gematik
Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

Elektronische Gesundheitskarte und Telematikinfrastruktur

Anbietertypsteckbrief

CVC TSPs für eGK

Anbietertyp Version:	1.2.0
Anbietertyp Status:	freigegeben

Version:	1.0.1
Revision:	17231
Stand:	04.09.2018
Status:	freigegeben
Klassifizierung:	öffentlich
Referenzierung:	gemAnbT_CVC_TSP_eGK_ATV_1.2.0

Historie Anbietertypversion und Anbietertypsteckbrief

Historie Anbietertypversion

Die Anbietertypversion ändert sich, wenn sich die Anforderungslage für den Anbietertyp ändert.

Anbietertyp-version	Beschreibung der Änderung	Referenz
1.0.0	Initiale Version	
1.0.1	Anpassung auf Releasestand 1.6.4	gemAnbT_CVC_TSP_eGK_ATV1.0.1
1.1.0	Anpassung auf Releasestand 2.1.1	gemAnbT_CVC_TSP_eGK_ATV1.1.0
1.1.1	Anpassung auf Releasestand 2.1.2	gemAnbT_CVC_TSP_eGK_ATV1.1.1
1.2.0	Anpassung auf Vorab-Releasestand ZIS	gemAnbT_CVC_TSP_eGK_ATV1.2.0

Historie Anbietertypsteckbrief

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

Version	Stand	Kap.	Grund der Änderung, besondere Hinweise	Bearbeiter
1.0.0	14.05.18		freigegeben	gematik
1.0.1	04.09.18		Korrektur der Übertragung der bekannten Änderung (redaktionell)	gematik

Inhaltsverzeichnis

1 Einführung

1.1 Zielsetzung und Einordnung des Dokumentes

Dieser Anbietertypsteckbrief verzeichnet verbindlich die Anforderungen der gematik an Anbieter TSP CVC eGK zur Sicherstellung des Betriebes der von ihnen verantworteten Serviceeinheiten.

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 Anbietertypsteckbrief richtet sich an:

- Anbieter TSP CVC eGK
- die gematik im Rahmen der Zulassungsverfahren, Bestätigungsverfahren, Kooperationsverträge und Anbieterverfahren

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) 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 Anbietertyp 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 Anbietertyp normativen Anforderungen.

Tabelle 1: Dokumente mit Anforderungen zu der Anbietertypversion

Dokumentenkürzel	Bezeichnung des Dokumentes	Version
gemRL_Betr_TI	Übergreifende Richtlinien zum Betrieb der TI	2.0.1
gemSpec_DS_Anbieter	Spezifikation Datenschutz- und Sicherheitsanforderungen der TI an Anbieter	1.0.1
gemSpec_Krypt	Übergreifende Spezifikation Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur	2.10.0
gemSpec_CVC_TSP	Spezifikation Trust Service Provider CVC	1.8.1
gemKPT_Betr	Betriebskonzept Online-Produktivbetrieb (ORS 2.1)	3.0.1
gemSpec_OM	Übergreifende Spezifikation Operations und Maintenance	1.8.0
gemKPT_Test	Testkonzept der TI	2.0.0

3 Blattanforderungen

Die folgenden Abschnitte verzeichnen alle für den Anbietertypen normativen Anforderungen der gematik an Anbieter TSP CVC eGK zur Sicherstellung des Betriebes der von ihnen verantworteten Serviceeinheiten (Blattanforderungen). Die Anforderungen sind gruppiert nach der Art der Nachweisführung ihrer Erfüllung als Grundlage der Zulassung.

3.1 Anforderungen zur betrieblichen Eignung

3.1.1 Prozessprüfung betriebliche Eignung

Sofern in diesem Abschnitt Anforderungen mit Vorgaben zu organisatorischen Maßnahmen wie Prozessen und Strukturvorgaben verzeichnet sind, muss deren Erfüllung im Rahmen von Prozessprüfungen nachgewiesen werden.

Tabelle 2: Anforderungen zur betrieblichen Eignung "Prozessprüfung"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
GS-A_4095	Übermittlung von Ad-hoc Reports	gemRL_Betr_TI
GS-A_5248	Konventionen zur Struktur von Prozessdaten	gemRL_Betr_TI
GS-A_5249	Reservierte Zeichen in den Prozessdaten	gemRL_Betr_TI

3.1.2 Anbietererklärung betriebliche Eignung

Sofern in diesem Abschnitt Anforderungen mit Vorgaben zu organisatorischen Maßnahmen wie Prozessen und Strukturvorgaben der Aufbauorganisation sowie der Umgebung verzeichnet sind, muss der Anbieter deren Umsetzung und Beachtung durch eine Anbietererklärung bestätigen bzw. zusagen.

Tabelle 3: Anforderungen zur betrieblichen Eignung "Anbietererklärung"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
TIP1-A_7261	Erreichbarkeit der TI-ITSM-Teilnehmer untereinander	gemKPT_Betr
TIP1-A_7262	Haupt- und Nebenzeit der TI-ITSM-Teilnehmer	gemKPT_Betr
TIP1-	Produktverantwortung der TI-ITSM-Teilnehmer	gemKPT_Betr

A_7263		
TIP1-A_7266	Mitwirkungspflichten im TI-ITSM-System	gemKPT_Betr
TIP1-A_6367	Definition eines Business-Servicekatalog der angebotenen TI Services	gemKPT_Betr
TIP1-A_6359	Definition der notwendigen Leistung anderer Anbieter durch Anbieter und SPEDs	gemKPT_Betr
TIP1-A_6360	Kontrolle bereitgestellter Leistungen durch Anbieter und SPEDs	gemKPT_Betr
TIP1-A_6388	TIP1-A_6388 Bereitstellung eines lokalen IT-Service-Managements durch Anbieter und SPEDs für ihre zu verantwortenden Serviceeinheiten	gemKPT_Betr
TIP1-A_6390	Mitwirkung im TI-ITSM durch Anbieter und SPEDs	gemKPT_Betr
TIP1-A_6393	Verantwortung für die Weiterleitung von Anfragen	gemKPT_Betr
TIP1-A_6377	Koordination von produktverantwortlichen Anbietern und Herstellern	gemKPT_Betr
TIP1-A_6415	Fortgeführte Wahrnehmung der Serviceverantwortung bei der Delegation von Aufgaben	gemKPT_Betr
TIP1-A_6371	2nd/ 3rd-Level-Support: Single-Point-of-Contact (SPOC) für Anbieter	gemKPT_Betr
A_13573	Alternative Serviceleistung der TI-ITSM-Teilnehmer im TI-ITSM-Teilnehmersupport	gemKPT_Betr
GS-A_4090	Kommunikationssprache	gemRL_Betr_TI
GS-A_4085	Etablierung von Kommunikationsschnittstellen durch die TI-ITSM-Teilnehmer	gemRL_Betr_TI
GS-A_4086	Erreichbarkeit der Kommunikationsschnittstellen	gemRL_Betr_TI
GS-A_3886	Nutzung des TI-ITSM-Systems bei der Übermittlung eines übergreifenden Vorgangs	gemRL_Betr_TI
GS-A_4088	Benennung von Ansprechpartnern	gemRL_Betr_TI
GS-A_5402	Eigenverantwortliches Handeln bei Ausfall von Kommunikationsschnittstellen	gemRL_Betr_TI
GS-A_5401	Verschlüsselte E-Mail-Kommunikation	gemRL_Betr_TI
GS-A_3920	Eskalationseinleitung durch den TI-ITSM-Teilnehmer	gemRL_Betr_TI

GS-A_3922	Mitwirkung bei Taskforces	gemRL_Betr_TI
GS-A_3984	Service Request zur Bereitstellung der TI-Testumgebung (RU/TU)	gemRL_Betr_TI
GS-A_4114	Bereitstellung von TI-Konfigurationsdaten	gemRL_Betr_TI
GS-A_5594	Identifikation von TI-Konfigurationsdaten	gemRL_Betr_TI
GS-A_4115	Datenänderung für TI-Konfigurationsdaten	gemRL_Betr_TI
GS-A_4399	Übermittlung von Produktdaten nach Abschluss von lokal autorisierten Produkt-Changes	gemRL_Betr_TI
A_13575	Qualität von RfCs	gemRL_Betr_TI
GS-A_4400	Produkt-RfC (Master-Change) erstellen	gemRL_Betr_TI
GS-A_4398	Prüfung auf genehmigungspflichtige Produktänderung	gemRL_Betr_TI
GS-A_5597	Produkt-RfC (Sub-Changes) erstellen	gemRL_Betr_TI
GS-A_5599	Beschreibung der Verifikation des Produkt-Changes im RfC	gemRL_Betr_TI
GS-A_5600	Beschreibung der Verifikation des Produkt-Changes in Auswirkung auf andere TI-Fachanwendungen im RfC	gemRL_Betr_TI
GS-A_5370	Prüfung auf Emergency Change	gemRL_Betr_TI
GS-A_4402	Mitwirkungspflicht bei der Bewertung vom Produkt-RfC	gemRL_Betr_TI
GS-A_5610	Bearbeitungsfristen in der Bewertung von Produkt-Changes	gemRL_Betr_TI
GS-A_5611	Umsetzung von autorisierten RFC	gemRL_Betr_TI
GS-A_4419	Nutzung der Testumgebung (RU/TU)	gemRL_Betr_TI
GS-A_4417	Stetige Aktualisierung des Change-Datensatzes im TI-ITSM-System	gemRL_Betr_TI
GS-A_5601	Nachweis der Wirksamkeit des Changes	gemRL_Betr_TI
GS-A_5602	Nachweis der Wirksamkeit des Changes in Auswirkung auf andere TI-Fachanwendungen	gemRL_Betr_TI
GS-A_4407	Bereitstellung der Dokumentation des Change Managements für genehmigungspflichtige Produkt-Changes	gemRL_Betr_TI
GS-A_4425	Übermittlung von Optimierungsmöglichkeiten zur Umsetzung von genehmigten Produkt-Changes	gemRL_Betr_TI

GS-A_4418	Übermittlung von Abweichungen vom Produkt-RfC	gemRL_Betr_TI
GS-A_4424	Umsetzung des Fallbackplans	gemRL_Betr_TI
GS-A_5366	Mitwirkungspflicht der TI-ITSM-Teilnehmer bei der Festsetzung von Standard-Produkt-Changes	gemRL_Betr_TI
GS-A_5378	Durchführung von Emergency-Changes durch TI-ITSM-Teilnehmer	gemRL_Betr_TI
GS-A_5361	Durchführung von Emergency Changes durch TI-ITSM-Anbieter bei Nichterreichbarkeit des Gesamtverantwortlichen der TI	gemRL_Betr_TI
GS-A_4405	Service Level Requirements im Change und Release Management	gemRL_Betr_TI
GS-A_4117	Informationsbereitstellung durch TI-ITSM-Teilnehmer	gemRL_Betr_TI
GS-A_5603	Eingangskanal für Informationen von TI-ITSM-Teilnehmern	gemRL_Betr_TI
GS-A_5608	Übermittlung von CSV-Dateien	gemRL_Betr_TI
GS-A_4121	Analyse Auswirkungen möglicher Schadensereignisse auf Sicherheit und Funktion der TI-Services	gemRL_Betr_TI
GS-A_4123	Entwicklung und Pflege der TI-Notfallvorsorgedokumentation	gemRL_Betr_TI
GS-A_4124	Umsetzung Vorkehrungen zur TI-Notfallvorsorge	gemRL_Betr_TI
GS-A_4126	Eskalation TI-Notfälle	gemRL_Betr_TI
GS-A_4127	Sofortmaßnahmen TI-Notfälle	gemRL_Betr_TI
GS-A_4128	Bewältigung der TI-Notfälle	gemRL_Betr_TI
GS-A_4129	Unterstützung bei TI-Notfällen	gemRL_Betr_TI
GS-A_4130	Festlegung der Schnittstellen des EMC	gemRL_Betr_TI
GS-A_4132	Durchführung der Wiederherstellung und TI-Notfällen	gemRL_Betr_TI
GS-A_4134	Auswertungen von TI-Notfällen	gemRL_Betr_TI
GS-A_4136	Statusinformation bei TI-Notfällen	gemRL_Betr_TI
GS-A_4137	Dokumentation im TI-Notfall-Logbuch	gemRL_Betr_TI
GS-A_4138	Erstellung des Wiederherstellungsberichts nach TI-Notfällen	gemRL_Betr_TI

3.1.3 Betriebshandbuch betriebliche Eignung

Sofern in diesem Abschnitt Anforderungen mit Vorgaben zu organisatorischen Maßnahmen wie Prozessen und Strukturvorgaben der Aufbauorganisation sowie der Umgebung verzeichnet sind, muss der Anbieter deren Umsetzung und Beachtung durch die Vorlage des Betriebshandbuches nachweisen.

Der Umfang und Inhalt des Betriebshandbuches ist der Definition in der Richtlinie Betrieb [gemRL_Betr_TI] zu entnehmen.

Tabelle 4: Anforderungen zur betrieblichen Eignung "Betriebshandbuch"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
	Es liegen keine Anforderungen vor	

3.2 Anforderungen zur sicherheitstechnischen Eignung

3.2.1 Sicherheitsgutachten

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

Hinweis:

Einige Anforderungen sind sowohl in diesem Anbietertypsteckbrief, als auch in zugehörigen Produkttypsteckbriefen enthalten, da ein Nachweis der Erfüllung (ggf. auch anteilig) in Abhängigkeit von der Umsetzung sowohl durch die Anbieter der Produkte (Produktzulassung bzw. -bestätigung), als auch durch den Anbieter von Betriebsleistungen (Anbieterzulassung bzw. -bestätigung) erfolgen muss.

Abhängig von der konkreten Umsetzung können allerdings entsprechend [gemRL_PruefSichEig] Anforderungen, die nur für die Anbieter der zugehörigen Produkte relevant sind, vom Sicherheitsgutachter als „entbehrlich“ bewertet werden. Weiterhin können Anforderungen, die zwar relevant sind, aber bereits vollständig vom Anbieter der zugehörigen Produkte erfüllt werden, vom Sicherheitsgutachter über Referenzieren der bestehenden Sicherheitsgutachten der Produktanbieter als umgesetzt bewertet werden.

Tabelle 5: Anforderungen zur sicherheitstechnischen Eignung "Sicherheitsgutachten"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
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_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_2671	Anforderungen an die Datenintegrität und -authentizität	gemSpec_CVC_TSP
TIP1−A_2672	Anforderungen an die Vertraulichkeit	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_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_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_2632	Schutz der Protokolldaten gegen Manipulation	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_4225	Nutzung eines HSM nach erfolgreicher Benutzerauthentisierung	gemSpec_CVC_TSP

TIP1−A_2618	Weitergabe sensitiver 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_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_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_2557	Inhalt der Ausgabepolicy des TSP-CVC	gemSpec_CVC_TSP
TIP1−A_2592	Darstellung der Zusammenarbeit der beteiligten Akteure im Sicherheitskonzept	gemSpec_CVC_TSP
TIP1−A_2604	Vernichtung der privaten Schlüssel bei Verlust der Zulassung	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-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_2605	Maßnahmen zur Vernichtung von Schlüsseln	gemSpec_CVC_TSP
TIP1−A_2607	Einsatz eines HSM	gemSpec_CVC_TSP

GS-A_2329-01	Umsetzung der Sicherheitskonzepte	gemSpec_DS_Anbieter
GS-A_2345-01	regelmäßige Reviews	gemSpec_DS_Anbieter
GS-A_5551	Betriebsumgebung in einem Mitgliedstaat der EU bzw. des EWR	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_3772-01	Notfallkonzept: Der Dienstanbieter soll dem BSI-Standard 100-4 folgen	gemSpec_DS_Anbieter
GS-A_2328-01	Pflege und Fortschreibung des Sicherheitskonzeptes und Notfallkonzeptes	gemSpec_DS_Anbieter
GS-A_2332-01	Notfallmanagement	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_3737-01	Sicherheitskonzept	gemSpec_DS_Anbieter
GS-A_2158-01	Trennung von kryptographischen Identitäten und Schlüsseln in Produktiv- und Testumgebungen	gemSpec_DS_Anbieter
GS-A_4984-01	Befolgen von herstellerspezifischen Vorgaben	gemSpec_DS_Anbieter
GS-A_2331-01	Sicherheitsvorfalls-Management	gemSpec_DS_Anbieter
GS-A_3753-01	Notfallkonzept	gemSpec_DS_Anbieter
GS-A_4367	Zufallszahlengenerator	gemSpec_Krypt
GS-A_4368	Schlüsselerzeugung	gemSpec_Krypt
GS-A_4365	CV-Zertifikate G2	gemSpec_Krypt
GS-A_4366	CV-CA-Zertifikate G2	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

Ein TSP CVC, der gleichzeitig eine VDA Qualifizierung für X.509 QES vorweist, kann ein reduziertes Sicherheitsgutachten vorlegen. Voraussetzung hierfür ist, dass der Anbieter

- ein qualifizierter Vertrauensdiensteanbieter für QES ist und die Konformität geeignet nachweist (z.B. mittels Qualifikationsbescheid der Bundesnetzagentur).
- erklärt, dass für die gegenständlichen Sicherheitsanforderungen der Betrieb des TSP CVC äquivalent zum VDA Bereich erfolgt.

Folgende Anforderungen müssen unter den o.g. Voraussetzungen nicht im Sicherheitsgutachten nachgewiesen werden:

Tabelle 6: nicht nachzuweisende Anforderungen

GS-A_3772-01	GS-A_4982-01	GS-A_2158-01
GS-A_4980-01	GS-A_4983-01	GS-A_2331-01
GS-A_3737-01	GS-A_4984-01	GS-A_2332-01
GS-A_4981-01	GS-A_2328-01	GS-A_2345-01
GS-A_3753-01	GS-A_2329-01	

3.2.2 Anbietererklärung sicherheitstechnische Eignung

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

Tabelle 7: Anforderungen zur sicherheitstechnischen Eignung "Anbietererklärung"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
TIP1−A_6532	Zulassung eines neuen Produkts: Aufgaben der TDI	gemKPT_Test
GS−A_5017−01	Meldung und Behandlung von Schwachstellen	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_5324−01	Teilnahme des Anbieters an Sitzungen des kISMS	gemSpec_DS_Anbieter
TIP1−A_6772	Partnerprodukte bei Interoperabilitätstests	gemKPT_Test
TIP1−A_6524	Testdokumentation gemäß Vorlagen	gemKPT_Test
TIP1−A_6536	Zulassung eines geänderten Produkts: Aufgaben der TDI	gemKPT_Test
TIP1−A_6529	Produkttypen: Mindestumfang der Interoperabilitätsprüfung	gemKPT_Test

GS-A_5555	Unverzügliche Meldung von erheblichen Sicherheitsvorfällen und -notfällen	gemSpec_DS_Anbieter
GS-A_2355-01	Meldung von erheblichen Schwachstellen und Bedrohungen	gemSpec_DS_Anbieter
GS-A_5562	Bereitstellung Produktinformationen	gemSpec_DS_Anbieter
GS-A_5563	Jahressicherheitsbericht	gemSpec_DS_Anbieter
GS-A_4526-01	Aufbewahrungsvorgaben an die Nachweise zu Sicherheitsmeldungen	gemSpec_DS_Anbieter
GS-A_5624	Auditrechte der gematik zur Informationssicherheit	gemSpec_DS_Anbieter
GS-A_4523-01	Bereitstellung Kontaktinformationen für Informationssicherheit	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_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
TIP1-A_6517	Eigenverantwortlicher Test: TBV	gemKPT_Test
TIP1-A_6519	Eigenverantwortlicher Test: Hersteller und Anbieter	gemKPT_Test
TIP1-A_6523	Zulassungstest: Hersteller und Anbieter	gemKPT_Test
TIP1-A_6538	Durchführung von Produkttests	gemKPT_Test
TIP1-A_6539	Durchführung von Produktübergreifenden Tests	gemKPT_Test
GS-A_4524-01	Meldung von Änderungen der Kontaktinformationen für Informationssicherheit	gemSpec_DS_Anbieter
TIP1-A_6533	Zulassung eines neuen Produkts: Aufgaben der Hersteller und Anbieter	gemKPT_Test
TIP1-A_6537	Zulassung eines geänderten Produkts: Aufgaben der Hersteller und Anbieter	gemKPT_Test
TIP1-A_6526	Produkttypen: Bereitstellung	gemKPT_Test
GS-A_3813	Datenschutzvorgaben Fehlermeldungen	gemSpec_OM

4 Anhang A – Verzeichnisse

4.1 Abkürzungen

Kürzel	Erläuterung
Afo-ID	Anforderungs-Identifikation
CC	Common Criteria
SPED	Service Provider Endnutzernahe Dienstleister

4.2 Tabellenverzeichnis

4.3 Referenzierte Dokumente

Neben den in Kapitel 2 angeführten Dokumenten werden referenziert:

[Quelle]	Herausgeber: Titel, Version
[gemRL_PruefSichEig].	gematik: Richtlinie zur Prüfung der Sicherheitseignung
[eIDAS]	Verordnung (EU) Nr. 910/2014 des europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG