird in einem schriftlichen Protokoll festgehalten. Im Protokoll werden neben den Ereignissen auch die agierenden Personen (Vier-Augen-Prinzip) sowie deren Rollen aufgeführt.

Die Produktionsschritte zur Erstellung der QSCD werden durch die im Produktionsprozesse beteiligten Personen (Vier-Augen-Prinzip) schriftlich auf einem Begleitformular zu jedem Produktionsjob protokolliert.

Zusätzlich werden vom Telekom Security Trust Center für den Betrieb der Infrastruktur alle sicherheitsrelevanten Ereignisse protokolliert. Das beinhaltet mindestens die folgenden Ereignisse:

- Erfolgreiche und erfolglose Zugriffsversuche auf Systeme der PKI,
- Durchgeführte Aktionen an und durch PKI- und sonstigen sicherheitsrelevanter Systeme,

- Änderungen an Sicherheitsprofil,
- Systemabstürze, Hardware-Ausfälle und andere Anomalien,
- Firewall- und Router-Aktivitäten,
- Zutritt und Verlassen von Einrichtungen des Trust Centers
- Ergebnisse von Netzwerkprüfungen (Schwachstellenüberprüfungen)
- Start und Beendigung des Loggingprozesses

## 5.4.2 Bearbeitungsintervall der Protokolle

Die erstellten Audit-Protokolle/Logging-Dateien werden permanent auf wichtige sicherheits- und betriebsrelevante Ereignisse untersucht. Ferner überprüft Telekom Security die Audit-Protokolle/Logging-Dateien auf verdächtige und ungewöhnliche Aktivitäten, als Folge von Unregelmäßigkeiten und Störungen.

Eingeleitete Maßnahmen, die als Reaktion aus der Auswertung von Audit-Protokollen/Logging-Dateien stammen, werden ebenfalls protokolliert.

## 5.4.3 Aufbewahrungszeitraum für Audit-Protokolle

Audit-Protokolle/Logging-Dateien werden nach Bearbeitung gemäß Kapitel [5.4.2](#) archiviert.

## 5.4.4 Schutz der Audit-Protokolle

Audit-Protokolle/Logging-Dateien werden gegen unbefugten Zugriff geschützt.

## 5.4.5 Sicherungsverfahren für Audit-Protokolle

Eine inkrementelle Sicherung von Audit-Protokollen/Logging-Dateien wird täglich durchgeführt.

## 5.4.6 Audit-Erfassungssystem (intern vs. extern)

Audit-Daten/Logging-Dateien von Anwendungs-, Netzwerk- und Betriebssystemebene werden automatisch erzeugt und aufgezeichnet. Manuell erzeugte Audit-Daten werden von Mitarbeitern der Telekom Security aufgezeichnet.

## 5.4.7 Benachrichtigung des Ereignis-auslösenden Subjekts

Ereignisse, die das Audit-Monitoringsystem erfasst, werden bewertet an das zuständige Trust Center Personal weitergeleitet. Ereignisse mit hoher Priorität werden unverzüglich auch außerhalb der Regelarbeitszeit an das Trust Center Personal weitergeleitet.

Sicherheitsvorfälle mit signifikanten Auswirkungen auf einen Trust Service oder auf personenbezogene Daten werden innerhalb von 24 Stunden an die zuständigen Behörden gemeldet, je nach Art und Kontext des Vorfalls.

## 5.4.8 Schwachstellenbewertung

Es erfolgt monatlich eine automatisierte Schwachstellenüberprüfung (Vulnerability-Scan). Mögliche Schwachstellen werden analysiert, bewertet und registriert. Basierend auf der Auswertung werden Maßnahmen festgelegt und in einem definierten Plan umgesetzt. Die Schwachstellenüberprüfungen, ihre Ergebnisse und Aktionen (Behebungen, Austausch, etc.) werden dokumentiert.

Kritische Schwachstellen werden über den ISMS-Prozess bearbeitet. Kritische Schwachstellen, die dem TSP mitgeteilt wurden, werden innerhalb von 48 Stunden vom ISMS-Team bewertet und ein Lösungsszenario aufgezeigt. Im Falle, dass eine umgehende und vollständige Beseitigung der Schwachstelle nicht möglich ist, wird ein Behandlungsplan erstellt, der die Minderung der kritischen Schwachstellen zum Inhalt hat.

Penetrationstest werden analog zu den Notfallübungen Dienstübergreifend geplant und koordiniert und finden mindestens einmal jährlich auf wechselnden Systemen statt. Um betriebliche Störungen zu vermeiden werden diese möglichst auf Testplattformen durchgeführt.

Sowohl Penetrationstest als auch Schwachstellenscan werden zusätzlich nach signifikanten System- und Netzwerkänderungen durchgeführt.

Zusätzlich werden einmal jährlich sogenannte Penetrationstests durchgeführt. Auch hier werden entsprechend Maßnahmen abgeleitet und umgesetzt, sofern dies notwendig ist. Die Penetrationstest und Schwachstellenscans werden von dafür geschultem Personal durchgeführt. Die eingesetzten Werkzeuge entsprechen dabei dem aktuellen Stand der Technik.

## 5.5 Archivierung von Daten

### 5.5.1 Art der archivierten Datensätze

Telekom Security archiviert folgende Daten:

- Antragsunterlagen in papiergebundener Form,
- alle Audit-/Event-Logging-Dateien, die gemäß Kapitel 5.4 erfasst werden.

### 5.5.2 Aufbewahrungszeitraum für archivierte Daten

Die Loggingdaten der TSP werden nicht dauerhaft archiviert und regelmäßig nach Auswertung gelöscht, im Sicherheitskonzept wird festgelegt, in welcher Weise und wie lange diese Daten aufbewahrt werden und wer darauf zugreifen darf.

Die Papierdokumente und elektronisch erfassten Antrags- und Zertifikatsdaten sowie die Daten der Zertifikatshistorie (Informationen über Beantragung, Änderung, Ausstellung, Freischaltung, ggf. Sperrung) werden über die Zertifikatsgültigkeit hinaus gemäß den gesetzlichen Anforderungen archiviert. Bei einer Zertifikatserneuerung verlängert sich die Aufbewahrungsfrist der ursprünglichen Dokumente und Daten entsprechend.

Die Kartenherausgeber können diese Daten über das Freigabeportal jederzeit einsehen. Die Antragsteller können die Daten bei Ihrer zuständigen Kammer einsehen oder schriftlich bei der Zertifizierungsstelle anfordern.

Die CA-Zertifikate sowie die von ihr ausgestellten Zertifikate und Sperrlisten werden nach Ablauf des Gültigkeitszeitraums archiviert.

### 5.5.3 Schutz von Archiven

Telekom Security stellt sicher, dass nur autorisierte und vertrauenswürdige Personen Zutritt zu Archiven erhalten. Archivdaten sind gegen unbefugte Lesezugriffe, Änderungen, Löschungen oder andere Manipulationen geschützt.

### 5.5.4 Sicherungsverfahren für Archive

Eine inkrementelle Sicherung der elektronischen Archive wird täglich durchgeführt.

### 5.5.5 Anforderungen an Zeitstempel von Datensätzen

Datensätze wie beispielsweise Zertifikate, Zertifikatssperrlisten, OSCP-Antworten, Logging-Dateien enthalten Informationen über Datum und Uhrzeit. Als Zeitquelle dient das Empfangssignal des DCF 77, aus dem die UTC abgeleitet wird. Die einzelnen Systeme gleichen die Systemzeit mit der Zeitquelle mehrmals am Tag ab.

### 5.5.6 Archiverfassungssystem (intern oder extern)

Telekom Security verwendet ausschließlich interne Archivierungssysteme.

### 5.5.7 Verfahren zur Beschaffung und Überprüfung von Archivinformationen

Nur autorisiertes und vertrauenswürdiges Personal erhält Zutritt zu Archiven und Zugang/Zugriff zu Archivdaten. Bei der Wiederherstellung der Archivdaten werden diese auf Authentizität verifiziert.

## 5.6 Schlüsselwechsel der Zertifizierungsstelle

Aufgrund der Nutzungsdauer der CA-Schlüssels ergibt sich die Notwendigkeit eines regelmäßigen Schlüsselwechsels. Dieser erfolgt zurzeit im dreijährigen Rhythmus. Es wird somit parallel mehrere gültige CA-Zertifikate geben.

Die Zertifizierungsstelle erzeugt rechtzeitig, vor Ablauf von CA-Zertifikaten, neue Zertifizierungsstellen-Schlüssel und beantragt neue CA-Zertifikate bei der entsprechenden Root-Zertifizierungsstelle, so dass neue CA-Zertifikate in der Regel mindestens zwei Wochen vor Ablauf der alten Zertifikate und Inbetriebnahme der neuen Zertifikate zur Verfügung stehen. Sollte wider Erwarten ein neues CA-Zertifikat nicht rechtzeitig bereitgestellt werden können, so wird vorübergehend bis zur Erstellung des neuen CA-Zertifikats das aktuelle CA-Zertifikat weiter für die Ausgabe von Teilnehmer-Zertifikaten verwendet und die Laufzeit der ausgestellten Zertifikate verkürzt.

## 5.7 Kompromittierung und Wiederanlauf nach einem Notfall

### 5.7.1 Umgang mit Störungen und Kompromittierungen

Telekom Security hat für das IT-Servicemanagement gemäß ITIL sowie für das ISMS Prozesse etabliert, über die Störungen und Sicherheitsvorfälle nach definierten Standard-Prozessen bearbeitet werden.

Durch die Festlegung aller erforderlichen Ansprechpartner und entsprechend eingerichteter Gruppen in den IT-Servicemanagement-System sowie der Etablierung einer Rufbereitschaft und des MoD (Manager on Duty) ist sichergestellt, dass die Bearbeitung von Störungen und Sicherheitsvorfälle kurzfristig beginnt, damit der Schaden möglichst gering bleibt und schnell beseitigt werden kann.

Betroffene Kunden werden sofern erforderlich schnellstmöglich informiert und in den Prozess eingebunden.

### 5.7.2 Beschädigung von EDV-Geräten, Software oder Daten

Bei einer Beschädigung der EDV-Komponenten, Software und/oder Daten wird der Vorfall unmittelbar untersucht und der Telekom Security Sicherheitsabteilung gemeldet. Das Ereignis initiiert eine entsprechende Eskalation, Störfalluntersuchung, Störfallreaktion bis hin zur finalen Störungsbeseitigung. Abhängig von der Störungsklassifizierung erfolgt die Wiederherstellung (Disaster Recovery).

Jegliche Hard- und Software, die zur Bereitstellung des Services erforderlich ist, wird als Vermögensgegenstand (Asset) und Anwendung im Konfigurationsmanagement der Telekom Security geführt.

### 5.7.3 Verfahren bei Kompromittierung von privaten Schlüsseln von Zertifizierungsstellen

Bei Kenntnisnahme über eine Kompromittierung privater Schlüssel von CA- oder Root-CA wird der Vorfall unmittelbar untersucht, beurteilt und die notwendigen Schritte eingeleitet.

Die betroffenen Beteiligten werden über die mögliche Kompromittierung schriftlich informiert. Falls erforderlich ist/sind das/die Zertifikate unverzüglich zu sperren und die entsprechenden Informationen an die Aufsichtsbehörde weiterzuleiten. Die Generierung neuer Schlüssel und Zertifikate ist gemäß den Arbeitsanweisungen zu dokumentieren und gemäß den Auflagen des jeweiligen Sicherheitskonzepts zu überwachen.

Von diesen Zertifikaten ausgestellte Benutzerzertifikate werden ebenfalls gesperrt. Die betroffenen Zertifikatsinhaber werden über die Sperrung informiert. Auskünfte zum Sperrstatus von Enduser-Zertifikaten sowie die Enduser-Zertifikate, die auf kompromittierten privaten Schlüsseln basieren sind unter Umständen nicht mehr gültig.

### 5.7.4 Geschäftskontinuität nach einem Notfall

Telekom Security hat für den Rechenzentrumsbetrieb einen Notfallplan entwickelt, implementiert und getestet, um die Auswirkungen von Katastrophen jeder Art (Naturkatastrophen oder Katastrophen menschlichen Ursprungs) zu mildern und die Verfügbarkeit kritischer Geschäftsprozesse schnellstmöglich wiederherzustellen. Dies umfasst auch alle Prozesse, Komponenten, Systeme und Dienste des Trust Centers. Dieser Plan wird mindestens jährlich

überprüft, getestet und entsprechend aktualisiert, um im Falle einer Katastrophe gezielt und strukturiert reagieren zu können.

Der Notfallplan enthält mindestens die folgenden Informationen:

- Die notwendigen Kriterien für die Aktivierung des Planes
- Mögliche Notfallmaßnahmen (je nach Situation)
- Benennung aller beteiligten Rollen und Eskalationsstufen
- Ausweichverfahren
- Wiederanlauf Verfahren
- Prozedur zur regelmäßigen Pflege, Aktualisierung und Weiterentwicklung
- Sensibilisierungsmaßnahmen
- Anforderungen an Aus- und Weiterbildung des betroffenen Personals
- Prozesse zur optionalen Einbindung des BSI in dessen Rolle als nationales CSIRT zur Unterstützung bei Notfall- oder Krisensituationen
- Wiederanlaufzeit
- Review-Zyklen des Notfallplans (mindestens jährlich)
- Regelmäßige Durchführung des Notfallplans zu Testzwecken (mindestens jährlich)
- Eine Prozedur zur Aufrechterhaltung oder fristgerechten Wiederherstellung der Geschäftstätigkeit nach Unterbrechung oder Ausfall kritischer Geschäftsprozesse
- Vorgaben zum regelmäßigen Backup aller relevanten Daten, die zur Wiederaufnahme des CA-Betriebs nach einem Notfall erforderlich sind, an sicheren, entfernt auseinander liegenden Orten, dazu zählen auch die Integritätsprüfung der Backups sowie regelmäßige dokumentierte Wiederherstellungstests.
- Eine Verpflichtung kritische kryptographische Geräte und Informationen an einem anderen Standort zu sichern bzw. vorzuhalten.
- Festlegung der maximal tolerierbaren Ausfallzeit und entsprechende Zeiten zur Wiederherstellung
- Häufigkeit, in der von kritischen Geschäftsinformationen und eingesetzter Software inkl. deren Konfiguration Sicherungskopien erstellt werden
- Räumliche Entfernung des oder der Ausweichstandorte bzw. -Einrichtungen zur Hauptgeschäftsstelle bzw. zum Rechenzentrum des Trust Centers
- Verfahren zur bestmöglichen Sicherung der Betriebsstätten und –Einrichtungen nach einer Katastrophe (Notbetrieb) bis zur Wiederherstellung eines den Anforderungen entsprechend gesicherten Normalbetriebs
- Nachbereitung inkl. Ursachenermittlung zur Vermeidung von Wiederholungen

Im Rahmen eines Compliance-Audits (siehe Kapitel 8) ist der Auditor berechtigt, die Details des Notfallplanes einzusehen.

## 5.8 Einstellung der Zertifizierungsdienste

Eine Betriebsbeendigung kann nur durch Telekom Security ausgesprochen werden. Es werden wirtschaftlich angemessene oder einzelvertraglich zugesagte Anstrengungen unternommen, Betroffene vorab über diese Betriebsbeendigungen zu informieren.

Im Falle der Einstellung des Zertifizierungsdienstes geht die Zertifizierungsstelle entsprechend den Vorgaben aus [ETSI EN 319 401] Kap. 7.12 vor und hat dafür einen Beendigungsplan erstellt, der folgende Maßnahmen beschreibt:

- Benachrichtigung der Endteilnehmer und vertrauenden Dritten über die geplante Einstellung des Dienstes inkl. einer Beschreibung möglicher Verfahren zum evtl. Abruf bzw. der Bereitstellung archivierter Daten,
- Fortführung der Sperrfunktionalitäten einschließlich der regelmäßigen Erstellung von Sperrlisten, Abruf der Zertifikatsstatusinformationen und Service Desk-Funktionen,
- Sperrung von ausgegebenen CA-Zertifikaten,
- eventuell erforderliche Übergangsregelungen auf eine Nachfolge-CA,

- je nach Ausgestaltung bestehender Einzelverträge entstehende Kostenerstattung,
- Aufbewahrung der Unterlagen und Archive der Zertifizierungsstelle

Vor der Einstellung des Dienstes werden alle möglichen Maßnahmen getroffen, um den potentiellen Schaden für alle Beteiligten möglichst gering zu halten, alle Beteiligten werden so früh wie möglich informiert.

Alle Rechte der Mitarbeiter der Zertifizierungsstelle und der Registrierungsstellen werden entzogen, die privaten Schlüssel der CA werden vernichtet. Alle noch Zertifikate werden gesperrt.

Alle elektronisch erfassten Daten mit Ausnahme der Zertifikate und Sperrlisten werden gelöscht. Die Zertifikate und Sperrlisten sowie Papierdokumente werden gem. Kap. 5.5 archiviert, um ggf. zur Beweissicherung in Gerichtsprozessen darauf zugreifen zu können.

## 6 Technische Sicherheitsaspekte

Die technischen Sicherheitsmaßnahmen sind in einem Sicherheitskonzept nach IT-Grundschutz festgelegt, deren Wirksamkeit ist auf Basis einer Bedrohungsanalyse nachgewiesen. Es werden die Vorgaben aus [ETSI EN 319 401] Kap. 7.5 umgesetzt.

### 6.1 Erzeugung und Installation von Schlüsselpaaren

#### 6.1.1 Generierung von Schlüsselpaaren

Alle für die End-Entity-, CA- und Signer-Zertifikate generierten Schlüssel müssen kryptografischen Mindestanforderungen genügen. Die zu verwendenden Algorithmen und Schlüssellängen werden durch die Spezifikationen der gematik vorgegeben. Für die qualifizierten Zertifikate gelten darüber hinaus die Anforderungen an Signaturschlüssellängen und Algorithmen gemäß eIDAS.

Es werden folgende kryptografischen Algorithmen und Schlüssellängen verwendet:

- X509 nonQES-CA- und EE-Zertifikate
  - G2: RSA-2048 + SHA256
  - G2.1: RSA-2048 + SHA256, ECDSA + SHA256 (Brainpool-256)
- X509 QES-CA und EE-Zertifikate:
  - G2: RSA-2048 + SHA256
  - G2.1: RSA-2048 + SHA256, ECDSA + SHA256 (Brainpool-256)
- CVC-CA- und EE-Zertifikate
  - G2: ECDSA + SHA256 (Brainpool-256)

##### 6.1.1.1 Root- und CA-Zertifikate

Die CVC- und nonQES-Root-Zertifikate werden nicht durch Telekom Security betrieben und daher hier nicht weiter beschrieben. Es wird dazu auf die Vorgaben der jeweiligen Betreiber der Root-CAs verwiesen, welche durch den TSP eingehalten werden.

Die QES-Root-Zertifikate werden von Telekom Security ebenfalls im hochsicheren Bereich des Trust Centers selbst betrieben, es gelten dazu die gleichen nachfolgenden Anforderungen wie für die CA-Zertifikate. Für die Root-CAs der Telekom Security wird ausschließlich eine Offline-CA ohne jegliche Netzwerkverbindung genutzt. Dementsprechend werden die Daten zwischen der QES-Root-CA und der HBA-CA manuell per Datenträger, mindestens im Vier-Augen-Prinzip, ausgetauscht und somit die Integrität und Vertraulichkeit gewährleistet.

Die Schlüssel der CA-Zertifikate werden auf Hardware Security Modules (HSM) erzeugt und gespeichert. Die Module sind nach FIPS 140-2 (CA- und non-QES-OCSP-/CRL-Signer-Zertifikate) oder CC EAL4+ (QES-OCSP-Signer-Zertifikate) evaluiert und entsprechen dem Stand der Technik.

Die Generierung der Schlüssel und Installation der Zertifikate erfolgt in einer dokumentierten Key-Zeremonie, mindestens im Vier-Augen-Prinzip von geschultem und vertrauenswürdigen Fachpersonal (Trusted Roles) in der gesicherten Umgebung des Trust Centers. An der Key-Zeremonie nehmen mindestens ein Verantwortlicher für die technische Abwicklung (Trust-Center-Administrator sowie ggf. zusätzlich der verantwortliche Operations-Manager) sowie ein Verantwortlicher für die organisatorische Abwicklung (Leiter VDA oder ein von ihm benannter Stellvertreter) teil. Die Generierung von QES-CA- oder Root-Zertifikaten erfolgt darüber hinaus in Anwesenheit mindestens eines weiteren unabhängigen Auditors.



Die Key-Zeremonie besteht aus mehreren Schritten:

1. gemeinsame Prüfung der Antragsunterlagen und Vorgaben für die zu erstellenden Schlüssel (Schlüssellängen, Algorithmen, zu nutzende Schlüsselgeneratoren und Speichermedien) durch alle o.g. Anwesenden.
2. Generierung der Schlüssel und des PKCS#10-Requests durch einen Trust Center Administrator unter der Kontrolle der weiteren Anwesenden.
  - a. Generierung des Hashwertes des PKCS#10-Requests durch den Trust Center Administrator unter der Kontrolle der weiteren Anwesenden.
  - b. Übertragung des Hashwerts in die Antragsunterlagen und Protokolle durch den Leiter VDA oder den von ihm benannten Stellvertreter unter der Kontrolle der weiteren Anwesenden.
3. Übergabe des Requests an die Root-CA entsprechend den Vorgaben des Root-CA-Betreibers durch den Leiter VDA oder den von ihm benannten Stellvertreter.
4. Entgegennahme des CA-Zertifikats vom Root-CA-Betreiber entsprechend den Vorgaben des Root-CA-Betreibers durch den Leiter VDA oder den von ihm benannten Stellvertreter.
5. Überprüfung des CA-Zertifikats durch den Trust Center Administrator sowie den Leiter VDA oder den von ihm benannten Stellvertreter, sowie den verantwortlichen Operations-Manager.
6. Inbetriebnahme des CA-Zertifikats durch den Trust Center Administrator im Beisein des verantwortlichen Operations-Managers und ggf. darüber hinaus in Anwesenheit des Leiters VDA oder den von ihm benannten Stellvertreter, sowie eines unabhängigen Prüfers bei QES-Zertifikaten.

Die Key-Zeremonie wird protokolliert, das Protokoll enthält mindestens folgende Angaben:

- Auftraggeber (intern/extern),
- anwesende(r) Vertreter des Auftraggebers,
- anwesende(r) Verantwortliche(r) für die technische Abwicklung,
- anwesende(r) Verantwortliche(r) für die organisatorische Abwicklung,
- technische Daten des ausstellenden Zertifikats (sofern relevant),
- technische Daten des zu erstellenden Zertifikats,
- PKCS#10-Request des zu erstellenden Zertifikats,
- verwendete Module zur Schlüsselerzeugung,
- Angaben zur Veröffentlichung des zu erstellenden Zertifikats,
- Angaben zu einer optionalen Videoaufzeichnung der Root-Zeremonie.

Das Protokoll wird in den einzelnen Abschnitten zu den o.g. Schritten durch die in den jeweiligen Schritten beteiligten Personen unterzeichnet. Hinweis: Bei den nonQES- und CVC-CA-Zertifikaten kann anstelle des unterschriebenen Protokolls die Key-Zeremonie auch im Change-Management-Tool elektronisch dokumentiert werden. In diesem Fall wird dazu ein Change mit entsprechenden Tasks für jeden Schritt erstellt und von den für die Tasks Verantwortlichen quittiert.

▪

Die CA-Zertifikate werden mit Inbetriebnahme in den Verzeichnissen veröffentlicht, siehe dazu auch Kap. 2.

### 6.1.1.2 End-Entity-Zertifikate

[HBA] Als Schlüsselmedium der HBA kommen ausschließlich zertifizierte QSCD zum Einsatz. Die Schlüssel der HBA werden im Rahmen der Kartenproduktion durch evaluierte Schlüsselgeneratoren auf der jeweiligen Karte selbst erzeugt. Die Gültigkeit der Zertifizierung der eingesetzten QSCD wird regelmäßig, sowie bei Bedarf in den internen und externen Audits (siehe Kap. 8), geprüft. Vor Ablauf einer Zertifizierung wird rechtzeitig der Einsatz einer anderen zertifizierten QSCD geplant und umgesetzt.

Sollte eine QSCD vor dem geplanten Ablauf ihre Zertifizierung verlieren, so wird dies als Sicherheitsvorfall gemäß Sicherheitsvorfall- und Notfallhandbuch bearbeitet.

[SMC-B] Als Schlüsselmedium der SMC-B kommen ausschließlich von der gematik zugelassene Smartcards zum Einsatz. Die Schlüssel der SMC-B werden im Rahmen der Kartenproduktion durch Schlüsselgeneratoren auf der jeweiligen Karte selbst erzeugt.

[SM-B] Als Schlüsselmedium kommen HSM zum Einsatz, die bei den antragstellenden Organisationen betrieben werden, d.h. die Schlüsselgenerierung obliegt den Antragstellern.

### 6.1.2 Zustellung privater Schlüssel an Endteilnehmer

Es gelten die Regelungen gemäß Kap. 4.4.

### 6.1.3 Zustellung öffentlicher Schlüssel an Zertifikatsaussteller

[HBA] [SMC-B] Es gelten die Regelungen gemäß Kap. 4.3.1.

[SM-B] Es gelten die Regelungen gemäß Kap. 3.2.1.

### 6.1.4 Zustellung öffentlicher CA-Schlüssel an Vertrauende Dritte

Die CA-Zertifikate werden in einem LDAP-Verzeichnis veröffentlicht, es gelten die Regelungen gemäß Kap. 2.

### 6.1.5 Schlüssellängen

Alle im Umfeld der Karten verwendeten Schlüssel und kryptografischen Algorithmen entsprechen den Vorgaben aus [gemSpec\_Krypt], welche wiederum auf den Vorgaben von BSI und BNetzA basieren. Alle Schlüssellängen werden vor Ausstellung eines Zertifikats überprüft.

### 6.1.6 Generierung der Parameter von öffentlichen Schlüsseln und Qualitätskontrolle

[HBA] [SMC-B] Die Qualität der Schlüssel wird dadurch gewährleistet, dass ausschließlich evaluierte Schlüsselgeneratoren (FIPS 140-2 oder CC EAL4+) zum Einsatz kommen, siehe Kap. 6.1.1.

[SM-B] Die Qualität der Schlüssel wird durch den TSP geprüft (Lint-Server).

## 6.1.7 Schlüsselverwendungen

Siehe Kapitel 7.1.

## 6.2 Schutz der privaten Schlüssel und der kryptografischen Module

Die Zertifizierungsstelle hat physikalische, organisatorische und prozessuale Mechanismen implementiert, um die Sicherheit von CA-Schlüsseln gewährleisten zu können.

Die Antragsteller sind verpflichtet, alle erforderlichen Vorkehrungen zu treffen, um den Verlust oder die unberechtigte Nutzung von privaten Schlüsseln zu verhindern.

### 6.2.1 Standards und Kontrollen für kryptografische Module

Die zur Generierung und Speicherung der geheimen Signaturschlüssel der Zertifizierungsstelle eingesetzten Module sind nach FIPS 140-2 oder CC EAL4+ evaluiert. Zudem wird sichergestellt, dass diese korrekt funktionieren.

Die Sicherung der Schlüssel der CA-Zertifikate wird unter Verwendung hochwertiger Mehrpersonen-Sicherungstechniken (siehe auch Kapitel 6.2.2) durchgeführt.

Zum Schutz der kryptografischen Geräte während Betrieb, Transport und Lagerung werden die herstellereigentlichen Mechanismen verwendet, die während der FIPS- und CC-Zertifizierungen geprüft wurden. Die Geräte werden hierbei getrennt von den zum Betrieb und zur Nutzung benötigten PED-Keys aufbewahrt, so dass die Kompromittierung einer einzelnen Lokation nicht ausreicht, um die Geräte missbräuchlich zu verwenden.

### 6.2.2 Mehrpersonenkontrolle (m von n) bei privaten Schlüsseln

Die Zertifizierungsstelle hat technische, organisatorische und prozessuale Mechanismen implementiert, die die Teilnahme mehrerer vertrauenswürdiger und geschulter Personen des Telekom Security Trust Centers (Trusted Roles) erfordern, um vertrauliche kryptografische CA-Operationen durchführen zu können. Die Verwendung des privaten Schlüssels wird durch einen geteilten Authentisierungsprozess (Trusted Path Authentication mit Key) geschützt. Jede am Prozess beteiligte Person verfügt über Geheimnisse, die nur in der Gesamtheit bestimmte Arbeiten ermöglichen.

### 6.2.3 Hinterlegung von privaten Schlüsseln

Eine Hinterlegung von privaten Schlüsseln bei Treuhändern außerhalb der Zertifizierungsstelle wird nicht durchgeführt.

### 6.2.4 Sicherung von privaten Schlüsseln

Die Zertifizierungsstelle behält für Wiederherstellungs- und Notfallzwecke Sicherungskopien (Back-Up) des Schlüsselmaterials aller CA-Zertifikate vor. Diese Schlüssel werden in

verschlüsselter Form innerhalb des kryptografischen Hardware-Moduls (HSM) und zugehörigen Schlüsselspeichergeräten gespeichert.

[HBA] [SMC-B] Aufgrund der ausschließlichen Nutzung von QSCD für HBA und von der gematik zugelassenen Smartcards für die SMC-B können keine privaten Schlüssel der Karten gesichert werden.

[SM-B] Eine eventuelle Sicherung der auf den HSM der Antragsteller erzeugten SM-B-Schlüssel obliegt den Antragstellern.

## 6.2.5 Archivierung von privaten Schlüsseln

Wenn die privaten CA-, OCSP- oder CRL-Signer-Schlüssel das Ende ihrer Gültigkeitsdauer erreicht haben, werden sie vernichtet. Eine Archivierung findet nicht statt.

Die Zertifizierungsstelle bietet keine Archivierung privater Schlüssel der HBA an.

## 6.2.6 Übertragung privater Schlüssel in oder von einem kryptografischen Modul

Die CA-Schlüssel der CA- sowie der OCSP- und -CRL-Signer werden auf den kryptografischen Hardware-Modulen (HSM) im Online-Betrieb generiert, eine Übertragung in andere kryptografische Module erfolgt gemäß Kap. 6.2.1 und 6.2.4.

## 6.2.7 Speicherung privater Schlüssel auf kryptografischen Modulen

Die Zertifizierungsstelle speichert CA-Schlüssel in sicherer Form auf kryptografischen Hardware-Security-Modulen (HSM), welche nach FIPS 140-2/ Level 3 oder CC EAL4+evaluiert sind.

## 6.2.8 Methode zur Aktivierung privater Schlüssel

Alle Antragsteller, Registratoren, Administratoren und Operatoren müssen die Aktivierungsdaten (z.B. PIN, Importpasswort) für ihren privaten Schlüssel gegen Verlust, Diebstahl, Änderung, Offenlegung und unbefugte Nutzung gemäß des vorliegenden CPS schützen.

Für Antragsteller gelten die Regelungen gemäß Kap. 4.1.2.2 zum Schutz der privaten Schlüssel.

Die Administratoren und TCOP müssen zum Schutz der privaten Schlüssel folgende Vorgaben einhalten:

- Festlegung eines Passworts bzw. einer PIN (gemäß Kapitel 6.4.1) oder Integration einer gleichwertigen Sicherheitsmaßnahme, um den Administrator oder Operator vor der Aktivierung des privaten Schlüssels zu authentisieren. Dies kann z. B. auch ein Kennwort zum Betrieb des privaten Schlüssels, ein Windows Anmelde- oder Bildschirmschoner-kennwort, ein Anmeldekennwort für das Netzwerk beinhalten.
- Ergreifung geeigneter Maßnahmen zum physischen Schutz des Administrator- oder Operator-Arbeitsplatzes vor unberechtigtem Zugriff.

Das Schlüsselmaterial für CA-Zertifikate wird entsprechend der Möglichkeiten der kryptographischen Hardware-Module (HSM) durch die autorisierten Personen aktiviert, siehe Kap.6.2.2.

Der zum CA-Zertifikat gehörende privaten Schlüssel bleibt aktiv bis das Zertifikat die Gültigkeit verliert oder ein Sperrgrund vorliegt

### 6.2.9 Methode zur Deaktivierung privater Schlüssel

Die Deaktivierung privater Schlüssel von Administratoren und TCOP erfolgt ereignisbezogen und obliegt dem Personal der Zertifizierungsstelle.

Für die Deaktivierung von privaten Schlüsseln einer Karte oder einer SM-B ist der Antragsteller verantwortlich.

Private CA-Schlüssel werden, wenn sie nicht mehr verwendet werden sollen, prinzipiell vernichtet (siehe Kap. 6.2.10) und in keinem Fall deaktiviert.

### 6.2.10 Methode zur Vernichtung privater Schlüssel

Die Vernichtung von CA-Schlüsseln erfordert die Teilnahme mehrerer vertrauenswürdiger Personen (Trusted Roles) des Trust Centers. Dabei ist sicherzustellen, dass nach Vernichtung keine Fragmente des Schlüssels übrigbleiben, die zu einer Rekonstruktion des Schlüssels führen könnten. Telekom Security verwendet zur sicheren Schlüsselvernichtung eine integrierte Löschfunktion des HSM.

Die Vernichtung privater Karten- oder SM-B-Schlüssel obliegt dem Antragsteller selbst.

### 6.2.11 Bewertung kryptografischer Module

Siehe Kap. 6.2.1.

## 6.3 Weitere Aspekte der Schlüsselverwaltung

### 6.3.1 Archivierung öffentlicher Schlüssel

Die Zertifizierungsstelle sichert und archiviert im Rahmen regelmäßiger Sicherungsmaßnahmen die Zertifikate (CA-, OCSP- und CRL-Signer- sowie Karten-Zertifikate).

### 6.3.2 Gültigkeitsdauer von Zertifikaten und Schlüsselpaaren

Das Gültigkeitsmodell basiert mit Ausnahme der QES-Zertifikate auf dem Schalenmodell, d.h. jedes Zertifikat ist maximal so lange gültig, wie das darüber liegende, ausstellende Zertifikat gültig ist.

Für die ausgegebenen QES-Zertifikate gilt abweichend das Kettenmodell.

Eine Rezertifizierung der Schlüssel wird nicht durchgeführt, so dass die Verwendungsdauer der privaten Schlüssel die Gültigkeitsdauer des Zertifikates nicht überschreitet.

## 6.4 Aktivierungsdaten

### 6.4.1 Generierung und Installation von Aktivierungsdaten

Zur Inbetriebnahme der CA- sowie OCSP- und CRL-Signer gelten die Anforderungen aus Kap. 6.1.

[HBA] [SMC-B]

Die Karten werden im Rahmen der Produktion mit PINs und PUKs versehen, es gibt dabei je nach Kartentyp und Sektor unterschiedliche Vorgaben:

- [HBA] Die HBA werden immer mit einer 5-stelligen Transport-PIN produziert, welche vor Nutzung der Karte in eine mindestens 6-stellige Wirk-PIN geändert werden muss
- [SMC-B] Die SMC-B können abhängig von den Sektoren spezifischen Vorgaben entweder mit einer Transport-PIN (s.o. analog zu HBA) oder direkt mit einer Wirk-PIN produziert werden

Die Karten und die zur Aktivierung benötigten PIN-Briefe werden separat und zeitversetzt dem Antragsteller zugesendet.

[SM-B]

Die Generierung und Installation von Aktivierungsdaten obliegt den Antragstellern, welche die HSM mit den SM-B-Schlüsseln betreiben.

### 6.4.2 Schutz von Aktivierungsdaten

Die Trust Center Administratoren bzw. von Telekom Security autorisierten Personen verpflichten sich, die Geheimnisanteile für die Aktivierung der privaten Schlüssel der CA- und OCSP- und CRL-Signer-Zertifikate zu schützen.

[HBA] [SMC-B] Die zur Aktivierung der Karten benötigten PINs werden in speziellen PIN-Briefen, welche eine Lesbarkeit der PINs durch geschlossene Umschläge verhindern, versendet.

[SM-B] Die zur Aktivierung der SM-B Schlüssel erforderlichen Aktivierungsdaten werden durch die Antragsteller generiert und verbleiben auch ausschließlich dort, somit sind die Antragsteller selbst verantwortlich für deren Schutz.

### 6.4.3 Weitere Aspekte von Aktivierungsdaten

Sofern Aktivierungsdaten für private Schlüssel, unabhängig vom Übertragungsmedium, übertragen werden, müssen die Trust Center-Administratoren die Übertragung mithilfe von Methoden zum Schutz gegen Verlust, Diebstahl, Änderung, unbefugter Offenlegung oder Nutzung dieser privaten Schlüssel strengstens schützen.

## 6.5 Sicherheitsbestimmungen für Computer

Die Sicherheitsmaßnahmen für Computer der Zertifizierungsstelle (z.B. Netzwerksicherheit, Zugriffskontrolle, Überwachung etc.) sind im Sicherheitskonzept beschrieben. Es werden die Vorgaben aus [ETSI EN 319 401] Kap. 7.4 umgesetzt.

Im Trust Center von Telekom Security kommen ausschließlich Systeme zum Einsatz, die für die Verwendung in Rechenzentren vorgesehen sind. Auf den Systemen sind, zusätzlich zum Betriebssystem, nur die für den Betrieb notwendigen Softwarekomponenten installiert. Auch für Dienste, Accounts, Protokolle und Ports gilt, dass nur aktiviert ist, was für den Betrieb erforderlich ist.

Die Systeme für Entwicklung, Test und Produktion sind vollkommen getrennt voneinander aufgebaut, sie befinden sich auf unterschiedlicher Hardware in verschiedenen Netzsegmenten, so dass eine gegenseitige Beeinflussung ausgeschlossen ist.

### 6.5.1 Spezifische technische Anforderungen an die Computersicherheit

Telekom Security stellt sicher, dass die Verwaltung der CA-Systeme, Verzeichnisdienste und OCSP-Responder vor unbefugtem Zugriff Dritter gesichert ist. Die Komponenten sind räumlich und logisch von anderen Systemen getrennt und sind nur von autorisiertem Personal zugänglich. Es werden aktuelle Schutzmechanismen (z.B. Firewalls, Zutrittsschutz, 4-Augen-Prinzip) eingesetzt, um die Komponenten vor internen und externen Eindringlingen zu schützen. Der direkte Zugriff auf CA- und OCSP-Responder-Datenbanken, welche die CA- und OCSP-Responder-Funktionalitäten unterstützen, ist auf geeignetes, geschultes und vertrauenswürdigen Betriebspersonal beschränkt.

Die Sicherheitsmaßnahmen umfassen

- Physikalische Sicherheit und Sicherung der Umgebung,
- die Systeme werden mit einem Integritätsschutz versehen, der, sofern anwendbar, vor Viren, sonstigem Schadcode und dem Einspielen unerlaubter Software schützt und mindestens täglich aktualisiert wird,
- Maßnahmen zur Gewährleistung der Nutzbarkeit von Datenträgern (Schutz vor Veralterung und Nichtlesbarkeit)
- Netzwerksicherheit und Firewall Management, inklusive Portsperrern und IP-Adressfilterung,
- Benutzerverwaltung der Accounts (alle Accounts der Mitarbeiter sind persönliche Accounts),
- Berechtigungsmatrix, Aufklärung, Sensibilisierung und Schulung/Ausbildung,
- Verfahrenskontrollen, Aktivitätsprotokollierung und Abschaltung bei Timeouts,
- Festlegung und Umsetzung einer Passwort-Policy für alle relevanten Systeme und Komponenten,
- Beschränkung des Zugriffs auf die Systeme und Daten auf die für diese Rollen identifizierten und authentifizierten Personen (siehe Kap. 5.2.3) mit den minimal erforderlichen Berechtigungen.

Arbeitsplätze, an denen die Ausstellung von Zertifikaten autorisiert wird, werden durch Multi-Faktor-Authentisierung abgesichert.

Administrative Remote-Zugriffe auf kritische Systeme werden nur dann zugelassen, wenn diese von Systemen ausgehen, die dem TSP gehören oder vom TSP kontrolliert werden und die temporär über einen verschlüsselten Kanal auf Basis einer Multifaktor-Authentisierung gegenüber einem gesicherten System im Netzwerk des TSP aufgebaut werden, welches die Verbindung zu den kritischen Systemen vermittelt.

Für nicht-administrative Remote-Zugriffe werden hinreichende Sicherheitsmaßnahmen getroffen, um die außerhalb der Räume des TSP abgerufenen, verarbeiteten oder gespeicherten Informationen angemessen zu schützen.

Die Vorgaben für Remote-Zugriffe sind in entsprechenden Policies festgelegt.

## 6.5.2 Bewertung der Computersicherheit

Im Rahmen der Sicherheitskonzepte werden unterschiedliche Bedrohungsanalysen durchgeführt, die die Wirksamkeit aller getroffenen Maßnahmen untersucht.

## 6.6 Technische Kontrollen des Lebenszyklus

### 6.6.1 Systementwicklungskontrollen

Es wird Software renommierter Hersteller eingesetzt, welche die für die Entwicklung von IT-Sicherheitssystemen üblichen Sicherheitsmaßnahmen beachten und langjährige Erfahrung in diesem Umfeld aufweisen.

Bereits in der Entwurfs- und Anforderungsspezifikationsphase eines Systementwicklungsprojekts erfolgt eine Analyse der Sicherheitsanforderungen, um sicherzustellen, dass die Sicherheit der Systeme von vornherein berücksichtigt wird.

Telekom Security hat Mechanismen und Kontrollen implementiert, um eingekaufte, entwickelte oder veränderte Software auf Schadelemente oder bösartigen Code (z.B. Trojaner, Viren) überwachen und schützen zu können. Die Integrität wird vor der Installation manuell verifiziert.

Neue Versionen der Software (geplante Updates) oder Fehlerbeseitigungen (kurzfristige Bugfixes) werden zunächst auf einem Entwicklungssystem des Herstellers/Entwicklers bereitgestellt und getestet.

Nach Prüfung erfolgt die Installation auf dem Telekom Security Testsystem. Erst nach ausgiebigen und erfolgreichen Tests erfolgt die Installation auf dem Telekom Security Wirksystem.

Das bei der Telekom Security etablierte Change-Management findet Anwendung.

### 6.6.2 Sicherheitsverwaltungskontrollen

Telekom Security hat Mechanismen und/oder Richtlinien implementiert, um die Konfiguration seiner CA-Systeme kontrollieren und überwachen zu können. Die Integrität wird vor der Installation manuell verifiziert.

Die Systemkonten (System Accounts) der Trust-Center-Administratoren werden spätestens nach 90 Kalendertagen überprüft. Nicht mehr benötigte Accounts werden deaktiviert.

Auf den Systemen des Trust Centers werden Betriebssysteme eingesetzt, die die Durchsetzung von Sicherheitseinstellungen unterstützen. Keines der Systeme kann ohne Benutzeranmeldung verwendet werden. Sicherheitskritische Einstellungen (beispielsweise Nutzkonten)



können nur im Vier-Augen-Prinzip verändert werden. Die Durchsetzung der Zugangsbeschränkungen an den Systemen wird durch die umgesetzte restriktive Passwort Policy unterstützt.

Besonders sicherheitskritische Applikationen (beispielsweise die Zertifikatsgenerierung) erfordern zusätzliche Authentisierungen des Bedieners im Trust Center.

Die eingesetzte Software wird laufend auf neu bekannt gewordene Schwachstellen durch Auswertung von Informationen aus geeigneten Quellen, z.B. der „Computer Emergency Response Teams“ (CERT) sowie der Hersteller, überprüft. Sofern sich bei der eingesetzten Software neue Schwachstellen ergeben, so werden diese bewertet werden und, sofern erforderlich, geeignete Maßnahmen zur Behebung oder Minimierung getroffen.

Telekom Security hat insbesondere Mechanismen zum Schutz des Sperrstatus-Dienstes (CRL, ARL, OCSP) gegen unbefugte Versuche implementiert, um Manipulationen an Sperrstatusinformationen (hinzufügen, löschen, ändern) zu verhindern. Diese Sicherungsmechanismen unterliegen der Überwachung des Alarmierungssystems, so dass eine permanente Überwachung der Konfiguration erfolgt. Darüber hinaus werden die Konfigurationsdateien aller Systeme regelmäßig, in einem maximalen Abstand von 3 Monaten überprüft.

### 6.6.3 Sicherheitskontrollen des Lebenszyklus

Telekom Security hat Mechanismen und Kontrollen implementiert, dass Sicherheitspatches innerhalb einer angemessenen Zeit, nachdem sie verfügbar sind, installiert werden. Die Integrität des Sicherheitspatches wird vor der Installation manuell verifiziert.

Ein Sicherheitspatch wird nicht installiert, wenn zusätzliche Sicherheitslücken oder Instabilitäten entstehen, welche die Vorteile der Anwendung des Sicherheitspatches überwiegen. Der Grund für die Nichtanwendung von Sicherheitspatches wird dokumentiert.

#### 6.6.3.1 Kapazitätsmanagement

Telekom Security führt alle PKI-Funktionen mit Hilfe vertrauenswürdiger und geeigneter Systeme durch. Die Systeme werden von Monitoring-Systemen fortlaufend auf Funktion und Kapazität geprüft, so dass im Bedarfsfall zeitnah eine Erweiterung von Ressourcen durchgeführt werden kann.

Die im Monitoring (periodisch alle 5 Minuten) erhobenen Daten zu CPU-, Speicher- und Disk-Auslastung sind mit Warn- und Alarm-Schwellen versehen. Spätestens mit Eintreten der Warn-Stufe wird die Ressourcen-Planung geprüft und ggf. durch Erweiterungen (z.B. Hardware-Nachrüstung, Verlagerung von Diensten

### 6.7 Maßnahmen zur Netzwerksicherheit

Die Zertifizierungsstelle setzt umfassende Maßnahmen zur Netzwerksicherheit um. Diese sind detailliert im Sicherheitskonzept festgelegt, nachfolgend werden einige grundsätzliche Maßnahmen beschrieben.

- Alle Netzanbindungen sind durch mehrstufige Firewallsysteme abgesichert und in verschiedene Sicherheitszonen eingestuft.
- Die Kommunikation über die Portale sind ausnahmslos TLS-gesichert.
- Alle berechtigten Nutzer müssen sich gegenüber den Systemen mit festgelegten Mechanismen authentifizieren, nicht mehr benötigte Accounts werden gelöscht oder deaktiviert.

- Das Trust Center ist redundant über getrennte Zuführungen sowohl mit der Telematik-Infrastruktur als auch mit dem Internet verbunden. Ein Übergang von der Telematik-Infrastruktur ins Internet oder umgekehrt wird durch mehrere Firewallsysteme verhindert.
- Die Administration der Systeme durch die Trust-Center-Administratoren erfolgt über ein getrenntes Netz, das ausschließlich für diesen Zweck zur Verfügung steht.

Es werden die Vorgaben aus [ETSI EN 319 401] Kap. 7.8 umgesetzt.

## 6.8 Zeitstempel

Zertifikate, Sperrlisten, Online-Statusprüfungen und andere wichtige Daten enthalten Datums- und Zeitinformationen die aus einer zuverlässigen Zeitquelle abgeleitet werden (siehe Kapitel 5.5.5).

## 7 Zertifikats-, Sperrlisten- und OCSP-Profile

Die verwendeten Profile entsprechen internationalen Standards sowie den Vorgaben der gematik und sind in [gemSpec\_PKI] detailliert beschrieben.

### 7.1 Zertifikatsprofile

Die Zertifikate enthalten gemäß den Anforderungen aus [RFC5280] mindestens die nachfolgend aufgeführten Inhalte.

[HBA] Für die QES-Zertifikate gelten darüber hinaus die Anforderungen aus [ETSI EN 319 412-2], d.h. die QES-Zertifikate der HBA enthalten zusätzliche Attribute.

#### 7.1.1 Versionsnummer

Alle X509-Zertifikate entsprechen der Version 3.

#### 7.1.2 Zertifikatserweiterungen

In den X509-Zertifikaten werden folgende Erweiterungen verpflichtend verwendet:

- authorityKeyIdentifier,
- admission (je nach Sektor inkl. der Telematik-ID),
- subjectKeyIdentifier
- basicConstraints (kritisch)
- keyUsage (kritisch),
- certificatePolicies,
- CRLDistributionPoint (nur bei nonQES-Zertifikaten),
- authorityInfoAccess,
- [HBA] bei QES-Zertifikaten folgende QCStatements gemäß [ETSI EN 319 412-5]:
  - esi4-qcStatement-1 (EU-qualified certificate)
  - esi4-qcStatement-4 (private key resides in a QSCD)
  - esi4-qcStatement-5 (URL to PKI Disclosure Statements (PDS))

Darüber hinaus können optional (auf Wunsch des Antragstellers) auch folgende Erweiterungen gesetzt werden:

- subjectAlternativeName,
- [HBA] bei QES-Zertifikaten
  - esi4-qcStatement-2 (limitation on the value of transactions).
  - restriction,

Darüber hinaus können weitere sektorspezifische Attribute gemäß [gemSpec\_PKI] aufgenommen werden.

### 7.1.3 OIDs der Algorithmen

Es kommen folgende Algorithmen zum Einsatz:

- CVC-G1-Zertifikate: authS\_ISO9796-2Withrsa\_sha256\_mutual authentication (1.3.36.3.5.2.4)
- CVC-G2-Zertifikate: sha256withRSAEncryption (1.2.840.113549.1.1.11)
- X509-Zertifikate: sha256withRSAEncryption (1.2.840.113549.1.1.11)

### 7.1.4 Namensformen

[HBA]

In den Subject-DN der X509-Zertifikate der HBA werden folgende Namensbestandteile aufgenommen:

- Country,
- commonName,
- givenName,
- surName,
- serialNumber (zur Gewährleistung der Eindeutigkeit (siehe Kap. 3.1.5)).

[SM(C)-B]

In den Subject-DN der X509-Zertifikate der SM(C)-B werden mindestens folgende Namensbestandteile aufgenommen:

- country und
- commonName.

Abhängig von den Vorgaben der Sektoren können noch folgende Bestandteile aufgenommen werden:

- serialNumber (zur Gewährleistung der Eindeutigkeit (siehe Kap. 3.1.5)),
- title,
- givenName,
- surName,
- serialNumber,
- organizationName,
- streetAddress,
- postalCode,
- localityName,
- stateOrProvinceName.

### 7.1.5 Namensbeschränkungen

Es werden nur die in Kap. 7.1.4 aufgeführten Namensbestandteile aufgenommen.

## 7.1.6 OIDs der Zertifizierungsrichtlinien

[SM(C)-B] Es wird folgende OID in alle X509-Zertifikate aufgenommen:

- gematik-OID für [gemRL\_TSL\_SP\_CP] (1.2.276.0.76.4.163)

[HBA] Es wird folgende OID in alle X509-Zertifikate aufgenommen:

- gematik-OID für [CP-HPC] (1.2.276.0.76.4.145)

[HBA] In den QES-Zertifikaten werden darüber hinaus folgende OIDs aufgenommen:

- gematik-OID für HBA-QES (1.2.276.0.76.4.72)
- id-etsi-qcp-natural-qscd (0.4.0.194112.1.2)

Darüber hinaus können optional noch weitere (Sektor- oder TSP-spezifische) OIDs aufgenommen werden.

## 7.1.7 Nutzung der Erweiterung der Policy-Beschränkungen

Keine Verwendung.

## 7.1.8 Syntax und Semantik der Policy-Qualifier

Siehe Kap. 7.1.6.

## 7.1.9 Verarbeitungssemantik für die Erweiterung der Zertifizierungsrichtlinien

Keine Bestimmungen.

## 7.2 Sperrlistenprofile

### 7.2.1 Versionsnummer

Alle Sperrlisten entsprechen der Version 2

### 7.2.2 Sperrlisten und Sperrlisteneintragserweiterungen.

Die TSP X509 non QES geben täglich neue X509-Standard-konforme Sperrlisten aus.

Es werden ausschließlich indirekte Sperrlisten angeboten, d.h. die CRLs werden von einem eigens dafür vorgesehenen CRL-Signer, welcher von dem jeweiligen CA-Zertifikat abgeleitet wird, signiert.

Die Sperrgründe werden in die Sperrliste aufgenommen.

Gespernte Zertifikate werden auch nach Ablauf ihrer Gültigkeit in den Sperrlisten geführt, d.h. diese werden bis zum Ablauf der Gültigkeit der CA nicht aus den Sperrlisten entfernt.

## 7.3 OCSP-Profile

Alle OCSP-Antworten werden gemäß den Anforderungen des [RFC6960] ausgestellt und von einem delegierten OCSP-Signer signiert.

Die OCSP-Signer-Zertifikate werden von der jeweiligen CA mit einer kurzen Gültigkeit ausgestellt und enthalten die Erweiterung id-pkix-ocsp-nocheck, cRLDistributionPoints sowie id-ad-ocsp werden nicht gesetzt.

OCSP-Antworten für gesperrte Zertifikate enthalten den Sperrgrund im Attribut revocation-Reason innerhalb der RevokedInfo. Hinsichtlich der Sperrgründe gelten die in Abschnitt 7.2.2 gemachten Angaben.

### 7.3.1 Versionsnummer

Es wird die Version 1 gemäß der OCSP-Spezifikation nach [RFC6960] unterstützt.

### 7.3.2 OCSP-Erweiterungen

Die OCSP-Responder sind konform zu [RFC6960] und [CommonPKI], d.h. in der OCSP-Response ist neben den Standardangaben auch die Erweiterung CertHash („Positivauskunft“ gemäß [CommonPKI]) sowie ArchiveCutOff mit dem Zeitpunkt des Gültigkeitsbeginns des zugehörigen CA-Zertifikats, enthalten.

## 8 Compliance-Audits und andere Prüfungen

Der Zertifizierungsdienst ist konform zu den in Kap. 1.1 aufgeführten ETSI-Normen. Zur Prüfung der Konformität werden die TSP sowohl durch interne Auditoren als auch durch eine anerkannte Prüfstelle (gemäß [ETSI EN 319403]) auditiert. Im Rahmen der Audits wird neben der Dokumentation (Sicherheitskonzept, Betriebskonzept sowie weitere interne Dokumente) die Umsetzung der Prozesse und Einhaltung der Vorgaben überprüft.

Darüber hinaus hat die gematik in Ihrer Aufgabe als Zulassungsstelle für die TSP das Recht, den Zertifizierungsdienst zu auditieren.

### 8.1 Intervall und Grund von Prüfungen

Compliance-Audits finden jährlich und zusätzlich bei Bedarf statt. Darüber hinaus werden jährlich Notfallübungen für mindestens einen Dienst im Trust Center durchgeführt.

### 8.2 Identität/Qualifikation des Prüfers

Die Trust Center-spezifischen Compliance-Audits werden von qualifizierten Mitarbeitern der Telekom Security oder einem Dritten (z.B. qualifiziertes Unternehmen wie TÜV IT) durchgeführt, die Erfahrung in den Bereichen Public-Key-Infrastructure-Technologie, Sicherheits-Auditing und Verfahren und Hilfsmittel der Informationssicherheit vorweisen können.

### 8.3 Beziehung des Prüfers zur prüfenden Stelle

Beim Prüfer für die ETSI-Zertifizierungen handelt es sich um einen unabhängigen und qualifizierten Auditor (z.B. Wirtschaftsprüfer, Gutachter).

Selbstaufsichtsmaßnahmen (Quality Assessments) werden von dafür qualifizierten Telekom Security Mitarbeitern durchgeführt.

### 8.4 Abgedeckte Bereiche der Prüfung

Zielsetzung der Überprüfung ist die Umsetzung dieses Dokuments. Es sind alle Prozesse zu prüfen, die mit der Lebenszyklusverwaltung von Zertifikaten in Verbindung stehen:

- Identitätsprüfungen der Antragsteller,
- Zertifikatsbeauftragungsverfahren,
- Bearbeitung von Zertifikatsaufträgen,
- Zertifikatserneuerung,
- Zertifikatssperrungen,
- Zutrittsschutz,
- Berechtigungs- und Rollenkonzept,
- Einbruchshemmende Maßnahmen,
- Personal.

In jedem Fall wird nach den jeweils gültigen Versionen der Audit-Kriterien der in Kap. 1.1 aufgeführten ETSI-Normen geprüft.

Das Telekom Security Trust Center führt jährlich eine Risikobewertung durch, welches u.a. auch die Produkte SM(C)-B und HBA abdeckt.

Die Überprüfung beinhaltet zumindest die folgenden Punkte:

- Identifikation vorhersehbarer externer, als auch interner Gefährdungen (d.h. insbesondere die zu Grunde liegenden Schwachstellen), welche
  - zu unbefugten Zugriffen auf relevante Daten oder Systeme,
  - zur Weitergabe oder einem Missbrauch von relevanten Daten,
  - zu Veränderungen oder Zerstörung von relevanten Daten,
  - zur Beeinträchtigung, Störung oder Ausfall von Teilen oder des gesamten Zertifikatsverwaltungsprozesses

führen können.

- Beurteilung der Eintrittswahrscheinlichkeit und der daraus resultierenden potenziellen Schäden (d.h. Schadenshöhe) durch das Ausnutzen einer Schwachstelle. Dabei ist der besondere Schutzbedarf der Zertifikatsdaten und des Zertifikatsverwaltungsprozesses zu berücksichtigen.
- Beurteilung der Wirksamkeit und Angemessenheit der getroffenen Gegenmaßnahmen (z.B. Richtlinien, Verfahren, eingesetzte Sicherheits-Systeme, Technologien, Versicherungen) welche die Gefährdung beseitigen oder das Risiko minimieren.

Basierend auf der Risikobewertung hat das Telekom Security Trust Center einen Sicherheitsplan entwickelt, der regelmäßig überprüft und bei Bedarf angepasst wird. Der Sicherheitsplan besteht aus Verfahren, Maßnahmen und Produkten um die Bewertung und das Management der während der Risikobewertung identifizierten Risiken zu unterstützen. Der Sicherheitsplan enthält entsprechend der Sensibilität der Daten und des Zertifikatsverwaltungsprozesses administrative, organisatorische, technische und physische Sicherheitsmaßnahmen. Im Rahmen der Prüfungen werden auch die im IT-Servicemanagement hinterlegten Assetlisten überprüft.

## 8.5 Maßnahmen zur Beseitigung von Mängeln oder Defiziten

Werden bei einem Compliance-Audit von einem Prüfer Mängel oder Fehler bei dem Betreiber der Zertifizierungsstelle festgestellt, wird darüber entschieden, welche Korrekturmaßnahmen zu treffen sind. Der Leiter Trust Center entscheidet zusammen mit dem Prüfer über geeignete Maßnahmen, deren Umsetzung in einem wirtschaftlich angemessenen Zeitraum durchzuführen sind. Bei schweren sicherheitskritischen Mängeln muss innerhalb von 10 Tagen ein Korrekturplan erstellt und die Abweichung behoben werden. Bei weniger schwerwiegenden Defiziten entscheidet der Leiter Trust Center über den Zeitrahmen der Behebung.

## 8.6 Mitteilung der Ergebnisse

Die Ergebnisse der Prüfung werden in einem vom Prüfer erstellten Bericht dokumentiert und Telekom Security übergeben.

Telekom Security behält sich vor, Ergebnisse bzw. Teilergebnisse zu veröffentlichen, wenn Missbrauch stattfand oder bei Schädigung des Ansehens der Telekom Security.



## 9 Weitere rechtliche Regelungen

### 9.1 Gebühren

#### 9.1.1 Entgelte für die Ausstellung oder Erneuerung von Zertifikaten

T-Systems berechnet für das Ausstellen, Erneuern und Verwalten der Karten Entgelte. Es gelten die Regelungen der mit dem Kunden vereinbarten vertraglichen Regelungen.

#### 9.1.2 Entgelte für den Zugriff auf Zertifikate

T-Systems berechnet für den Zugriff auf Zertifikate im Verzeichnisdienst keine Entgelte.

#### 9.1.3 Entgelte für den Zugriff auf Sperr- oder Statusinformationen

T-Systems berechnet für den Zugriff auf Sperr- oder Statusinformationen keine Entgelte.

#### 9.1.4 Entgelte für andere Leistungen

T-Systems ist berechtigt, für andere Leistungen Entgelte zu berechnen. Es gelten die Regelungen der mit dem Kunden vereinbarten vertraglichen Regelungen.

#### 9.1.5 Erstattung von Entgelten

Die Erstattung von Entgelten durch T-Systems erfolgt auf Basis der gesetzlichen Regelungen des deutschen Rechts. Darüber hinaus gelten die Regelungen der mit dem Kunden vereinbarten vertraglichen Regelungen

### 9.2 Finanzielle Verantwortung, Versicherungsschutz

Die finanziellen Verantwortlichkeiten werden in den mit dem Kunden vereinbarten vertraglichen Regelungen festgelegt.

#### 9.2.1 Versicherungsschutz

Die Telekom Security verfügt über die Deutsche Telekom AG über einen Betriebs- und Vermögenshaftpflichtversicherungsschutz. Es ist sichergestellt, dass die Anforderungen, die sich hinsichtlich des Versicherungsschutzes ergeben, erfüllt werden. Darüber hinaus besteht eine Deckungsvorsorge nach dem § 10 VDG.

## 9.2.2 Sonstige finanzielle Mittel

Mit der Deutsche Telekom AG (Amtsgericht Bonn HRB 6794) als herrschendem Unternehmen ist am 09.03.2007 ein Beherrschungs- und Gewinnabführungsvertrag geschlossen, sodass die Deutsche Telekom AG immer alle Verluste der Gesellschaft übernimmt.

## 9.2.3 Versicherungs- oder Gewährleistungsschutz für Endteilnehmer

Nicht anwendbar.

## 9.3 Vertraulichkeit betrieblicher Informationen

### 9.3.1 Umfang von vertraulichen Informationen

Als vertraulich gelten alle Informationen von PKI-Beteiligten (siehe Kap. 1.3), die nicht veröffentlicht oder zur Veröffentlichung explizit freigegeben werden und die nicht unter Kap. 9.3.2 fallen.

### 9.3.2 Umfang von nicht vertraulichen Informationen

Unter nicht vertraulichen Informationen werden alle impliziten und expliziten Informationen eingestuft, die in ausgegebenen Zertifikaten, Sperrlisten, Statusinformationen enthalten sind oder davon abgeleitet werden können.

### 9.3.3 Verantwortung zum Schutz vertraulicher Informationen

Die Verantwortlichkeit für den Schutz der vertraulichen Informationen sowie für die Einhaltung der datenschutzrechtlichen Bestimmungen liegt bei Telekom Security als Zertifizierungsstelle.

Darüber hinaus sind auch die Kammermitarbeiter durch die Übernahme von Tätigkeiten im Rahmen der Freigabe und Attributbestätigung verpflichtet, vertrauliche Informationen entsprechend zu behandeln.

## 9.4 Datenschutz

### 9.4.1 Datenschutzkonzept

Zur Leistungserbringung muss Telekom Security personenbezogene Daten elektronisch speichern und verarbeiten. Telekom Security stellt die technischen und organisatorischen Sicherheitsvorkehrungen und Maßnahmen gemäß § 64 BDSG sicher.

Entsprechend den Konzernvorgaben wurde ein Datenschutzkonzept erstellt. Dieses Datenschutzkonzept fasst die datenschutzrelevanten Aspekte um den PKI-Dienst zusammen.

Das Datenschutzkonzept kann in Auszügen auf Anforderung bereitgestellt werden.

## 9.4.2 Vertraulich zu behandelnde Daten

Für personenbezogene Daten gelten die Regelungen analog zu Kap. 9.3.1.

## 9.4.3 Nicht vertraulich zu behandelnde Daten

Für personenbezogene Daten gelten die Regelungen analog zu Kap. 9.3.2.

## 9.4.4 Verantwortung für den Schutz vertraulicher Daten

Für personenbezogene Daten gelten die Regelungen analog zu Kap. 9.3.3.

## 9.4.5 Mitteilung und Zustimmung zur Nutzung vertraulicher Daten

Der Antragsteller muss der Nutzung von personenbezogenen Daten durch die Zertifizierungsstelle und der zuständigen Kammer zustimmen, soweit dies zur Leistungserbringung erforderlich ist.

Ferner dürfen alle Informationen veröffentlicht werden, die nach Kap. 9.4.3 als nicht vertraulich behandelt werden.

## 9.4.6 Offenlegung gemäß gerichtlicher oder verwaltungsmäßiger Prozesse

Die Verpflichtung zur Geheimhaltung der vertraulichen Informationen oder personenbezogener Daten entfällt, soweit die Offenlegung kraft Gesetzes oder kraft Entscheidung eines Gerichtes oder einer Verwaltungsbehörde angeordnet wird bzw. zur Durchsetzung von Rechtsansprüchen dient. Sobald Anhaltspunkte für die Einleitung eines gerichtlichen oder behördlichen Verfahrens bestehen, die zur Offenlegung vertraulicher oder privater Informationen führen könnten, wird die an dem Verfahren beteiligte Vertragspartei die andere Vertragspartei hierüber unter Beachtung der gesetzlichen Bestimmungen informieren.

## 9.4.7 Andere Umstände zur Offenlegung von Daten

Keine Bestimmungen.

## 9.5 Rechte des geistigen Eigentums (Urheberrecht)

Dieses Dokument ist urheberrechtlich geschützt, alle geistigen Eigentumsrechte obliegen Telekom Security. Jegliche andere Nutzung (z.B. Vervielfältigung, Verwendung von Texten und Bildern, Änderung oder Erzeugung eines vergleichbaren oder abgeleiteten Dokuments, Weitergabe an Personen ohne Interesse an dem in diesem Dokument beschriebenen Dienst), auch auszugsweise, bedarf der vorherigen ausdrücklichen schriftlichen Genehmigung des Herausgebers dieses Dokuments (siehe Kapitel 1.5.1).

## 9.6 Zusicherungen und Gewährleistungen

### 9.6.1 Zusicherungen und Gewährleistungen der Zertifizierungsstelle

Telekom Security verpflichtet sich,

- keine unrichtigen Angaben in Zertifikate aufzunehmen, die den Registrierungsstellen, die den Zertifikatsauftrag genehmigen oder das Zertifikat ausstellen, bekannt sind oder von ihnen stammen,
- dass keine Fehler in Zertifikaten enthalten sind, die vom Personal der Registrierungsstellen, die den Zertifikatsauftrag genehmigen oder das Zertifikat ausstellen, gemacht wurden und auf unsachgemäße und sorglose Zertifikatserzeugung und Verwaltung zurück zu führen sind,
- dass alle Zertifikate den Anforderungen dieses Dokuments genügen und
- dass die Sperrfunktionalitäten und die Nutzung der CA-Datenbank (Verzeichnisdienst, OCSP-Responder) allen wesentlichen Anforderungen der geltenden CP/CPS erfüllen.

Hinweis: Die Beantragung der Karten über die Antragsportale ist nicht vollständig barrierefrei. Die umgesetzten Maßnahmen sind in den Portalen dokumentiert und von jeder Portalseite direkt aufrufbar. Telekom Security bietet zur Unterstützung bei der Beantragung und Akzeptanz der Zertifikate kostenlosen telefonischen Support. Im Bedarfsfall, d.h. im Falle von Antragstellern mit schweren körperlichen Beeinträchtigungen, kann darüber hinaus Support vor Ort beim Antragsteller angeboten werden.

### 9.6.2 Zusicherungen und Gewährleistungen der Registrierungsstelle (RA)

Siehe 9.6.1, da Telekom Security sowohl Zertifizierungsstelle als auch einzige Registrierungsstelle ist.

### 9.6.3 Zusicherungen und Gewährleistungen des Endteilnehmers

Endteilnehmer verpflichten sich:

- Eine Identifizierung durchzuführen
  - Persönlich zur Identifizierung zu Erscheinen und einen gültigen amtlichen Ausweis vorzulegen.
  - Mittels eines Ausweises mit Online-AusweisFunction.
- Die Angaben im Zertifikatsantrag vollständig und korrekt anzugeben, Name und Titel sind entsprechend dem vorgelegten amtlichen Ausweis anzugeben.
- Zu überprüfen, dass die im Endteilnehmer-Zertifikat aufgenommenen Zertifikatsinhalte der Wahrheit entsprechen.
- Bei Aktivierung der Karten die fünfstelligen Transport-PINs zu prüfen und durch neue, mindestens sechsstellige PINs zu ersetzen.

- Die Schlüssel und Zertifikate nur in den zulässigen Anwendungen einzusetzen, die Anwendung muss dabei den im Zertifikat eingetragenen Schlüsselverwendungen genügen.
- Das ausgestellte Zertifikat ausschließlich für autorisierte und legale Zwecke die diesem CPS entsprechen zu verwenden und nicht den Regelungen dieser Erklärung widersprechen.
- Tatsächlich als Endteilnehmer zu agieren und mit seinem privaten Schlüssel, dem der im Zertifikat enthaltene öffentliche Schlüssel zugeordnet ist, keine CA-Funktionalitäten durchzuführen, wie z.B. Signatur von Zertifikaten oder Sperrlisten.
- Die Karten nicht mit Anwendungen oder Maschinen zu nutzen, deren Funktionen unbekannt, verdächtig oder unzuverlässig erscheint.
- Den privaten Schlüssel angemessen zu schützen und nicht weiterzugeben, insbesondere die Anforderungen an technische Schutzmaßnahmen des privaten Schlüssels umzusetzen.
- Die Karten immer in persönlichem Gewahrsam zu halten.
- In gewissen Zeitabständen die PINs zu ändern und die PINs wenn möglich nicht zu notieren.
- Bei dem Verdacht, dass jemand Kenntnis über eine PIN erlangt hat, die PIN sofort zu ändern.
- Den privaten Schlüssel nach Ablauf der Gültigkeit oder der Sperrung des Zertifikates nicht mehr zu nutzen, außer zur Entschlüsselung.
- Das Zertifikat unverzüglich zu sperren und nicht mehr zu nutzen, wenn
  - Der private Schlüssel verloren ist, gestohlen wurde oder der Verdacht auf Kompromittierung oder Manipulation (z.B. durch Beschädigung der Karte) besteht.
  - Die Kontrolle über den privaten Schlüssel nicht mehr sichergestellt ist, z.B. durch Kompromittieren der PINs/PUKs.
  - Wesentliche Angaben im Zertifikat nicht mehr stimmen.
  - Das Zertifikat nicht mehr genutzt werden soll (Außerbetriebnahme).
- Das Zertifikat nicht mehr zu nutzen, wenn bekannt wird, dass das Zertifikat der Zertifizierungsstelle kompromittiert wurde.
- die rechtlichen Konsequenzen zu tragen, die durch die Nichteinhaltung der vorliegenden CP/CPS beschriebenen Pflichten entstehen,

Darüber hinaus wird dem Endteilnehmer empfohlen:

- Kartenleser mit PIN-Pad zu nutzen.
- Den Computer immer auf dem aktuellen Sicherheitsstand zu halten.
- Aktuelle Antiviren- und Firewallsoftware zu nutzen.
- Den Computer durch Passwörter für BIOS, Bildschirmschoner usw. oder mittels Chipkarte vor unberechtigtem Zugriff zu schützen.
- Grundsätzlich nur Informationen zu signieren, deren Inhalt vorher geprüft wurde.
- Bei Zweifel an der Erstellung einer elektronischen Signatur, diese vor dem Versand selbst noch einmal nachzuprüfen.

Hinweis: Telekom Security behält sich vor, weiteren Pflichten, Zusicherungen, Zusagen und Gewährleistungen gegenüber dem Endteilnehmers abzuschließen.

## 9.6.4 Zusicherungen und Gewährleistungen von Vertrauenden Dritten

Es existieren keine vertraglichen Vereinbarungen mit vertrauenden Dritten. Vertrauende Dritte müssen selbst über hinreichende Informationen und Kenntnisse verfügen, um den Umgang mit Zertifikaten und dessen Validierung bewerten zu können. Der Vertrauende Dritte ist selbst für seine Entscheidungsfindung verantwortlich, ob die die zur Verfügung gestellten Informationen zuverlässig und vertrauensvoll sind.

## 9.6.5 Zusicherungen und Gewährleistungen anderer Teilnehmer

Keine Bestimmungen.

## 9.7 Haftungsausschluss

Es gelten die mit dem Kunden vereinbarten vertraglichen Regelungen.

## 9.8 Haftungsbeschränkungen

Für Schäden aus der Verletzung von Leben, Körper und Gesundheit sowie für Schäden, die auf vorsätzliche Pflichtverletzungen zurückzuführen sind, haftet die Zertifizierungsstelle unbegrenzt. Im Übrigen wird die Haftung für Schäden, die auf einer fahrlässigen Pflichtverletzung beruhen einzelvertraglich geregelt.

## 9.9 Schadensersatz

Es gelten die mit dem Kunden vereinbarten vertraglichen Regelungen.

## 9.10 Laufzeit und Beendigung

### 9.10.1 Laufzeit

Dieses CPS ist ab dem auf dem Deckblatt angegebenen Datum gültig.

### 9.10.2 Beendigung

Die Gültigkeit endet bei der Veröffentlichung eines neuen CPS oder mit der Einstellung der Zertifizierungsdienste der Zertifizierungsstelle.

### 9.10.3 Wirkung der Beendigung und Fortbestand

Bei der Beendigung der Herausgabe von Karten bleiben die in der CP/CPS enthaltenen Regelungen weiterhin gültig, bis das letzte ausgegebene Zertifikat seine Gültigkeit verliert.

### 9.11 Individuelle Mitteilungen und Kommunikation mit Teilnehmern

Falls nicht anders vertraglich vereinbart, werden für individuelle Mitteilungen an die Zertifizierungsstelle die jeweils gültigen Kontaktinformationen (Anschrift, E-Mail etc.) bekannt gegeben.

### 9.12 Änderungen

Um auf sich ändernde Marktanforderungen, Sicherheitsanforderungen, Gesetzeslagen etc. zu reagieren, behält sich Telekom Security das Recht vor, Änderungen und Anpassungen dieses Dokuments durchzuführen.

#### 9.12.1 Verfahren für Änderungen

Änderungen des CP/CPS können nur durch Telekom Security gemäß dem beschriebenen Freigabeprozess (siehe Kap. 1.5) durchgeführt werden. Bei jeder offiziellen Änderung erhält dieses Dokument eine neue aufsteigende Versionsnummer und Veröffentlichungsdatum.

Änderungen treten unverzüglich mit der Veröffentlichung in Kraft.

Aktualisierte Versionen setzen die vorherigen Dokumentenversionen außer Kraft. Im Falle widersprüchlicher Bestimmungen entscheidet Telekom Security über die weitere Vorgehensweise.

#### 9.12.2 Benachrichtigungsverfahren und -zeitraum

Neue Versionen dieses Dokuments werden nach Veröffentlichung auf der Website des Trust-Centers ([www.telesec.de](http://www.telesec.de)) veröffentlicht. An anderen Stellen, u. a. den AGB, wird auf die CPS verlinkt. Neben dem Dokument selbst, werden auf der Website Versionsnummer und Datum der Veröffentlichung bereitgestellt, sodass neue Versionen direkt erkennbar sind.

Vor Veröffentlichung auf der Website wird außerdem die Bundesnetzagentur als zuständige Aufsichtsbehörde informiert.

#### 9.12.3 Umstände, die zu einer Änderung der OID führen

Keine Regelungen.

### 9.13 Bestimmungen zur Beilegung von Streitigkeiten

Im Falle von Streitigkeiten führen die Parteien unter Berücksichtigung getroffener Vereinbarungen, Regelungen und geltender Gesetze die Einigung herbei.

Telekom Security ist daran gelegen, Streitigkeiten mit ihren Kunden im direkten Kontakt zu klären. Der Kunde kann sich hierzu an den Kundenservice über folgende Kontakte wenden:

- Telefon (nur aus Deutschland erreichbar, kostenfrei): 0800 1183307
- E-Mail: [service.map@telekom.de](mailto:service.map@telekom.de)

Verfahren bei außergerichtlicher Streitbeilegung:

- Information zur Verbraucherstreitbeilegung nach § 36 Verbraucherstreitbeilegungsgesetz (VSBG): Die Deutsche Telekom nimmt nicht an Streitbeilegungsverfahren vor einer Verbraucherschlichtungsstelle teil.
- Informationen zur Online-Streitbeilegung nach Artikel 14 Abs. 1 der EU-Verordnung über Online-Streitbeilegung in Verbraucherangelegenheiten (ODR-VO): Die EU-Kommission stellt eine Plattform zur Online-Streitbeilegung (OS-Plattform) verbraucherrechtlicher Streitigkeiten, die aus Online-Kaufverträgen und Online-Dienstleistungsverträgen resultieren, bereit. Diese Plattform ist im Internet unter <http://ec.europa.eu/consumers/odr/> erreichbar.

Im Falle gerichtlicher Streitbeilegung ist der Gerichtsstand der Sitz der Deutsche Telekom Security GmbH in Bonn.

## 9.14 Geltendes Recht

Es gilt deutsches Recht.

## 9.15 Einhaltung geltenden Rechts

Das vorliegende Dokument unterliegt den geltenden deutschen Gesetzen, Vorschriften, Richtlinien, Verordnungen, Erlassen und Anordnungen, insbesondere den darin beschriebenen Import und Export Bestimmungen von Security-Komponenten (Software, Hardware oder technischer Informationen). Geltende zwingende Gesetze, Vorschriften, Richtlinien, Verordnungen, Erlasse und Anordnungen setzen die entsprechenden Bestimmungen des vorliegenden Dokuments außer Kraft.

## 9.16 Verschiedene Bestimmungen

### 9.16.1 Vollständiger Vertrag

Nicht anwendbar.

### 9.16.2 Abtretung

Nicht anwendbar.

### 9.16.3 Salvatorische Klausel

Sollte eine Bestimmung dieses CP/CPS unwirksam oder undurchführbar sein oder werden, so berührt dies die Wirksamkeit dieser Erklärung im Übrigen nicht. Statt der unwirksamen und undurchführbaren Bestimmung gilt eine solche Bestimmung als vereinbart, die dem



wirtschaftlichen Zweck dieses Dokuments in rechtswirksamer Weise am nächsten kommt. Das Gleiche gilt für die Ergänzung etwaiger Vertragslücken.

#### 9.16.4 Vollstreckung (Rechtsanwaltsgebühren und Rechtsverzicht)

Nicht anwendbar.

#### 9.16.5 Höhere Gewalt

Mit dieser Regelung soll sichergestellt werden, dass die Vertragspartner nicht in Verzug geraten, wenn sich die Leistung infolge höherer Gewalt verzögert oder unmöglich wird.

#### 9.17 Sonstige Bestimmungen

Nicht anwendbar.

## A Referenzen

<b>Referenz</b>	<b>Dokumentenbezeichnung</b>
[CP-HPC]	Bundesärztekammer et al: Gemeinsame Policy für die Ausgabe der HPC – Zertifikatsrichtlinie HPC
[gemRL_TSL_SP_CP]	gematik: Gemeinsame Zertifizierungsrichtlinie für Teilnehmer der gematik-TSL
[gemSpec_TSP_X.509]	gematik: Spezifikation Trust Service Provider X.509
[gemSpec_CVC_TSP]	gematik: Spezifikation Trust Service Provider CVC
[gemSpec_Krypt]	gematik: Einführung der Gesundheitskarte – Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur
[gemSpec_PKI]	gematik: Übergreifende Spezifikation. Spezifikation PKI
[BDSG]	Datenschutzgesetz, Bundesgesetzblatt I 2003 S.66.
[PKCS]	RSA Security Inc., RSA Laboratories „Public Key Cryptography Standards“
[PKIX]	RFCs und Spezifikationen der IETF Arbeitsgruppe Public Key Infrastructure (X.509)
[RFC3647]	Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework, Network Working Group, IETF, 2003
[RFC5280]	Internet X.509 Public Key Infrastructure: Certificate and Certificate Revocation List (CRL) Profile
[RFC6960]	Internet X.509 Public Key Infrastructure: Online Certificate Status Protocol - OCSP
[X.509]	Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks, Recommendation X.509 (08/05), Recommendation X.509 (2005) Corrigendum 1 (01/07)
[CommonPKI]	T7 & Teletrust: Common PKI Specifications for interoperable applications
[AlgKat]	Bundesnetzagentur: Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung: Übersicht über geeignete Algorithmen
[ETSI EN 319 401]	Electronic Signatures and Infrastructures (ESI): General Policy Requirements for TSPs
[ETSI EN 319 411-1]	Electronic Signatures and Infrastructures (ESI): General Policy and security requirements for TSPs

[ETSI EN 319 411-2]	Electronic Signatures and Infrastructures (ESI): Requirements for TSPs issuing EU qualified certificates
[ETSI EN 319 412-2]	Electronic Signatures and Infrastructures (ESI): Certificate profile for certificates issued to natural persons
[ETSI EN 319 412-5]	Electronic Signatures and Infrastructures (ESI): Certificate Profiles: QCStatements

Tabelle 5: Referenzen und mitgeltende Unterlagen