

Elektronische Gesundheitskarte und Telematikinfrastuktur

Anbietertypsteckbrief

Fachdienst KOM-LE

Anbietertyp 1.3.2
Version:
Anbietertyp Status: freigegeben

Version: 1.0.0
Revision: 199599
Stand: 02.03.2020
Status: freigegeben
Klassifizierung: öffentlich
Referenzierung: gemAnbT_FD_KOMLE_ATV_1.3.2

Historie Anbietertypversion und Anbietertypsteckbrief

Historie Anbietertypversion

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

Anbietertypversion	Beschreibung der Änderung	Referenz
1.0.0	Initiale Version	gemAnbT_FD_KOMLE_ATV1.0.0
1.1.0	Anpassung auf Vorab-Releasestand ZIS	gemAnbT_FD_KOMLE_ATV1.1.0
1.2.0	Anpassung auf Releasestand 3.1.0	gemAnbT_FD_KOMLE_ATV1.2.0
1.3.0	Anpassung auf Releasestand 3.1.1	gemAnbT_FD_KOMLE_ATV1.3.0
1.3.1	Anpassung auf Releasestand 3.1.2	gemAnbT_FD_KOMLE_ATV1.3.1

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	02.03.20		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.....	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	11
3.2 Anforderungen zur sicherheitstechnischen Eignung	12
3.2.1 Sicherheitsgutachten	12
3.2.2 Anbietererklärung sicherheitstechnische Eignung	14
4 Anhang A – Verzeichnisse	16
4.1 Abkürzungen	16
4.2 Tabellenverzeichnis	16
4.3 Referenzierte Dokumente	16

1 Einführung

1.1 Zielsetzung und Einordnung des Dokumentes

Anbietertypsteckbriefe verzeichnen verbindlich die Anforderungen der gematik an Anbieter eines Fachdienstes KOM-LE 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 des Fachdienstes KOM-LE
- 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, Leistungsbeschreibung) festgelegt und bekannt gegeben.

1.4 Abgrenzung des Dokumentes

Dieses Dokument macht keine Aussagen zur Aufteilung der Produktentwicklung bzw. Produktherstellung auf verschiedene Hersteller und Anbieter.

Dokumente zu den Zulassungsverfahren für den Produkttyp sind nicht aufgeführt. Die geltenden Verfahren und Regelungen zur Beantragung und Durchführung von Zulassungsverfahren können der Homepage der gematik entnommen werden.

1.5 Methodik

Die im Dokument verzeichneten 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
gemKPT_Betr	Betriebskonzept Online-Produktivbetrieb	3. 5 6.0
gemSpec_Net	Übergreifende Spezifikation Netzwerk	1.1 6 7.0
gemRL_Betr_TI	Übergreifende Richtlinien zum Betrieb der TI	2. 3 4.0
gemSpec_DS_Anbieter	Spezifikation Datenschutz- und Sicherheitsanforderungen der TI an Anbieter	1.1.0
gemSpec_FD_KOMLE	Spezifikation Fachdienst KOM-LE	1. 8 9.0
gemRL_TSL_SP_CP	Certificate Policy Gemeinsame Zertifizierungsrichtlinie für Teilnehmer der gematik-TSL	2. 4 5.0
gemSpec_Krypt	Übergreifende Spezifikation Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur	2.1 5 6.0
gemSpec_PKI	Übergreifende Spezifikation – Spezifikation PKI	2. 7 8.0

3 Blattanforderungen

Die folgenden Abschnitte verzeichnen alle für den Anbiertypen normativen Anforderungen der gematik an Anbieter eines Fachdienstes KOM-LE 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_18236-01	Übermittlung von Performance-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_4106-01	Reportinhalte des Performance-Reports	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
A_18784	Bereitstellung Schlüssel und Zertifikat für Clientmodul als passwortgeschützte PKCS#12 Datei	gemSpec_FD_KOMLE
A_18236	Übermittlung von Performance-Reports	gemRL_Betr_TI
GS-A_4106	Reportinhalte des Performance-Reports	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_18238	Service Level - Übermittlung von Performance-Reports	gemKPT_Betr
A_18240	Reporting der technischen Service Level	gemKPT_Betr
A_18241	Reporting der organisatorischen Service Level	gemKPT_Betr
TIP1-A_6359-02	Definition der notwendigen Leistung anderer Anbieter durch Anbieter	gemKPT_Betr

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
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_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_7265-02	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
A_17735	Rohdatenreporting	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_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_3889	Schließung eines übergreifenden Incidents	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_3917	Bereitstellung der ITSM-Dokumentation bei Audits	gemRL_Betr_TI
GS-A_3922	Mitwirkung bei Taskforces	gemRL_Betr_TI

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
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
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_4125	TI-Notfallerkennung	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

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
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_5250	Ablehnung der Lösung eines übergreifenden Incidents	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_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_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_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_5607	Inhalte eines Servicekataloges der angebotenen TI-Services	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

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
GS-A_5611	Umsetzung von autorisierten RFC	gemRL_Betr_TI
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_7265	Serviceleistung der TI-ITSM-Teilnehmer im TI-ITSM-Teilnehmersupport	gemKPT_Betr

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_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_4085	Etablierung von Kommunikationsschnittstellen durch die TI-ITSM-Teilnehmer	gemRL_Betr_TI
GS-A_4086	Erreichbarkeit der Kommunikationsschnittstellen	gemRL_Betr_TI

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
GS-A_4088	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
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_5343	Definition inhaltlicher Auszüge aus dem Betriebshandbuch	gemRL_Betr_TI
GS-A_5370	Prüfung auf Emergency Change	gemRL_Betr_TI
GS-A_5400	Prüfung der Lösung durch den Melder eines übergreifenden Incidents	gemRL_Betr_TI
GS-A_3911	Service Level Requirements im übergreifenden Incident Management	gemRL_Betr_TI
GS-A_3972	Service Level Requirements im übergreifenden Problem Management für TI-ITSM-Teilnehmer	gemRL_Betr_TI
GS-A_4405	Service Level Requirements im Change und Release Management	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.

Tabelle 5: Anforderungen zur sicherheitstechnischen Eignung "Sicherheitsgutachten"

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_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

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
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 herstellerepezifischen 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
KOM-LE-A_216 4	Passwörter nicht im Klartext speichern	gemSpec_FD_KOMLE
KOM-LE-A_216 6	Keine Änderung oder Löschung des Passwortes durch Dritte	gemSpec_FD_KOMLE
KOM-LE-A_218 5	Mail Server darf nur Nachrichten aus der TI verarbeiten	gemSpec_FD_KOMLE
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_4388	DNSSEC-Kontext	gemSpec_Krypt
GS-A_5035	Nichtverwendung des SSL-Protokolls	gemSpec_Krypt

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
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

3.2.2 Anbietererklärung sicherheitstechnische Eignung

In diesem Abschnitt sind alle Anforderungen an das Bestätigungsobjekt Fachdienst KOM-LE verzeichnet, deren Erfüllung der Anbieter zum Nachweis der sicherheitstechnischen Eignung durch eine Erklärung belegt.

Tabelle 6: 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 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_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_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

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
GS-A_5566	kDSM: Sicherstellung der Datenschutzanforderungen 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
KOM-LE-A_213 3	Durchführung eines Accountings zur Abrechnung	gemSpec_FD_KOMLE
KOM-LE-A_213 7	Protokollierung zum Zwecke der Fehler- bzw. Störungsbehebung	gemSpec_FD_KOMLE
KOM-LE-A_230 2	Erzeugung Schlüssel und Bezug TLS-Zertifikate für Clientmodule	gemSpec_FD_KOMLE
GS-A_4367	Zufallszahlengenerator	gemSpec_Krypt
GS-A_4720	Verwendung registrierter Werte für subjectDN	gemSpec_PKI

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"	11
Tabelle 5: Anforderungen zur sicherheitstechnischen Eignung "Sicherheitsgutachten" ...	12
Tabelle 6: Anforderungen zur sicherheitstechnischen Eignung "Anbietererklärung"	14

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