

Verzeichnis der Anforderungen zur betrieblichen Eignung von Fachdienstbetreibern

Anbietertyp Version: 1.3.0
Anbietertyp Status: freigegeben

Version: 1.2.1
Revision: 182539
Stand: 04.12.2019
Status: freigegeben
Klassifizierung: öffentlich
Referenzierung: gemVZ_Afo_BetrEig_VSDM_FD_1.3.0

Historie Verzeichnis der Anforderungen

Historie Verzeichnisversion

Die Verzeichnisversion ändert sich, wenn sich die Anforderungslage für den Hersteller ändert.

| Verzeichnisversion | Beschreibung der Änderung | Referenz |
|--------------------|----------------------------------|---------------------------------|
| 1.2.0 | Initiale Version | gemVZ_Afo_BetrEig_VSDM_FD_1.2.0 |
| 1.3.0 | Anpassung auf Releasestand 3.1.0 | gemVZ_Afo_BetrEig_VSDM_FD_1.3.0 |

Historie Steckbrief

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

| Version | Stand | Kap. | Grund der Änderung, besondere Hinweise | Bearbeiter |
|---------|----------|------|--|------------|
| 1.0.0 | 15.05.19 | | freigegeben | gematik |
| 1.1.0 | 28.06.19 | 2 | Aktualisierung | gematik |
| 1.2.0 | 02.10.19 | 2 | Aktualisierung R3.1.2 | gematik |
| 1.2.1 | 04.12.19 | 2 | Aktualisierung gemSpec_Perf-Version | 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 | 7 |
| 3.1 Anforderungen zur betrieblichen Eignung | 7 |
| 3.1.1 Prozessprüfung betriebliche Eignung | 7 |
| 3.1.2 Anbietererklärung betriebliche Eignung | 7 |
| 3.1.3 Betriebshandbuch betriebliche Eignung | 13 |
| 3.2 Anforderungen zur sicherheitstechnischen Eignung | 14 |
| 3.2.1 Sicherheitsgutachten | 14 |
| 3.2.2 Anbietererklärung sicherheitstechnische Eignung | 16 |
| 4 Anhang A – Verzeichnisse | 17 |
| 4.1 Abkürzungen | 17 |
| 4.2 Tabellenverzeichnis | 17 |
| 4.3 Referenzierte Dokumente | 17 |

1 Einführung

1.1 Zielsetzung und Einordnung des Dokumentes

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

Das Anforderungsverzeichnis richtet sich an:

- Anbieter Fachdienste VSDM
- 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_PKI | Übergreifende Spezifikation – Spezifikation PKI | 2.7.0 |
| gemKPT_Betr | Betriebskonzept Online-Produktivbetrieb | 3.5.0 |
| gemSpec_Perf | Übergreifende Spezifikation Performance und Mengengerüst TI-Plattform | 2.9.1 |
| gemRL_TSL_SP_CP | Certificate Policy Gemeinsame Zertifizierungsrichtlinie für Teilnehmer der gematik-TSL | 2.4.0 |
| gemSpec_DS_Anbieter | Spezifikation Datenschutz- und Sicherheitsanforderungen der TI an Anbieter | 1.1.0 |
| gemSpec_Net | Übergreifende Spezifikation Netzwerk | 1.16.0 |
| gemSpec_Krypt | Übergreifende Spezifikation Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur | 2.15.0 |
| gemKPT_Test | Testkonzept der TI | 2.5.0 |
| gemRL_Betr_TI | Übergreifende Richtlinien zum Betrieb der TI | 2.3.0 |

3 Blattanforderungen

Die folgenden Abschnitte verzeichnen alle für den Anbietertypen normativen Anforderungen der gematik an die Anbieter Fachdienste VSDM 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) |
|-----------|---|-------------------|
| A_18237 | Lieferung von Performance-Rohdaten-Reports | 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 |

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) |
|--------|-----------------|-------------------|
|--------|-----------------|-------------------|

| | | |
|-------------|---|-------------|
| A_13573 | Alternative Serviceleistung der TI-ITSM-Teilnehmer im TI-ITSM-Teilnehmersupport | gemKPT_Betr |
| A_18238 | Service Level - Übermittlung von Performance-Reports | gemKPT_Betr |
| A_18239 | Service Level - Lieferung von Rohdaten-Performance-Reports | gemKPT_Betr |
| A_18240 | Reporting der technischen Service Level | gemKPT_Betr |
| A_18241 | Reporting der organisatorischen Service Level | gemKPT_Betr |
| TIP1-A_6359 | Definition der notwendigen Leistung anderer Anbieter durch Anbieter und SPEDs | gemKPT_Betr |
| TIP1-A_6360 | Kontrolle bereitgestellter Leistungen durch Anbieter und SPEDs | gemKPT_Betr |
| TIP1-A_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_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_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_7266 | Mitwirkungspflichten im TI-ITSM-System | gemKPT_Betr |
| TIP1-A_6083 | Anzahl der Fachdienste als Referenzobjekte | gemKPT_Test |
| TIP1-A_6519 | Eigenverantwortlicher Test: Hersteller und Anbieter | gemKPT_Test |
| TIP1-A_6523 | Zulassungstest: Hersteller und Anbieter | gemKPT_Test |
| TIP1-A_6526 | Produkttypen: Bereitstellung | gemKPT_Test |
| VSDM-A_2812 | Bereitstellung Testkartensätze | gemKPT_Test |

| | | |
|-------------|--|---------------|
| VSDM-A_2814 | Eindeutigkeit der Testkartenschlüssel | gemKPT_Test |
| VSDM-A_2815 | Berücksichtigung von Vorgaben zur Schlüsselerzeugung | gemKPT_Test |
| VSDM-A_2825 | Bereitstellen von VSD-Updates | gemKPT_Test |
| VSDM-A_2826 | Bereitstellen datumsbasierter VSD-Updates | gemKPT_Test |
| VSDM-A_2830 | Integration multipler Anbieter | gemKPT_Test |
| VSDM-A_2831 | Verwendung von Testkarten | gemKPT_Test |
| VSDM-A_2832 | Umsetzung des Flip/Flop-Verfahrens | gemKPT_Test |
| VSDM-A_3029 | Bereitstellung von Testkarten | gemKPT_Test |
| VSDM-A_3030 | Bereitstellung von spezifikationsabweichende Testkarten | gemKPT_Test |
| A_13575 | Qualität von RFCs | gemRL_Betr_TI |
| A_17735 | Rohdatenreporting | gemRL_Betr_TI |
| A_17764 | Verwendung CI-ID | 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 |
| GS-A_3876 | Prüfung auf übergreifenden Incident | 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_3888 | Verifikation vor Schließung eines übergreifenden Incident | 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_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_3922 | Mitwirkung bei Taskforces | gemRL_Betr_TI |
| GS-A_3958 | Problemerkennung durch TI-ITSM-Teilnehmer | gemRL_Betr_TI |
| GS-A_3959 | Prüfung auf übergreifendes Problem | gemRL_Betr_TI |
| GS-A_3964 | Festlegung von Dringlichkeit und Auswirkung von übergreifenden Problems | gemRL_Betr_TI |
| GS-A_3971 | Verifikation vor Schließung eines übergreifenden Problems | gemRL_Betr_TI |
| GS-A_3972 | Service Level Requirements im übergreifenden Problem Management für TI-ITSM-Teilnehmer | 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_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 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_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_4085 | Etablierung von Kommunikationsschnittstellen durch die 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_4090 | Kommunikationssprache | gemRL_Betr_TI |
| GS-A_4100 | Messung der Service Level | 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_4117 | Informationsbereitstellung durch TI-ITSM-Teilnehmer | gemRL_Betr_TI |
| GS-A_4121 | Analyse Auswirkungen möglicher Schadensereignisse auf Sicherheit und Funktion der TI-Services | gemRL_Betr_TI |
| GS-A_4123 | Entwicklung und Pflege der TI-Notfallvorsorgedokumentation | gemRL_Betr_TI |
| GS-A_4124 | Umsetzung Vorkehrungen zur TI-Notfallvorsorge | gemRL_Betr_TI |
| GS-A_4126 | Eskalation TI-Notfälle | gemRL_Betr_TI |
| GS-A_4127 | Sofortmaßnahmen TI-Notfälle | gemRL_Betr_TI |
| GS-A_4128 | Bewältigung der TI-Notfälle | gemRL_Betr_TI |
| GS-A_4129 | Unterstützung bei TI-Notfällen | gemRL_Betr_TI |
| GS-A_4130 | Festlegung der Schnittstellen des EMC | gemRL_Betr_TI |
| GS-A_4132 | Durchführung der Wiederherstellung und TI-Notfällen | gemRL_Betr_TI |
| GS-A_4134 | Auswertungen von TI-Notfällen | gemRL_Betr_TI |
| GS-A_4136 | Statusinformation bei TI-Notfällen | gemRL_Betr_TI |
| GS-A_4137 | Dokumentation im TI-Notfall-Logbuch | gemRL_Betr_TI |
| GS-A_4138 | Erstellung des Wiederherstellungsberichts nach TI-Notfällen | gemRL_Betr_TI |
| GS-A_4397 | Teilnahme am Service Review | 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_4402 | Mitwirkungspflicht bei der Bewertung vom Produkt-RfC | 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_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_5370 | Prüfung auf Emergency Change | 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_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 | Bearbeitungsfristen in der Bewertung von Produkt-Changes | gemRL_Betr_TI |
| GS-A_5611 | Umsetzung von autorisierten RFC | gemRL_Betr_TI |
| A_17267 | Performance - Lieferung von Rohdaten - Fachdienste VSDM | gemSpec_Perf |
| A_17268 | Performance - Erfassung von Rohdaten - Fachdienste VSDM | gemSpec_Perf |
| A_17668 | Performance - Rohdaten-Performance-Berichte - Format der Einträge des Performance-Berichts | gemSpec_Perf |
| A_17671 | Performance - Rohdaten-Performance-Berichte - Format des Performance-Berichts | gemSpec_Perf |
| A_17679 | Performance - Rohdaten-Performance-Berichte - Berichtsintervall | gemSpec_Perf |
| A_17755 | Performance - Rohdaten-Performance-Berichte - Name der Berichte | gemSpec_Perf |
| A_17756 | Performance - Rohdaten-Performance-Berichte - Korrektheit | gemSpec_Perf |
| A_17757 | Performance - Rohdaten-Performance-Berichte - Zu liefernden Berichte | gemSpec_Perf |
| A_17758 | Performance - Rohdaten-Performance-Berichte - Frist für Nachlieferung | gemSpec_Perf |

3.1.3 Betriebshandbuch betriebliche Eignung

Sofern in diesem Abschnitt Anforderungen mit Vorgaben zu organisatorischen
Maßnahmen wie Prozessen und Strukturvorgaben der Aufbauorganisation sowie der

Umgebung verzeichnet sind, muss der Anbieter deren Umsetzung und Beachtung durch die Vorlage des Betriebshandbuches nachweisen.

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

Tabelle 4: Anforderungen zur betrieblichen Eignung "Betriebshandbuch"

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

3.2 Anforderungen zur sicherheitstechnischen Eignung

3.2.1 Sicherheitsgutachten

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

Hinweis:

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

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

Tabelle 5: Anforderungen zur sicherheitstechnischen Eignung "Sicherheitsgutachten" für alle Fachdienste

| Afo-ID | Afo-Bezeichnung | Quelle (Referenz) |
|--------------|--|---------------------|
| GS-A_4330 | Einbringung des Komponentenzertifikats | gemRL_TSL_SP_CP |
| 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_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 herstellerepezifischen Vorgaben | gemSpec_DS_Anbieter |
| GS-A_5626 | kDSM: Auftragsverarbeitung | gemSpec_DS_Anbieter |
| GS-A_4359 | X.509-Identitäten für die Durchführung einer TLS-Authentifizierung | 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_4387 | TLS-Verbindungen, nicht Version 1.0 | gemSpec_Krypt |
| GS-A_5035 | Nichtverwendung des SSL-Protokolls | gemSpec_Krypt |
| GS-A_5131 | Hash-Algorithmus bei OCSP/CertID | gemSpec_Krypt |
| GS-A_5322 | Weitere Vorgaben für TLS-Verbindungen | gemSpec_Krypt |
| GS-A_3839 | DNSSEC, Zonen mittels DNSSEC sichern | gemSpec_Net |
| GS-A_3841 | Nameserver-Implementierungen, Einsatz von TSIG | gemSpec_Net |
| GS-A_4808 | Nameserver-Implementierungen, nichtautorisierte Zonentransfers | gemSpec_Net |

| | | |
|-----------|---|-------------|
| GS-A_4641 | Initiale Einbringung TI-Vertrauensanker | gemSpec_PKI |
| GS-A_4748 | Initiale Einbringung TSL-Datei | gemSpec_PKI |

Tabelle 6: Anforderungen zur sicherheitstechnischen Eignung "Sicherheitsgutachten" spezifisch für die Fachdienste CMS und VSDD

| Afo-ID | Afo-Bezeichnung | Quelle (Referenz) |
|-----------|---|-------------------|
| GS-A_4380 | Card-to-Server (C2S) Authentisierung und Trusted Channel G2 | gemSpec_Krypt |

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_4473-01 | kDSM: Unverzügliche Benachrichtigung bei Verstößen gemäß Art. 34 DSGVO | 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_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_5564 | kDSM: Ansprechpartner für Datenschutz | gemSpec_DS_Anbieter |
| GS-A_5565 | kDSM: Unverzügliche Behebung von Verstößen gemäß Art. 34 DSGVO | 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" | 7 |
| Tabelle 3: Anforderungen zur betrieblichen Eignung "Anbietererklärung" | 7 |
| Tabelle 4: Anforderungen zur betrieblichen Eignung "Betriebshandbuch" | 14 |
| Tabelle 5: Anforderungen zur sicherheitstechnischen Eignung "Sicherheitsgutachten" für alle Fachdienste..... | 14 |
| Tabelle 6: Anforderungen zur sicherheitstechnischen Eignung "Sicherheitsgutachten" spezifisch für die Fachdienste CMS und VSDD | 16 |
| Tabelle 7: Anforderungen zur sicherheitstechnischen Eignung "Anbietererklärung" | 16 |

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 |