

**Elektronische Gesundheitskarte und Telematikinfrastuktur**

# **Produkttypsteckbrief**

## ***Prüfvorschrift***

# **Trust Service Provider CVC**

Produkttyp Version: 1.4.1-0  
Produkttyp Status: freigegeben

Version: 1.0.0  
Revision: 60910  
Stand: 28.11.2018  
Status: freigegeben  
Klassifizierung: öffentlich  
Referenzierung: gemProdT\_CVC\_TSP\_PTV\_1.4.1-0

---

## Historie Produkttypversion und Produkttypsteckbrief

---

### Historie Produkttypversion

Die Produkttypversion ändert sich, wenn sich die Anforderungslage für den Produkttyp ändert und die Umsetzung durch Produktentwicklungen ebenfalls betroffen ist.

Produkttyp-version	Beschreibung der Änderung	Referenz
1.0.0	Initiale Version auf Dokumentenebene	[gemProdT_CVC_TSP_PTV1.0.0]
1.1.0	Losübergreifende Synchronisation	[gemProdT_CVC_TSP_PTV1.1.0]
1.2.0	P11-Änderungsliste	[gemProdT_CVC_TSP_PTV1.2.0]
1.3.0	Ergänzung Kapitel 5, Anpassung OPB1	[gemProdT_CVC_TSP_PTV1.3.0]
1.3.0-1	Anpassung auf Releasestand 1.6.3	[gemProdT_CVC_TSP_PTV1.3.0-1]
1.4.0-0	Anpassung auf Releasestand 1.6.4	[gemProdT_CVC_TSP_PTV1.4.0-0]
1.4.0-1	Anpassung auf Releasestand 2.1.2	[gemProdT_CVC_TSP_PTV1.4.0-1]
1.4.1-0	Anpassung auf Releasestand 2.1.3-1	[gemProdT_CVC_TSP_PTV1.4.1-0]

### Historie Produkttypsteckbrief

Die Dokumentenversion des Produkttypsteckbriefs ändert sich mit jeder inhaltlichen oder redaktionellen Änderung des Produkttypsteckbriefs und seinen referenzierten Dokumenten. Redaktionelle Änderungen haben keine Auswirkung auf die Produkttypversion.

Version	Stand	Kap.	Grund der Änderung, besondere Hinweise	Bearbeiter
1.0.0	28.11.18		freigegeben	gematik

---

## Inhaltsverzeichnis

---

<b>1</b>	<b>Einführung.....</b>	<b>4</b>
1.1	Zielsetzung und Einordnung des Dokumentes .....	4
1.2	Zielgruppe .....	4
1.3	Geltungsbereich .....	4
1.4	Abgrenzung des Dokumentes .....	4
1.5	Methodik.....	5
<b>2</b>	<b>Dokumente .....</b>	<b>6</b>
<b>3</b>	<b>Blattanforderungen .....</b>	<b>7</b>
3.1	Anforderungen zur funktionalen Eignung .....	7
3.1.1	Produkttest/Produktübergreifender Test .....	7
3.1.2	Herstellererklärung funktionale Eignung .....	8
3.2	Anforderungen zur sicherheitstechnischen Eignung .....	12
3.2.1	CC-Evaluierung .....	12
3.2.2	Sicherheitsgutachten .....	12
3.2.3	Herstellererklärung sicherheitstechnische Eignung.....	16
3.3	Anforderungen zur elektrischen, mechanischen und physikalischen Eignung.....	18
<b>4</b>	<b>Produkttypspezifische Merkmale .....</b>	<b>19</b>
<b>5</b>	<b>Anhang A – Verzeichnisse .....</b>	<b>21</b>
5.1	Abkürzungen.....	21
5.2	Tabellenverzeichnis.....	21
5.3	Referenzierte Dokumente.....	21

---

# 1 Einführung

---

## 1.1 Zielsetzung und Einordnung des Dokumentes

Dieser Produkttypsteckbrief verzeichnet verbindlich die Anforderungen der gematik an Herstellung und Betrieb von Produkten des Produkttyps Trust Service Provider CVC oder verweist auf Dokumente, in denen verbindliche Anforderungen mit ggf. anderer Notation zu finden sind. Die Anforderungen bilden die Grundlage für die Erteilung von Zulassungen, Zertifizierungen bzw. Bestätigungen durch die gematik (Wenn im weiteren Dokument vereinfachend der Begriff „Zulassung“ verwendet wird, so ist dies der besseren Lesbarkeit geschuldet und umfasst übergreifend neben dem Verfahren der Zulassung auch Zertifizierungen und Bestätigungen der gematik-Zulassungsstelle.).

Die Anforderungen werden über ihren Identifier, ihren Titel sowie die Dokumentenquelle referenziert. Die Anforderungen mit ihrem vollständigen, normativen Inhalt sind dem jeweils referenzierten Dokument zu entnehmen.

## 1.2 Zielgruppe

Der Produkttypsteckbrief richtet sich an Trust Service Provider CVC-Hersteller und -Anbieter sowie Hersteller und Anbieter von Produkttypen, die hierzu eine Schnittstelle besitzen.

Das Dokument ist außerdem zu verwenden von:

- der gematik im Rahmen des Zulassungsverfahrens
- Auditoren

Bei zentralen Diensten der TI-Plattform und fachanwendungsspezifischen Diensten beziehen sich Anforderungen, die sowohl an Anbieter als auch Hersteller gerichtet sind, jeweils auf den Anbieter als Zulassungsnehmer, bei dezentralen Produkten auf den Hersteller.

## 1.3 Geltungsbereich

Dieses Dokument enthält normative Festlegungen zur Telematikinfrastruktur des deutschen Gesundheitswesens. Der Gültigkeitszeitraum der vorliegenden Version und deren Anwendung in Zulassungsverfahren werden durch die gematik GmbH in gesonderten Dokumenten (z.B. Dokumentenlandkarte, Leistungsbeschreibung) festgelegt und bekannt gegeben.

## 1.4 Abgrenzung des Dokumentes

Dieses Dokument macht keine Aussagen zur Aufteilung der Produktentwicklung bzw. Produktherstellung auf verschiedene Hersteller und Anbieter.

Dokumente zu den Zulassungsverfahren für den Produkttyp sind nicht aufgeführt. Die geltenden Verfahren und Regelungen zur Beantragung und Durchführung von Zulassungsverfahren können der Homepage der gematik entnommen werden.

## 1.5 Methodik

Die im Dokument verzeichneten Anforderungen werden tabellarisch dargestellt. Die Tabellenspalten haben die folgende Bedeutung:

**Afo-ID:** Identifiziert die Anforderung eindeutig im Gesamtbestand aller Festlegungen der gematik.

**Afo-Bezeichnung:** Gibt den Titel einer Anforderung informativ wieder, um die thematische Einordnung zu erleichtern. Der vollständige Inhalt der Anforderung ist dem Dokument zu entnehmen, auf das die Quellenangabe verweist.

**Quelle (Referenz):** Verweist auf das Dokument, das die Anforderung definiert.

## 2 Dokumente

Die nachfolgenden Dokumente enthalten alle für den Produkttyp normativen Anforderungen.

**Tabelle 1: Dokumente mit Anforderungen zu der Produkttypversion**

Dokumenten Kürzel	Bezeichnung des Dokumentes	Version
gemSpec_OM	Übergreifende Spezifikation Operations und Maintenance	1.10.0
gemSpec_Krypt	Übergreifende Spezifikation Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur	2.11.0
gemSpec_PKI	Übergreifende Spezifikation – Spezifikation PKI	2.3.0
gemKPT_Test	Testkonzept der TI	2.1.0
gemSpec_CVC_TSP	Spezifikation Trust Service Provider CVC	1.10.0
gemSpec_OID	Spezifikation Festlegung von OIDs	3.2.0
gemSpec_Net	Übergreifende Spezifikation Netzwerk	1.14.0
gemSpec_DS_Anbieter	Spezifikation Datenschutz- und Sicherheitsanforderungen der TI an Anbieter	1.0.1

### Errata

Neben den vorgenannten Dokumenten werden auf der Internetseite der gematik bei Bedarf Errata-Dokumente mit normativen Ergänzungen bzw. Korrekturen zu den Spezifikationsdokumenten veröffentlicht. Sofern in den Errata der vorliegende Produkttyp benannt wird, sind diese bei der Umsetzung des Produkttyps entsprechend der Vorgabe in der Dokumentenlandkarte zu berücksichtigen. Dabei kann eine abweichende Produkttypversion festgelegt werden.

Dokumenten Kürzel	Bezeichnung des Dokuments	Version
gemErrata_R2.1.3-1	Errata zu Release 2.1.3-1	1.0.0

## 3 Blattanforderungen

Die folgenden Abschnitte verzeichnen alle für den Produkttypen normativen Anforderungen, die für die Herstellung und den Betrieb von Produkten des Produkttyps notwendig sind (Blattanforderungen). Die Anforderungen sind gruppiert nach der Art der Nachweisführung ihrer Erfüllung als Grundlage der Zulassung, Zertifizierung bzw. Bestätigung.

### 3.1 Anforderungen zur funktionalen Eignung

#### 3.1.1 Produkttest/Produktübergreifender Test

In diesem Abschnitt sind alle funktionalen und nichtfunktionalen Anforderungen an den technischen Teil des Produkttyps verzeichnet, deren Umsetzung im Zuge von Zulassungstests durch die gematik geprüft wird.

**Tabelle 2: Anforderungen zur funktionalen Eignung  
"Produkttest/Produktübergreifender Test"**

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
TIP1-A_2568	Erzeugen von CV-Zertifikaten mit Profilen, die einer Qualifizierung bedürfen	gemSpec_CVC_TSP
TIP1-A_2659	Name der CA	gemSpec_CVC_TSP
TIP1-A_3029	Name einer Test-CVC-CA	gemSpec_CVC_TSP
TIP1-A_3032	Signierung des Test-CV-Zertifikats durch die Test-CVC-CA	gemSpec_CVC_TSP
GS-A_3695	Grundlegender Aufbau Versionsnummern	gemSpec_OM
GS-A_5025	Versionierung von Produkten auf Basis von zentralen Produkttypen der TI-Plattform und fachanwendungsspezifischen Diensten durch die Produktidentifikation	gemSpec_OM
GS-A_5054	Versionierung von Produkten durch die Produktidentifikation erweitert um Klartextnamen	gemSpec_OM
GS-A_4626	CPI für CV-Zertifikate einer Karte	gemSpec_PKI
GS-A_4627	Verwendung des Feldes Certificate Authority Reference	gemSpec_PKI
GS-A_4630	CHR des CV-Zertifikats einer Chipkarte	gemSpec_PKI
GS-A_4631	CHA des CV-Zertifikats einer Karte	gemSpec_PKI
GS-A_4633	OID für CV-Zertifikate einer Karte	gemSpec_PKI

GS-A_4634	Öffentlicher Schlüssel eines CV-Zertifikats	gemSpec_PKI
GS-A_4636	Aufbau eines CV-Zertifikats zur Authentisierung	gemSpec_PKI
GS-A_4986	Datenobjekt für das Feld Card Profile Identifier in G2	gemSpec_PKI
GS-A_4987	Wert des Card Profile Identifier in G2	gemSpec_PKI
GS-A_4988	Datenobjekt für das Feld Certificate Authority Reference in G2	gemSpec_PKI
GS-A_4989	Länge der Certificate Authority Reference in G2	gemSpec_PKI
GS-A_4990	Verwendung des Feldes Certificate Authority Reference in G2	gemSpec_PKI
GS-A_4992	Datenobjekt für den öffentlichen Schlüssel	gemSpec_PKI
GS-A_4993	Aufbau eines öffentlichen Schlüssel	gemSpec_PKI
GS-A_4994	Datenobjekt für die Certificate Holder Reference	gemSpec_PKI
GS-A_4995	Wertfeld der Certificate Holder Reference	gemSpec_PKI
GS-A_4996	Wertfeld des Certificate Holder Authorization Templates	gemSpec_PKI
GS-A_4997	Aufbau der Certificate Holder Authorization Templates	gemSpec_PKI
GS-A_4998	Datenobjekt des Certificate Effective Date	gemSpec_PKI
GS-A_4999	Länge des Certificate Effective Date	gemSpec_PKI
GS-A_5000	Format des Certificate Effective Date	gemSpec_PKI
GS-A_5001	Datenobjekt des Certificate Expiration Date	gemSpec_PKI
GS-A_5002	Länge des Certificate Expiration Date	gemSpec_PKI
GS-A_5003	Format des Certificate Expiration Date	gemSpec_PKI
GS-A_5004	Tag der zu signierenden Nachricht M eines CV-Zertifikates	gemSpec_PKI
GS-A_5005	Datenstruktur der zu signierenden Nachricht M eines CV-Zertifikates	gemSpec_PKI
GS-A_5006	Signatur des Zertifikatsdatenobjekts	gemSpec_PKI
GS-A_5007	Tag eines Zertifikatsdatenobjekts	gemSpec_PKI
GS-A_5008	Aufbau eines Zertifikatsdatenobjekts	gemSpec_PKI

### 3.1.2 Herstellererklärung funktionale Eignung

In diesem Abschnitt sind alle funktionalen und nichtfunktionalen Anforderungen an den technischen Teil des Produkttyps verzeichnet, deren durchgeführte bzw. geplante

Umsetzung und Beachtung der Hersteller bzw. der Anbieter durch eine Herstellererklärung bestätigt bzw. zusagt.

**Tabelle 3: Anforderungen zur funktionalen Eignung "Herstellererklärung"**

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
GS-A_2162	Kryptographisches Material in Entwicklungs- und Testumgebungen	gemKPT_Test
TIP1-A_6079	Updates von Referenzobjekten	gemKPT_Test
TIP1-A_6080	Softwarestand von Referenzobjekten	gemKPT_Test
TIP1-A_6081	Bereitstellung der Referenzobjekte	gemKPT_Test
TIP1-A_6085	Referenzobjekte eines Produkts	gemKPT_Test
TIP1-A_6088	Unterstützung bei Fehlernachstellung	gemKPT_Test
TIP1-A_6093	Ausprägung der Referenzobjekte	gemKPT_Test
TIP1-A_7333	Parallelbetrieb von Release oder Produkttypversion	gemKPT_Test
TIP1-A_7334	Risikoabschätzung bezüglich der Interoperabilität	gemKPT_Test
TIP1-A_7335	Bereitstellung der Testdokumentation	gemKPT_Test
TIP1-A_7358	Qualität des Produktmusters	gemKPT_Test
TIP1-A_2557	Inhalt der Ausgabepolicy des TSP-CVC	gemSpec_CVC_TSP
TIP1-A_2564	Erzeugen von CV-Zertifikaten mit registrierten Zugriffsprofilen	gemSpec_CVC_TSP
TIP1-A_2565	Einholung von Qualifizierungen	gemSpec_CVC_TSP
TIP1-A_2566	Nachweis über die Qualifizierung	gemSpec_CVC_TSP
TIP1-A_2568	Erzeugen von CV-Zertifikaten mit Profilen, die einer Qualifizierung bedürfen	gemSpec_CVC_TSP
TIP1-A_2592	Darstellung der Zusammenarbeit der beteiligten Akteure im Sicherheitskonzept	gemSpec_CVC_TSP
TIP1-A_2593	Schützenswerte Objekte des TSP-CVC	gemSpec_CVC_TSP
TIP1-A_2594	Vorgaben zum Schutzbedarf durch die gematik	gemSpec_CVC_TSP
TIP1-A_2595	Spezifische Erhöhung des Schutzbedarfs ist zulässig	gemSpec_CVC_TSP
TIP1-A_2596	Schutzbedarf darf nicht erniedrigt werden	gemSpec_CVC_TSP
TIP1-A_2598	Verwendung des Schlüsselpaars der CVC-CA	gemSpec_CVC_TSP
TIP1-A_2599	Begrenzung der Lebensdauer des Schlüsselpaars der CVC-	gemSpec_CVC_TSP

	CA	
TIP1-A_2600	Gültigkeitsdauer der CVC-CA Schlüssel	gemSpec_CVC_TSP
TIP1-A_2601	Ablauf der Gültigkeitsdauer des privaten Schlüssels der CVC-CA	gemSpec_CVC_TSP
TIP1-A_2602	Weiterverwendung des privaten Schlüssels einer CVC-CA	gemSpec_CVC_TSP
TIP1-A_2603	Vernichtung nicht mehr benötigter Schlüssel	gemSpec_CVC_TSP
TIP1-A_2604	Vernichtung der privaten Schlüssel bei Verlust der Zulassung	gemSpec_CVC_TSP
TIP1-A_2606	Information über die Vernichtung aller Schlüsselpaare an gematik	gemSpec_CVC_TSP
TIP1-A_2611	Berücksichtigung des Klonens im Sicherheitskonzept	gemSpec_CVC_TSP
TIP1-A_2619	Authentizität des öffentlichen Schlüssels der CVC-CA bei Zertifikatsbeantragung	gemSpec_CVC_TSP
TIP1-A_2626	Berücksichtigung von Notfallmaßnahmen im Sicherheitskonzept	gemSpec_CVC_TSP
TIP1-A_2627	Wechsel der Schlüsselversion bei der CVC-CA	gemSpec_CVC_TSP
TIP1-A_2633	Prüfung der Protokolldaten durch die gematik	gemSpec_CVC_TSP
TIP1-A_2634	Berücksichtigung von Rollen	gemSpec_CVC_TSP
TIP1-A_2635	Definition der Rollen und Festlegungen ihrer Aufgaben	gemSpec_CVC_TSP
TIP1-A_2636	Benennung von Mitarbeitern gegenüber gematik	gemSpec_CVC_TSP
TIP1-A_2637	Berücksichtigung von Zugriffen auf das HSM im Vier-Augen-Prinzip	gemSpec_CVC_TSP
TIP1-A_2650	Behandlung negativer Prüfergebnisse im Sicherheitskonzept	gemSpec_CVC_TSP
TIP1-A_2654	Antrag für ein CVC-CA-Zertifikat bei der CVC-Root-CA	gemSpec_CVC_TSP
TIP1-A_2655	Konsistenz des CA-Namens	gemSpec_CVC_TSP
TIP1-A_2656	Beantragung und Rollen	gemSpec_CVC_TSP
TIP1-A_2657	Korrektheit der Angaben	gemSpec_CVC_TSP
TIP1-A_2658	Nutzung der Schnittstelle zur Beantragung eines CVC-CA-Zertifikats	gemSpec_CVC_TSP
TIP1-A_2660	CA-Namen bei Betrieb mehrerer CVC-CAs	gemSpec_CVC_TSP
TIP1-A_2665	Berechtigung des Antragstellers für CV-Zertifikate	gemSpec_CVC_TSP
TIP1-A_2666	Schriftliche Beantragung von CV-Zertifikaten durch einen	gemSpec_CVC_TSP

	Kartenherausgeber	
TIP1-A_2669	Ausgangsdaten der CV-Zertifikatserzeugung, die durch die CVC-CA zur Verfügung gestellt werden	gemSpec_CVC_TSP
TIP1-A_2671	Anforderungen an die Datenintegrität und -authentizität	gemSpec_CVC_TSP
TIP1-A_2672	Anforderungen an die Vertraulichkeit	gemSpec_CVC_TSP
TIP1-A_2673	Berücksichtigung von Eingangsdaten gemäß [gemSpec_PKI]	gemSpec_CVC_TSP
TIP1-A_2676	Verwendung der Eingangsdaten	gemSpec_CVC_TSP
TIP1-A_2677	Signierung des CV-Zertifikats durch die CVC-CA	gemSpec_CVC_TSP
TIP1-A_2680	Eindeutigkeit der Zuordnung zwischen CAR und Schlüsselpaar der CVC-CA	gemSpec_CVC_TSP
TIP1-A_2695	Verfahren zur Zeitsynchronisierung	gemSpec_CVC_TSP
TIP1-A_2696	Sicherstellung der Zuordnung von CV-Zertifikaten bei mehreren CVC-CAs mit gleichem Namen	gemSpec_CVC_TSP
TIP1-A_3029	Name einer Test-CVC-CA	gemSpec_CVC_TSP
TIP1-A_3030	Betrieb von Test-CVC-CAs	gemSpec_CVC_TSP
TIP1-A_3031	Registrierung einer Test-CVC-CA	gemSpec_CVC_TSP
TIP1-A_4228	Angaben in der Beantragung eines CVC-CA-Zertifikats	gemSpec_CVC_TSP
TIP1-A_4229	Optionale Sicherheitsmechanismen bei Ausgabe von Test-CV-Zertifikaten	gemSpec_CVC_TSP
TIP1-A_5378	Setzen der Certificate Effective Date (CED)	gemSpec_CVC_TSP
TIP1-A_5379	Setzen der Certificate Expiration Date (CXD)	gemSpec_CVC_TSP
TIP1-A_5381	Zugang zu HSM-Systemen im Vier-Augen-Prinzip	gemSpec_CVC_TSP
GS-A_4820	Schnittstelle I_NTP_Time_Information, Nutzung durch Zentrale Dienste der TI-Plattform	gemSpec_Net
GS-A_4821	Schnittstelle I_NTP_Time_Information, Ersatzverfahren für Zentrale Dienste der TI-Plattform	gemSpec_Net
GS-A_5082	OID-Festlegung für Flaglisten bei CV-Zertifikaten der Kartengeneration 2	gemSpec_OID
GS-A_3695	Grundlegender Aufbau Versionsnummern	gemSpec_OM
GS-A_3696	Zeitpunkt der Erzeugung neuer Versionsnummern	gemSpec_OM
GS-A_3697	Anlass der Erhöhung von Versionsnummern	gemSpec_OM
GS-A_3702	Inhalt der Selbstauskunft von Produkten außer Karten	gemSpec_OM

GS-A_3804	Eigenschaften eines FehlerLog-Eintrags	gemSpec_OM
GS-A_3805	Loglevel zur Bezeichnung der Granularität FehlerLog	gemSpec_OM
GS-A_3806	Loglevel in der Referenz- und Testumgebung	gemSpec_OM
GS-A_3807	Fehlerspeicherung ereignisgesteuerter Nachrichtenverarbeitung	gemSpec_OM
GS-A_4541	Nutzung der Produkttypversion zur Kompatibilitätsprüfung	gemSpec_OM
GS-A_4543	Rückgabe der Selbstauskunft von zentralen Produkttypen der TI-Plattform und fachanwendungsspezifischen Diensten	gemSpec_OM
GS-A_5018	Sicherheitsrelevanter Fehler an organisatorischen Schnittstellen	gemSpec_OM
GS-A_5033	Betriebsdokumentation der zentralen Produkte der TI-Plattform und anwendungsspezifischen Diensten	gemSpec_OM
GS-A_5038	Festlegungen zur Vergabe einer Produktversion	gemSpec_OM
GS-A_5039	Änderung der Produktversion bei Änderungen der Produkttypversion	gemSpec_OM
GS-A_4257	Hauptsitz und Betriebsstätte	gemSpec_PKI
GS-A_4628	Zuordnung zwischen CAR und Schlüsselpaar des Herausgebers für Gen1	gemSpec_PKI
GS-A_4991	Zuordnung von CAR zu Schlüsselpaar des Herausgebers für G2	gemSpec_PKI

## 3.2 Anforderungen zur sicherheitstechnischen Eignung

### 3.2.1 CC-Evaluierung

Eine Zertifizierung nach Common Criteria [CC] ist nicht erforderlich.

### 3.2.2 Sicherheitsgutachten

Die in diesem Abschnitt verzeichneten Anforderungen sind Gegenstand der Prüfung der Sicherheitseignung gemäß [gemRL\_PruefSichEig]. Das entsprechende Sicherheitsgutachten ist der gematik vorzulegen.

**Tabelle 4: Anforderungen zur sicherheitstechnischen Eignung "Sicherheitsgutachten"**

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
TIP1-A_2557	Inhalt der Ausgabepolicy des TSP-CVC	gemSpec_CVC_TSP
TIP1-A_2592	Darstellung der Zusammenarbeit der beteiligten	gemSpec_CVC_TSP

	Akteure im Sicherheitskonzept	
TIP1-A_2593	Schützenswerte Objekte des TSP-CVC	gemSpec_CVC_TSP
TIP1-A_2594	Vorgaben zum Schutzbedarf durch die gematik	gemSpec_CVC_TSP
TIP1-A_2595	Spezifische Erhöhung des Schutzbedarfs ist zulässig	gemSpec_CVC_TSP
TIP1-A_2596	Schutzbedarf darf nicht erniedrigt werden	gemSpec_CVC_TSP
TIP1-A_2598	Verwendung des Schlüsselpaars der CVC-CA	gemSpec_CVC_TSP
TIP1-A_2599	Begrenzung der Lebensdauer des Schlüsselpaars der CVC-CA	gemSpec_CVC_TSP
TIP1-A_2600	Gültigkeitsdauer der CVC-CA Schlüssel	gemSpec_CVC_TSP
TIP1-A_2601	Ablauf der Gültigkeitsdauer des privaten Schlüssels der CVC-CA	gemSpec_CVC_TSP
TIP1-A_2602	Weiterverwendung des privaten Schlüssels einer CVC-CA	gemSpec_CVC_TSP
TIP1-A_2604	Vernichtung der privaten Schlüssel bei Verlust der Zulassung	gemSpec_CVC_TSP
TIP1-A_2605	Maßnahmen zur Vernichtung von Schlüsseln	gemSpec_CVC_TSP
TIP1-A_2607	Einsatz eines HSM	gemSpec_CVC_TSP
TIP1-A_2608	Speicherung und Anwendung des privaten Schlüssels in einem HSM	gemSpec_CVC_TSP
TIP1-A_2609	Einsatz einer Chipkarte als HSM	gemSpec_CVC_TSP
TIP1-A_2610	Möglichkeit zum Klonen eines HSM	gemSpec_CVC_TSP
TIP1-A_2611	Berücksichtigung des Klonens im Sicherheitskonzept	gemSpec_CVC_TSP
TIP1-A_2612	Anwendung des Vier-Augen-Prinzips beim Klonen eines HSMs	gemSpec_CVC_TSP
TIP1-A_2613	Protokollierung beim Klonen eines HSMs	gemSpec_CVC_TSP
TIP1-A_2614	Nachvollziehbarkeit über die Klone eines HSMs	gemSpec_CVC_TSP
TIP1-A_2615	Einsatz der Klone eines HSMs im geschützten Bereich der Betriebsstätte	gemSpec_CVC_TSP
TIP1-A_2616	Evaluierung von HSMs – TSP-CVC	gemSpec_CVC_TSP
TIP1-A_2617	Vorgaben an die Funktionalität des HSM der CVC-CA	gemSpec_CVC_TSP
TIP1-A_2618	Weitergabe sensibler Schlüssel	gemSpec_CVC_TSP
TIP1-A_2620	Backup und Verfügbarkeit der CVC-CA für Produktiv- und Testumgebung	gemSpec_CVC_TSP

TIP1-A_2621	Backup-HSMs – sicherer Schlüsseltransport CVC-CA	gemSpec_CVC_TSP
TIP1-A_2622	Erzeugung eines Backup-HSMs – Einhaltung weiterer Vorgaben	gemSpec_CVC_TSP
TIP1-A_2626	Berücksichtigung von Notfallmaßnahmen im Sicherheitskonzept	gemSpec_CVC_TSP
TIP1-A_2628	Protokollierung durch den TSP-CVC - Ereignisse	gemSpec_CVC_TSP
TIP1-A_2629	Protokollierung durch den TSP-CVC – Profil ungleich 0	gemSpec_CVC_TSP
TIP1-A_2630	Protokollierung pro Bestellung/Produktionslauf (Profil gleich 0)	gemSpec_CVC_TSP
TIP1-A_2631	Nachvollziehbarkeit bei Produktion mit Profil 0	gemSpec_CVC_TSP
TIP1-A_2632	Schutz der Protokolldaten gegen Manipulation	gemSpec_CVC_TSP
TIP1-A_2634	Berücksichtigung von Rollen	gemSpec_CVC_TSP
TIP1-A_2635	Definition der Rollen und Festlegungen ihrer Aufgaben	gemSpec_CVC_TSP
TIP1-A_2636	Benennung von Mitarbeitern gegenüber gematik	gemSpec_CVC_TSP
TIP1-A_2637	Berücksichtigung von Zugriffen auf das HSM im Vier-Augen-Prinzip	gemSpec_CVC_TSP
TIP1-A_2641	Geschützter Bereich	gemSpec_CVC_TSP
TIP1-A_2642	Verwendung mehrerer geschützter Bereiche	gemSpec_CVC_TSP
TIP1-A_2644	Schutz von HSM-Klonen	gemSpec_CVC_TSP
TIP1-A_2645	Zugriffe auf Systeme der CVC-CA über Arbeitsplatzrechner (oder Systeme) außerhalb des geschützten Bereichs	gemSpec_CVC_TSP
TIP1-A_2647	Sicherer Betrieb von Systemkomponenten	gemSpec_CVC_TSP
TIP1-A_2648	Vier-Augen-Prinzip bei Beantragung des CVC-CA-Zertifikats	gemSpec_CVC_TSP
TIP1-A_2649	Konsistenzprüfung des ausgestellten CVC-CA-Zertifikats	gemSpec_CVC_TSP
TIP1-A_2650	Behandlung negativer Prüfergebnisse im Sicherheitskonzept	gemSpec_CVC_TSP
TIP1-A_2671	Anforderungen an die Datenintegrität und -authentizität	gemSpec_CVC_TSP
TIP1-A_2672	Anforderungen an die Vertraulichkeit	gemSpec_CVC_TSP
TIP1-A_2691	Protokollierung durch den TSP-CVC - Werte	gemSpec_CVC_TSP
TIP1-A_2692	Protokollierung durch den TSP-CVC – Profil gleich 0	gemSpec_CVC_TSP

TIP1-A_4223	Ordnungsgemäße Sicherung des privaten Schlüssels der CVC-CA	gemSpec_CVC_TSP
TIP1-A_4224	Verwendung von privaten Schlüsseln einer CVC-CA	gemSpec_CVC_TSP
TIP1-A_4225	Nutzung eines HSM nach erfolgreicher Benutzerauthentisierung	gemSpec_CVC_TSP
GS-A_2158-01	Trennung von kryptographischen Identitäten und Schlüsseln in Produktiv- und Testumgebungen	gemSpec_DS_Anbieter
GS-A_2328-01	Pflege und Fortschreibung des Sicherheitskonzeptes und Notfallkonzeptes	gemSpec_DS_Anbieter
GS-A_2329-01	Umsetzung der Sicherheitskonzepte	gemSpec_DS_Anbieter
GS-A_2331-01	Sicherheitsvorfalls-Management	gemSpec_DS_Anbieter
GS-A_2332-01	Notfallmanagement	gemSpec_DS_Anbieter
GS-A_2345-01	regelmäßige Reviews	gemSpec_DS_Anbieter
GS-A_3078	Anbieter einer Schlüsselverwaltung: verpflichtende Migrationsstrategie bei Schwächung kryptographischer Primitive	gemSpec_DS_Anbieter
GS-A_3125	Schlüsselinstallation und Verteilung: Dokumentation gemäß Minimalitätsprinzip	gemSpec_DS_Anbieter
GS-A_3130	Krypto_Schlüssel_Installation: Dokumentation der Schlüsselinstallation gemäß Minimalitätsprinzip	gemSpec_DS_Anbieter
GS-A_3139	Krypto_Schlüssel: Dienst Schlüsselableitung	gemSpec_DS_Anbieter
GS-A_3141	Krypto_Schlüssel_Ableitung: Maßnahmen bei Bekanntwerden von Schwächen in der Schlüsselableitungsfunktion	gemSpec_DS_Anbieter
GS-A_3149	Krypto_Schlüssel_Archivierung: Dokumentation der Schlüsselarchivierung gemäß Minimalitätsprinzip	gemSpec_DS_Anbieter
GS-A_3737-01	Sicherheitskonzept	gemSpec_DS_Anbieter
GS-A_3753-01	Notfallkonzept	gemSpec_DS_Anbieter
GS-A_3772-01	Notfallkonzept: Der Dienstanbieter soll dem BSI-Standard 100-4 folgen	gemSpec_DS_Anbieter
GS-A_4980-01	Umsetzung der Norm ISO/IEC 27001	gemSpec_DS_Anbieter
GS-A_4981-01	Erreichen der Ziele der Norm ISO/IEC 27001 Annex A	gemSpec_DS_Anbieter
GS-A_4982-01	Umsetzung der Maßnahmen der Norm ISO/IEC 27002	gemSpec_DS_Anbieter
GS-A_4983-01	Umsetzung der Maßnahmen aus dem BSI-Grundschutz	gemSpec_DS_Anbieter
GS-A_4984-01	Befolgen von herstellerepezifischen Vorgaben	gemSpec_DS_Anbieter

GS-A_5551	Betriebsumgebung in einem Mitgliedstaat der EU bzw. des EWR	gemSpec_DS_Anbieter
GS-A_5557	Security Monitoring	gemSpec_DS_Anbieter
GS-A_5558	Aktive Schwachstellenscans	gemSpec_DS_Anbieter
GS-A_4363	CV-Zertifikate G1	gemSpec_Krypt
GS-A_4364	CV-CA-Zertifikate G1	gemSpec_Krypt
GS-A_4365	CV-Zertifikate G2	gemSpec_Krypt
GS-A_4366	CV-CA-Zertifikate G2	gemSpec_Krypt
GS-A_4367	Zufallszahlengenerator	gemSpec_Krypt
GS-A_4368	Schlüsselerzeugung	gemSpec_Krypt
GS-A_4393	Algorithmus bei der Erstellung von Hashwerten von Zertifikaten oder öffentlichen Schlüsseln	gemSpec_Krypt
GS-A_5079	Migration von Algorithmen und Schlüssellängen bei PKI-Betreibern	gemSpec_Krypt

### 3.2.3 Herstellererklärung sicherheitstechnische Eignung

Sofern in diesem Abschnitt Anforderungen verzeichnet sind, muss der Hersteller bzw. der Anbieter deren Umsetzung und Beachtung zum Nachweis der sicherheitstechnischen Eignung durch eine Herstellererklärung bestätigen bzw. zusagen.

**Tabelle 5: Anforderungen zur sicherheitstechnischen Eignung "Herstellererklärung"**

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
TIP1-A_6517	Eigenverantwortlicher Test: TBV	gemKPT_Test
TIP1-A_6518	Eigenverantwortlicher Test: TDI	gemKPT_Test
TIP1-A_6519	Eigenverantwortlicher Test: Hersteller und Anbieter	gemKPT_Test
TIP1-A_6523	Zulassungstest: Hersteller und Anbieter	gemKPT_Test
TIP1-A_6524	Testdokumentation gemäß Vorlagen	gemKPT_Test
TIP1-A_6526	Produkttypen: Bereitstellung	gemKPT_Test
TIP1-A_6532	Zulassung eines neuen Produkts: Aufgaben der TDI	gemKPT_Test
TIP1-A_6533	Zulassung eines neuen Produkts: Aufgaben der Hersteller und Anbieter	gemKPT_Test
TIP1-A_6536	Zulassung eines geänderten Produkts: Aufgaben der TDI	gemKPT_Test

TIP1-A_6537	Zulassung eines geänderten Produkts: Aufgaben der Hersteller und Anbieter	gemKPT_Test
TIP1-A_6538	Durchführung von Produkttests	gemKPT_Test
TIP1-A_6539	Durchführung von Produktübergreifenden Tests	gemKPT_Test
TIP1-A_6772	Partnerprodukte bei Interoperabilitätstests	gemKPT_Test
GS-A_2355-01	Meldung von erheblichen Schwachstellen und Bedrohungen	gemSpec_DS_Anbieter
GS-A_4523-01	Bereitstellung Kontaktinformationen für Informationssicherheit	gemSpec_DS_Anbieter
GS-A_4524-01	Meldung von Änderungen der Kontaktinformationen für Informationssicherheit	gemSpec_DS_Anbieter
GS-A_4526-01	Aufbewahrungsvorgaben an die Nachweise zu Sicherheitsmeldungen	gemSpec_DS_Anbieter
GS-A_4530-01	Maßnahmen zur Behebung von erheblichen Sicherheitsvorfällen und Notfällen	gemSpec_DS_Anbieter
GS-A_4532-01	Nachweis der Umsetzung von Maßnahmen in Folge eines erheblichen Sicherheitsvorfalls oder Notfalls	gemSpec_DS_Anbieter
GS-A_5017-01	Meldung und Behandlung von Schwachstellen	gemSpec_DS_Anbieter
GS-A_5324-01	Teilnahme des Anbieters an Sitzungen des kISMS	gemSpec_DS_Anbieter
GS-A_5555	Unverzügliche Meldung von erheblichen Sicherheitsvorfällen und -notfällen	gemSpec_DS_Anbieter
GS-A_5556	Unverzügliche Behebung von erheblichen Sicherheitsvorfällen und -notfällen	gemSpec_DS_Anbieter
GS-A_5559	Bereitstellung Ergebnisse von Schwachstellenscans	gemSpec_DS_Anbieter
GS-A_5560	Entgegennahme und Prüfung von Meldungen der gematik	gemSpec_DS_Anbieter
GS-A_5561	Bereitstellung 24/7-Kontaktpunkt	gemSpec_DS_Anbieter
GS-A_5562	Bereitstellung Produktinformationen	gemSpec_DS_Anbieter
GS-A_5563	Jahressicherheitsbericht	gemSpec_DS_Anbieter
GS-A_5624	Auditrechte der gematik zur Informationssicherheit	gemSpec_DS_Anbieter
GS-A_5541	TLS-Verbindungen als TLS-Klient zur Störungsampel oder SM	gemSpec_Krypt
GS-A_5580	TLS-Klient zur Störungsampel oder zum SM (Zertifikatsprüfung)	gemSpec_Krypt
GS-A_5581	"TUC vereinfachte Zertifikatsprüfung" (Komponenten-PKI)	gemSpec_Krypt

GS-A_3813	Datenschutzvorgaben Fehlermeldungen	gemSpec_OM
-----------	-------------------------------------	------------

### 3.3 Anforderungen zur elektrischen, mechanischen und physikalischen Eignung

Anforderungen an die elektrische, physikalische oder mechanische Eignung werden von der gematik nicht erhoben.

## 4 Produktypspezifische Merkmale

In diesem Kapitel werden Anforderungen gelistet, welche abhängig vom Zertifikatsnehmer des TSP CVC nicht relevant sind und demnach nicht erfüllt werden können.

**Tabelle 6: Nicht relevante Anforderungen in der speziellen Ausprägung des TSP CVC für Karteninhaber (eGK)**

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
TIP1-A_2568	Erzeugen von CV-Zertifikaten mit Profilen, die einer Qualifizierung bedürfen	gemSpec_CVC_TSP
TIP1-A_2629	Protokollierung durch den TSP-CVC - Profil ungleich 0	gemSpec_CVC_TSP
TIP1-A_2565	Einholung von Qualifizierungen	gemSpec_CVC_TSP
TIP1-A_5378	Setzen der Certificate Effective Date (CED)	gemSpec_CVC_TSP

**Tabelle 7: Nicht relevante Anforderungen in der speziellen Ausprägung des TSP CVC für Karteninhaber (HBA, SM-B)**

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
TIP1-A_2692	Protokollierung durch den TSP-CVC - Profil gleich 0	gemSpec_CVC_TSP
TIP1-A_2630	Protokollierung pro Bestellung/Produktionslauf (Profil gleich 0)	gemSpec_CVC_TSP
TIP1-A_2631	Nachvollziehbarkeit bei Produktion mit Profil 0	gemSpec_CVC_TSP

**Tabelle 8: Nicht relevante Anforderungen in der speziellen Ausprägung des TSP CVC für Karteninhaber (gSMC)**

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
TIP1-	Protokollierung durch den TSP-CVC -	gemSpec_CVC_TSP

A_2692	Profil gleich 0	
TIP1-A_2630	Protokollierung pro Bestellung/Produktionslauf (Profil gleich 0)	gemSpec_CVC_TSP
TIP1-A_2631	Nachvollziehbarkeit bei Produktion mit Profil 0	gemSpec_CVC_TSP
TIP1-A_2565	Einholung von Qualifizierungen	gemSpec_CVC_TSP
TIP1-A_2568	Erzeugen von CV-Zertifikaten mit Profilen, die einer Qualifizierung bedürfen	gemSpec_CVC_TSP

## 5 Anhang A – Verzeichnisse

### 5.1 Abkürzungen

Kürzel	Erläuterung
Afo-ID	Anforderungs-Identifikation
CC	Common Criteria

### 5.2 Tabellenverzeichnis

Tabelle 1: Dokumente mit Anforderungen zu der Produkttypversion .....	6
Tabelle 2: Anforderungen zur funktionalen Eignung "Produkttest/Produktübergreifender Test" .....	7
Tabelle 3: Anforderungen zur funktionalen Eignung "Herstellereklärung" .....	9
Tabelle 4: Anforderungen zur sicherheitstechnischen Eignung "Sicherheitsgutachten"...	12
Tabelle 5: Anforderungen zur sicherheitstechnischen Eignung "Herstellereklärung" .....	16
Tabelle 6: Nicht relevante Anforderungen in der speziellen Ausprägung des TSP CVC für Karteninhaber (eGK).....	19
Tabelle 7: Nicht relevante Anforderungen in der speziellen Ausprägung des TSP CVC für Karteninhaber (HBA, SM-B).....	19
Tabelle 8: Nicht relevante Anforderungen in der speziellen Ausprägung des TSP CVC für Karteninhaber (gSMC).....	19

### 5.3 Referenzierte Dokumente

Neben den in Kapitel 2 angeführten Dokumenten werden referenziert:

[Quelle]	Herausgeber: Titel, Version
[CC]	Internationaler Standard: Common Criteria for Information Technology Security Evaluation <a href="https://www.commoncriteriaportal.org/cc/">https://www.commoncriteriaportal.org/cc/</a>
[gemRL_PruefSichEig].	gematik: Richtlinie zur Prüfung der

	Sicherheitseignung
--	--------------------