Einführung der Gesundheitskarte

Produkttypsteckbrief

Prüfvorschrift

CVC-Root – ECC

Produkttypversion: **1.3.0-2**

Produkttypstatus: **freigegeben**

Version:	1.1.0
Revision:	\main\rel_opb1\rel_ors2\2
Stand:	21.04.2017
Status:	freigegeben
Klassifizierung:	öffentlich
Referenz:	[gemProdT_CVC_Root_ECC_PTV1.3.0-2]

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.

Produkttypversion	Beschreibung der Änderung	Referenz
1.0.0	Initiale Version auf Dokumentenebene	gemProdT_CVC_Root_ECC_PTV1.0.0
1.1.0	Losübergreifende Synchronisation	gemProdT_CVC_Root_ECC_PTV1.1.0
1.2.0	P11-Änderungsliste	gemProdT_CVC_Root_ECC_PTV1.2.0
1.3.0	P12-Änderungsliste	gemProdT_CVC_Root_ECC_PTV1.3.0
1.3.0-1	Anpassung auf Releasestand 1.6.3	gemProdT_CVC_Root_ECC_PTV1.3.0-1
1.3.0-2	Anpassung auf Releasestand 1.6.4	gemProdT_CVC_Root_ECC_PTV1.3.0-2

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	21.04.17		freigegeben	gematik
1.1.0	18.12.17	2	Aktualisierung auf Release 2.1.1	gematik

Inhaltsverzeichnis

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 CVC-Root – ECC in der Produkttypversion 1.3.0-2 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[1] durch die gematik.

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 CVC-Root – ECC-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] 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.

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

Dokumentenkürzel	Bezeichnung des Dokuments	Version
gemKPT_Test	Testkonzept	1.10.0
gemSpec_CVC_Root	Spezifikation CVC-Root	1.7.2
gemSpec_ISM	Spezifikation koordinierendes ISM	1.4.1
gemSpec_Krypt	Spezifikation kryptographischer Algorithmen in der TI	2.9.0
gemSpec_Net	Spezifikation Netzwerk	1.12.0
gemSpec_OID	Spezifikation Festlegung von OIDs	3.1.0.0
gemSpec_OM	Spezifikation Operations und Maintenance	1.8.0
gemSpec_PKI	Spezifikation PKI (mit Anhang A)	2.1.0
gemSpec_SiBetrUmg	Spezifikation der Sicherheitsanforderungen an die Betriebsumgebung	1.4.0
gemSpec_Sich_DS	Spezifikation Sicherheits-/Datenschutzanforderungen	1.4.1

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.

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_5212	Wechsel der Schlüsselversion bei der CVC-Root-CA, Cross-Zertifizierung	gemSpec_CVC_Root
TIP1-A_5213	Wechsel der Schlüsselversion bei der CVC-Root-CA, Verfügbarkeit der Crosszertifizierungsdaten	gemSpec_CVC_Root
TIP1-A_5214	Wechsel der Schlüsselversion bei der CVC-Root-CA	gemSpec_CVC_Root
TIP1-A_5238	Veröffentlichung des öffentlichen Root-Schlüssels	gemSpec_CVC_Root
TIP1-A_5241	Bereitstellung von Cross-Zertifikaten (Link-Zertifikaten)	gemSpec_CVC_Root
TIP1-A_5260	Berücksichtigung von Eingangsdaten gemäß [gemSpec_PKI] bei Ausstellung von CVC-CA-Zertifikaten	gemSpec_CVC_Root
TIP1-A_5261	Verwendung der Eingangsdaten des TSP-CVC	gemSpec_CVC_Root
TIP1-A_5263	Setzen des Datums in Certificate Authority Reference (CAR)	gemSpec_CVC_Root
TIP1-A_5264	Setzen der Certificate Effective Date (CED)	gemSpec_CVC_Root
TIP1-A_5265	Setzen der Certificate Expiration Date (CXD)	gemSpec_CVC_Root
TIP1-A_5266	Signierung des CVC-CA-Zertifikats durch die CVC-Root-CA	gemSpec_CVC_Root
TIP1-A_5270	CVC-PKCS#10-Request, Konkretisierungen für die Kartengeneration 2	gemSpec_CVC_Root
TIP1-A_5367	CVC-PKCS#10-Request für Kartengeneration 2, Object Identifier der Attribute	gemSpec_CVC_Root
TIP1-A_5272	CVC-PKCS#10-Request, Angabe der Attribute	gemSpec_CVC_Root
TIP1-A_5273	CVC-PKCS#10-Request, Kodierung	gemSpec_CVC_Root
TIP1-A_5274	Signierung des Test-CVC-CA-Zertifikats durch die Test-CVC-Root-CA	gemSpec_CVC_Root

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
GS-A_3695	Grundlegender Aufbau Versionsnummern	gemSpec_OM
GS-A_3696	Zeitpunkt der Erzeugung neuer 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_5038	Festlegungen zur Vergabe einer Produktversion	gemSpec_OM
GS-A_3702	Inhalt der Selbstauskunft von Produkten außer Karten	gemSpec_OM
GS-A_4543	Rückgabe der Selbstauskunft von zentralen Produkttypen der TI-Plattform und fachanwendungsspezifischen Diensten	gemSpec_OM
GS-A_3804	Eigenschaften eines FehlerLog-Eintrags	gemSpec_OM
GS-A_3807	Fehlerspeicherung ereignisgesteuerter Nachrichtenverarbeitung	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_5213	CA-Flaglist für CVC-CA eines Profiltyps	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)
TIP1-A_6516	Eigenverantwortlicher Test: Test & Transitionmanager	gemKPT_Test
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_2769	Kompatibilität und Interoperabilität der Schnittstellen	gemKPT_Test
TIP1-A_6538	Durchführung von Produkttests	gemKPT_Test
TIP1-A_6539	Durchführung von Produktübergreifenden Tests	gemKPT_Test
TIP1-A_2781	Dauerhafte Verfügbarkeit in der Testumgebung	gemKPT_Test
TIP1-A_6524	Testdokumentation gemäß Vorlagen	gemKPT_Test
TIP1-A_6525	Produkttypen: Testziele	gemKPT_Test
TIP1-A_6526	Produkttypen: Bereitstellung	gemKPT_Test
TIP1-A_6772	Partnerprodukte bei Interoperabilitätstests	gemKPT_Test
TIP1-A_6529	Produkttypen: Mindestumfang der Interoperabilitätsprüfung	gemKPT_Test
TIP1-A_6531	Zulassung eines neuen Produkts: Aufgaben des TBV	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_6535	Zulassung eines geänderten Produkts: Aufgaben des TBV	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_5173	Inhalt der Ausgabepolicy der CVC-Root-CA	gemSpec_CVC_Root
TIP1-A_5176	Betrieb der CVC-Root-CA nach Zulassung der gematik	gemSpec_CVC_Root
TIP1-A_5182	Verlust der Verfügbarkeit der CVC-Root-CA	gemSpec_CVC_Root
TIP1-A_5183	Verwendung des Schlüsselpaars der CVC-Root-CA	gemSpec_CVC_Root
TIP1-A_5185	Maximale Gültigkeitsdauer des Schlüsselpaars der CVC-Root-CA	gemSpec_CVC_Root
TIP1-A_5186	Ablauf der Gültigkeitsdauer des privaten Schlüssels der CVC-Root-CA	gemSpec_CVC_Root
TIP1-A_5187	Weiterverwendung des privaten Schlüssels einer CVC-Root-CA	gemSpec_CVC_Root

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
TIP1-A_5189	Vernichtung der privaten Schlüssel bei Verlust der Zulassung der CVC-Root-CA	gemSpec_CVC_Root
TIP1-A_5191	Information über die Vernichtung aller Schlüsselpaare durch die CVC-Root-CA an gematik	gemSpec_CVC_Root
TIP1-A_5380	Zugang zu HSM-Systemen im Vier-Augen-Prinzip	gemSpec_CVC_Root
TIP1-A_5205	Schlüsselbackup bei der gematik	gemSpec_CVC_Root
TIP1-A_5206	Verfahrensbeschreibung Datensicherung der CVC-Root-CA	gemSpec_CVC_Root
TIP1-A_5207	Quorum der Wiederherstellung	gemSpec_CVC_Root
TIP1-A_5208	Import aktuell genutzter CVC-Root-Schlüsselpaare	gemSpec_CVC_Root
TIP1-A_5212	Wechsel der Schlüsselversion bei der CVC-Root-CA, Cross-Zertifizierung	gemSpec_CVC_Root
TIP1-A_5213	Wechsel der Schlüsselversion bei der CVC-Root-CA, Verfügbarkeit der Crosszertifizierungsdaten	gemSpec_CVC_Root
TIP1-A_5214	Wechsel der Schlüsselversion bei der CVC-Root-CA	gemSpec_CVC_Root
TIP1-A_5215	Planmäßiger Wechsel der Schlüsselversion bei der CVC-Root-CA	gemSpec_CVC_Root
TIP1-A_5216	Planmäßiger Wechsel der Schlüsselversion bei der CVC-Root-CA, Erzeugung des Cross-Zertifikats	gemSpec_CVC_Root
TIP1-A_5219	Schlüsselerzeugung nach Anordnung durch die gematik	gemSpec_CVC_Root
TIP1-A_5227	Prüfung der Protokolldaten durch die gematik	gemSpec_CVC_Root
TIP1-A_5230	Benennung von Mitarbeitern gegenüber der gematik durch die CVC-Root-CA	gemSpec_CVC_Root
TIP1-A_5231	Berücksichtigung von Zugriffen auf das HSM im Vier-Augen-Prinzip, CVC-Root-CA	gemSpec_CVC_Root
TIP1-A_5239	Sicherstellung der Integrität und Authentizität des öffentlichen Schlüssels bei Veröffentlichung	gemSpec_CVC_Root
TIP1-A_5240	Bereitstellung des Fingerprints zum öffentlichen Schlüssel	gemSpec_CVC_Root
TIP1-A_5241	Bereitstellung von Cross-Zertifikaten (Link-Zertifikaten)	gemSpec_CVC_Root
TIP1-A_5243	Information an die CVC-CAs über die Verfügbarkeit einer neuen Root-Version	gemSpec_CVC_Root
TIP1-A_5245	Schnittstelle zur Einsicht und Übermittlung von Registrierungsdaten	gemSpec_CVC_Root
TIP1-A_5246	Daten zum TSP-CVC	gemSpec_CVC_Root
TIP1-A_5247	Daten zur CVC-CA	gemSpec_CVC_Root
TIP1-A_5248	Betrieb von Test-CVC-Root-CAs	gemSpec_CVC_Root
TIP1-A_5249	Backup und Verfügbarkeit der CVC-Root-CA für Produktiv- und Testumgebung	gemSpec_CVC_Root
TIP1-A_5250	Schriftlicher Antrag auf Ausstellung eines CVC-CA-Zertifikats	gemSpec_CVC_Root
TIP1-A_5251	Eingangsdaten zur Erzeugung eines CVC-CA-Zertifikats, die durch den TSP-CVC zur Verfügung gestellt werden	gemSpec_CVC_Root
TIP1-A_5252	CVC-PKCS#10-Request zur Erzeugung eines CVC-CA-Zertifikats	gemSpec_CVC_Root
TIP1-A_5253	Übergabe des CVC-CA-Zertifikats an den TSP-CVC	gemSpec_CVC_Root

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
TIP1-A_5254	Prüfung des schriftlichen Antrags auf Ausstellung eines CVC-CA-Zertifikats	gemSpec_CVC_Root
TIP1-A_5255	Ergebnis der Prüfung des schriftlichen Antrags auf Ausstellung eines CVC-CA-Zertifikats	gemSpec_CVC_Root
TIP1-A_5256	Vereinbarung zur Übergabe des CVC-PKCS#10-Requests	gemSpec_CVC_Root
TIP1-A_5257	Prüfung des Mitarbeiters des TSP-CVC und dessen Berechtigung	gemSpec_CVC_Root
TIP1-A_5258	Prüfung des CVC-PKCS#10-Requests	gemSpec_CVC_Root
TIP1-A_5259	Erstellung eines CVC-CA-Zertifikats	gemSpec_CVC_Root
TIP1-A_5262	Setzen der Certificate Authority Reference (CAR)	gemSpec_CVC_Root
TIP1-A_5266	Signierung des CVC-CA-Zertifikats durch die CVC-Root-CA	gemSpec_CVC_Root
TIP1-A_5267	Protokollierung	gemSpec_CVC_Root
TIP1-A_5268	CVC-PKCS#10-Request, Format des technischen Requests	gemSpec_CVC_Root
TIP1-A_5270	CVC-PKCS#10-Request, Konkretisierungen für die Kartengeneration 2	gemSpec_CVC_Root
TIP1-A_5272	CVC-PKCS#10-Request, Angabe der Attribute	gemSpec_CVC_Root
TIP1-A_5273	CVC-PKCS#10-Request, Kodierung	gemSpec_CVC_Root
TIP1-A_5274	Signierung des Test-CVC-CA-Zertifikats durch die Test-CVC-Root-CA	gemSpec_CVC_Root
TIP1-A_5275	Entgegennahme der Informationen zur Zulassung und Registrierung	gemSpec_CVC_Root
TIP1-A_5276	Protokollierung der Entgegennahme der Informationen zur Zulassung und Registrierung	gemSpec_CVC_Root
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_4541	Nutzung der Produkttypversion zur Kompatibilitätsprüfung	gemSpec_OM
GS-A_5039	Änderung der Produktversion bei Änderungen der Produkttypversion	gemSpec_OM
GS-A_3813	Datenschutzvorgaben Fehlermeldungen	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_4257	Hauptsitz und Betriebsstätte	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 ITSEC [ITSEC] oder Common Criteria 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_5173	Inhalt der Ausgabepolicy der CVC-Root-CA	gemSpec_CVC_Root
TIP1-A_5174	Inhalt des Sicherheitskonzepts der CVC-Root-CA	gemSpec_CVC_Root
TIP1-A_5175	Darstellung der Zusammenarbeit verschiedener Organisationen	gemSpec_CVC_Root
TIP1-A_5183	Verwendung des Schlüsselpaars der CVC-Root-CA	gemSpec_CVC_Root
TIP1-A_5184	Begrenzung der Lebensdauer des Schlüsselpaars der CVC-Root-CA	gemSpec_CVC_Root
TIP1-A_5185	Maximale Gültigkeitsdauer des Schlüsselpaars der CVC-Root-CA	gemSpec_CVC_Root
TIP1-A_5186	Ablauf der Gültigkeitsdauer des privaten Schlüssels der CVC-Root-CA	gemSpec_CVC_Root
TIP1-A_5187	Weiterverwendung des privaten Schlüssels einer CVC-Root-CA	gemSpec_CVC_Root
TIP1-A_5188	Vernichtung nicht mehr benötigter Schlüssel durch die CVC-Root-CA	gemSpec_CVC_Root
TIP1-A_5189	Vernichtung der privaten Schlüssel bei Verlust der Zulassung der CVC-Root-CA	gemSpec_CVC_Root
TIP1-A_5190	Maßnahmen zur Vernichtung der Schlüsselpaare durch die CVC-Root-CA	gemSpec_CVC_Root
TIP1-A_5192	Einsatz eines HSM, CVC-Root-CA	gemSpec_CVC_Root
TIP1-A_5193	Schlüsselgenerierung im HSM der CVC-Root-CA	gemSpec_CVC_Root
TIP1-A_5194	Speicherung und Anwendung des privaten Schlüssels in einem HSM, CVC-Root-CA	gemSpec_CVC_Root
TIP1-A_5195	Einsatz einer Chipkarte als HSM, CVC-Root-CA	gemSpec_CVC_Root
TIP1-A_5196	Ordnungsgemäße Sicherung des privaten Schlüssels der CVC-Root-CA	gemSpec_CVC_Root
TIP1-A_5197	Verwendung von privaten Schlüsseln einer CVC-Root-CA	gemSpec_CVC_Root
TIP1-A_5198	Evaluierung von HSMs - CVC-Root-CA	gemSpec_CVC_Root
TIP1-A_5199	Vorgaben an die Funktionalität des HSM der CVC-Root-CA	gemSpec_CVC_Root
TIP1-A_5200	Nutzung eines HSM nach erfolgreicher Benutzerauthentisierung	gemSpec_CVC_Root

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
TIP1-A_5201	Speicherung und Auswahl von Schlüsselpaaren im HSM der CVC-Root-CA	gemSpec_CVC_Root
TIP1-A_5202	Keine Weitergabe sensitiver Schlüssel durch die CVC-Root-CA	gemSpec_CVC_Root
TIP1-A_5203	Verwendung eines Backup-HSMs durch die CVC-Root-CA	gemSpec_CVC_Root
TIP1-A_5204	Backup-HSMs - sicherer Schlüsseltransport CVC-Root-CA	gemSpec_CVC_Root
TIP1-A_5220	Protokollierung durch die CVC-Root-CA - Ereignisse	gemSpec_CVC_Root
TIP1-A_5221	Protokollierung durch die CVC-Root-CA - Werte pro Ereignis	gemSpec_CVC_Root
TIP1-A_5222	Protokollierung durch die CVC-Root-CA - Generierung eines neuen Schlüsselpaares	gemSpec_CVC_Root
TIP1-A_5223	Protokollierung durch die CVC-Root-CA - Aktivierung eines neuen Schlüsselpaares	gemSpec_CVC_Root
TIP1-A_5224	Protokollierung durch die CVC-Root-CA - Erzeugung eines CVC-CA-Zertifikats	gemSpec_CVC_Root
TIP1-A_5225	Nachvollziehbarkeit bei Produktion von CVC-CA-Zertifikaten	gemSpec_CVC_Root
TIP1-A_5226	Schutz der Protokolldaten gegen Manipulation	gemSpec_CVC_Root
TIP1-A_5228	Berücksichtigung von Rollen	gemSpec_CVC_Root
TIP1-A_5229	Definition der Rollen in der CVC-Root-CA und Festlegungen ihrer Aufgaben	gemSpec_CVC_Root
TIP1-A_5230	Benennung von Mitarbeitern gegenüber der gematik durch die CVC-Root-CA	gemSpec_CVC_Root
TIP1-A_5231	Berücksichtigung von Zugriffen auf das HSM im Vier-Augen-Prinzip, CVC-Root-CA	gemSpec_CVC_Root
TIP1-A_5232	Umsetzung der definierten Prozesse durch die CVC-Root-CA	gemSpec_CVC_Root
TIP1-A_5233	Geschützter Bereich der CVC-Root-CA	gemSpec_CVC_Root
TIP1-A_5234	Verwendung mehrerer geschützter Bereiche der CVC-Root-CA	gemSpec_CVC_Root
TIP1-A_5235	Schutz von HSM der CVC-Root-CA	gemSpec_CVC_Root
TIP1-A_5236	Zugriffe auf Systeme der CVC-Root-CA über Arbeitsplatzrechner (oder Systeme) außerhalb des geschützten Bereichs	gemSpec_CVC_Root
TIP1-A_5237	Sicherer Betrieb von Systemkomponenten der CVC-Root-CA	gemSpec_CVC_Root
TIP1-A_5372	Systemtechnische Trennung bei Aufbau und Betrieb der CVC-Root-CA	gemSpec_CVC_Root
TIP1-A_5249	Backup und Verfügbarkeit der CVC-Root-CA für Produktiv- und Testumgebung	gemSpec_CVC_Root
GS-A_4503	Dokumentation des ISM	gemSpec_ISM
GS-A_4505	Jährliche Prüfung der Dokumentation des ISM	gemSpec_ISM
GS-A_4529	Meldung von schwerwiegenden Sicherheitsvorfällen und -notfällen	gemSpec_ISM
GS-A_4537	Meldung von Informationssicherheitsrisiken	gemSpec_ISM
GS-A_4539	Meldung von angepassten Risikoleveln	gemSpec_ISM
GS-A_4363	CV-Zertifikate G1	gemSpec_Krypt
GS-A_4364	CV-CA-Zertifikate G1	gemSpec_Krypt

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
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
GS-A_3760	Gutachten zur Einhaltung der Sicherheitsanforderungen für Dienstbetreiber	gemSpec_SiBetrUmg
GS-A_4980	Umsetzung der Norm ISO/IEC 27001	gemSpec_SiBetrUmg
GS-A_4981	Erreichen der Ziele der Norm ISO/IEC 27001 Annex A	gemSpec_SiBetrUmg
GS-A_4982	Umsetzung der Maßnahmen der Norm ISO/IEC 27002	gemSpec_SiBetrUmg
GS-A_4983	Umsetzung der Maßnahmen aus dem BSI-Grundschutz	gemSpec_SiBetrUmg
GS-A_4984	Befolgen von herstellerspezifischen Vorgaben	gemSpec_SiBetrUmg
GS-A_3737	Spezifisches Sicherheitskonzept: Mindestumfang des spezifischen Sicherheitskonzeptes..	gemSpec_SiBetrUmg
GS-A_3747	Technische_Komponenten: Dokumentation der technischen Komponenten und der geforderten Sicherheitsfunktionalität.	gemSpec_SiBetrUmg
GS-A_3753	Notfallkonzept: Der Dienstanbieter muss ein Notfallkonzept erstellen	gemSpec_SiBetrUmg
GS-A_3772	Notfallkonzept: Der Dienstanbieter soll dem BSI-Standard 100-4 folgen	gemSpec_SiBetrUmg
GS-A_3756	Umsetzung_Maßnahmen_spezifisches_Siko: Umsetzung und Prüfbarkeit von Maßnahmen	gemSpec_SiBetrUmg
GS-A_2012	Verantwortung der Anbieter und Betreiber für Einhaltung der Anforderungen Datenschutz und Informationssicherheit	gemSpec_Sich_DS
GS-A_2021	Anwendung der einheitlichen Methoden der Informationssicherheit durch Betreiber und Anbieter	gemSpec_Sich_DS
GS-A_2046	Umsetzung der Anforderungen aus [gemSpec_SiBetrUmg] durch Anbieter von zentralen Produkten	gemSpec_Sich_DS
GS-A_4944	Produktentwicklung: Behebung von Sicherheitsmängeln	gemSpec_Sich_DS
GS-A_4945	Produktentwicklung: Qualitätssicherung	gemSpec_Sich_DS
GS-A_4946	Produktentwicklung: sichere Programmierung	gemSpec_Sich_DS
GS-A_4947	Produktentwicklung: Schutz der Vertraulichkeit und Integrität	gemSpec_Sich_DS
GS-A_2047	Gestaltung der Umgebung von zentralen Produkten durch Betreiber für Schutzbedarf "mittel"	gemSpec_Sich_DS
GS-A_2309	ISM der Beteiligten: Rollen und Verantwortlichkeiten	gemSpec_Sich_DS
GS-A_2326	ISM der Beteiligten: Etablierung	gemSpec_Sich_DS
GS-A_2328	ISM der Beteiligten: Pflege und Fortschreibung der Sicherheitskonzepte	gemSpec_Sich_DS
GS-A_2329	ISM der Beteiligten: Umsetzung der Sicherheitskonzepte	gemSpec_Sich_DS

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
GS-A_2330	ISM der Beteiligten: Schwachstellen-Management	gemSpec_Sich_DS
GS-A_2331	ISM der Beteiligten: Sicherheitsvorfalls-Management	gemSpec_Sich_DS
GS-A_2332	ISM der Beteiligten: Notfallmanagement	gemSpec_Sich_DS
GS-A_2333	ISM der Beteiligten: Meldung an das koordinierende ISM	gemSpec_Sich_DS
GS-A_2339	ISM der Beteiligten: regelmäßige Reviews	gemSpec_Sich_DS
GS-A_2343	ISM der Beteiligten: eigene Audits	gemSpec_Sich_DS
GS-A_2345	ISM der Beteiligten: Reviews und Trendanalysen	gemSpec_Sich_DS
GS-A_2347	ISM der Beteiligten: Grundlagen neuer Planungsphasen	gemSpec_Sich_DS
GS-A_2360	ISM der Beteiligten: Meldung von Restrisiken	gemSpec_Sich_DS
GS-A_2361	ISM der Beteiligten: Vorfallsmanagement	gemSpec_Sich_DS
GS-A_2362	ISM der Beteiligten: Bericht lokaler Sicherheitsvorfälle	gemSpec_Sich_DS
GS-A_2363	ISM der Beteiligten: Meldung schwerwiegender Sicherheitsvorfälle	gemSpec_Sich_DS
GS-A_2366	ISM der Beteiligten: Notfallbewältigung	gemSpec_Sich_DS
GS-A_3078	Anbieter einer Schlüsselverwaltung: verpflichtende Migrationsstrategie bei Schwächung kryptographischer Primitive	gemSpec_Sich_DS
GS-A_3125	Schlüsselinstallation und Verteilung: Dokumentation gemäß Minimalitätsprinzip	gemSpec_Sich_DS
GS-A_3130	Krypto_Schlüssel_Installation: Dokumentation der Schlüsselinstallation gemäß Minimalitätsprinzip	gemSpec_Sich_DS
GS-A_3139	Krypto_Schlüssel: Dienst Schlüsselableitung	gemSpec_Sich_DS
GS-A_3141	Krypto_Schlüssel_Ableitung: Maßnahmen bei Bekanntwerden von Schwächen in der Schlüsselableitungsfunktion	gemSpec_Sich_DS
GS-A_3149	Krypto_Schlüssel_Archivierung: Dokumentation der Schlüsselarchivierung gemäß Minimalitätsprinzip	gemSpec_Sich_DS

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)
GS-A_4504	Bereitstellung der Dokumentation des ISM bei Audits	gemSpec_ISM
GS-A_4506	Übermittlung von Security Reports	gemSpec_ISM
GS-A_4507	Bereitstellung des Security Reports in der Erprobung	gemSpec_ISM
GS-A_4508	Bereitstellung des Security Reports im Produktivbetrieb	gemSpec_ISM
GS-A_4509	Dateiformat und -struktur des Security Reports	gemSpec_ISM
GS-A_4511	Aufschlüsselung pro TI-Produkt	gemSpec_ISM

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
GS-A_4512	Dateistruktur der Informationen in den Security Reports	gemSpec_ISM
GS-A_4513	Kennzahl 01: Budgetierung der Informationssicherheit	gemSpec_ISM
GS-A_4514	Kennzahl 02: Schulungstage mit Bezug zur Informationssicherheit je Mitarbeiter	gemSpec_ISM
GS-A_4515	Kennzahl 03: Anzahl der externen und internen Informationssicherheits-Audits	gemSpec_ISM
GS-A_4516	Kennzahl 04: Behebungszeit von in internen oder externen Audits festgestellten Abweichungen	gemSpec_ISM
GS-A_4517	Kennzahl 05: Vollständigkeit der Erfassung organisationseigener Werte (Assets)	gemSpec_ISM
GS-A_4518	Kennzahl 06: Prozesstreue in der Änderungsverwaltung (Change Management)	gemSpec_ISM
GS-A_4519	Kennzahl 7 Anteil sicherheitsrelevanter Änderungen (Security Changes)	gemSpec_ISM
GS-A_4520	Kennzahl 08: Anzahl privilegierter Benutzer	gemSpec_ISM
GS-A_4521	Kennzahl 09: Regeltests der Notfallpläne anhand von Notfallübungen	gemSpec_ISM
GS-A_4522	Kennzahl 10: Regelprüfung des Dokumentationsrahmenwerks des ISM der Anbieter	gemSpec_ISM
GS-A_4523	Bereitstellung Kommunikationsschnittstelle für Informationssicherheit	gemSpec_ISM
GS-A_4524	Meldung von Kontaktinformationen zum Informationssicherheitsmanagement	gemSpec_ISM
GS-A_4525	Audit-Unterstützung des Koordinators für Informationssicherheit	gemSpec_ISM
GS-A_4526	Aufbewahrungsvorgaben an die Nachweise zu den im Security Report gemachten Angaben	gemSpec_ISM
GS-A_4527	Audit-Kennzahlen	gemSpec_ISM
GS-A_4528	Meldung von lokalen Sicherheitsvorfällen	gemSpec_ISM
GS-A_4530	Maßnahmen zur Behebung von schwerwiegenden Sicherheitsvorfällen und -notfällen	gemSpec_ISM
GS-A_4531	Unverzügliche Umsetzung von Maßnahmen bei schwerwiegenden Sicherheitsvorfällen und -notfällen	gemSpec_ISM
GS-A_4532	Kontrolle der Umsetzung von Maßnahmen in Folge eines schwerwiegenden Sicherheitsvorfalls oder -notfalls	gemSpec_ISM
GS-A_4533	Berücksichtigung von Änderungen im Umfeld der Informationssicherheit und Ergebnissen des technischen Fortschritts	gemSpec_ISM
GS-A_4534	Berücksichtigung von Änderungen der Informationssicherheitsanforderungen der TI	gemSpec_ISM
GS-A_4535	Kontrolle der Umsetzung von Maßnahmen durch die gematik	gemSpec_ISM
GS-A_4538	Nutzen des Risikobewertungstemplate	gemSpec_ISM
GS-A_4540	Risikoreporting	gemSpec_ISM
GS-A_3784	Nachweis durch ISO27001 Zertifikat	gemSpec_SiBetrUmg
GS-A_5324	Teilnahme des Anbieters an Sitzungen des kDSMS/kISMS	gemSpec_Sich_DS

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
GS-A_2156	Auditierungen der Zulassungsnehmer	gemSpec_Sich_DS
GS-A_5017	ISM der Beteiligten: Schließen von Schwachstellen	gemSpec_Sich_DS
GS-A_2355	ISM der Beteiligten: Nutzung des Problem-Management-Prozesses	gemSpec_Sich_DS
GS-A_2356	ISM der Beteiligten: Nutzung des Incident-Management-Prozesses	gemSpec_Sich_DS
GS-A_2357	ISM der Beteiligten: Nutzung der Prozesse und Reports des Betriebs	gemSpec_Sich_DS
GS-A_2359	ISM der Beteiligten: Nutzung der Sicherheits-Technologien des koordinierenden ISM	gemSpec_Sich_DS

3.3 Anforderungen zur elektrischen, mechanischen und physikalischen Eignung

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

4 Produkttypspezifische Merkmale

Es liegen keine optionalen Ausprägungen des Produkttyps vor.

Anhang A – Verzeichnisse

A1 – Abkürzungen

Kürzel	Erläuterung
Afo-ID	Anforderungs-Identifikation
CC	Common Criteria

A2 – Tabellenverzeichnis

A3 – Referenzierte Dokumente

Neben den in Kapitel 2 angeführten Dokumenten werden referenziert:

[Quelle]	Herausgeber: Titel, Version
[BSI_2006a]	BSI (29.09.2006): Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik (Common Criteria) https://www.bsi.bund.de/Schutzprofile
[gemRL_PruefSichEig]	gematik: Richtlinie zur Prüfung der Sicherheitseignung
[ITSEC]	BMI bzw. GMBl: (28.06.1991): Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik („Information Technology Security Evaluation Criteria) https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/ITSicherheitskriterien/itsec-dt_pdf.pdf?__blob=publicationFile