

Elektronische Gesundheitskarte und Telematikinfrastruktur

Anbietertypsteckbrief

SMC-B

Anbietertyp Version: 1.2.3
Anbietertyp Status: freigegeben

Version: 1.0.0
Revision: 74983
Stand: 19.02.2019
Status: freigegeben
Klassifizierung: öffentlich
Referenzierung: gemAnbT_SMC-B_ATV_1.2.3

Historie Anbietertypversion und Anbietertypsteckbrief

Historie Anbietertypversion

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

| Anbietertypversion | Beschreibung der Änderung | Referenz |
|--------------------|--|------------------------|
| 0.9.0 | Initiale Version auf Dokumentenebene | |
| 1.0.0 | freigegeben | |
| 1.0.1 | Anpassung auf Releasestand 1.6.4 | gemAnbT_SMC-B_ATV1.0.1 |
| 1.1.0 | Anpassung auf Releasestand 2.1.1 | gemAnbT_SMC-B_ATV1.1.0 |
| 1.1.1 | Anpassung auf Releasestand 2.1.2 | gemAnbT_SMC-B_ATV1.1.1 |
| 1.2.0 | Anpassung auf Vorab-Releasestand ZIS | gemAnbT_SMC-B_ATV1.2.0 |
| 1.2.1 | Anpassung auf Vorab-Releasestand ZIS (2.1.3-1) | gemAnbT_SMC-B_ATV1.2.1 |
| 1.2.2 | Anpassung auf Vorab-Releasestand ZIS (3.0.0) | gemAnbT_SMC-B_ATV1.2.2 |
| 1.2.3 | Errata 3.0.0-2 | gemAnbT_SMC-B_ATV1.2.3 |

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 | 19.02.19 | | freigegeben | gematik |

Inhaltsverzeichnis

| | | |
|----------|--|-----------|
| 1 | Einführung..... | 4 |
| 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..... | 4 |
| 2 | Dokumente | 6 |
| 3 | Blattanforderungen | 8 |
| 3.1 | Anforderungen zur betrieblichen Eignung | 8 |
| 3.1.1 | Prozessprüfung betriebliche Eignung | 8 |
| 3.1.2 | Anbietererklärung betriebliche Eignung | 9 |
| 3.1.3 | Betriebshandbuch betriebliche Eignung..... | 12 |
| 3.2 | Anforderungen zur sicherheitstechnischen Eignung | 14 |
| 3.2.1 | Sicherheitsgutachten | 14 |
| 3.2.2 | Anbietererklärung sicherheitstechnische Eignung..... | 25 |
| 4 | Anhang A – Verzeichnisse | 27 |
| 4.1 | Abkürzungen..... | 27 |
| 4.2 | Tabellenverzeichnis..... | 27 |
| 4.3 | Referenzierte Dokumente..... | 27 |

1 Einführung

1.1 Zielsetzung und Einordnung des Dokumentes

Anbietertypsteckbriefe verzeichnen verbindlich die Anforderungen der gematik an Anbieter SMC-B 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 SMC-B
- 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

| Dokumenten Kürzel | Bezeichnung des Dokumentes | Version |
|---------------------------|--|---------|
| gemSpec_PINPUK_TI | Übergreifende Spezifikation PIN/PUK-Policy für Smartcards der Telematikinfrastruktur | 1.3.0 |
| gemSpec_Net | Übergreifende Spezifikation Netzwerk | 1.14.0 |
| gemSpec_PKI | Übergreifende Spezifikation – Spezifikation PKI | 2.4.0 |
| gemSpec_CVC_TSP | Spezifikation Trust Service Provider CVC | 1.11.0 |
| gemSpec_SMC-B_ObjSys_G2_1 | Spezifikation der Security Module Card SMC-B Objektsystem | 4.3.0 |
| gemSpec_Krypt | Übergreifende Spezifikation Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur | 2.12.0 |
| gemSpec_X_509_TSP | Spezifikation Trust Service Provider X.509 | 1.12.0 |
| gemSpec_SMC-B_ObjSys | Spezifikation der Security Module Card SMC-B Objektsystem | 3.12.0 |
| gemSpec_DS_Anbieter | Spezifikation Datenschutz- und Sicherheitsanforderungen der TI an Anbieter | 1.1.0 |
| gemKPT_Betr | Betriebskonzept Online-Produktivbetrieb | 3.2.0 |
| gemRL_Betr_TI | Übergreifende Richtlinien zum Betrieb der TI | 2.0.1 |
| gemRL_TSL_SP_CP | Certificate Policy Gemeinsame Zertifizierungsrichtlinie für Teilnehmer der gematik-TSL | 2.2.0 |

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.

| Dokumenten Kürzel | Bezeichnung des Dokuments | Version |
|--------------------|----------------------------|---------|
| gemErrata_R3.0.0-2 | Errata zum Release 3.0.0-2 | 1.0.0 |

3 Blattanforderungen

Die folgenden Abschnitte verzeichnen alle für den Anbietertypen normativen Anforderungen der gematik an Anbieter SMC-B 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_3889 | Schließung eines übergreifenden Incidents | gemRL_Betr_TI |
| GS-A_3905 | Ablehnung eines übergreifenden Incidents | gemRL_Betr_TI |
| GS-A_3907 | Lösung von übergreifenden Incidents | gemRL_Betr_TI |
| GS-A_3975 | Prüfung auf Serviceverantwortung zum übergreifenden Problem | gemRL_Betr_TI |
| GS-A_3976 | Ablehnung der Lösungsunterstützung | gemRL_Betr_TI |
| GS-A_3982 | Ablehnung eines übergreifenden Problems | gemRL_Betr_TI |
| GS-A_3987 | Initiierung eines Change Request | gemRL_Betr_TI |
| GS-A_3988 | Prüfung der Lösung durch den Melder eines übergreifenden Problems | gemRL_Betr_TI |
| GS-A_3990 | Schließung eines übergreifenden Problems | gemRL_Betr_TI |
| GS-A_3991 | WDB-Aktualisierung nach Schließung eines übergreifenden Problems | gemRL_Betr_TI |
| GS-A_4085 | Etablierung von Kommunikationsschnittstellen durch die TI-ITSM-Teilnehmer | gemRL_Betr_TI |
| GS-A_4095 | Übermittlung von Ad-hoc-Reports | gemRL_Betr_TI |
| GS-A_4101 | Übermittlung der Service Level Messergebnisse | gemRL_Betr_TI |
| GS-A_4106 | Reportinhalte des Performance-Reports | gemRL_Betr_TI |

| | | |
|-----------|---|---------------|
| GS-A_4114 | Bereitstellung von TI-Konfigurationsdaten | gemRL_Betr_TI |
| GS-A_4115 | Datenänderung für TI-Konfigurationsdaten | gemRL_Betr_TI |
| GS-A_4125 | TI-Notfallerkennung | 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 |
| GS-A_5250 | Ablehnung der Lösung eines übergreifenden Incidents | 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_5601 | Nachweis der Wirksamkeit eines Changes | gemRL_Betr_TI |
| GS-A_5602 | Nachweis der Wirksamkeit eines Changes in Auswirkung auf andere TI-Fachanwendungen | 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_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_6367 | Definition eines Business-Servicekatalog der angebotenen TI Services | gemKPT_Betr |
| TIP1-A_6371 | 2nd/ 3rd-Level-Support: Single-Point-of-Contact (SPOC) für Anbieter | gemKPT_Betr |
| TIP1-A_6377 | Koordination von produktverantwortlichen Anbietern und Herstellern | gemKPT_Betr |
| TIP1-A_6388 | Bereitstellung eines lokalen IT-Service-Managements durch Anbieter und SPEDs für ihre zu verantwortenden Serviceeinheiten | gemKPT_Betr |

| | | |
|-------------|---|---------------|
| TIP1-A_6389 | Erreichbarkeit der 1st-Level (UHD), 2nd/3rd-Level (SPOCs) der Anbieter und SPEDs | 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_6415 | Fortgeführte Wahrnehmung der Serviceverantwortung bei der Delegation von Aufgaben | gemKPT_Betr |
| TIP1-A_6419 | Reportingfrequenz des Service Level Reports | gemKPT_Betr |
| TIP1-A_6437 | Datenaufbewahrung von Performancedaten | gemKPT_Betr |
| TIP1-A_7258 | Definition eines Technischen Kennzahlenkataloges | gemKPT_Betr |
| TIP1-A_7259 | Mindestinhalte des Technischen Kennzahlenkataloges | gemKPT_Betr |
| TIP1-A_7260 | Mindesterreichbarkeitszeiten im Anwendersupport | gemKPT_Betr |
| TIP1-A_7261 | Erreichbarkeit der TI-ITSM-Teilnehmer untereinander | gemKPT_Betr |
| TIP1-A_7262 | Haupt- und Nebenzeit der TI-ITSM-Teilnehmer | gemKPT_Betr |
| TIP1-A_7263 | Produktverantwortung der TI-ITSM-Teilnehmer | gemKPT_Betr |
| TIP1-A_7265 | Serviceleistung der TI-ITSM-Teilnehmer im TI-ITSM-Teilnehmersupport | gemKPT_Betr |
| TIP1-A_7266 | Mitwirkungspflichten im TI-ITSM-System | gemKPT_Betr |
| A_13575 | Qualität von RfCs | gemRL_Betr_TI |
| GS-A_3884 | Festlegung von Dringlichkeit und Auswirkung von übergreifenden Incidents | gemRL_Betr_TI |
| GS-A_3886 | Nutzung des TI-ITSM-Systems bei der Übermittlung eines übergreifenden Vorgangs | gemRL_Betr_TI |
| GS-A_3904 | Annahme eines übergreifenden Incidents | gemRL_Betr_TI |
| GS-A_3917 | Bereitstellung der ITSM-Dokumentation bei Audits | gemRL_Betr_TI |
| GS-A_3922 | Mitwirkung bei Taskforces | gemRL_Betr_TI |
| GS-A_3959 | Prüfung auf übergreifendes Problem | gemRL_Betr_TI |
| GS-A_3971 | Verifikation vor Schließung eines übergreifenden Problems | gemRL_Betr_TI |
| GS-A_3977 | Annahme der Verantwortung zur Lösungsunterstützung | gemRL_Betr_TI |
| GS-A_3981 | Annahme eines übergreifenden Problems | gemRL_Betr_TI |
| GS-A_3983 | Ursachenanalyse eines übergreifenden Problems durch Serviceverantwortlichen | gemRL_Betr_TI |
| GS-A_3984 | Service Request zur Bereitstellung der TI-Testumgebung | gemRL_Betr_TI |

| | | |
|-----------|---|---------------|
| | (RU/TU) | |
| GS-A_3986 | Koordination bei übergreifenden Problems | gemRL_Betr_TI |
| GS-A_3989 | Ablehnung der Lösung eines übergreifenden Problems | gemRL_Betr_TI |
| GS-A_4090 | Kommunikationssprache | gemRL_Betr_TI |
| GS-A_4121 | Analyse Auswirkungen möglicher Schadensereignisse auf Sicherheit und Funktion der TI-Services | 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_4397 | Teilnahme am Service Review | gemRL_Betr_TI |
| GS-A_4402 | Mitwirkungspflicht bei der Bewertung vom Produkt-RfC | gemRL_Betr_TI |
| GS-A_4417 | Stetige Aktualisierung des Change-Datensatzes im TI-ITSM-System | gemRL_Betr_TI |
| GS-A_4418 | Übermittlung von Abweichungen vom Produkt-RfC | gemRL_Betr_TI |
| GS-A_4419 | Nutzung der Testumgebung (RU/TU) | gemRL_Betr_TI |
| GS-A_4424 | Umsetzung des Fallbackplans | gemRL_Betr_TI |
| GS-A_4425 | Übermittlung von Optimierungsmöglichkeiten zur Umsetzung von genehmigten Produkt-Changes | gemRL_Betr_TI |
| GS-A_4855 | Auditierung von TI-ITSM-Teilnehmern | gemRL_Betr_TI |
| GS-A_5351 | Prüfung von Service Requests | gemRL_Betr_TI |
| GS-A_5352 | Lösung bzw. Bearbeitung des Service Requests | gemRL_Betr_TI |
| GS-A_5361 | Durchführung von Emergency-Changes durch TI-ITSM-Teilnehmer bei Nichterreichbarkeit des Gesamtverantwortlichen TI | gemRL_Betr_TI |
| GS-A_5366 | Mitwirkungspflicht der TI-ITSM-Teilnehmer bei der Festsetzung von Standard-Produkt-Changes | gemRL_Betr_TI |
| GS-A_5377 | Durchführung einer Problemstornierung | gemRL_Betr_TI |

| | | |
|-----------|--|-----------------|
| GS-A_5378 | Durchführung von Emergency-Changes durch TI-ITSM-Teilnehmer | gemRL_Betr_TI |
| GS-A_5400 | Prüfung der Lösung durch den Melder eines übergreifenden Incidents | gemRL_Betr_TI |
| GS-A_5401 | Verschlüsselte E-Mail-Kommunikation | gemRL_Betr_TI |
| GS-A_5402 | Eigenverantwortliches Handeln bei Ausfall von Kommunikationsschnittstellen | gemRL_Betr_TI |
| GS-A_5449 | Typisierung eines übergreifenden Incidents als „sicherheitsrelevant“ | gemRL_Betr_TI |
| GS-A_5450 | Typisierung eines übergreifenden Incidents als „datenschutzrelevant“ | gemRL_Betr_TI |
| GS-A_5587 | Ablehnung der Lösungsunterstützung bei einem übergreifenden Incident | gemRL_Betr_TI |
| GS-A_5588 | Abbruch der Problembearbeitung | gemRL_Betr_TI |
| GS-A_5589 | Prüfung auf Verantwortung zur Lösungsunterstützung | gemRL_Betr_TI |
| GS-A_5590 | Nutzung Business-Servicekatalog bei der Erfassung von Service Requests | gemRL_Betr_TI |
| GS-A_5591 | Verifikation des Service Requests | gemRL_Betr_TI |
| GS-A_5592 | Schließung des Service Requests | gemRL_Betr_TI |
| GS-A_5593 | Schließung des Service Requests ohne Verifikation | gemRL_Betr_TI |
| GS-A_5594 | Identifikation von TI-Konfigurationsdaten | gemRL_Betr_TI |
| GS-A_5603 | Eingangskanal für Informationen von TI-ITSM-Teilnehmern | gemRL_Betr_TI |
| GS-A_5604 | Bewertung der Messergebnisse | gemRL_Betr_TI |
| GS-A_5606 | Unterstützung bei Definition von Kapazitätsanforderungen | gemRL_Betr_TI |
| GS-A_5608 | Übermittlung von CSV-Dateien | 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 |
| A_15170 | Sektorzulassung für zugelassene TSP-CVC | gemSpec_CVC_TSP |

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) |
|-----------|--|-------------------|
| GS-A_3876 | Prüfung auf übergreifenden Incident | gemRL_Betr_TI |
| GS-A_3888 | Verifikation vor Schließung eines übergreifenden Incident | gemRL_Betr_TI |
| GS-A_3902 | Prüfung auf Serviceverantwortung | gemRL_Betr_TI |
| GS-A_3911 | Service Level Requirements im übergreifenden Incident Management | gemRL_Betr_TI |
| GS-A_3920 | Eskalationseinleitung durch den TI-ITSM-Teilnehmer | gemRL_Betr_TI |
| GS-A_3958 | Problemerkennung durch TI-ITSM-Teilnehmer | gemRL_Betr_TI |
| GS-A_3964 | Festlegung von Dringlichkeit und Auswirkung von übergreifenden Problems | gemRL_Betr_TI |
| GS-A_3972 | Service Level Requirements im übergreifenden Problem Management für TI-ITSM-Teilnehmer | gemRL_Betr_TI |
| GS-A_4086 | Erreichbarkeit der Kommunikationsschnittstellen | gemRL_Betr_TI |
| GS-A_4088 | Benennung von Ansprechpartnern | gemRL_Betr_TI |
| GS-A_4094 | Format und Übermittlung von konsolidierten Reports | gemRL_Betr_TI |
| GS-A_4100 | Messung der Service Level | gemRL_Betr_TI |
| GS-A_4117 | Informationsbereitstellung durch TI-ITSM-Teilnehmer | gemRL_Betr_TI |
| GS-A_4123 | Entwicklung und Pflege der TI-Notfallvorsorgedokumentation | 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 |
| GS-A_4398 | Prüfung auf genehmigungspflichtige Produktänderung | gemRL_Betr_TI |
| GS-A_4399 | Übermittlung von Produktdaten nach Abschluss von lokal autorisierten Produkt-Changes | gemRL_Betr_TI |
| GS-A_4400 | Produkt-RfC (Master-Change) erstellen | gemRL_Betr_TI |
| GS-A_4405 | Service Level Requirements im Change und Release Management | gemRL_Betr_TI |
| GS-A_4407 | Bereitstellung der Dokumentation des Change Managements für genehmigungspflichtige Produkt-Changes | gemRL_Betr_TI |

| | | |
|-----------|--|---------------|
| GS-A_5343 | Definition inhaltlicher Auszüge aus dem Betriebshandbuch | gemRL_Betr_TI |
| GS-A_5370 | Prüfung auf Emergency Change | gemRL_Betr_TI |

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 Produkthanbieter als umgesetzt bewertet werden.

Tabelle 5: Anforderungen zur sicherheitstechnischen Eignung "Sicherheitsgutachten"

| Afo-ID | Afo-Bezeichnung | Quelle (Referenz) |
|-----------|--|-------------------|
| GS-A_4173 | Erbringung von Verzeichnisdienstleistungen | gemRL_TSL_SP_CP |
| GS-A_4191 | Einsatz interoperabler Systeme durch einen externen Dienstleister | gemRL_TSL_SP_CP |
| GS-A_4230 | Gewährleistung der Online-Verfügbarkeit von Sperrinformationen | gemRL_TSL_SP_CP |
| GS-A_4247 | Obligatorische Vorgaben für das Rollenkonzept | gemRL_TSL_SP_CP |
| GS-A_4249 | Standort für Backup-HSM | gemRL_TSL_SP_CP |
| GS-A_4255 | Nutzung des HSM im kontrollierten Bereich | gemRL_TSL_SP_CP |
| GS-A_4259 | Vorgaben für die informationstechnische Trennung sicherheitskritischer Bestandteile der Systemumgebung | gemRL_TSL_SP_CP |
| GS-A_4260 | Manipulationsschutz veröffentlichter Daten | gemRL_TSL_SP_CP |
| GS-A_4261 | Vorgaben zur Betriebsumgebung für | gemRL_TSL_SP_CP |

| | | |
|-----------|---|-----------------|
| | sicherheitskritische Bestandteile des Systems | |
| GS-A_4268 | Anforderungen an den Einsatz freier Mitarbeiter | gemRL_TSL_SP_CP |
| GS-A_4270 | Aufzeichnung von technischen Ereignissen | gemRL_TSL_SP_CP |
| GS-A_4271 | Aufzeichnung von organisatorischen Ereignissen | gemRL_TSL_SP_CP |
| GS-A_4272 | Aufbewahrungsfrist für sicherheitsrelevante Protokolldaten | gemRL_TSL_SP_CP |
| GS-A_4273 | Schutz vor Zugriff, Löschung und Manipulation elektronischer Protokolldaten | gemRL_TSL_SP_CP |
| GS-A_4274 | Archivierung von für den Zertifizierungsprozess relevanten Daten | gemRL_TSL_SP_CP |
| GS-A_4275 | Dokumentationspflicht für Prozesse zum Schlüsselwechsel | gemRL_TSL_SP_CP |
| GS-A_4276 | Aktionen und Verantwortlichkeit im Rahmen der Notfallplanung | gemRL_TSL_SP_CP |
| GS-A_4279 | Fortbestand von Archiven und die Abrufmöglichkeit einer vollständigen Widerrufsliste | gemRL_TSL_SP_CP |
| GS-A_4284 | Beachtung des betreiberspezifischen Sicherheitskonzepts bei der Erzeugung von Schlüsselpaaren | gemRL_TSL_SP_CP |
| GS-A_4285 | Sicherheitsniveau bei der Generierung von Signaturschlüsseln | gemRL_TSL_SP_CP |
| GS-A_4287 | Sichere Aufbewahrung des privaten Schlüssels einer CA | gemRL_TSL_SP_CP |
| GS-A_4288 | Verwendung eines Backup-HSM zum Im-/Export von privaten Schlüsseln | gemRL_TSL_SP_CP |
| GS-A_4289 | Unterstützung des sicheren Löschen von Schlüsseln durch HSM | gemRL_TSL_SP_CP |
| GS-A_4290 | Generieren und Löschen von Schlüsselpaaren gemäß Vier-Augen-Prinzip | gemRL_TSL_SP_CP |
| GS-A_4291 | Berechnungen mit dem privaten Schlüssel gemäß Vier-Augen-Prinzip | gemRL_TSL_SP_CP |
| GS-A_4292 | Protokollierung der HSM-Nutzung | gemRL_TSL_SP_CP |
| GS-A_4294 | Bedienung des Schlüsselgenerierungssystems | gemRL_TSL_SP_CP |
| GS-A_4295 | Berücksichtigung des aktuellen Erkenntnisstands bei der Generierung von Schlüsseln | gemRL_TSL_SP_CP |
| GS-A_4304 | Speicherung und Anwendung von privaten Schlüsseln | gemRL_TSL_SP_CP |

| | | |
|-------------|---|-----------------|
| GS-A_4305 | Ordnungsgemäße Sicherung des privaten Schlüssels | gemRL_TSL_SP_CP |
| GS-A_4306 | Verwendung von privaten Schlüsseln | gemRL_TSL_SP_CP |
| GS-A_4307 | Vorgaben an HSM-Funktionalität | gemRL_TSL_SP_CP |
| GS-A_4308 | Speicherung und Auswahl von Schlüsselpaaren im HSM | gemRL_TSL_SP_CP |
| GS-A_4309 | Verwendung von zertifizierten kryptographischen Modulen | gemRL_TSL_SP_CP |
| GS-A_4310 | Vorgaben an die Prüftiefe der Evaluierung eines HSM | gemRL_TSL_SP_CP |
| GS-A_4311 | Hinterlegung des privaten Signaturschlüssels | gemRL_TSL_SP_CP |
| GS-A_4312 | Aktivierung privater Schlüssel | gemRL_TSL_SP_CP |
| GS-A_4313 | Deaktivierung privater Schlüssel | gemRL_TSL_SP_CP |
| GS-A_4314 | Sichere Übermittlung von Aktivierungsdaten | gemRL_TSL_SP_CP |
| GS-A_4315 | Konformität zum betreiberspezifischen Sicherheitskonzept | gemRL_TSL_SP_CP |
| GS-A_4316 | Härtung von Betriebssystemen | gemRL_TSL_SP_CP |
| GS-A_4317 | Obligatorische Sicherheitsmaßnahmen | gemRL_TSL_SP_CP |
| GS-A_4396 | Speicherung hinterlegter Root- und CA-Schlüssel | gemRL_TSL_SP_CP |
| GS-A_4925 | CP-Test, Keine Verwendung von Echtdaten | gemRL_TSL_SP_CP |
| A_16178 | Bezug des CV-Zertifikats mit dem Zugriffsprofil Null für SM-B KTR-Adv | gemSpec_CVC_TSP |
| TIP1-A_2557 | Inhalt der Ausgabepolicy des TSP-CVC | gemSpec_CVC_TSP |
| TIP1-A_2579 | Korrektur privater Schlüssel in der Chipkarte | gemSpec_CVC_TSP |
| TIP1-A_2580 | Erzeugung des privaten Schlüssels der Chipkarte | gemSpec_CVC_TSP |
| TIP1-A_2582 | Vertraulichkeit des privaten Schlüssels der Chipkarte | gemSpec_CVC_TSP |
| TIP1-A_2583 | Zuordnung des privaten Schlüssels zu Identitäten | gemSpec_CVC_TSP |
| TIP1-A_2584 | Schlüsselpaare und CV-Zertifikate | gemSpec_CVC_TSP |
| TIP1-A_2586 | Personalisierung von CV-Zertifikaten für ein Sicherheitsmodul vom Typ B | gemSpec_CVC_TSP |
| TIP1-A_2590 | Vernichtung fehlerhafter Chipkarten vor deren Ausgabe | gemSpec_CVC_TSP |

| | | |
|-------------|--|-----------------|
| TIP1-A_2591 | Ausgabe fehlerfreier Chipkarten | 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-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 sensativer 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_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_4222 | Authentizität des öffentlichen Root-Schlüssels | 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_2076-01 | kDSM: Datenschutzmanagement nach BSI | gemSpec_DS_Anbieter |
| GS-A_2158-01 | Trennung von kryptographischen Identitäten und Schlüsseln in Produktiv- und Testumgebungen | gemSpec_DS_Anbieter |
| GS-A_2214-01 | kDSM: Anbieter müssen jährlich die Auftragsverarbeiter kontrollieren | 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_5626 | kDSM: Auftragsverarbeitung | gemSpec_DS_Anbieter |
| GS-A_4357 | X.509-Identitäten für die Erstellung und Prüfung digitaler nicht-qualifizierter elektronischer Signaturen | gemSpec_Krypt |
| GS-A_4359 | X.509-Identitäten für die Durchführung einer TLS-Authentifizierung | gemSpec_Krypt |
| GS-A_4361 | X.509-Identitäten für die Erstellung und Prüfung digitaler Signaturen | gemSpec_Krypt |
| GS-A_4362 | X.509-Identitäten für Verschlüsselungszertifikate | gemSpec_Krypt |
| 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_4384 | TLS-Verbindungen | gemSpec_Krypt |
| GS-A_4385 | TLS-Verbindungen, Version 1.2 | gemSpec_Krypt |
| GS-A_4386 | TLS-Verbindungen, optional Version 1.1 | gemSpec_Krypt |
| GS-A_4387 | TLS-Verbindungen, nicht Version 1.0 | gemSpec_Krypt |
| GS-A_4388 | DNSSEC-Kontext | gemSpec_Krypt |
| GS-A_4393 | Algorithmus bei der Erstellung von Hashwerten von Zertifikaten oder öffentlichen Schlüsseln | gemSpec_Krypt |

| | | |
|-----------|--|-------------------|
| GS-A_5035 | Nichtverwendung des SSL-Protokolls | gemSpec_Krypt |
| GS-A_5079 | Migration von Algorithmen und Schlüssellängen bei PKI-Betreibern | gemSpec_Krypt |
| GS-A_5131 | Hash-Algorithmus bei OCSP/CertID | gemSpec_Krypt |
| GS-A_5322 | Weitere Vorgaben für TLS-Verbindungen | gemSpec_Krypt |
| GS-A_5338 | HBA/SMC-B – Erzeugung asymmetrischer Schlüsselpaare auf der jeweiligen Karte selbst | gemSpec_Krypt |
| GS-A_5339 | TLS-Verbindungen, erweiterte Webbrowser-Interoperabilität | gemSpec_Krypt |
| GS-A_5386 | kartenindividuelle geheime und private Schlüssel G2-Karten | gemSpec_Krypt |
| GS-A_4054 | Paketfilter Default Deny | gemSpec_Net |
| GS-A_4062 | Sicherheitskomponenten bei Netzübergängen zu Fremdnetzen | gemSpec_Net |
| GS-A_4817 | Produkttypen der Fachanwendungen sowie der zentralen TI-Plattform, Einbringung des DNSSEC Trust Anchor für den Namensraum TI | gemSpec_Net |
| GS-A_2227 | Keine Kartendubletten | gemSpec_PINPUK_TI |
| GS-A_2228 | Trennung von Karte und PIN/PUK-Brief | gemSpec_PINPUK_TI |
| GS-A_2229 | Prozesse und Maßnahmen zur Aushändigung von Karte und PIN/PUK-Brief | gemSpec_PINPUK_TI |
| GS-A_2230 | PIN/PUK-Erzeugung: Länge PIN/PUK (Kartenherausgeber) | gemSpec_PINPUK_TI |
| GS-A_2232 | PIN/PUK-Erzeugung: Verfahren für PIN/PUK-Auswahl | gemSpec_PINPUK_TI |
| GS-A_2234 | PIN/PUK-Erzeugung: Zufallsgenerator für PIN/PUK | gemSpec_PINPUK_TI |
| GS-A_2235 | PIN/PUK-Erzeugung: Ableitung von PIN | gemSpec_PINPUK_TI |
| GS-A_2236 | PIN/PUK-Erzeugung: Ableitung der PIN aus eindeutig dem Versicherten zugeordneten Daten | gemSpec_PINPUK_TI |
| GS-A_2237 | PIN/PUK-Erzeugung: kein Rückschluss von PIN/PUK auf Schlüssel | gemSpec_PINPUK_TI |
| GS-A_2238 | PIN/PUK-Erzeugung: Informationen an Karteninhaber bei selbstständiger Wahl der PIN | gemSpec_PINPUK_TI |
| GS-A_2239 | PIN/PUK-Erzeugung: Ableitung von PIN im Sicherheitsmodul | gemSpec_PINPUK_TI |
| GS-A_2240 | PIN/PUK-Speicherung: Verschlüsselung der PIN außerhalb von Sicherheitsmodulen | gemSpec_PINPUK_TI |

| | | |
|-----------|--|-------------------|
| GS-A_2242 | PIN/PUK-Speicherung: Integrität der PIN außerhalb von Sicherheitsmodulen | gemSpec_PINPUK_TI |
| GS-A_2244 | PIN/PUK-Speicherung: Verschlüsselung unterschiedlicher PINs mit unterschiedlichen Schlüsseln | gemSpec_PINPUK_TI |
| GS-A_2246 | PIN/PUK-Speicherung: Verschlüsselung gleicher PINs führt zu unterschiedlichen verschlüsselten Werten | gemSpec_PINPUK_TI |
| GS-A_2247 | PIN/PUK-Speicherung: Wiederholte Verschlüsselung der PIN führt zu unterschiedlichen Werten | gemSpec_PINPUK_TI |
| GS-A_2248 | PIN/PUK-Speicherung: unterschiedliche Schlüssel für unterschiedliche Zwecke | gemSpec_PINPUK_TI |
| GS-A_2249 | PIN/PUK-Speicherung: Dokumentation der Zwecke | gemSpec_PINPUK_TI |
| GS-A_2250 | PIN/PUK-Speicherung: Entschlüsselung nur durch berechtigten Empfänger | gemSpec_PINPUK_TI |
| GS-A_2252 | PIN/PUK-Löschung: Löschung von PIN/PUK nach Ablauf der Speicherdauer | gemSpec_PINPUK_TI |
| GS-A_2253 | PIN/PUK-Transport: Sicherer PIN-Transport beim Kartenherausgeber bzw. Kartenpersonalisierer | gemSpec_PINPUK_TI |
| GS-A_2254 | PIN/PUK-Transport: Schutz außerhalb geschützter Hardware beim Kartenherausgeber bzw. Kartenpersonalisierer | gemSpec_PINPUK_TI |
| GS-A_2255 | PIN/PUK-Transport: Verteilung beschränken | gemSpec_PINPUK_TI |
| GS-A_2256 | PIN/PUK-Transport: einmalige PIN-Erstellung beim Kartenherausgeber bzw. Kartenpersonalisierer | gemSpec_PINPUK_TI |
| GS-A_2260 | PIN/PUK-Transport: Transport außerhalb eines Sicherheitsmoduls | gemSpec_PINPUK_TI |
| GS-A_2261 | PIN/PUK-Transport: Transport außerhalb eines Sicherheitsmoduls - kein Klartext | gemSpec_PINPUK_TI |
| GS-A_2264 | PIN/PUK-Transport: elektronische PIN-Verteilung | gemSpec_PINPUK_TI |
| GS-A_2266 | PIN/PUK-Transport: Verschlüsselung gleicher PINs muss zu unterschiedlichen Werten führen | gemSpec_PINPUK_TI |
| GS-A_2270 | PIN/PUK-Transport: Unterschiedliche verschlüsselte Werte auch bei gleichen PINs | gemSpec_PINPUK_TI |
| GS-A_2271 | PIN/PUK-Transport: kein Rückschluss auf vorher benutzte Schlüssel | gemSpec_PINPUK_TI |
| GS-A_2274 | PIN/PUK-Transport: Löschung der PIN nach Transport | gemSpec_PINPUK_TI |
| GS-A_2276 | PIN/PUK-Transport: Aktivitäten im Vier-Augen- | gemSpec_PINPUK_TI |

| | | |
|----------------|--|---------------------------|
| | Prinzip bei der Zuordnung einer PIN/PUK zu einer Karte | |
| GS-A_2277 | PIN/PUK-Transport: Aktivitäten im Vier-Augen-Prinzip beim Rücksetzen des Fehlbedienungs Zählers | gemSpec_PINPUK_TI |
| GS-A_2284 | PIN/PUK-Änderung: Änderungen durch Kartenpersonalisierer im Vier-Augen-Prinzip | gemSpec_PINPUK_TI |
| GS-A_2285 | PIN/PUK-Änderung: Prozess bei Kompromittierung beim Kartenherausgeber bzw. Kartenpersonalisierer | gemSpec_PINPUK_TI |
| GS-A_2287 | PIN/PUK-Löschung: Nachweis der Löschung nicht mehr gebrauchter PIN beim Kartenherausgeber bzw. Kartenpersonalisierer | gemSpec_PINPUK_TI |
| GS-A_2291 | PIN/PUK-Löschung: Löschen von nicht mehr benötigten Klartext-PIN | gemSpec_PINPUK_TI |
| GS-A_2292 | PIN/PUK-Löschung: Außerbetriebnahme der PIN und Karte | gemSpec_PINPUK_TI |
| GS-A_2295 | Schutz der Schlüssel für PIN/PUK gemäß Hierarchiestufe 4 | gemSpec_PINPUK_TI |
| GS-A_5085 | PIN/PUK-Änderung: Prozess bei Kompromittierungsmeldung durch Karteninhaber | gemSpec_PINPUK_TI |
| GS-A_5209 | PIN/PUK-Speicherung: PIN/PUK unverzüglich löschen | gemSpec_PINPUK_TI |
| GS-A_5387 | Beachten von Vorgaben bei der Kartenpersonalisierung | gemSpec_PINPUK_TI |
| GS-A_4641 | Initiale Einbringung TI-Vertrauensanker | gemSpec_PKI |
| GS-A_4748 | Initiale Einbringung TSL-Datei | gemSpec_PKI |
| Card-G2-A_3589 | Schlüsselspeicherung | gemSpec_SMC-B_ObjSys |
| Card-G2-A_3589 | Schlüsselspeicherung | gemSpec_SMC-B_ObjSys_G2.1 |
| TIP1-A_3548 | Schützenswerte Objekte | gemSpec_X.509_TSP |
| TIP1-A_3549 | Vorgaben zum Schutzbedarf durch die gematik | gemSpec_X.509_TSP |
| TIP1-A_3550 | Spezifische Erhöhung des Schutzbedarfs ist zulässig | gemSpec_X.509_TSP |
| TIP1-A_3554 | Gesicherte interne Schnittstellen des TSP-X.509 QES und TSP-X.509 nonQES | gemSpec_X.509_TSP |
| TIP1-A_3555 | Datenaustausch zwischen gematik und TSP-X.509 nonQES und gematik Root-CA | gemSpec_X.509_TSP |

| | | |
|-------------|---|-------------------|
| TIP1-A_3557 | Gesicherte externe Schnittstellen des TSP-X.509 nonQES | gemSpec_X.509_TSP |
| TIP1-A_3590 | Eindeutige Verbindung Personen- und Organisationszertifikatsnehmer und privater Schlüssel | gemSpec_X.509_TSP |
| TIP1-A_3595 | Anforderungen von LEO- und KTR-Institutionen | gemSpec_X.509_TSP |
| TIP1-A_3596 | Umsetzung Erstellungsdienst TSP-X.509 QES und TSP-X.509 nonQES für Personen- und Organisationszertifikate | gemSpec_X.509_TSP |
| TIP1-A_3660 | Trennung der TSP-X.509-Betriebsumgebungen | gemSpec_X.509_TSP |
| TIP1-A_3881 | Schutzbedarf darf nicht verringert werden | gemSpec_X.509_TSP |
| TIP1-A_4230 | Datenschutzgerechte Antrags- und Sperrprozesse | gemSpec_X.509_TSP |
| TIP1-A_4231 | Löschung gespeicherter X.509-Zertifikate | gemSpec_X.509_TSP |
| TIP1-A_4232 | Löschung von TSP-X.509 nonQES-Zertifikatstatusinformationen, Zertifikats- und Sperranträge | gemSpec_X.509_TSP |
| TIP1-A_4234 | Protokollierung von OCSP-Anfragen | gemSpec_X.509_TSP |
| TIP1-A_4235 | Fehlerprotokollierung | gemSpec_X.509_TSP |
| TIP1-A_5087 | Berücksichtigung und Umsetzung übergeordneter Herausgeberpolicies | gemSpec_X.509_TSP |

Ein TSPs X.509 nonQES, der gleichzeitig eine VDA-Qualifizierung 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 Vorlage eines Zertifikats)
- erklärt, dass für die gegenständlichen Sicherheitsanforderungen der Betrieb des TSP X.509 nonQES äquivalent zum ZDA -Bereich erfolgt.

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

Tabelle 6: nicht nachzuweisende Anforderungen

| | | | | |
|-----------|-----------|-----------|--------------|--------------|
| GS-A_4173 | GS-A_4275 | GS-A_4305 | GS-A_2328-01 | GS-A_2329-01 |
| GS-A_4191 | GS-A_4276 | GS-A_4306 | GS-A_4980-01 | GS-A_2331-01 |
| GS-A_4230 | GS-A_4279 | GS-A_4307 | GS-A_4981-01 | GS-A_2332-01 |
| GS-A_3130 | GS-A_4284 | GS-A_4308 | GS-A_4982-01 | GS-A_3139 |
| GS-A_4249 | GS-A_4285 | GS-A_4309 | GS-A_4983-01 | GS-A_3141 |
| GS-A_4255 | GS-A_4287 | GS-A_4310 | GS-A_4984-01 | GS-A_3149 |

| | | | | |
|--------------|-----------|-----------|--------------|--------------|
| GS-A_4259 | GS-A_4288 | GS-A_4311 | GS-A_3772-01 | GS-A_2076-01 |
| GS-A_4261 | GS-A_4289 | GS-A_4312 | GS-A_4367 | GS-A_3078 |
| GS-A_4268 | GS-A_4290 | GS-A_4313 | GS-A_4368 | GS-A_3125 |
| GS-A_4270 | GS-A_4291 | GS-A_4314 | GS-A_3737-01 | TIP1-A_3548 |
| GS-A_4271 | GS-A_4292 | GS-A_4315 | GS-A_2214-01 | TIP1-A_3550 |
| GS-A_4272 | GS-A_4294 | GS-A_4316 | GS-A_3753-01 | TIP1-A_3554 |
| GS-A_4273 | GS-A_4295 | GS-A_4317 | GS-A_5626 | TIP1-A_4230 |
| GS-A_4274 | GS-A_4304 | GS-A_4906 | GS-A_2158-01 | TIP1-A_4235 |
| GS-A_2345-01 | | | | |

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) |
|--------------|---|---------------------|
| GS-A_2355-01 | Meldung von erheblichen Schwachstellen und Bedrohungen | gemSpec_DS_Anbieter |
| GS-A_4468-02 | kDSM: Jährlicher Datenschutzbericht der TI | gemSpec_DS_Anbieter |
| GS-A_4473-01 | kDSM: Unverzügliche Benachrichtigung bei Verstößen gemäß Art. 34 DSGVO | gemSpec_DS_Anbieter |
| GS-A_4478-01 | kDSM: Nachweis der Umsetzung von Maßnahmen in Folge eines gravierenden Datenschutzverstoßes | gemSpec_DS_Anbieter |
| GS-A_4479-01 | kDSM: Meldung von Änderungen der Kontaktinformationen zum Datenschutzmanagement | 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 | gemSpec_DS_Anbieter |

| | | |
|--------------|---|---------------------|
| | Sicherheitsvorfällen und Notfällen | |
| 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_5324-02 | kDSM: Teilnahme des Anbieters an Sitzungen des kDSM | 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_5564 | kDSM: Ansprechpartner für Datenschutz | gemSpec_DS_Anbieter |
| GS-A_5565 | kDSM: Unverzügliche Behebung von Verstößen gemäß Art. 34 DSGVO | gemSpec_DS_Anbieter |
| GS-A_5566 | kDSM: Sicherstellung der Datenschutzerfordernisse in Unterbeauftragungsverhältnissen | gemSpec_DS_Anbieter |
| GS-A_5624 | Auditrechte der gematik zur Informationssicherheit | gemSpec_DS_Anbieter |
| GS-A_5625 | kDSM: Auditrechte der gematik zum Datenschutz | gemSpec_DS_Anbieter |

4 Anhang A – Verzeichnisse

4.1 Abkürzungen

| Kürzel | Erläuterung |
|--------|-----------------------------|
| Afo-ID | Anforderungs-Identifikation |

4.2 Tabellenverzeichnis

| | |
|--|----|
| Tabelle 1: Dokumente mit Anforderungen zu der Anbietertypversion | 6 |
| Tabelle 2: Anforderungen zur betrieblichen Eignung "Prozessprüfung" | 8 |
| Tabelle 3: Anforderungen zur betrieblichen Eignung "Anbietererklärung" | 9 |
| Tabelle 4: Anforderungen zur betrieblichen Eignung "Betriebshandbuch" | 13 |
| Tabelle 5: Anforderungen zur sicherheitstechnischen Eignung "Sicherheitsgutachten" ... | 14 |
| Tabelle 6: nicht nachzuweisende Anforderungen | 24 |
| Tabelle 7: Anforderungen zur sicherheitstechnischen Eignung "Anbietererklärung" | 25 |

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 |