Elektronische Gesundheitskarte und Telematikinfrastruktur

Anbietertypsteckbrief

Prüfvorschrift

Anbieter

Sektoraler Identity Provider

Anbietertyp Version:	1.1.0
Anbietertyp Status:	freigegeben

Version:	1.0.0
Revision:	477966
Stand:	11.07.2022
Status:	zur Abstimmung freigegeben
Klassifizierung:	öffentlich_Entwurf
Referenzierung:	gemAnbT_IDP-Sek_ATV_1.1.0

Historie Anbietertypversion und Anbietertypsteckbrief

Historie Anbietertypversion

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

Anbietertypversion	Beschreibung der Änderung	Referenz
1.0.0	initiale Version	gemAnbT_IDP-Sek_ATV_1.0.0
1.0.2	Anpassung aufgrund der Einarbeitung der Änderungen aus ePA_Maintenance_21.5 und Betr_Maintenance_21.3	gemAnbT_IDP-Sek_ATV_1.0.2
1.0.3	Anpassung aufgrund der Einarbeitung der Änderungen aus IDP_Maintenance_22.1	gemAnbT_IDP-Sek_ATV_1.0.3
1.1.0	Anpassung aufgrund der Einarbeitung Feature IdP-Förderation	gemAnbT_IDP-Sek_ATV_1.1.0

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 Anbietertypversion.

Version	Stand	Kap.	Grund der Änderung, besondere Hinweise	Bearbeiter
1.0.0	11.07.22		zur Abstimmung freigegeben	gematik

Inhaltsverzeichnis

1 Einführung 4
1.1 Zielsetzung und Einordnung des Dokumentes 4
1.2 Zielgruppe 4
1.3 Geltungsbereich 4
1.4 Abgrenzung des Dokumentes 4
1.5 Methodik 4
2 Dokumente 6
3 Normative Festlegungen 8
3.1 Festlegungen zur betrieblichen Eignung 8
3.1.1 Prozessprüfung betriebliche Eignung 8
3.1.2 Anbietererklärung betriebliche Eignung 13
3.1.3 Betriebshandbuch betriebliche Eignung 22
3.2 Festlegungen zur sicherheitstechnischen Eignung 25
3.2.1 Sicherheitsgutachten 25
3.2.2 Anbietererklärung sicherheitstechnische Eignung 28
4 Anhang – Verzeichnisse 30
4.1 Abkürzungen 30
4.2 Tabellenverzeichnis 30

63 # 1 Einführung

64 ## 1.1 Zielsetzung und Einordnung des Dokumentes

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

68 Die normativen Festlegungen werden über ihren Identifier, ihren Titel sowie die
69 Dokumentenquelle referenziert. Die normativen Festlegungen mit ihrem vollständigen,
70 normativen Inhalt sind dem jeweils referenzierten Dokument zu entnehmen.

71 ## 1.2 Zielgruppe

72 Der Anbietertypsteckbrief richtet sich an:

73 - Anbieter eines sektoralen Identity Provider
74 - die gematik im Rahmen der Zulassungsverfahren, Bestätigungsverfahren,
75 Kooperationsverträge und Anbieterverfahren.

76 ## 1.3 Geltungsbereich

77 Dieses Dokument enthält normative Festlegungen zur Telematikinfrastruktur des
78 deutschen Gesundheitswesens. Der Gültigkeitszeitraum der vorliegenden Version und
79 deren Anwendung in Zulassungsverfahren werden durch die gematik GmbH in
80 gesonderten Dokumenten (z. B. gemPTV_ATV_Festlegungen, Leistungsbeschreibung)
81 festgelegt und bekannt gegeben.

82 ## 1.4 Abgrenzung des Dokumentes

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

85 Dokumente zu den Zulassungsverfahren für den Anbietertyp sind nicht aufgeführt. Die
86 geltenden Verfahren und Regelungen zur Beantragung und Durchführung von
87 Zulassungsverfahren können dem Fachportal der gematik (
88 https://fachportal.gematik.de/downloadcenter/zulassungs-bestaetigungsantraege-
89 verfahrensbeschreibungen) entnommen werden.

90 ## 1.5 Methodik

91 Die im Dokument verzeichneten normativen Festlegungen werden tabellarisch
92 dargestellt. Die Tabellenspalten haben die folgende Bedeutung:

ID: Identifiziert die normative Festlegung eindeutig im Gesamtbestand aller Festlegungen der gematik.

Bezeichnung: Gibt den Titel einer normativen Festlegung informativ wieder, um die thematische Einordnung zu erleichtern. Der vollständige Inhalt der normativen Festlegung ist dem Dokument zu entnehmen, auf das die Quellenangabe verweist.

Quelle (Referenz): Verweist auf das Dokument, das die normative Festlegung definiert.

2 Dokumente

Die nachfolgenden Dokumente enthalten alle für den Anbietertyp normativen Festlegungen.

Tabelle 1: Dokumente mit Festlegungen zu der Anbietertypversion

Dokumentenkürzel	Bezeichnung des Dokumentes	Version
gemSpec_Krypt	Übergreifende Spezifikation Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur	2.2~~12~~.0
gemKPT_Betr	Betriebskonzept Online-Produktivbetrieb	3.1~~35~~.0
gemRL_Betr_TI	Übergreifende Richtlinien zum Betrieb der TI	2.6.0
gemSpec_DS_Anbieter	Spezifikation Datenschutz- und Sicherheitsanforderungen der TI an Anbieter	1.4.0
gemSpec_Perf	Übergreifende Spezifikation Performance und Mengengerüst TI-Plattform	2.21~~7~~.0
gemSpec_IDP_Sek	Spezifikation Sektoraler Identity Provider	~~12~~.0.0 CC
gemF_IDP_Federation	Feature Spezifikation IDP Föderation	1.0.0 CC

Die Bestätigungs-/Zulassungsbedingungen für den Anbietertyp "Anbieter sektoraler IDP" werden im Dokument [gemZul_Anbieter] im Downloadcenter der gematik im Abschnitt "Zulassungen und Bestätigungen durch die gematik" veröffentlicht.

Die in folgender Tabelle aufgeführten Dokumente und Web-Inhalte sind informative Beistellungen und sind nicht Gegenstand der Bestätigung / Zulassung.

Tabelle 2 Informative Dokumente und Web-Inhalte

Quelle	Herausgeber: Bezeichnung / URL	Version Branch / Tag
[gemRL_PruefSichEig_DS]	gematik: Richtlinie zur Prüfung der Sicherheitseignung	
[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	

[OWASP Top 10 Report]	OWASP: https://owasp.org/www-project-top-ten/#div-main	
[BSI RZ]	BSI: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/RZ-Sicherheit/Standort-Kriterien_Rechenzentren.pdf	
[ANDROIDAPPLINKS]	https://developer.android.com/studio/write/app-link-indexing	
[APPLEUNIVERSAL]	https://developer.apple.com/ios/universal-links/	

Hinweis:

- Ist kein Herausgeber angegeben, wird angenommen, dass die gematik für Herausgabe und Veröffentlichung der Quelle verantwortlich ist.
- Ist keine Version angegeben, bezieht sich die Quellenangabe auf die aktuellste Version.
- Bei Quellen aus gitHub werden als Version Branch und / oder Tag verwendet.

3 Normative Festlegungen

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

3.1 Festlegungen zur betrieblichen Eignung

3.1.1 Prozessprüfung betriebliche Eignung

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

Tabelle 3: Festlegungen zur betrieblichen Eignung "Prozessprüfung"

ID	Bezeichnung	Quelle (Referenz)
A_13575	Qualität von RfCs	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_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_3920	Eskalationseinleitung durch den TI-ITSM-Teilnehmer	gemRL_Betr_TI
GS-A_3922	Mitwirkung bei Taskforces	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_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_3982	Ablehnung eines übergreifenden Problems	gemRL_Betr_TI
GS-A_3983	Ursachenanalyse eines übergreifenden Problems durch Serviceverantwortlichen	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_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_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_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_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_4402	Mitwirkungspflicht bei der Bewertung vom Produkt-RfC	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_4424	Umsetzung des Fallbackplans	gemRL_Betr_TI
GS-A_4425	Übermittlung von Optimierungsmöglichkeiten zur Umsetzung von genehmigten Produkt-Changes	gemRL_Betr_TI
GS-A_5248	Konventionen zur Struktur von Prozessdaten	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_5370	Prüfung auf Emergency Change	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_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_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_5606	Unterstützung bei Definition von Kapazitätsanforderungen	gemRL_Betr_TI
GS-A_5608	Übermittlung von CSV-Dateien	gemRL_Betr_TI
GS-A_5611	Umsetzung von autorisierten RFC	gemRL_Betr_TI
GS-A_2355-02	Meldung von erheblichen Schwachstellen und Bedrohungen	gemSpec_DS_Anbieter
GS-A_4468-02	kDSM: Jährlicher Datenschutzbericht der TI	gemSpec_DS_Anbieter

GS-A_4473-01	kDSM: 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_4530-01	Maßnahmen zur Behebung von erheblichen Sicherheitsvorfällen und Notfällen	gemSpec_DS_Anbieter
GS-A_4532-01	Nachweis der Umsetzung von Maßnahmen in Folge eines erheblichen Sicherheitsvorfalls oder Notfalls	gemSpec_DS_Anbieter
GS-A_5555	Unverzügliche Meldung von erheblichen Sicherheitsvorfällen und -notfällen	gemSpec_DS_Anbieter
GS-A_5556	Unverzügliche Behebung von erheblichen Sicherheitsvorfällen und -notfällen	gemSpec_DS_Anbieter
GS-A_5559-01	Bereitstellung Ergebnisse von Schwachstellenscans	gemSpec_DS_Anbieter
GS-A_5560	Entgegennahme und Prüfung von Meldungen der gematik	gemSpec_DS_Anbieter
GS-A_5561	Bereitstellung 24/7-Kontaktpunkt	gemSpec_DS_Anbieter
GS-A_5562	Bereitstellung Produktinformationen	gemSpec_DS_Anbieter
GS-A_5563	Jahressicherheitsbericht	gemSpec_DS_Anbieter
GS-A_5564	kDSM: Ansprechpartner für Datenschutz	gemSpec_DS_Anbieter
GS-A_5565	kDSM: Unverzügliche Behebung von Verstößen gemäß Art. 34 DSGVO	gemSpec_DS_Anbieter
A_23051	Authenticator-Module für Android und iOS	gemSpec_IDP_Sek
A_20569	Performance – Standortredundanz	gemSpec_Perf
A_20570	Performance – Standortübergreifende Redundanz	gemSpec_Perf

A_22057	Performance - Rohdaten - Verpflichtung des Anbieters (Rohdatenerfassung v.02)	gemSpec_Perf

135

136

137 3.1.2 Anbietererklärung betriebliche Eignung

138 Sofern in diesem Abschnitt Festlegungen mit Vorgaben zu organisatorischen Maßnahmen
139 wie Prozessen und Strukturvorgaben der Aufbauorganisation sowie der Umgebung
140 verzeichnet sind, muss der Anbieter deren Umsetzung und Beachtung durch eine
141 Anbietererklärung bestätigen bzw. zusagen.

142

143 **Tabelle 4: Festlegungen zur betrieblichen Eignung "Anbietererklärung"**

ID	Bezeichnung	Quelle (Referenz)
A_22357-03	Verfügbarkeit sektoraler IDP	gemF_IDP_Federation
A_22833	Performance – Sektoraler Identity Provider in der Föderation – Bearbeitungszeiten unter Last	gemF_IDP_Federation
A_22954	Umsetzung definierter Releases durch den Anbieter	gemF_IDP_Federation
A_22996	Performance - Rohdaten - Zeitpunkte der Übermittlungen (Rohdatenerfassung v.02)	gemF_IDP_Federation
A_18176	Mitwirkungspflichten bei der Einrichtung von Probes des Service Monitorings	gemKPT_Betr
A_18239-01	Service Level - Lieferung von Rohdaten-Performance-Reports	gemKPT_Betr
A_18240	Reporting der technischen Service Level	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
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_3886-01	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_3917	Bereitstellung der ITSM-Dokumentation bei Audits	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_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_4085	Etablierung von Kommunikationsschnittstellen durch die TI-ITSM-Teilnehmer	gemRL_Betr_TI
GS-A_4086	Erreichbarkeit der Kommunikationsschnittstellen	gemRL_Betr_TI
GS-A_4088-01	Benennung von Ansprechpartnern	gemRL_Betr_TI
GS-A_4090	Kommunikationssprache	gemRL_Betr_TI
GS-A_4095	Übermittlung von Ad-hoc-Reports	gemRL_Betr_TI
GS-A_4100	Messung der Service Level	gemRL_Betr_TI
GS-A_4101	Übermittlung der Service Level Messergebnisse	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_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_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_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_4855-02	Auditierung von TI-ITSM-Teilnehmern	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_5343	Definition inhaltlicher Auszüge aus dem Betriebshandbuch	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_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_5590	Nutzung Business-Servicekatalog bei der Erfassung von Service Requests	gemRL_Betr_TI
GS-A_5591	Verifikation des Service Requests	gemRL_Betr_TI
GS-A_5592	Schließung des Service Requests	gemRL_Betr_TI

GS-A_5593	Schließung des Service Requests ohne Verifikation	gemRL_Betr_TI
GS-A_5594	Identifikation von TI-Konfigurationsdaten	gemRL_Betr_TI
GS-A_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_5609	Abnahme des Servicekataloges	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_22243-01	Nutzung bestehender SGB-Datensätze bei Registrierung für Endanwender (Versicherte)	gemSpec_IDP_Sek
A_22277	Authenticator-Module: Schutz vor überalterter Software	gemSpec_IDP_Sek
A_22306	Information des Nutzers bei fehlender Installation des gewählten Authenticator-Moduls	gemSpec_IDP_Sek
A_22506	Unabhängiges Betriebspersonal pro Standort des sektoralen Identity Provider	gemSpec_IDP_Sek
A_22509	Ausschluss bei fehlenden Authenticator-Modul Versionsnummern (Rohdatenerfassung v.02)	gemSpec_IDP_Sek

A_22512	Schutz der Schnittstellen des sektoralen Identity Provider ins Internet	gemSpec_IDP_Sek
A_22534	Bereitstellung von Validierungsidentitäten durch den sektoralen IDP für das Service Monitoring	gemSpec_IDP_Sek
A_22535	Kein Personenbezug der Validierungsidentitäten	gemSpec_IDP_Sek
A_22567	Informationsverpflichtung über Mandanten des Anbieters sektoraler IDP	gemSpec_IDP_Sek
A_22644	Entity Statement - Prüfung angebotener URLs	gemSpec_IDP_Sek
A_22661	Serverseitige Registrierungsdaten	gemSpec_IDP_Sek
A_22662	Registrierung beim Federation Master durch organisatorischen Prozess	gemSpec_IDP_Sek
A_22694	Georedundanz des sektoralen Identity Provider	gemSpec_IDP_Sek
A_22695	Mindestabstand für Georedundanz des sektoralen Identity Provider	gemSpec_IDP_Sek
A_22710	Vorlaufzeit bei geplantem Schlüsselwechsel	gemSpec_IDP_Sek
A_22824	Verhalten bei Vollauslastung	gemSpec_IDP_Sek
A_22838	Entgegennahme von Sperrmeldungen	gemSpec_IDP_Sek
A_23051	Authenticator-Module für Android und iOS	gemSpec_IDP_Sek
A_23053	Bereitstellung von Testinstanzen	gemSpec_IDP_Sek
A_23054	Skalierung von Testinstanzen	gemSpec_IDP_Sek
A_23057	Version der Staginginstanz	gemSpec_IDP_Sek
A_23058	Änderung der Version der Integrationsinstanz	gemSpec_IDP_Sek
A_23059	Bereitstellung Simulation (Mock) der Außenschnittstellen	gemSpec_IDP_Sek
A_23060	Testversion Authenticator-Moduls für Testinstanzen	gemSpec_IDP_Sek
A_23061	Betriebssysteme der Testversion des Authenticator-Moduls	gemSpec_IDP_Sek
A_23062	Funktionsumfang der Testversion des Authenticator-Moduls	gemSpec_IDP_Sek
A_23063	Bereitstellung Testidentitäten	gemSpec_IDP_Sek

A_23065	Bereitstellung Authentisierungsmöglichkeiten für den Einsatz in automatisierten Tests	gemSpec_IDP_Sek
A_23096	Übertragung RU/TU auf Testinstanzen im Internet	gemSpec_IDP_Sek
A_20244	Performance - IdP-Dienst - Skalierung	gemSpec_Perf
A_20569	Performance – Standortredundanz	gemSpec_Perf
A_20570	Performance – Standortübergreifende Redundanz	gemSpec_Perf
A_22003-01	Performance - Rohdaten - Nachlieferung auf Anforderung (Rohdatenerfassung v.02)	gemSpec_Perf
A_22225	Definition Marktanteil (MA) des Anbieters einer Anwendung oder eines Dienstes	gemSpec_Perf
A_22228	Performance - Sektoraler Identity Provider - Anzahl paralleler Sessions - Internet	gemSpec_Perf
A_22620	Rohdaten - Umsetzungszeit für Änderung der Lieferintervalle	gemSpec_Perf
~~A_19869~~	~~Performance - Rohdaten-Performance-Berichte - zu liefernde Berichte der TI-ITSM-Teilnehmer~~	~~gemRL_Betr_TI~~
~~GS-A_2329-01~~	~~Umsetzung der Sicherheitskonzepte~~	~~gemSpec_DS_Anbieter~~
~~A_22243~~	~~Nutzung bestehender SGB-Datensätze bei Registrierung für Endanwender (Versicherte)~~	~~gemSpec_IDP_Sek~~
~~A_22249~~	~~Verhalten bei Vollauslastung~~	~~gemSpec_IDP_Sek~~
~~A_22251~~	~~Registrierungsdaten beim IDP-Dienst~~	~~gemSpec_IDP_Sek~~
~~A_22256~~	~~Vorlaufzeit bei geplantem Schlüsselwechsel~~	~~gemSpec_IDP_Sek~~
~~A_22272~~	~~Registrierungsdaten des IDP-Dienstes~~	~~gemSpec_IDP_Sek~~
~~A_22305~~	~~Serverseitige Registrierungsdaten~~	~~gemSpec_IDP_Sek~~
~~A_22329~~	~~Entgegennahme von Sperrmeldungen~~	~~gemSpec_IDP_Sek~~
~~A_22353~~	~~Ermöglichung einer organisatorischen Registrierung~~	~~gemSpec_IDP_Sek~~
~~A_22354~~	~~Discovery Document - Prüfung der angebotenen URLs~~	~~gemSpec_IDP_Sek~~

~~A_20248~~	~~Performance – Lieferung von Rohdaten – IdP-Dienst~~	~~gemSpec_Perf~~
~~A_21975~~	~~Performance – Rohdaten – Default-Werte für Lieferintervalle (Rohdatenerfassung v.02)~~	~~gemSpec_Perf~~
~~A_22226~~	~~Performance – Sektoraler Identity Provider – Bearbeitungszeit unter Last~~	~~gemSpec_Perf~~
~~A_22357~~	~~Verfügbarkeit sektoraler IDP~~	~~gemSpec_Perf~~

3.1.3 Betriebshandbuch betriebliche Eignung

Sofern in diesem Abschnitt Festlegungen mit Vorgaben zu organisatorischen Maßnahmen wie Prozessen und Strukturvorgaben der Aufbauorganisation sowie der Umgebung verzeichnet sind, muss der Anbieter deren Umsetzung und Beachtung durch die Vorlage des Betriebshandbuches nachweisen.

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

Tabelle 5: Festlegungen zur betrieblichen Eignung "Betriebshandbuch"

ID	Bezeichnung	Quelle (Referenz)
GS-A_3876	Prüfung auf übergreifenden Incident	gemRL_Betr_TI
GS-A_3888	Verifikation vor Schließung eines übergreifenden Incident	gemRL_Betr_TI
GS-A_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_3984	Service Request zur Bereitstellung der TI-Testumgebung (RU/TU)	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_4088-01	Benennung von Ansprechpartnern	gemRL_Betr_TI
GS-A_4100	Messung der Service Level	gemRL_Betr_TI
GS-A_4117	Informationsbereitstellung durch TI-ITSM-Teilnehmer	gemRL_Betr_TI
GS-A_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_4136	Statusinformation bei TI-Notfällen	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_4402	Mitwirkungspflicht bei der Bewertung vom Produkt-RfC	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_5248	Konventionen zur Struktur von Prozessdaten	gemRL_Betr_TI
GS-A_5343	Definition inhaltlicher Auszüge aus dem Betriebshandbuch	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_5370	Prüfung auf Emergency Change	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_5591	Verifikation des Service Requests	gemRL_Betr_TI
GS-A_5592	Schließung des Service Requests	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_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_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

155

3.2 Festlegungen zur sicherheitstechnischen Eignung

3.2.1 Sicherheitsgutachten

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

Tabelle 6: Festlegungen zur sicherheitstechnischen Eignung "Sicherheitsgutachten"

ID	Bezeichnung	Quelle (Referenz)
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_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_3130	Krypto_Schlüssel_Installation: Dokumentation der Schlüsselinstallation gemäß Minimalitätsprinzip	gemSpec_DS_Anbieter
GS-A_3139	Krypto_Schlüssel: Dienst Schlüsselableitung	gemSpec_DS_Anbieter
GS-A_3149	Krypto_Schlüssel_Archivierung: Dokumentation der Schlüsselarchivierung gemäß Minimalitätsprinzip	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_5551	Betriebsumgebung in einem Mitgliedstaat der EU bzw. des EWR	gemSpec_DS_Anbieter
GS-A_5626	kDSM: Auftragsverarbeitung	gemSpec_DS_Anbieter
A_22235	Information des Versicherten über Änderungen an Authentifizierungsfaktoren	gemSpec_IDP_Sek
A_22239	Schützenswerte Objekte	gemSpec_IDP_Sek
A_22240	Berücksichtigung OWASP-Top-10-Risiken	gemSpec_IDP_Sek
A_22241	Interner Datenaustausch der Komponenten des sektoralen Identity Provider	gemSpec_IDP_Sek
A_22242-01	Gesicherte externe Schnittstellen des sektoralen Identity Provider	gemSpec_IDP_Sek
A_22244	Trennung der Betriebsumgebungen	gemSpec_IDP_Sek
A_22245	Datenschutzgerechte Einrichtungs- und Sperrprozesse	gemSpec_IDP_Sek
A_22246	Löschung von Nutzerinformationen	gemSpec_IDP_Sek
A_22250	Schutz der Verbindung zum sektoralen Identity Provider	gemSpec_IDP_Sek
A_22334-01	Verifikation des Versicherten vor erster Nutzung	gemSpec_IDP_Sek
A_22691	Sicherer Betrieb des Produkts nach Betriebshandbuch	gemSpec_IDP_Sek
A_22692	Kriterien für die Standortwahl von Rechenzentren	gemSpec_IDP_Sek
A_22750	Gerätebindung und Authentisierung	gemSpec_IDP_Sek
A_22829	Anbieter sektoraler IDP Speicherung Schlüsselmaterial in HSM	gemSpec_IDP_Sek
A_22838	Entgegennahme von Sperrmeldungen	gemSpec_IDP_Sek
A_22839	Fehlerprotokollierung	gemSpec_IDP_Sek
A_22865	Verpflichtende Verfahren zur Identifikation von Nutzern	gemSpec_IDP_Sek
A_22867	Niederschwellige Authentifizierungsverfahren	gemSpec_IDP_Sek
A_22943	Richtlinien zum TLS-Verbindungsaufbau	gemSpec_IDP_Sek
A_22980	Grundlage zur Prüfung der TLS-Zertifikate mittels Certificate Transparency	gemSpec_IDP_Sek

A_22982	Bereitstellung der öffentlichen Schlüssel der TLS-Zertifikate	gemSpec_IDP_Sek
A_22987	Mindestmaß für eine "gematik-ehealth-loa-substantial" Authentisierungsstärke	gemSpec_IDP_Sek
A_22988	Mindestmaß für eine "gematik-ehealth-loa-high" Authentisierungsstärke	gemSpec_IDP_Sek
A_23002	sicherer Betrieb der fachlichen Operationen in einer Vertrauenswürdigen Ausführungsumgebung (VAU)	gemSpec_IDP_Sek
A_23019	Anforderungen an den sicherer Betrieb der fachlichen Operationen in einer Vertrauenswürdigen Ausführungsumgebung (VAU)	gemSpec_IDP_Sek
A_23021	Trennung von Diensten der Föderation und weiteren unterstützten Anwendungen	gemSpec_IDP_Sek
A_23022	Prozesse zum Ändern oder Löschen personenbezogener Daten	gemSpec_IDP_Sek
A_23023	Sicherung externen Schnittstellen gegen bösartige Eingaben	gemSpec_IDP_Sek
A_23025	Interpretation "gematik-ehealth-loa-high"	gemSpec_IDP_Sek
A_23099	Datenverarbeitung innerhalb Europa	gemSpec_IDP_Sek
A_23100	Sicherstellung des Datenverkehrs ausschließlich in europäische Union	gemSpec_IDP_Sek
A_23101	Durchsetzung der eGK-Sperrfrist	gemSpec_IDP_Sek
A_23102	Weitere Verfahren zur Identifikation von Nutzern	gemSpec_IDP_Sek
A_23103	Nutzer Einwilligung Vertrauensniveauabsenkung	gemSpec_IDP_Sek
A_17124	TLS-Verbindungen (ECC-Migration)	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_5322	Weitere Vorgaben für TLS-Verbindungen	gemSpec_Krypt

GS-A_5339	TLS-Verbindungen, erweiterte Webbrowser-Interoperabilität	gemSpec_Krypt
~~A_22234~~	~~Vertrauensniveau "substanziell" gemäß eIDAS-Verordnung~~	~~gemSpec_IDP_Sek~~
~~A_22236~~	~~Auskunft an Versicherten~~	~~gemSpec_IDP_Sek~~
~~A_22242~~	~~Gesicherte externe Schnittstellen des sektoralen Identity Provider~~	~~gemSpec_IDP_Sek~~
~~A_22247~~	~~Fehlerprotokollierung~~	~~gemSpec_IDP_Sek~~
~~A_22258~~	~~Authentifikationsverfahren genügen Vertrauensniveau "substanziell"~~	~~gemSpec_IDP_Sek~~
~~A_22333~~	~~Schutz der Attribute während des Transports~~	~~gemSpec_IDP_Sek~~
~~A_22334~~	~~Verifikation des Versicherten vor erster Nutzung~~	~~gemSpec_IDP_Sek~~

3.2.2 Anbietererklärung sicherheitstechnische Eignung

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

Tabelle 7: Festlegungen zur sicherheitstechnischen Eignung "Anbietererklärung"

ID	Bezeichnung	Quelle (Referenz)
GS-A_2214-01	kDSM: Anbieter müssen jährlich die Auftragsverarbeiter kontrollieren	gemSpec_DS_Anbieter
GS-A_2329-01	Umsetzung der Sicherheitskonzepte	gemSpec_DS_Anbieter
GS-A_4526-01	Aufbewahrungsvorgaben an die Nachweise zu Sicherheitsmeldungen	gemSpec_DS_Anbieter
GS-A_4984-01	Befolgen von herstellerspezifischen Vorgaben	gemSpec_DS_Anbieter
GS-A_5324-01	Teilnahme des Anbieters an Sitzungen des kISMS	gemSpec_DS_Anbieter
GS-A_5324-02	kDSM: Teilnahme des Anbieters an Sitzungen des kDSM	gemSpec_DS_Anbieter

GS-A_5557	Security Monitoring	gemSpec_DS_Anbieter
GS-A_5558	Aktive Schwachstellenscans	gemSpec_DS_Anbieter
GS-A_5566	kDSM: Sicherstellung der Datenschutzanforderungen in Unterbeauftragungsverhältnissen	gemSpec_DS_Anbieter
A_22236	Auskunft an Versicherten	gemSpec_IDP_Sek
A_22710	Vorlaufzeit bei geplantem Schlüsselwechsel	gemSpec_IDP_Sek
A_23006	Subdomäne für Webservice-Endpunkte in der VAU	gemSpec_IDP_Sek
~~A_22238~~	~~Sicherer Betrieb des Produkts nach Handbuch~~	~~gemSpec_IDP_Sek~~
~~A_22248~~	~~Richtlinien für den Paketfilter zum Internet~~	~~gemSpec_IDP_Sek~~
~~A_22256~~	~~Vorlaufzeit bei geplantem Schlüsselwechsel~~	~~gemSpec_IDP_Sek~~
~~A_22329~~	~~Entgegennahme von Sperrmeldungen~~	~~gemSpec_IDP_Sek~~

172

173

174

4 Anhang – Verzeichnisse

4.1 Abkürzungen

Kürzel	Erläuterung
ID	Identifikation
CC	Common Criteria

4.2 Tabellenverzeichnis

Tabelle 1: Dokumente mit Festlegungen zu der Anbietertypversion 6
Tabelle 2 Informative Dokumente und Web-Inhalte 6
Tabelle 3: Festlegungen zur betrieblichen Eignung "Prozessprüfung" 8
Tabelle 4: Festlegungen zur betrieblichen Eignung "Anbietererklärung" 13
Tabelle 5: Festlegungen zur betrieblichen Eignung "Betriebshandbuch" 22
Tabelle 6: Festlegungen zur sicherheitstechnischen Eignung "Sicherheitsgutachten" 25
Tabelle 7: Festlegungen zur sicherheitstechnischen Eignung "Anbietererklärung".....28