

Elektronische Gesundheitskarte und Telematikinfrastruktur

Anbietertypsteckbrief

Anbieter ePA-Aktensystem

Anbietertyp 2.3.0
Version:
Anbietertyp Status: freigegeben

Version: 1.0.0
Revision: 382324
Stand: 09.07.2021
Status: freigegeben
Klassifizierung: öffentlich
Referenzierung: gemAnbT_Aktensystem_ePA_ATV_2.3.0

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	Erstellung	gemAnbT_Aktensystem_ePA_ATV_1.0.0
1.1.0	Anpassung auf Releasestand 3.1.0	gemAnbT_Aktensystem_ePA_ATV_1.1.0
1.1.1	Anpassung auf Releasestand 3.1.1	gemAnbT_Aktensystem_ePA_ATV_1.1.1
1.1.2	Anpassung auf Releasestand 3.1.2	gemAnbT_Aktensystem_ePA_ATV_1.1.2
1.1.3	Anpassung auf Releasestand 3.1.3	gemAnbT_Aktensystem_ePA_ATV_1.1.3
1.1.4	Anpassung auf Releasestand 3.1.3 Hotfix 2	gemAnbT_Aktensystem_ePA_ATV_1.1.4
2.0.0	Anpassung auf Releasestand 4.0.0	gemAnbT_Aktensystem_ePA_ATV_2.0.0
2.0.1	Anpassung auf Releasestand 4.0.1	gemAnbT_Aktensystem_ePA_ATV_2.0.1
2.1.0	Anpassung auf Releasestand 4.0.2	gemAnbT_Aktensystem_ePA_ATV_2.1.0
2.2.0	Anpassung auf Releasestand ePA 2.0.3	gemAnbT_Aktensystem_ePA_ATV_2.2.0
2.3.0	Anpassung auf Releasestand ePA 2.0.4	gemAnbT_Aktensystem_ePA_ATV_2.3.0

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 Anbiertypversion.

Version	Stand	Kap.	Grund der Änderung, besondere Hinweise	Bearbeiter
1.0.0	09.07.21		freigegeben	gematik

Inhaltsverzeichnis

1 Einführung	5
1.1 Zielsetzung und Einordnung des Dokumentes	5
1.2 Zielgruppe	5
1.3 Geltungsbereich	5
1.4 Abgrenzung des Dokumentes	5
1.5 Methodik	5
2 Dokumente	7
3 Blattanforderungen.....	8
3.1 Anforderungen zur betrieblichen Eignung	8
3.1.1 Prozessprüfung betriebliche Eignung.....	8
3.1.2 Anbietererklärung betriebliche Eignung	11
3.1.3 Betriebshandbuch betriebliche Eignung	17
3.1.4 Zuordnung der Anforderungen nach Anbieterkonstellation.....	18
3.1.4.1 Konstellation I (Normalfall).....	18
3.1.4.2 Konstellation II (Auslagerung Betrieb)	18
3.1.4.3 Konstellation III (Auslagerung Betrieb und UHD).....	19
3.2 Anforderungen zur sicherheitstechnischen Eignung	20
3.2.1 Sicherheitsgutachten	20
3.2.1.1 Beauftragung von Betreibern	28
3.2.2 Anbietererklärung sicherheitstechnische Eignung	29
3.2.2.1 Beauftragung von Betreibern	30
4 Anbietertypspezifische Merkmale	31
5 Anhang A – Verzeichnisse	32
5.1 Abkürzungen	32
5.2 Tabellenverzeichnis	32
5.3 Referenzierte Dokumente	32

1 Einführung

1.1 Zielsetzung und Einordnung des Dokumentes

Anbietertypsteckbriefe verzeichnen verbindlich die Anforderungen der gematik an den Anbieter ePA-Aktensystem 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 ePA-Aktensystem
- 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. gemPTV_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 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_Zugangsgateway_Vers	Spezifikation Zugangsgateway des Versicherten ePA	1.6.3
gemSpec_PKI	Übergreifende Spezifikation – Spezifikation PKI	2.10.3
gemSpec_DM_ePA	Datenmodell ePA	1.9.0
gemSpec_SGD_ePA	Spezifikation Schlüsselgenerierungsdienst ePA	1.4.2
gemSpec_Dokumentenverwaltung	Spezifikation Dokumentenverwaltung ePA	1.9.0
gemSpec_Krypt	Übergreifende Spezifikation Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur	2.19.1
gemKPT_Betr	Betriebskonzept Online-Produktivbetrieb	3.11.0 CC
gemSpec_Aktensystem	Spezifikation Aktensystem ePA	1.8.1
gemSpec_Net	Übergreifende Spezifikation Netzwerk	1.20.2
gemRL_Betr_TI	Übergreifende Richtlinien zum Betrieb der TI	2.5.1
gemSpec_Authentisierung_Vers	Spezifikation Authentisierung des Versicherten ePA	1.4.1
gemSpec_Perf	Übergreifende Spezifikation Performance und Mengengerüst TI-Plattform	2.13.0
gemSpec_DS_Anbieter	Spezifikation Datenschutz- und Sicherheitsanforderungen der TI an Anbieter	1.3.0
gemSpec_Autorisierung	Spezifikation Autorisierung ePA	1.8.1

3 Blattanforderungen

Die folgenden Abschnitte verzeichnen alle für den Anbiertypen normativen Anforderungen der gematik an den Anbieter ePA-Aktensystem 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_3876	Prüfung auf übergreifenden Incident	gemRL_Betr_TI
GS-A_3884	Festlegung von Dringlichkeit und Auswirkung von übergreifenden Incidents	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_3959	Prüfung auf übergreifendes Problem	gemRL_Betr_TI
GS-A_3964	Festlegung von Dringlichkeit und Auswirkung von übergreifenden Problems	gemRL_Betr_TI
GS-A_3975	Prüfung auf Serviceverantwortung zum übergreifenden Problem	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_3987	Initiierung eines Change Request	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_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_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_4424	Umsetzung des Fallbackplans	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_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_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_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_5608	Übermittlung von CSV-Dateien	gemRL_Betr_TI
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 Datenschutzverstößes	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_4530-01	Maßnahmen zur Behebung von erheblichen Sicherheitsvorfällen und Notfällen	gemSpec_DS_Anbieter
GS-A_4532-01	Nachweis der Umsetzung von Maßnahmen in Folge eines erheblichen Sicherheitsvorfalls oder Notfalls	gemSpec_DS_Anbieter
GS-A_5017-01	Meldung und Behandlung von Schwachstellen	gemSpec_DS_Anbieter
GS-A_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

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_16217-01	Mindesterreichbarkeitszeiten im Versichertensupport (09:00-17:00 Uhr)	gemKPT_Betr
A_18176	Mitwirkungspflichten bei der Einrichtung von Probes des Service Monitorings	gemKPT_Betr
A_18238	Service Level - Übermittlung von Performance- Reports	gemKPT_Betr
A_18239-01	Service Level - Lieferung von Rohdaten- Performance-Reports	gemKPT_Betr
A_18240	Reporting der technischen Service Level	gemKPT_Betr
A_20111	Erreichbarkeit des Versicherten Help Desk (VHD)	gemKPT_Betr
A_20476	Funktionalität, Interoperabilität, Sicherheit in der PU	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_7258	Definition eines Technischen Kennzahlenkataloges	gemKPT_Betr
TIP1-A_7259	Mindestinhalte des Technischen Kennzahlenkataloges	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
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

A_19869	Performance - Rohdaten-Performance-Berichte - zu liefernde Berichte der TI-ITSM-Teilnehmer	gemRL_Betr_TI
GS-A_3886-01	Nutzung des TI-ITSM-Systems bei der Übermittlung eines übergreifenden Vorgangs	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_3971	Verifikation vor Schließung eines übergreifenden Problems	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_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_3988	Prüfung der Lösung durch den Melder 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

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_4419	Nutzung der Testumgebung (RU/TU)	gemRL_Betr_TI
GS-A_4425	Übermittlung von Optimierungsmöglichkeiten zur Umsetzung von genehmigten Produkt-Changes	gemRL_Betr_TI
GS-A_4855-02	Auditierung von TI-ITSM-Teilnehmern	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_5402	Eigenverantwortliches Handeln bei Ausfall von Kommunikationsschnittstellen	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_5594	Identifikation von TI-Konfigurationsdaten	gemRL_Betr_TI
GS-A_5597	Produkt-RfC (Sub-Changes) erstellen	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_5610	Bearbeitungsfristen in der Bewertung von Produkt-Changes	gemRL_Betr_TI
GS-A_5611	Umsetzung von autorisierten RFC	gemRL_Betr_TI
A_14127-03	Anbieter ePA-Aktensystem - PTR für Anbieterliste (RFC Service-Discovery)	gemSpec_Aktensystem
A_14128-02	Anbieter ePA-Aktensystem - Resource Records FQDN ePA	gemSpec_Aktensystem
A_14512	Anbieter ePA-Aktensystem - Anbieterkennung im Protokolleintrag für Verwaltungsprotokoll	gemSpec_Aktensystem
A_14513-01	Anbieter ePA-Aktensystem - Schutz der Protokolldaten	gemSpec_Aktensystem
A_14921	Anbieter ePA-Aktensystem - lokale Redundanz im Standort des ePA-Aktensystems	gemSpec_Aktensystem
A_14922	Anbieter ePA-Aktensystem - standortübergreifende Redundanz der Komponenten des ePA-Aktensystems	gemSpec_Aktensystem
A_14995	Anbieter ePA-Aktensystem - Schließen des Aktenkontos Schriftform	gemSpec_Aktensystem
A_15002-02	Anbieter ePA-Aktensystem - Abbruch bei existierendem Konto	gemSpec_Aktensystem
A_15027	Anbieter ePA-Aktensystem - Schließen des Aktenkontos elektronisch	gemSpec_Aktensystem
A_15028	Anbieter ePA-Aktensystem - Kündigung Schriftform	gemSpec_Aktensystem
A_15029	Anbieter ePA-Aktensystem - Schließen des Aktenkontos elektronisch	gemSpec_Aktensystem
A_15037	Anbieter ePA-Aktensystem - Status Konto initialisieren	gemSpec_Aktensystem
A_15141	Anbieter ePA-Aktensystem - Verwaltungsprotokolle zur Problemlösung mit Zustimmung des Versicherten	gemSpec_Aktensystem
A_15245	Anbieter ePA-Aktensystem - standortübergreifende Redundanz und Verfügbarkeit	gemSpec_Aktensystem
A_15246	Anbieter ePA-Aktensystem - OID als homeCommunityID für Aktenanbieter	gemSpec_Aktensystem

A_15617-01	Anbieter ePA-Aktensystem - Berücksichtigung Datenübernahme aus Altsystem bei Kontoinitialisierung	gemSpec_Aktensystem
A_15659-01	Anbieter ePA-Aktensystem - Exportpaket unter URL verfügbar machen	gemSpec_Aktensystem
A_15703	Anbieter ePA-Aktensystem - Verfügbarkeit Export-Paket	gemSpec_Aktensystem
A_15842	Anbieter ePA-Aktensystem - Ergonomie der Benutzerführung	gemSpec_Aktensystem
A_15846	Anbieter ePA-Aktensystem - Schnittstellen für die Unterstützung der barrierefreien Bedienungsmöglichkeit	gemSpec_Aktensystem
A_17969-04	Anbieter ePA-Aktensystem - Schnittstellenadressierung	gemSpec_Aktensystem
A_21546	Anbieter ePA-Aktensystem - Telematik-ID für KTR-Berechtigung	gemSpec_Aktensystem
A_21755	Anbieter ePA-Aktensystem - Information über erfolgreichen Import des Exportpakets	gemSpec_Aktensystem
A_14839	Home Community ID als OID URN	gemSpec_DM_ePA
A_21142	SZZP mit mehreren Produktinstanzen	gemSpec_Net
A_15208-01	Performance - ePA-Aktensystem - Spitzenlastvorgaben	gemSpec_Perf
A_15212	Performance - ePA-Aktensystem - Skalierung	gemSpec_Perf
A_15213-01	Performance - ePA-Aktensystem - Spitzenlastvorgaben TU	gemSpec_Perf
A_15214	Performance - ePA-Aktensystem - Speicherkapazität TU	gemSpec_Perf
A_15698	Performance - ePA-Aktensystem - Verbindungsaufbau	gemSpec_Perf
A_15743	Performance - ePA-Aktensystem - Bestandsdaten	gemSpec_Perf
A_16177	Performance - ePA-Aktensystem - Verfügbarkeit	gemSpec_Perf
A_17293	Performance - Lieferung von Rohdaten - ePA-Aktensystem	gemSpec_Perf
A_17668-01	Performance - Rohdaten-Performance-Berichte - Format der Einträge des Rohdaten-Performance-Berichts	gemSpec_Perf

A_17967	Performance – Schlüsselgenerierungsdienst – am FD - Spitzenlastvorgaben	gemSpec_Perf
A_17978	Performance - Schlüsselgenerierungsdienst - am FD - Skalierung	gemSpec_Perf
A_17979	Performance - Schlüsselgenerierungsdienst - am FD - Verfügbarkeit	gemSpec_Perf
A_17981	Performance - Schlüsselgenerierungsdienst - am FD - Lieferung von Rohdaten	gemSpec_Perf
A_17998	Performance - ePA-Aktensystem - Zugangsgateway des Versicherten - Lastvorgaben	gemSpec_Perf
A_20518	Performance - Schlüsselgenerierungsdienst - am FD - Spitzenlastvorgaben TU	gemSpec_Perf
GS-A_5523	Performance – zentrale Dienste – Redundanzlösung	gemSpec_Perf
A_17883	Weiterführung der Schlüsselableitungsfunktionalität bei SGD-Instanzwechsel	gemSpec_SGD_ePA

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_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_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_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_5343	Definition inhaltlicher Auszüge aus dem Betriebshandbuch	gemRL_Betr_TI
GS-A_5361	Durchführung von Emergency-Changes durch TI-ITSM-Teilnehmer bei Nichterreichbarkeit des Gesamtverantwortlichen TI	gemRL_Betr_TI
GS-A_5370	Prüfung auf Emergency Change	gemRL_Betr_TI

3.1.4 Zuordnung der Anforderungen nach Anbieterkonstellation

Der aufgeführten Konstellationen aus dem gemKPT_Betr folgend ergeben sich die Zuordnungen der in diesem Anbietertypsteckbrief aufgeführten Anforderungen in folgenden 3 Konstellationen:

3.1.4.1 Konstellation I (Normalfall)

Der Anbieter ePA-Aktensystem erfüllt alle Anforderungen dieses Anbietertypsteckbriefes aus den Kapiteln 3.1.1 bis 3.2.2 selbst.

3.1.4.2 Konstellation II (Auslagerung Betrieb)

Der Anbieter ePA-Aktensystem erfüllt alle unter Tabelle Tab_KPT_Betr_TI_007 selbst.

Der vom Anbieter ePA-Aktensystem beauftragte Unterauftragnehmer vertritt den Anbieter und erbringt für diesen alle Anforderungen dieses Anbiertypsteckbriefes aus den Kapiteln 3.1.1 bis 3.2.2, mit der Ausnahme der unter Tabelle Tab_KPT_Betr_TI_007 aufgeführten Anforderungen.

Tabelle 5: Tab_KPT_Betr_TI_007 Liste der Bereitstellung eines UHD zugeordneten Anforderungen

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
TIP1-A_6388-02	Bereitstellung eines lokalen IT-Service-Managements durch Anbieter für ihre zu verantwortenden Serviceeinheiten	gemKPT_Betr
A_16217	Mindesterreichbarkeitszeiten im Versichertensupport	gemKPT_Betr
TIP1-A_6389-02	Erreichbarkeit der 1st-Level (UHD), 2nd/3rd-Level (SPOCs) der Anbieter	gemKPT_Betr

In dieser Konstellation hat der Anbieter zudem die Anforderungen in Tabelle "Tab_KPT_Betr_TI Anforderungen Anbietererklärung" durch eine Anbietererklärung nachzuweisen.

Tabelle 6: Tab_KPT_Betr_TI Anforderungen Anbietererklärung

GS-A_4473-01	GS-A_4478-01	GS-A_4479-01	GS-A_4523-01	GS-A_4524-01
GS-A_5555	GS-A_5556	GS-A_5560	GS-A_5561	GS-A_5564
GS-A_5565				

3.1.4.3 Konstellation III (Auslagerung Betrieb und UHD)

Der vom Anbieter ePA-Aktensystem beauftragte Unterauftragnehmer vertritt den Anbieter und erbringt für diesen alle Anforderungen dieses Anbiertypsteckbriefes aus den Kapiteln 3.1.1 bis 3.2.2, inklusive der unter Tabelle Tab_KPT_Betr_TI_007 aufgeführten Anforderungen.

Sollte der Anbieter ePA-Aktensystem für die Erbringung des UHD einen zweiten Unterauftragnehmer beauftragen, so erfüllt dieser Unterauftragnehmer anstelle des ersten die unter Tabelle Tab_KPT_Betr_TI_007 aufgeführten Anforderungen.

Der Anbieter hat zudem die Anforderungen in Tabelle "Tab_KPT_Betr_TI Anforderungen Anbietererklärung" durch eine Anbietererklärung nachzuweisen.

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 7: Tab_Anf_SiGu Anforderungen zur sicherheitstechnischen Eignung
"Sicherheitsgutachten"**

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
A_14513-01	Anbieter ePA-Aktensystem - Schutz der Protokolldaten	gemSpec_Aktensystem
A_14921	Anbieter ePA-Aktensystem - lokale Redundanz im Standort des ePA-Aktensystems	gemSpec_Aktensystem
A_14922	Anbieter ePA-Aktensystem - standortübergreifende Redundanz der Komponenten des ePA-Aktensystems	gemSpec_Aktensystem
A_14993	Anbieter ePA-Aktensystem - Mailadresse validieren	gemSpec_Aktensystem
A_14994	Anbieter ePA-Aktensystem - Schriftliche Kontoeröffnung	gemSpec_Aktensystem
A_14996	Anbieter ePA-Aktensystem - Manuelle Ergänzung Mailadresse	gemSpec_Aktensystem
A_14997	Anbieter ePA-Aktensystem - Einwilligung dokumentieren	gemSpec_Aktensystem
A_15024	Anbieter ePA-Aktensystem - Elektronische Kontoeröffnung	gemSpec_Aktensystem
A_15025	Anbieter ePA-Aktensystem - Übernahme Mailadresse für Geräteverwaltung	gemSpec_Aktensystem
A_15026	Anbieter ePA-Aktensystem - Keine Kontoeröffnung bei Nicht-Einwilligung	gemSpec_Aktensystem
A_15038	Anbieter ePA-Aktensystem - Initialisiertes Konto löschen	gemSpec_Aktensystem
A_15039-01	Anbieter ePA-Aktensystem - Aktives Konto löschen	gemSpec_Aktensystem
A_15040	Anbieter ePA-Aktensystem - Aktives Konto kündigen	gemSpec_Aktensystem

A_15041	Anbieter ePA-Aktensystem - Gekündigtes Konto löschen	gemSpec_Aktensystem
A_15042-01	Anbieter ePA-Aktensystem - Gekündigtes Konto einfrieren	gemSpec_Aktensystem
A_15043	Anbieter ePA-Aktensystem - Eingefrorenes Konto löschen	gemSpec_Aktensystem
A_15048	Anbieter ePA-Aktensystem - Authentifizierung des neuen Aktenanbieters	gemSpec_Aktensystem
A_15051	Anbieter ePA-Aktensystem - Authentisierung gegenüber einem neuen Aktenanbieter	gemSpec_Aktensystem
A_15103	Anbieter ePA-Aktensystem - Konzept zur Verhinderung von Profilbildung	gemSpec_Aktensystem
A_15104	Anbieter ePA-Aktensystem - Ordnungsgemäße IT-Administration	gemSpec_Aktensystem
A_15105	Anbieter ePA-Aktensystem - Zwei-Faktor-Authentisierung von Administratoren	gemSpec_Aktensystem
A_15107	Anbieter ePA-Aktensystem - Keine unzulässige Weitergabe von Daten	gemSpec_Aktensystem
A_15109	Anbieter ePA-Aktensystem - Unterschiedliche Mitarbeiter für Vertragsverwaltung und ePA-Aktensystem	gemSpec_Aktensystem
A_15119	Anbieter ePA-Aktensystem - Löschkonzept	gemSpec_Aktensystem
A_15125	Anbieter ePA-Aktensystem - Information des Versicherten zur Wahrnehmung der Betroffenenrechte bei der Aktenkontoeröffnung	gemSpec_Aktensystem
A_15126	Anbieter ePA-Aktensystem - Ausreichende Informationen für eine informierte Einwilligung bei der Aktenkontoeröffnung	gemSpec_Aktensystem
A_15127	Anbieter ePA-Aktensystem - Information der Versicherten und Leistungserbringer zur Wahrnehmung der Betroffenenrechte während der Aktennutzung	gemSpec_Aktensystem
A_15128	Anbieter ePA-Aktensystem - Schutz der transportierten Daten im ePA-Aktensystem	gemSpec_Aktensystem

A_15141	Anbieter ePA-Aktensystem - Verwaltungsprotokolle zur Problemlösung mit Zustimmung des Versicherten	gemSpec_Aktensystem
A_15148	Anbieter ePA-Aktensystem - Durchführung einer Bedrohungsanalyse	gemSpec_Aktensystem
A_15154	Anbieter ePA-Aktensystem - Ermittlung von Standard-Aktenutzung	gemSpec_Aktensystem
A_15155	Anbieter ePA-Aktensystem - Abweichung von Standard-Aktenutzung	gemSpec_Aktensystem
A_15156	Anbieter ePA-Aktensystem - Einsatz zertifizierter HSM	gemSpec_Aktensystem
A_15157	Anbieter ePA-Aktensystem - Sicherer Betrieb und Nutzung eines HSMs	gemSpec_Aktensystem
A_15158	Anbieter ePA-Aktensystem - Informationstechnische Trennung	gemSpec_Aktensystem
A_15160-01	Anbieter ePA-Aktensystem - Zusätzliche Autorisierung von sensiblen Anwendungsfällen	gemSpec_Aktensystem
A_15163	Anbieter ePA-Aktensystem - Angriffen entgegenwirken	gemSpec_Aktensystem
A_15167	Anbieter ePA-Aktensystem - Social Engineering Angriffen entgegenwirken	gemSpec_Aktensystem
A_15187	Anbieter ePA-Aktensystem - Vertragsdaten ändern	gemSpec_Aktensystem
A_15188	Anbieter ePA-Aktensystem - Ausschluss einer Änderung der KVNR im Aktenkonto	gemSpec_Aktensystem
A_15245	Anbieter ePA-Aktensystem - standortübergreifende Redundanz und Verfügbarkeit	gemSpec_Aktensystem
A_15433	Anbieter ePA-Aktensystem - Einsicht der Einwilligung durch Versicherten	gemSpec_Aktensystem
A_15434	Anbieter ePA-Aktensystem - Schließen des Kontos nach Ablauf der Kündigungsfrist	gemSpec_Aktensystem
A_15435	Anbieter ePA-Aktensystem - Löschen aller Daten beim Schließen des Aktenkontos	gemSpec_Aktensystem
A_15545	Anbieter ePA-Aktensystem - Mailadresse für Gerätefreischaltung zur Kontoaktivierung	gemSpec_Aktensystem

A_15660	Anbieter ePA-Aktensystem – Verantwortlichkeit für das Exportpaket	gemSpec_Aktensystem
A_15780	Anbieter ePA-Aktensystem - Widerspruchsfrist bei Kontolöschung	gemSpec_Aktensystem
A_15822	Anbieter ePA-Aktensystem - Schließung der Akte nur durch den Besitzer	gemSpec_Aktensystem
A_15823	Anbieter ePA-Aktensystem – Versicherte über sensible Änderungen informieren.	gemSpec_Aktensystem
A_15824	Anbieter ePA-Aktensystem - Sichere Speicherung von Daten	gemSpec_Aktensystem
A_15870	Anbieter ePA-Aktensystem - Abbruch bei Nichtverfügbarkeit anderer Anbieter	gemSpec_Aktensystem
A_15896	Anbieter ePA-Aktensystem – Ausschluss automatisierte Computerprogramme bei der Kontoinitialisierung	gemSpec_Aktensystem
A_15897	Anbieter ePA-Aktensystem – Ausschluss automatisierter Computerprogramme bei der Prüfung auf existierenden Konten	gemSpec_Aktensystem
A_16323–01	ePA-Aktensystem - Verbot von medizinisch irrelevantem Inhalt	gemSpec_Aktensystem
A_16411	Anbieter ePA-Aktensystem - Information des Versicherten über die Erstellung des Exportpakets	gemSpec_Aktensystem
A_16412	Anbieter ePA-Aktensystem - Information des Versicherten nach Abschluss des Imports des Exportpakets	gemSpec_Aktensystem
A_17075–01	Anbieter ePA-Aktensystem - Information über Verwendung eines zugelassenen ePA-Frontend des Versicherten	gemSpec_Aktensystem
A_17865	Anbieter ePA-Aktensystem - Rollenausschluss für Anbieter eines ePA-Aktensystems	gemSpec_Aktensystem
A_18083	Anbieter ePA-Aktensystem - Validierung Mailadresse vor Übernahme	gemSpec_Aktensystem
A_18084–01	ePA-Aktensystem - Benachrichtigung bei Identitätswechsel	gemSpec_Aktensystem
A_18169	Anbieter des ePA-Aktensystem - Aktenkonto für eigene Zwecke der Betriebsüberwachung	gemSpec_Aktensystem

A_18765	Gemeinsame Kontaktstelle von Signaturdienst und ePA-Aktensystem	gemSpec_Aktensystem
A_18782	Anbieter ePA-Aktensystem - E-Mail-Notifikation an alte Mailadresse	gemSpec_Aktensystem
A_18954	Sicherer Betrieb des Produkts nach Handbuch	gemSpec_Aktensystem
A_19122	Anbieter ePA-Aktensystem – Trennung zu anderen Mandanten	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
A_21106	Anbieter ePA-Aktensystem – Signaturschlüssel für Protokolle	gemSpec_Aktensystem
A_21107	Anbieter ePA-Aktensystem – Speicherung Signaturschlüssel für Protokolle im HSM	gemSpec_Aktensystem
A_21108	Anbieter ePA-Aktensystem – Aufbewahren der Verwaltungsprotokolle bei Schließen der Akte	gemSpec_Aktensystem
A_21109	Anbieter ePA-Aktensystem – Hinweis zur selbstständigen Sicherung der Protokolle bei Schließen der Akte	gemSpec_Aktensystem
A_21238	Anbieter ePA-Aktensystem - Information des Versicherten bei Fehlschlagen des Imports des Exportpakets	gemSpec_Aktensystem
A_21239	Anbieter ePA-Aktensystem – Verhalten bei Nichtabholen des Exportpakets	gemSpec_Aktensystem
A_21240–01	Anbieter ePA-Aktensystem – Löschen der Daten des alten Aktensystems erst nach erfolgreicher Migration	gemSpec_Aktensystem
A_21248–01	Anbieter ePA-Aktensystem - Unabhängigkeit des Betreibers eines ePA-Aktensystems vom Betreiber eines KTR-Consumers	gemSpec_Aktensystem
A_21548	Anbieter ePA-Aktensystem - Information der Vertreter über neuen FQDN nach Abschluss des Aktenumzugs	gemSpec_Aktensystem
A_15091	Komponente Authentisierung Versicherter - Verwendung eines HSM	gemSpec_Authentisierung_Vers

A_13956	Komponente Autorisierung -Separierung der Schnittstellen für verschiedene Umgebungen	gemSpec_Autorisierung
A_14366	Komponente Autorisierung - Verwendung eines HSM	gemSpec_Autorisierung
A_17551-01	Prüfanforderungen zur Konfigurierbarkeit von Value Sets	gemSpec_DM_ePA
A_21214-02	Konfiguration neuer strukturierter Dokumente im Rahmen der Veröffentlichung durch die gematik	gemSpec_DM_ePA
A_20714	Abstimmung der Maßnahmen im Security Monitoring mit gematik	gemSpec_DS_Anbieter
A_20715	kontinuierliche Verbesserung und Dokumentation des Security Monitorings	gemSpec_DS_Anbieter
A_20716	Überwachung von Systemen	gemSpec_DS_Anbieter
A_20717	Zentrale Auswertung sicherheitsrelevanter Ereignisse	gemSpec_DS_Anbieter
A_20718	Reaktion auf detektierte Ereignisse	gemSpec_DS_Anbieter
A_20719	Weiterleitung erkannter Alarme an TI SIEM	gemSpec_DS_Anbieter
A_20720	Weiterleitung von Logdaten (Rohdaten) an 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_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 herstellerepezifischen 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
A_14562	Komponente ePA-Dokumentenverwaltung – Kein physischer Zugang des Anbieters zu Systemen der VAU	gemSpec_Dokumentenverwaltung

A_14563	Komponente ePA-Dokumentenverwaltung – Nutzdatenbereinigung vor physischem Zugang zu Systemen der VAU	gemSpec_Dokumentenverwaltung
A_14564–01	Komponente ePA-Dokumentenverwaltung – Private Schlüssel von Dienstzertifikaten im HSM	gemSpec_Dokumentenverwaltung
A_15540	Komponente ePA-Dokumentenverwaltung – TLS-Schnittstelle I_Document_Management_Connect	gemSpec_Dokumentenverwaltung
A_15746	Sicherstellung der Verfügbarkeit des betreiberspezifischen Schlüssels	gemSpec_Krypt
A_20519	Wechsel des betreiberspezifischen Schlüssels	gemSpec_Krypt
GS–A_3841	Nameserver-Implementierungen, Einsatz von TSIG	gemSpec_Net
GS–A_4808	Nameserver-Implementierungen, nichtautorisierte Zonentransfers	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_4641	Initiale Einbringung TI-Vertrauensanker	gemSpec_PKI
GS–A_4748	Initiale Einbringung TSL-Datei	gemSpec_PKI
A_17880	Zeitsynchronität mit der TI	gemSpec_SGD_ePA
A_17884	Migrationskonzept bei SGD- Instanzwechsel	gemSpec_SGD_ePA
A_17885	ePA-Aktensystem-spezifische Ableitungsschlüssel eines SGD-Instanz	gemSpec_SGD_ePA
A_17886	Migration SGD-Instanz	gemSpec_SGD_ePA
A_17889	HTTPS-Schnittstelle SGD	gemSpec_SGD_ePA
A_17891	HTTPS-Schnittstelle SGD, DoS-Schutz	gemSpec_SGD_ePA
A_17907	SGD, Sicherheitsbegutachtung SGD-HSM	gemSpec_SGD_ePA
A_17911–01	SGD-HSM: Schlüsselerstellung und Veränderung im Mehr-Augen-Prinzip	gemSpec_SGD_ePA
A_17916	Verfügbarkeit der Schlüssel in einem SGD-HSM	gemSpec_SGD_ePA

A_17917	Schutz des SGD-HSM-Firmware-Moduls	gemSpec_SGD_ePA
A_17953	SGD, täglicher Abgleich CA-Zertifikate TSL und Liste im SGD-HSM	gemSpec_SGD_ePA
A_17965	SGD: Löschen der Client-AUT-Zertifikate und OCSP-Responses	gemSpec_SGD_ePA
A_18010	SGD-HSM, Entfernen von abgelaufenen Prüfschlüsseln/Zertifikaten	gemSpec_SGD_ePA
A_21274	SGD-HSM, Entfernen von abgelaufenen Root-Schlüsseln	gemSpec_SGD_ePA
A_14016	Zugangsgateway des Versicherten, Schutz vor Angriffen aus dem Internet	gemSpec_Zugangsgateway_Vers
A_14017	Zugangsgateway des Versicherten, Sicherung zum Transportnetz Internet durch Paketfilter	gemSpec_Zugangsgateway_Vers
A_14019-01	Zugangsgateway des Versicherten, Richtlinien für den Paketfilter zum Internet	gemSpec_Zugangsgateway_Vers
A_14026	Zugangsgateway des Versicherten, Redundanz der Paketfilter im Zugangsdienst für Versicherte	gemSpec_Zugangsgateway_Vers
A_14034	Zugangsgateway des Versicherten, Übergang des ePA-Aktensystems zur TI	gemSpec_Zugangsgateway_Vers
A_15196	Zugangsgateway des Versicherten, Schutz vor volumetrischen DoS-Angriffen	gemSpec_Zugangsgateway_Vers
A_19126	Zugangsgateway des Versicherten, OCSP-Status für das OCSP-Stapling	gemSpec_Zugangsgateway_Vers

3.2.1.1 Beauftragung von Betreibern

Der Anbieter kann einen Betreiber mit dem operativen Betrieb des Aktensystems beauftragen. Die Tabelle Tab_Anf_nDelegBetr enthält die Anforderungen aus Tabelle Tab_Anf_SiGu, die der Anbieter nicht vollständig an den Betreiber delegieren kann.

Der Anbieter muss die Anforderungen in Tabelle Tab_Anf_nDelegBetr in einem Sicherheitsgutachten des Anbieters nachweisen, sofern der Anbieter keine im § 274 Abs. 1 SGB V genannte Organisation ist, die gemäß § 274 Abs. 1 SGB V regelmäßig durch eine im § 274 Abs. 1 SGB V benannte Stelle geprüft wird. Ist der Anbieter eine im § 274 Abs. 1 SGB V genannte Organisation, ist die Umsetzung der Anforderungen in Tabelle Tab_Anf_nDelegBetr durch eine Anbietererklärung nachzuweisen, so dass für einen solchen Anbieter kein Sicherheitsgutachten für die Anforderungen (aus Tab_Anf_nDelegBetr) notwendig ist.

Tabelle 8: Tab_Anf_nDelegBetr Anforderungen, die ein Anbieter nicht vollständig an einen Betreiber delegieren kann

A_14993	A_14994	A_14996	A_14997	A_15024
A_15026	A_15038	A_15039	A_15040	A_15041
A_15042	A_15043	A_15103	A_15109	A_15125
A_15126	A_15127	A_15141	A_15160	A_15167
A_15187	A_15433	A_15435	A_15780	A_15822
A_15823	A_15824	A_15870	A_15896	A_15897
A_16322	A_16323	A_17075	A_17865	A_17886
A_17916	A_17917	A_18084	A_18765	GS-A_2076-0 1
GS-A_2214-0 1	GS-A_2328-0 1	GS-A_2329-0 1	GS-A_2331-0 1	GS-A_2332-0 1
GS-A_2345-0 1	GS-A_5551	GS-A_5626		

Der beauftragte Betreiber muss im Sicherheitsgutachten des Betreibers alle Anforderungen aus Tabelle Tab_Anf_SiGu berücksichtigen. Für die Anforderungen aus Tabelle Tab_Anf_nDelegBetr ist im Sicherheitsgutachten des Betreibers zu dokumentieren, ob der Betreiber einen Anteil bei der Umsetzung hat oder die Umsetzung aus Sicht des Betreibers vollständig durch den Anbieter erfolgen muss.

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 9: Anforderungen zur sicherheitstechnischen Eignung "Anbietererklärung"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
A_15436	Anbieter ePA-Aktensystem - Kündigung durch Anbieter ePA-Aktensystem	gemSpec_Aktensystem
A_17551-01	Prüfanforderungen zur Konfigurierbarkeit von Value Sets	gemSpec_DM_ePA

A_19174	Bereitstellung Übersicht Internet-Schnittstellen der TI	gemSpec_DS_Anbieter
A_19175	Zustimmung zu regelmäßigen Schwachstellenscans durch die gematik	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_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

3.2.2.1 Beauftragung von Betreibern

Beauftragt der Anbieter einen Betreiber mit dem operativen Betrieb des Aktensystems, hat der Betreiber die Umsetzung der Anforderungen aus Tabelle Tab_Anf_Betr zu erklären.

Tabelle 10: Tab_Anf_Betr Anforderungen an Betreiber

GS-A_5625	GS-A_5566	GS-A_5561	GS-A_5624	GS-A_5324-02
GS-A_5324-01	GS-A_4526-01			

Der Anbieter selbst hat die Umsetzung der Anforderungen in Tabelle Tab_Anf_Anbieter zu erklären.

Tabelle 11: Tab_Anf_Anbieter Anforderungen an Anbieter

A_15436	GS-A_5566	GS-A_5324-01	GS-A_4524-01	GS-A_5625
GS-A_5324-02				

4 Anbietertypspezifische Merkmale

Es liegen keine optionalen Ausprägungen des Produkttyps vor.

5 Anhang A – Verzeichnisse

5.1 Abkürzungen

Kürzel	Erläuterung
Afo-ID	Anforderungs-Identifikation
CC	Common Criteria

5.2 Tabellenverzeichnis

Tabelle 1: Dokumente mit Anforderungen zu der Anbietertypversion	7
Tabelle 2: Anforderungen zur betrieblichen Eignung "Prozessprüfung"	8
Tabelle 3: Anforderungen zur betrieblichen Eignung "Anbietererklärung"	11
Tabelle 4: Anforderungen zur betrieblichen Eignung "Betriebshandbuch"	17
Tabelle 5: Tab_KPT_Betr_TI_007 Liste der Bereitstellung eines UHD zugeordneten Anforderungen	19
Tabelle 6: Tab_KPT_Betr_TI Anforderungen Anbietererklärung	19
Tabelle 7: Tab_Anf_SiGu Anforderungen zur sicherheitstechnischen Eignung "Sicherheitsgutachten"	20
Tabelle 8: Tab_Anf_nDelegBetr Anforderungen, die ein Anbieter nicht vollständig an einen Betreiber delegieren kann	29
Tabelle 9: Anforderungen zur sicherheitstechnischen Eignung "Anbietererklärung"	29
Tabelle 10: Tab_Anf_Betr Anforderungen an Betreiber	30
Tabelle 11: Tab_Anf_AnB Anforderungen an Anbieter	30

5.3 Referenzierte Dokumente

Neben den in Kapitel 2 angeführten Dokumenten werden referenziert:

[Quelle]	Herausgeber: Titel, Version
[gemRL_PruefSi chEig].	gematik: Richtlinie zur Prüfung der Sicherheitseignung

[ITSEC]	BMI bzw. GMBI: (28.06.1991): Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik („Information Technology Security Evaluation Criteria) https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/ITSicherheitskriterien/itsec-dt_pdf.pdf?__blob=publicationFile (zuletzt geprüft am 11.01.2012)
[eIDAS]	Verordnung (EU) Nr. 910/2014 des europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG