

Elektronische Gesundheitskarte und Telematikinfrastruktur

Anbietertypsteckbrief

Signaturdienst

| | |
|----------------------|-------------|
| Anbietertyp Version: | 1.0.6 |
| Anbietertyp Status: | freigegeben |

| | |
|------------------|------------------------|
| Version: | 1.0.0 |
| Revision: | 654302 |
| Stand: | 21.06.23 |
| Status: | freigegeben |
| Klassifizierung: | öffentlich |
| Referenzierung: | gemAnbT_SigD_ATV_1.0.6 |

Historie Anbietertypversion und Anbietertypsteckbrief

Historie Anbietertypversion

Die Anbietertypversion ändert sich, wenn sich die normativen Festlegungen für den Anbietertyp ändern.

| Anbietertypversion | Beschreibung der Änderung | Referenz |
|--------------------|---|------------------------|
| 1.0.0 | Initiale Version | gemAnbT_SigD_ATV_1.0.0 |
| 1.0.1 | Anpassung an Releasestand 4.0.0 | gemAnbT_SigD_ATV_1.0.1 |
| 1.0.2 | Anpassung an Releasestand 4.0.1 | gemAnbT_SigD_ATV_1.0.2 |
| 1.0.4 | Anpassung aufgrund der Einarbeitung der Änderungen aus ePA_Maintenance_21.5 und Betr_Maintenance_21.3 sowie redaktionelle Anpassungen | gemAnbT_SigD_ATV_1.0.4 |
| 1.0.5 | Anpassung aufgrund der Einarbeitung Feature IDP-Federation | gemAnbT_SigD_ATV_1.0.5 |
| 1.0.6 | Anpassung aufgrund der Einarbeitung der Änderungen aus Betr_Maintenance_23.2 | gemAnbT_SigD_ATV_1.0.6 |

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 | 21.06.23 | | 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 Normative Festlegungen | 7 |
| 3.1 Festlegungen zur betrieblichen Eignung | 7 |
| 3.1.1 Prozessprüfung betriebliche Eignung..... | 7 |
| 3.1.2 Anbietererklärung betriebliche Eignung | 8 |
| 3.1.3 Betriebshandbuch betriebliche Eignung | 14 |
| 3.2 Festlegungen zur sicherheitstechnischen Eignung | 15 |
| 3.2.1 Sicherheitsgutachten | 15 |
| 3.2.2 Anbietererklärung sicherheitstechnische Eignung | 21 |
| 4 Produktspezifische Merkmale | 23 |
| 4.1 Optionale Ausprägungen | 23 |
| 5 Anhang A – Verzeichnisse | 24 |
| 5.1 Abkürzungen | 24 |
| 5.2 Tabellenverzeichnis | 24 |
| 5.3 Referenzierte Dokumente | 24 |

1 Einführung

1.1 Zielsetzung und Einordnung des Dokumentes

Anbietertypsteckbriefe verzeichnen verbindlich die normativen Festlegungen der gematik an Anbieter zur Sicherstellung des Betriebes der von ihnen verantworteten Serviceeinheiten.

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 Anbietertypsteckbrief richtet sich an:

- Anbieter Signaturdienst
- 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. PTV_ATV_Festlegungen) 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 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 Anbietertyp normativen Festlegungen.

Tabelle 1: Dokumente mit normativen Festlegungen

| Dokumenten Kürzel | Bezeichnung des Dokumentes | Version |
|---------------------|--|-----------------------|
| gemRL_TSL_SP_CP | Certificate Policy Gemeinsame Zertifizierungsrichtlinie für Teilnehmer der gematik-TSL | 2.1 01 .20 |
| gemSpec_SigD | Spezifikation Signaturdienst | 1.5.0 |
| gemSpec_Krypt | Übergreifende Spezifikation Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur | 2.2 48 .0 |
| gemKPT_Betr | Betriebskonzept Online-Produktivbetrieb | 3.2 45 .0 |
| gemRL_Betr_TI | Übergreifende Richtlinien zum Betrieb der TI | 2. 78 .0 |
| gemSpec_PKI | Übergreifende Spezifikation – Spezifikation PKI | 2.1 45 .40 |
| gemSpec_Perf | Übergreifende Spezifikation Performance und Mengengerüst TI-Plattform | 2.2 69 .20 |
| gemSpec_DS_Anbieter | Spezifikation Datenschutz- und Sicherheitsanforderungen der TI an Anbieter | 1.5.0 |
| gemSpec_Aktensystem | Spezifikation Aktensystem ePA | 1.5 23 .01 |

3 Normative Festlegungen

Die folgenden Abschnitte verzeichnen alle für den Anbietertypen normativen Festlegungen der gematik an Anbieter Signaturdienst zur Sicherstellung des Betriebes der von ihnen verantworteten Serviceeinheiten. Die Festlegungen sind gruppiert nach der Art der Nachweisführung ihrer Erfüllung als Grundlage der Zulassung.

3.1 Festlegungen zur betrieblichen Eignung

3.1.1 Prozessprüfung betriebliche Eignung

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

Tabelle 2: Festlegungen zur betrieblichen Eignung "Prozessprüfung"

| ID | Bezeichnung | Quelle (Referenz) |
|--------------|---|---------------------|
| A_18237 | Lieferung von Performance-Rohdaten-Reports | 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_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_2355-02 | 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: Unverzögliche 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 |

| ID | Bezeichnung | Quelle (Referenz) |
|--------------|---|---------------------|
| GS-A_4524-01 | Meldung von Änderungen der Kontaktinformationen für Informationssicherheit | 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_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_5559-01 | 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 |
| A_22057 | Performance - Rohdaten - Verpflichtung des Anbieters (Rohdatenerfassung v.02) | gemSpec_Perf |

3.1.2 Anbietererklärung betriebliche Eignung

Sofern in diesem Abschnitt Festlegungen 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: Festlegungen zur betrieblichen Eignung "Anbietererklärung"

| ID | Bezeichnung | Quelle (Referenz) |
|---------|---|-------------------|
| A_18176 | Mitwirkungspflichten bei der Einrichtung von Probes des Service Monitorings | gemKPT_Betr |

| ID | Bezeichnung | Quelle (Referenz) |
|----------------|---|-------------------|
| A_18240 | Reporting der technischen Service Level | gemKPT_Betr |
| A_20111 | Erreichbarkeit des Versicherten Help Desk (VHD) | gemKPT_Betr |
| TIP1-A_6359-02 | Definition der notwendigen Leistung anderer Anbieter durch Anbieter | gemKPT_Betr |
| TIP1-A_6360-02 | Kontrolle bereitgestellter Leistungen durch Anbieter | gemKPT_Betr |
| TIP1-A_6367-02 | Definition eines Business-Servicekatalog der angebotenen TI Services | gemKPT_Betr |
| TIP1-A_6371-02 | 2nd-Level-Support: Single-Point-of-Contact (SPOC) für Anbieter | gemKPT_Betr |
| TIP1-A_6377-02 | Koordination von produktverantwortlichen Anbietern und Herstellern | gemKPT_Betr |
| TIP1-A_6388-02 | Bereitstellung eines lokalen IT-Service-Managements durch Anbieter für ihre zu verantwortenden Servicekomponenten | gemKPT_Betr |
| TIP1-A_6389-02 | Erreichbarkeit der 1st-Level (UHD), 2nd-Level (SPOCs) der Anbieter | gemKPT_Betr |
| TIP1-A_6390-02 | Mitwirkung im TI-ITSM durch Anbieter | gemKPT_Betr |
| TIP1-A_6393-02 | Verantwortung für die Weiterleitung von Anfragen | gemKPT_Betr |
| TIP1-A_6415-02 | Fortgeführte Wahrnehmung der Serviceverantwortung bei der Delegation von Aufgaben | gemKPT_Betr |
| TIP1-A_6437 | Datenaufbewahrung von Performancedaten | 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_7265-03 | Serviceleistung der TI-ITSM-Teilnehmer im TI-ITSM-Teilnehmersupport zur Haupt- und Nebenzeit | gemKPT_Betr |
| TIP1-A_7266 | Mitwirkungspflichten im TI-ITSM-System | gemKPT_Betr |
| A_13575 | Qualität von RfCs | gemRL_Betr_TI |

| ID | Bezeichnung | Quelle (Referenz) |
|--------------|--|-------------------|
| A_17735 | Rohdatenreporting | gemRL_Betr_TI |
| A_17764 | Verwendung CI-ID | gemRL_Betr_TI |
| A_18237 | Lieferung von Performance-Rohdaten-Reports | gemRL_Betr_TI |
| A_18363 | Berechnung von Performance-Kenngrößen aus Rohdaten | gemRL_Betr_TI |
| A_18403 | Erstellung einer Root Cause Analysis im Incident - Prio 1 | gemRL_Betr_TI |
| A_18404 | Erstellung einer Root Cause Analysis im Incident - Prio 2 bis 4 | gemRL_Betr_TI |
| A_18405 | Erstellung einer Root Cause Analysis durch am Incident beteiligte TI-ITSM-Teilnehmer | gemRL_Betr_TI |
| A_18406 | Nachlieferung zu einer Root Cause Analysis | gemRL_Betr_TI |
| A_18407 | Unterstützung bei Change-Verifikation | gemRL_Betr_TI |
| A_19869 | Performance - Rohdaten-Performance-Berichte - zu liefernde Berichte der TI-ITSM-Teilnehmer | gemRL_Betr_TI |
| GS-A_3884 | Festlegung von Dringlichkeit und Auswirkung von übergreifenden Incidents | gemRL_Betr_TI |
| GS-A_3886-01 | Nutzung des TI-ITSM-Systems bei der Übermittlung eines übergreifenden Vorgangs | gemRL_Betr_TI |
| GS-A_3889 | Schließung eines übergreifenden Incidents | gemRL_Betr_TI |
| GS-A_3902 | Prüfung auf Serviceverantwortung | gemRL_Betr_TI |
| GS-A_3904 | Annahme 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_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_3975 | Prüfung auf Serviceverantwortung zum übergreifenden Problem | gemRL_Betr_TI |
| GS-A_3976 | Ablehnung der Lösungsunterstützung | gemRL_Betr_TI |

| ID | Bezeichnung | Quelle (Referenz) |
|-----------|---|-------------------|
| GS-A_3977 | Annahme der Verantwortung zur Lösungsunterstützung | gemRL_Betr_TI |
| GS-A_3981 | Annahme eines übergreifenden Problems | gemRL_Betr_TI |
| GS-A_3982 | Ablehnung 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 (RU/TU) | gemRL_Betr_TI |
| GS-A_3986 | Koordination bei übergreifenden Problemen | 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_3989 | Ablehnung der Lösung 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_4090 | Kommunikationssprache | 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_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 |

| ID | Bezeichnung | Quelle (Referenz) |
|-----------|---|-------------------|
| 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_5250 | Ablehnung der Lösung eines übergreifenden Incidents | 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 |

| ID | Bezeichnung | Quelle (Referenz) |
|-----------------------|--|------------------------|
| GS-A_5588 | Abbruch der Problembearbeitung | gemRL_Betr_TI |
| GS-A_5589 | Prüfung auf Verantwortung zur Lösungsunterstützung | gemRL_Betr_TI |
| GS-A_5594 | Identifikation von TI-Konfigurationsdaten | 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 |
| 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_5610-02 | Bearbeitungsfristen in der Bewertung von Produkt-Changes | gemRL_Betr_TI |
| GS-A_5611 | Umsetzung von autorisierten RFC | gemRL_Betr_TI |
| A_18018 | Performance - Signaturdienst - Spitzenlastvorgaben | gemSpec_Perf |
| A_22003-01 | Performance - Rohdaten - Nachlieferung auf Anforderung (Rohdatenerfassung v.02) | gemSpec_Perf |
| A_22996 | Performance - Rohdaten - Zeitpunkte der Übermittlungen (Rohdatenerfassung v.02) | gemSpec_Perf |
| A_16217-01 | Mindesterreichbarkeitszeiten im Versichertensupport (09:00-17:00 Uhr) | gemKPT_Betr |
| A_18239-01 | Service Level – Lieferung von Rohdaten-Performance-Reports | gemKPT_Betr |

| ID | Bezeichnung | Quelle (Referenz) |
|-----------------------|--|-------------------|
| A_17668-07 | Performance—Rohdaten—Performance-Berichte—Format der Einträge des Rohdaten—Performance-Berichts | gemSpec_Perf |
| A_17985 | Performance—Signaturdienst—Lieferung von Rohdaten | gemSpec_Perf |

3.1.3 Betriebshandbuch betriebliche Eignung

Sofern in diesem Abschnitt Festlegungen 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: Festlegungen zur betrieblichen Eignung "Betriebshandbuch"

| ID | 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_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_4086 | Erreichbarkeit der Kommunikationsschnittstellen | gemRL_Betr_TI |
| GS-A_4088-01 | Benennung von Ansprechpartnern | 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 |

| ID | Bezeichnung | Quelle (Referenz) |
|-----------|--|-------------------|
| 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_4407 | Bereitstellung der Dokumentation des Change Managements für genehmigungspflichtige Produkt-Changes | gemRL_Betr_TI |
| GS-A_5370 | Prüfung auf Emergency Change | gemRL_Betr_TI |

3.2 Festlegungen zur sicherheitstechnischen Eignung

3.2.1 Sicherheitsgutachten

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

Tabelle 5: Festlegungen zur sicherheitstechnischen Eignung "Sicherheitsgutachten"

| ID | Bezeichnung | Quelle (Referenz) |
|-----------|--|-------------------|
| 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_4261 | Vorgaben zur Betriebsumgebung für sicherheitskritische Bestandteile des Systems | gemRL_TSL_SP_CP |

| ID | Bezeichnung | Quelle (Referenz) |
|-----------|---|-------------------|
| 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 |

| ID | Bezeichnung | Quelle (Referenz) |
|-----------|---|---------------------|
| 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_18765 | Gemeinsame Kontaktstelle von Signaturdienst und ePA-Aktensystem | gemSpec_Aktensystem |
| A_19123 | Dokumentationspflicht zur gemeinsamen Kontaktstelle | gemSpec_Aktensystem |
| A_19124 | Mitarbeiter der Kontaktstelle haben keinen Zugriff auf das ePA-Aktensystem und Signaturdienst | gemSpec_Aktensystem |

| ID | Bezeichnung | Quelle (Referenz) |
|--------------|---|---------------------|
| A_21716 | Unverzügliche Bewertung von Schwachstellen | gemSpec_DS_Anbieter |
| A_21718 | Umsetzen von Gegenmaßnahmen in Abhängigkeit der Kritikalität | gemSpec_DS_Anbieter |
| A_21719 | Weiterleitung von Reports TI SIEM | gemSpec_DS_Anbieter |
| 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_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 |

| ID | Bezeichnung | Quelle (Referenz) |
|--------------|---|---------------------|
| 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-Grundsatz | 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_5626 | kDSM: Auftragsverarbeitung | gemSpec_DS_Anbieter |
| A_17124-01 | TLS-Verbindungen (ECC-Migration) | gemSpec_Krypt |
| GS-A_4357-02 | X.509-Identitäten für die Erstellung und Prüfung digitaler nicht-qualifizierter elektronischer Signaturen | gemSpec_Krypt |
| GS-A_4367 | Zufallszahlengenerator | gemSpec_Krypt |
| GS-A_4368 | Schlüsselerzeugung | gemSpec_Krypt |
| GS-A_4384-01 | TLS-Verbindungen | gemSpec_Krypt |
| GS-A_4385 | TLS-Verbindungen, Version 1.2 | gemSpec_Krypt |
| GS-A_4387 | TLS-Verbindungen, nicht Version 1.0 | 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_4641 | Initiale Einbringung TI-Vertrauensanker | gemSpec_PKI |
| GS-A_4748 | Initiale Einbringung TSL-Datei | gemSpec_PKI |
| A_17336-01 | Signaturdienst - Sicherheitsniveau der Authentisierung auf dem Vertrauensniveau "hoch" | gemSpec_SigD |

| ID | Bezeichnung | Quelle (Referenz) |
|------------|--|-------------------|
| A_17339 | Signaturdienst - Speicherung privater Schlüssel mit einem HSM | gemSpec_SigD |
| A_17372 | Signaturdienst - Schutz des Auftrags der Krankenkasse während des Transports | gemSpec_SigD |
| A_17375-01 | Signaturdienst - P_Create_Identity | gemSpec_SigD |
| A_17382 | Signaturdienst - Schutz gegen OWASP Top 10-Risiken | gemSpec_SigD |
| A_17528 | Signaturdienst - Schutz der Verbindung zum Signaturdienst | gemSpec_SigD |
| A_17808 | Signaturdienst - P_Delete_Identity | gemSpec_SigD |
| A_17853-01 | Signaturdienst - Auskunft an Versicherten | gemSpec_SigD |
| A_17864 | Signaturdienst - Anbieter des Signaturdienstes ist kein Anbieter eines ePA-Aktensystems | gemSpec_SigD |
| A_18710 | Maximale Gültigkeit einer Authentifizierung | gemSpec_SigD |
| A_18711 | Signaturdienst – Nutzung einer erfolgreichen Authentifizierung | gemSpec_SigD |
| A_19033 | Schützenswerte Objekte | gemSpec_SigD |
| A_19037 | Gesicherte interne Schnittstellen des Anbieters Signaturdienst | gemSpec_SigD |
| A_19038 | Datenaustausch zwischen gematik und Anbieter Signaturdienst | gemSpec_SigD |
| A_19039 | Gesicherte externe Schnittstellen des Anbieters Signaturdienst | gemSpec_SigD |
| A_19040 | Eindeutige Verbindung Zertifikatsnehmer und privater Schlüssel | gemSpec_SigD |
| A_19041-01 | Umsetzung Signaturdienst für Zertifikate | gemSpec_SigD |
| A_19042 | Trennung der Signaturdienst-Betriebsumgebungen | gemSpec_SigD |
| A_19043 | Datenschutzgerechte Antrags- und Sperrprozesse | gemSpec_SigD |
| A_19044 | Löschung von Signaturdienst-Zertifikatsstatusinformationen, Zertifikats- und Sperranträgen | gemSpec_SigD |
| A_19045 | Fehlerprotokollierung | gemSpec_SigD |

| ID | Bezeichnung | Quelle (Referenz) |
|-------------------------|--|--------------------------|
| GS-A_4357-01 | X.509-Identitäten für die Erstellung und Prüfung digitaler nicht-qualifizierter elektronischer Signaturen | gemSpec_Krypt |

3.2.2 Anbietererklärung sicherheitstechnische Eignung

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

Tabelle 6: Festlegungen zur sicherheitstechnischen Eignung "Anbietererklärung"

| ID | Bezeichnung | Quelle (Referenz) |
|--------------------|--|--------------------------------|
| A_19174 | Bereitstellung Übersicht Internet-Schnittstellen der TI | gemSpec_DS_Anbieter |
| A_19175 | Zustimmung zu regelmäßigen Schwachstellenscans durch die gematik | gemSpec_DS_Anbieter |
| A_21717 | Bereitstellung der Bewertung von Schwachstellen gegenüber der gematik | gemSpec_DS_Anbieter |
| A_21720 | Beteiligung an Coordinated Vulnerability Disclosure | gemSpec_DS_Anbieter |
| GS-A_2214-01 | kDSM: Anbieter müssen jährlich die Auftragsverarbeiter kontrollieren | gemSpec_DS_Anbieter |
| GS-A_4526-01 | Aufbewahrungsvorgaben an die Nachweise zu Sicherheitsmeldungen | 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_5557 | Security Monitoring | gemSpec_DS_Anbieter |
| GS-A_5558 | Aktive Schwachstellenscans | gemSpec_DS_Anbieter |
| GS-A_5566 | kDSM: Sicherstellung der Datenschutzanforderungen in Unterbeauftragungsverhältnissen | gemSpec_DS_Anbieter |
| GS-A_5624-01 | Auditrechte der gematik zur Informationssicherheit | gemSpec_DS_Anbieter |

| ID | Bezeichnung | Quelle (Referenz) |
|-----------|---|---------------------|
| GS-A_5625 | kDSM: Auditrechte der gematik zum Datenschutz | gemSpec_DS_Anbieter |
| A_18958 | Sicherer Betrieb des Produkts nach Handbuch | gemSpec_SigD |

4 Produktspezifische Merkmale

4.1 Optionale Ausprägungen

Die bisherige Wahlfreiheit, ob Produkt Performance-Rohdaten oder Performance-Reports an die gematik übermittelt werden besteht nicht mehr. Die Lieferung von Performance-Rohdaten ist verbindlich vorgeschrieben.

5 Anhang A – Verzeichnisse

5.1 Abkürzungen

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

5.2 Tabellenverzeichnis

| | |
|---|----|
| Tabelle 1: Dokumente mit normativen Festlegungen | 6 |
| Tabelle 2: Festlegungen zur betrieblichen Eignung "Prozessprüfung" | 7 |
| Tabelle 3: Festlegungen zur betrieblichen Eignung "Anbietererklärung" | 8 |
| Tabelle 4: Festlegungen zur betrieblichen Eignung "Betriebshandbuch" | 14 |
| Tabelle 5: Festlegungen zur sicherheitstechnischen Eignung "Sicherheitsgutachten" | 15 |
| Tabelle 6: Festlegungen zur sicherheitstechnischen Eignung "Anbietererklärung" | 21 |

5.3 Referenzierte Dokumente

Neben den in Kapitel 2 angeführten Dokumenten werden referenziert:

| [Quelle] | Herausgeber: Titel, Version |
|-------------------------|--|
| [gemRL_PruefSichEig_DS] | gematik: Richtlinie zur Prüfung der Sicherheitseignung |