

Elektronische Gesundheitskarte und Telematikinfrastruktur

Produkttypsteckbrief

Prüfvorschrift

CVC-Root – ECC

Produkttyp Version: 1.5.0-0
Produkttyp Status: freigegeben

Version: 1.0.1
Revision: 434714
Stand: 28.01.2022
Status: freigegeben
Klassifizierung: öffentlich
Referenzierung: gemProdT_CVC_Root_ECC_PTV_1.5.0-0

Historie Produkttypversion und Produkttypsteckbrief

Historie Produkttypversion

Die Produkttypversion ändert sich, wenn sich die normativen Festlegungen für den Produkttyp ändern 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 |
| 1.3.0-3 | Anpassung auf Releasestand 2.1.2 | gemProdT_CVC_Root_ECC_PTV1.3.0-3 |
| 1.4.0-0 | Anpassung auf Releasestand 3.1.0 | gemProdT_CVC_Root_ECC_PTV1.4.0-0 |
| 1.5.0-0 | Einarbeitung CI_Maintenance_21.2 | gemProdT_CVC_Root_ECC_PTV1.5.0-0 |

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 | 21.01.2022 | | freigegeben | gematik |

| | | | | |
|-------|------------|--|-----------|---------|
| 1.0.1 | 28.01.2022 | | Korrektur | gematik |
|-------|------------|--|-----------|---------|

Inhaltsverzeichnis

| | |
|--|-----------|
| 1 Einführung | 5 |
| 1.1 Zielsetzung und Einordnung des Dokumentes | 5 |
| 1.2 Zielgruppe | 5 |
| 1.3 Geltungsbereich | 5 |
| 1.4 Abgrenzung des Dokumentes | 5 |
| 1.5 Methodik | 6 |
| 2 Dokumente | 7 |
| 3 Normative Festlegungen | 8 |
| 3.1 Festlegungen zur funktionalen Eignung..... | 8 |
| 3.1.1 Produkttest/Produktübergreifender Test..... | 8 |
| 3.1.2 Herstellererklärung funktionale Eignung..... | 10 |
| 3.2 Festlegungen zur sicherheitstechnischen Eignung | 15 |
| 3.2.1 CC-Evaluierung | 15 |
| 3.2.2 Sicherheitsgutachten | 15 |
| 3.2.3 Herstellererklärung sicherheitstechnische Eignung..... | 19 |
| 3.3 Festlegungen zur elektrischen, mechanischen und physikalischen Eignung | 20 |
| 4 Produktypspezifische Merkmale | 21 |
| 5 Anhang A – Verzeichnisse | 22 |
| 5.1 Abkürzungen | 22 |
| 5.2 Tabellenverzeichnis | 22 |
| 5.3 Referenzierte Dokumente..... | 22 |

1 Einführung

1.1 Zielsetzung und Einordnung des Dokumentes

Dieser Produkttypsteckbrief verzeichnet verbindlich die normativen Festlegungen der gematik an die Herstellung und den Betrieb von Produkten des Produkttyps CVC-Root – ECC oder verweist auf Dokumente, in denen verbindliche normative Festlegungen mit ggf. anderer Notation zu finden sind. Die normativen Festlegungen bilden die Grundlage für die Erteilung von Zulassungen, Zertifizierungen bzw. Bestätigungen durch die gematik (Wenn im Weiteren 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 normativen Festlegungen werden über ihren Identifier, ihren Titel sowie die Dokumentenquelle referenziert. Die normativen Festlegungen 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 normative Festlegungen, 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. gemPTV_ATV_Festlegungen, 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 normativen Festlegungen werden tabellarisch dargestellt. Die Tabellenspalten haben die folgende Bedeutung:

ID: Identifiziert die normative Festlegung eindeutig im Gesamtbestand aller Festlegungen der gematik.

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

Quelle (Referenz): Verweist auf das Dokument, das die normative Festlegung definiert.

2 Dokumente

Die nachfolgenden Dokumente enthalten alle für den Produkttyp normativen Festlegungen.

Tabelle 1: Dokumente mit Festlegungen zu der Produkttypversion

| Dokumenten Kürzel | Bezeichnung des Dokumentes | Version |
|---------------------|--|---------|
| gemSpec_OM | Übergreifende Spezifikation Operations und Maintenance | 1.14.0 |
| gemSpec_PKI | Übergreifende Spezifikation – Spezifikation PKI | 2.11.1 |
| gemKPT_Test | Testkonzept der TI | 2.8.4 |
| gemSpec_Net | Übergreifende Spezifikation Netzwerk | 1.21.0 |
| gemSpec_DS_Anbieter | Spezifikation Datenschutz- und Sicherheitsanforderungen der TI an Anbieter | 1.3.1 |
| gemSpec_Krypt | Übergreifende Spezifikation Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur | 2.20.0 |
| gemSpec_CVC_Root | Spezifikation CVC-Root | 1.9.0 |
| gemSpec_OID | Spezifikation Festlegung von OIDs | 3.11.0 |

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 Normative Festlegungen

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

3.1 Festlegungen zur funktionalen Eignung

3.1.1 Produkttest/Produktübergreifender Test

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

Tabelle 2: Festlegungen zur funktionalen Eignung "Produkttest/Produktübergreifender Test"

| ID | 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_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_5367 | CVC-PKCS#10-Request für Kartengeneration 2, Object Identifier der Attribute | gemSpec_CVC_Root |
| GS-A_3695 | Grundlegender Aufbau Versionsnummern | 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_5025 | Versionierung von Produkten auf Basis von zentralen Produkttypen der TI-Plattform und fachanwendungsspezifischen Diensten durch die Produktidentifikation | gemSpec_OM |
| GS-A_4629 | CHR des CV-Zertifikats einer CVC-CA | 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 |
| GS-A_5213-01 | CA-Flaglist für CVC-CA eines Profiltyps | gemSpec_PKI |

3.1.2 Herstellererklärung funktionale Eignung

In diesem Abschnitt sind alle funktionalen und nichtfunktionalen Festlegungen 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: Festlegungen zur funktionalen Eignung "Herstellererklärung"

| ID | Bezeichnung | Quelle (Referenz) |
|-------------|--|-------------------|
| A_20065 | Nutzung der Dokumententemplates der gematik | gemKPT_Test |
| GS-A_2162 | Kryptographisches Material in Entwicklungs- und Testumgebungen | gemKPT_Test |
| TIP1-A_4191 | Keine Echtdaten in RU und TU | 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_6517-01 | Eigenverantwortlicher Test: TBI | 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_6524-01 | 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 |
| 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_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 |
| 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_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 |
| 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 |
| TIP1-A_5380 | Zugang zu HSM-Systemen im Vier-Augen-Prinzip | 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_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_3813 | Datenschutzvorgaben Fehlermeldungen | gemSpec_OM |
| GS-A_4541 | Nutzung der Produkttypversion zur Kompatibilitätsprüfung | 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_4991 | Zuordnung von CAR zu Schlüsselpaar des Herausgebers für G2 | gemSpec_PKI |

3.2 Festlegungen 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 Festlegungen sind Gegenstand der Prüfung der Sicherheitseignung gemäß [gemRL_PruefSichEig]. Das entsprechende Sicherheitsgutachten ist der gematik vorzulegen.

Tabelle 4: Festlegungen zur sicherheitstechnischen Eignung "Sicherheitsgutachten"

| ID | Bezeichnung | Quelle (Referenz) |
|-------------|---|-------------------|
| TIP1-A_5173 | Inhalt der Ausgabepolicy 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 |
| TIP1-A_5201 | Speicherung und Auswahl von Schlüsselpaaren im HSM der CVC-Root-CA | gemSpec_CVC_Root |
| TIP1-A_5202 | Keine Weitergabe sensibler 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 Schlüsselpaars | 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_5249 | Backup und Verfügbarkeit der CVC-Root-CA für Produktiv- und Testumgebung | gemSpec_CVC_Root |
| TIP1-A_5372 | Systemtechnische Trennung bei Aufbau und Betrieb der CVC-Root-CA | gemSpec_CVC_Root |
| 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 herstellerspezifischen 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_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 Festlegungen 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: Festlegungen zur sicherheitstechnischen Eignung "Herstellererklärung"

| ID | Bezeichnung | Quelle (Referenz) |
|--------------|---|---------------------|
| 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 | Unverzögliche Meldung von erheblichen Sicherheitsvorfällen und -notfällen | gemSpec_DS_Anbieter |
| GS-A_5556 | Unverzögliche 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 |

3.3 Festlegungen zur elektrischen, mechanischen und physikalischen Eignung

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

4 Produktypspezifische Merkmale

Es liegen keine optionalen Ausprägungen des Produktyps vor.

5 Anhang A – Verzeichnisse

5.1 Abkürzungen

| Kürzel | Erläuterung |
|--------|-----------------|
| ID | Identifikation |
| CC | Common Criteria |

5.2 Tabellenverzeichnis

| | |
|--|----|
| Tabelle 1: Dokumente mit Festlegungen zu der Produkttypversion..... | 7 |
| Tabelle 2: Festlegungen zur funktionalen Eignung "Produkttest/Produktübergreifender Test"..... | 8 |
| Tabelle 3: Festlegungen zur funktionalen Eignung "Herstellereerklärung" | 10 |
| Tabelle 4: Festlegungen zur sicherheitstechnischen Eignung "Sicherheitsgutachten" | 15 |
| Tabelle 5: Festlegungen zur sicherheitstechnischen Eignung "Herstellereerklärung" | 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 https://www.commoncriteriaportal.org/cc/ |
| [gemRL_PruefSichEig] | gematik: Richtlinie zur Prüfung der Sicherheitseignung |