Elektronische Gesundheitskarte und Telematikinfrastruktur

Anbietertypsteckbrief

Signaturdienst

Anbietertyp Version:	1.1.0-0
Anbietertyp Status:	freigegeben

Version:	1.0.0_CC
Revision:	1766852
Stand:	27.10.2026
Status:	freigegeben
Klassifizierung:	öffentlich_Entwurf
Referenzierung:	gemAnbT_SigD_ATV_1.1.0-0

Historie Anbietertypversion und Anbietertypsteckbrief

Gender-Hinweis
Aus Gründen der besseren Lesbarkeit wird in diesem Dokument überwiegend die männliche Form verwendet. Sämtliche Personenbezeichnungen gelten gleichermaßen für alle Geschlechter.

Historie Anbietertypversion

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

Anbietertypversion	Beschreibung der Änderung	Referenz
1.0.0	Initiale Version	gemAnbT_SigD_ATV_1.0.0
1.0.1	Anpassung an Releasestand 4.0.0	gemAnbT_SigD_ATV_1.0.1
1.0.2	Anpassung an Releasestand 4.0.1	gemAnbT_SigD_ATV_1.0.2
1.0.4	Anpassung aufgrund der Einarbeitung der Änderungen aus ePA_Maintenance_21.5 und Betr_Maintenance_21.3 sowie redaktionelle Anpassungen	gemAnbT_SigD_ATV_1.0.4
1.0.5	Anpassung aufgrund der Einarbeitung Feature IDP-Federation	gemAnbT_SigD_ATV_1.0.5
1.0.6	Anpassung aufgrund der Einarbeitung der Änderungen aus Betr_Maintenance_23.2	gemAnbT_SigD_ATV_1.0.6
1.0.7	Anpassung für **ePA für Alle**	gemAnbT_SigD_ATV_1.0.7
1.0.8	Anpassung aufgrund der Einarbeitung der Änderungen aus IDP_24.3	gemAnbT_SigD_ATV_1.0.8
1.0.9	Anpassung auf ePA für alle Release 3.0.2	gemAnbT_SigD_ATV_1.0.9
1.0.10	Anpassung auf ePA für alle Release 3.0.5	gemAnbT_SigD_ATV_1.0.10
1.0.11	Anpassung auf ePA für alle Release 3.1.3	gemAnbT_SigD_ATV_1.0.11
1.0.12-0	Anpassung auf ePA für alle Release 3.1.3-1	gemAnbT_SigD_ATV_1.0.12-0

1.0.12-1	Anpassung auf ePA für alle Release 3.1.3-2	gemAnbT_SigD_ATV_1.0.12-1
1.0.12-2	Anpassung auf ePA für alle Release 3.1.3-4	gemAnbT_SigD_ATV_1.0.12-2
1.1.0-0	Anpassung auf ePA für alle 27	gemAnbT_SigD_ATV_1.1.0-0

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	27.10.2026		ePA für alle 27	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 Normative Festlegungen 9
3.1 Festlegungen zur betrieblichen Eignung 9
3.1.1 Prozessprüfung betriebliche Eignung 9
3.1.2 Anbietererklärung betriebliche Eignung 10
3.1.3 Betriebshandbuch betriebliche Eignung 16
3.2 Festlegungen zur sicherheitstechnischen Eignung 18
3.2.1 Sicherheitsgutachten 18
3.2.2 Anbietererklärung sicherheitstechnische Eignung 21
3.2.3 Prozessprüfung 22
4 Produktspezifische Merkmale 23
4.1 Optionale Ausprägungen 23
5 Anhang A – Verzeichnisse 24
5.1 Abkürzungen 24
5.2 Tabellenverzeichnis 24

1 Einführung

1.1 Zielsetzung und Einordnung des Dokumentes

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

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

1.2 Zielgruppe

Der Anbietertypsteckbrief richtet sich an:

- Anbieter Signaturdienst
- die gematik im Rahmen der Zulassungsverfahren, Bestätigungsverfahren, Kooperationsverträge und Anbieterverfahren

1.3 Geltungsbereich

Dieses Dokument enthält normative Festlegungen zur Telematikinfrastruktur des deutschen Gesundheitswesens. Der Gültigkeitszeitraum der vorliegenden Version und deren Anwendung in Zulassungsverfahren werden durch die gematik GmbH in gesonderten Dokumenten (z. B. PTV_ATV_Festlegungen) festgelegt und bekannt gegeben.

1.4 Abgrenzung des Dokumentes

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

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

1.5 Methodik

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

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

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

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

2 Dokumente

Die nachfolgenden Dokumente enthalten alle für den Anbietertyp normativen Festlegungen.

Tabelle 1: Dokumente mit normativen Festlegungen

Dokumentenkürzel	Bezeichnung des Dokumentes	Version
gemKPT_Betr	Betriebskonzept Online-Produktivbetrieb	3.69.0
gemRL_Betr_TI	Übergreifende Richtlinien zum Betrieb der TI	2.23.0
gemRL_TSL_SP_CP	Certificate Policy Gemeinsame Zertifizierungsrichtlinie für Teilnehmer der gematik-TSL	2.15.0
gemSpec_DS_Anbieter	Spezifikation Datenschutz- und Sicherheitsanforderungen der TI an Anbieter	2.2.0
gemSpec_Krypt	Übergreifende Spezifikation Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur	2.51.0
gemSpec_Perf	Übergreifende Spezifikation Performance und Mengengerüst TI-Plattform	2.88.0
gemSpec_PKI	Übergreifende Spezifikation – Spezifikation PKI	2.28.0
gemSpec_SigD	Spezifikation Signaturdienst	1.10.0

Hinweis: Die in der Tabelle aufgeführten Dokumente sind als ganzes normativ und gelten mit.

Weiterhin sind die in folgender Tabelle aufgeführten Dokumente und Web-Inhalte als ganzes normativ und gelten mit. Sie sind Gegenstand der Bestätigung / Zulassung. Details finden sich in den Bestätigungs-/Zulassungsbedingungen für das Bestätigung-/Zulassungsobjekt.

Tabelle 2: Mitgeltende Dokumente und Web-Inhalte

Quelle	Herausgeber: Bezeichnung / URL	Version Branch / Tag

Die Bestätigungs-/Zulassungsbedingungen für den Anbietertyp werden im Dokument [gemZul_Anbieter] im Fachportal der gematik im Abschnitt Zulassung veröffentlicht.

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

Tabelle 3: Informative Dokumente und Web-Inhalte

Quelle	Herausgeber: Bezeichnung / URL	Version Branch / Tag
[gemRL_PruefSichEig_DS]	gematik: Richtlinie zur Prüfung der Sicherheitseignung https://gemspec.gematik.de/docs/gemRL/gemRL_PruefSichEig_DS/latest/	latest
[gemRL_Betr_TI]	gematik: Richtlinie Betrieb https://gemspec.gematik.de/docs/gemRL/gemRL_Betr_TI/latest/	latest
[gemTI_SEC_Standard]	gematik: TI Security Standard https://gemspec.gematik.de/docs/gemTI/gemTI_SEC_Standard/gemTI_SEC_Standard_V1.0.0/	1.0.0

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 Signaturdienst zur Sicherstellung des Betriebes der von ihnen verantworteten Serviceeinheiten. Die Festlegungen sind gruppiert nach der Art der Nachweisführung ihrer Erfüllung als Grundlage der Zulassung.

3.1 Festlegungen zur betrieblichen Eignung

3.1.1 Prozessprüfung betriebliche Eignung

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

Tabelle 4: Festlegungen zur betrieblichen Eignung "Prozessprüfung"

ID	Bezeichnung	Quelle (Referenz)
GS-A_4085	Kommunikation - Etablierung von Kommunikationsschnittstellen durch die TI-ITSM-Teilnehmer	gemRL_Betr_TI
GS-A_4101	Service Level Management - Übermittlung der Service Level Messergebnisse	gemRL_Betr_TI
GS-A_4125	Incident Management - TI-Notfallerkennung	gemRL_Betr_TI
GS-A_4400-01	Change Management - Request for Change erstellen	gemRL_Betr_TI
GS-A_5597-01	Change Management - RfC (Sub-Changes) erstellen	gemRL_Betr_TI
GS-A_5601-01	Change Management - Nachweis der Wirksamkeit eines Changes (Verifikation)	gemRL_Betr_TI
GS-A_5602-01	Change Management - Nachweis der Wirksamkeit eines Changes in Auswirkung auf andere TI-Anwendungen (Verifikation)	gemRL_Betr_TI
GS-A_5610-03	Change Management - Vorlaufzeiten in der Bewertung von Changes	gemRL_Betr_TI
A_22057	Performance - Betriebsdatenlieferung - Verpflichtung des Anbieters	gemSpec_Perf
A_26175	Performance - Selbstauskunft - Verpflichtung des Anbieters	gemSpec_Perf

A_26178	Performance - Selbstauskunft - Umsetzungszeit zur Änderung des Lieferintervalls	gemSpec_Perf
GS-A_4095-02	Performance - Ad-hoc-Reports - Lieferverpflichtung	gemSpec_Perf

3.1.2 Anbietererklärung betriebliche Eignung

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

Tabelle 5: Festlegungen zur betrieblichen Eignung "Anbietererklärung"

ID	Bezeichnung	Quelle (Referenz)
A_18176-01	Monitoring - Probing - Unterstützung bei der Einrichtung und Betrieb	gemKPT_Betr
A_23551	Monitoring - Eigenmonitoring	gemKPT_Betr
A_23552	Monitoring - Eigenmonitoring - Verhalten bei Auffälligkeiten oder Anomalien	gemKPT_Betr
A_24609	Monitoring - Anomalieerkennung - Anforderungskriterien Anomalieerkennungssystem	gemKPT_Betr
A_24981	Auskunftsfähigkeit bei Verdacht einer Servicebeeinträchtigung im Verantwortungsbereich	gemKPT_Betr
A_26816	Reporting - Frist zur Übermittlung von Datenlieferungen	gemKPT_Betr
A_27947-01	Monitoring - Probing - Sicherstellen der Voraussetzungen für die Einrichtung	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_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_7265-05	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	Change Management - Qualität von RfC	gemRL_Betr_TI
A_17764	Configuration Management - Verwendung CI-ID	gemRL_Betr_TI
A_18405	Incident Management - Erstellung einer Root Cause Analysis durch am Incident beteiligte TI-ITSM-Teilnehmer	gemRL_Betr_TI
A_18406	Incident Management - Nachlieferung zu einer Root Cause Analysis	gemRL_Betr_TI
A_18407-01	Change Management - Unterstützung bei Change-Verifikation	gemRL_Betr_TI
A_24968	Problem Management - Probleme während Lösungsphase als "Pending" kennzeichnen	gemRL_Betr_TI
A_24983	Incident Management - Erstellung einer Root Cause Analysis im Incident - Prio 1 bis 2	gemRL_Betr_TI
A_24984	Incident Management - Erstellung einer Root Cause Analysis im Incident - Prio 3 bis 4	gemRL_Betr_TI

A_25902	Redundanz - Bereitstellung Redundanzkonzept	gemRL_Betr_TI
A_25917	Redundanz - Kontrollierte Validierung des Redundanzkonzept	gemRL_Betr_TI
A_26014	Redundanz - Umsetzung Redundanzkonzept	gemRL_Betr_TI
A_26501	Kommunikation - Benennung von Ansprechpartnern und Kontakten (FULL)	gemRL_Betr_TI
A_26815	Service Level Management - Bereitstellung der Service Level für das Service Level-Review	gemRL_Betr_TI
GS-A_3884	Incident Management - Festlegung von Dringlichkeit und Auswirkung von übergreifenden Incidents	gemRL_Betr_TI
GS-A_3886-01	Kommunikation - Nutzung des TI-ITSM-Systems bei der Übermittlung eines übergreifenden Vorgangs	gemRL_Betr_TI
GS-A_3889	Incident Management - Schließung eines übergreifenden Incidents	gemRL_Betr_TI
GS-A_3902	Incident Management - Prüfung auf Serviceverantwortung	gemRL_Betr_TI
GS-A_3904	Incident Management - Annahme eines übergreifenden Incidents	gemRL_Betr_TI
GS-A_3905	Incident Management - Ablehnung eines übergreifenden Incidents	gemRL_Betr_TI
GS-A_3907	Incident Management - Lösung von übergreifenden Incidents	gemRL_Betr_TI
GS-A_3922	Koordinierung - Mitwirkung bei Taskforces	gemRL_Betr_TI
GS-A_3959	Problem Management - Prüfung auf übergreifendes Problem	gemRL_Betr_TI
GS-A_3971	Problem Management - Verifikation vor Schließung eines übergreifenden Problems	gemRL_Betr_TI
GS-A_3975	Problem Management - Prüfung auf Serviceverantwortung zum übergreifenden Problem	gemRL_Betr_TI
GS-A_3976	Problem Management - Ablehnung der Lösungsunterstützung	gemRL_Betr_TI
GS-A_3977	Problem Management - Annahme der Verantwortung zur Lösungsunterstützung	gemRL_Betr_TI
GS-A_3981	Problem Management - Annahme eines übergreifenden Problems	gemRL_Betr_TI

GS-A_3982	Problem Management - Ablehnung eines übergreifenden Problems	gemRL_Betr_TI
GS-A_3983	Problem Management - Ursachenanalyse eines übergreifenden Problems durch Serviceverantwortlichen	gemRL_Betr_TI
GS-A_3984	Problem Management - Service Request zur Bereitstellung der TI-Testumgebung (RU/TU)	gemRL_Betr_TI
GS-A_3986	Problem Management - Koordination bei übergreifenden Problems	gemRL_Betr_TI
GS-A_3987	Problem Management - Initiierung eines Change Request	gemRL_Betr_TI
GS-A_3988	Problem Management - Prüfung der Lösung durch den Melder eines übergreifenden Problems	gemRL_Betr_TI
GS-A_3989	Problem Management - Ablehnung der Lösung eines übergreifenden Problems	gemRL_Betr_TI
GS-A_3990	Problem Management - Schließung eines übergreifenden Problems	gemRL_Betr_TI
GS-A_3991	Problem Management - WDB-Aktualisierung nach Schließung eines übergreifenden Problems	gemRL_Betr_TI
GS-A_4090	Kommunikation - Kommunikationssprache	gemRL_Betr_TI
GS-A_4114	Configuration Management - Bereitstellung von TI-Konfigurationsdaten	gemRL_Betr_TI
GS-A_4115	Configuration Management - Datenänderung für TI-Konfigurationsdaten	gemRL_Betr_TI
GS-A_4121	Notfall Management - Analyse Auswirkungen möglicher Schadensereignisse auf Sicherheit und Funktion der TI-Services	gemRL_Betr_TI
GS-A_4124	Notfall Management - Umsetzung Vorkehrungen zur TI-Notfallvorsorge	gemRL_Betr_TI
GS-A_4126	Notfall Management - Eskalation TI-Notfälle	gemRL_Betr_TI
GS-A_4127	Notfall Management - Sofortmaßnahmen TI-Notfälle	gemRL_Betr_TI
GS-A_4128	Notfall Management - Bewältigung der TI-Notfälle	gemRL_Betr_TI
GS-A_4129	Notfall Management - Unterstützung bei TI-Notfällen	gemRL_Betr_TI

GS-A_4130	Notfall Management - Festlegung der Schnittstellen des EMC	gemRL_Betr_TI
GS-A_4132	Notfall Management - Durchführung der Wiederherstellung und TI-Notfällen	gemRL_Betr_TI
GS-A_4134	Notfall Management - Auswertungen von TI-Notfällen	gemRL_Betr_TI
GS-A_4397	Service Level Management - Teilnahme am Service Review	gemRL_Betr_TI
GS-A_4399-01	Configuration Management - Übermittlung von Produktdaten nach Abschluss von autorisierten Normal-Changes	gemRL_Betr_TI
GS-A_4402-01	Change Management - Mitwirkungspflicht bei der Bewertung vom RfC	gemRL_Betr_TI
GS-A_4419	Change Management - Nutzung der Testumgebung (RU/TU)	gemRL_Betr_TI
GS-A_4425-01	Change Management - Übermittlung von Optimierungsmöglichkeiten zur Umsetzung von genehmigten Changes	gemRL_Betr_TI
GS-A_5250	Incident Management - Ablehnung der Lösung eines übergreifenden Incidents	gemRL_Betr_TI
GS-A_5361	Change Management - Durchführung von Emergency-Changes durch TI-ITSM-Teilnehmer bei Nichterreichbarkeit des Gesamtverantwortlichen TI	gemRL_Betr_TI
GS-A_5366-01	Change Management - Mitwirkungspflicht der TI-ITSM-Teilnehmer bei der Festsetzung von Standard-Changes	gemRL_Betr_TI
GS-A_5377	Problem Management - Durchführung einer Problemstornierung	gemRL_Betr_TI
GS-A_5378	Change Management - Durchführung von Emergency-Changes durch TI-ITSM-Teilnehmer	gemRL_Betr_TI
GS-A_5400	Incident Management - Prüfung der Lösung durch den Melder eines übergreifenden Incidents	gemRL_Betr_TI
GS-A_5401-01	Kommunikation - Verschlüsselte E-Mail-Kommunikation	gemRL_Betr_TI
GS-A_5402	Kommunikation - Eigenverantwortliches Handeln bei Ausfall von Kommunikationsschnittstellen	gemRL_Betr_TI

GS-A_5449	Incident Management - Typisierung eines übergreifenden Incidents als „sicherheitsrelevant“	gemRL_Betr_TI
GS-A_5450	Incident Management - Typisierung eines übergreifenden Incidents als „datenschutzrelevant“	gemRL_Betr_TI
GS-A_5587	Incident Management - Ablehnung der Lösungsunterstützung bei einem übergreifenden Incident	gemRL_Betr_TI
GS-A_5588	Problem Management - Abbruch der Problembearbeitung	gemRL_Betr_TI
GS-A_5589	Problem Management - Prüfung auf Verantwortung zur Lösungsunterstützung	gemRL_Betr_TI
GS-A_5594	Configuration Management - Identifikation von TI-Konfigurationsdaten	gemRL_Betr_TI
GS-A_5599-01	Change Management - Beschreibung der Verifikation des Changes im RfC	gemRL_Betr_TI
GS-A_5600-01	Change Management - Beschreibung der Verifikation des Changes in Auswirkung auf andere TI-Services im RfC	gemRL_Betr_TI
GS-A_5603	Knowledge Management - Eingangskanal für Informationen von TI-ITSM-Teilnehmern	gemRL_Betr_TI
GS-A_5604	Service Level Management - Bewertung der Messergebnisse	gemRL_Betr_TI
GS-A_5606	Performance Management / Capacity - Unterstützung bei Definition von Kapazitätsanforderungen	gemRL_Betr_TI
GS-A_5611	Change Management - Umsetzung von autorisierten RfC	gemRL_Betr_TI
A_18018-01	Performance - Signaturdienst - Spitzenlastvorgaben	gemSpec_Perf
A_22003-01	Performance - Betriebsdatenlieferung v2 - Nachlieferung auf Anforderung	gemSpec_Perf
A_22996	Performance - Betriebsdatenlieferung v2 - Zeitpunkte der Übermittlungen	gemSpec_Perf
A_23347-01	Performance - Wartungsfenster - Durchführung	gemSpec_Perf
A_23615-01	Performance - Wartungsfenster und Ausfall - Ausnahme zum ausfallfreien Betrieb	gemSpec_Perf

A_24962	Performance - Servicezeiten des Anbieters basierend auf Produkttypen	gemSpec_Perf
A_26151-01	Redundanz - Lokale Redundanz	gemSpec_Perf
A_26152	Redundanz - Standortübergreifende Redundanz	gemSpec_Perf
A_26186	Redundanz - Wiederherstellungszeitraum - 5 Tage	gemSpec_Perf
A_27538	Performance - Signaturdienst - Verfügbarkeit	gemSpec_Perf
A_28220	Performance - Last- und Bearbeitungszeiten - Verpflichtung des Anbieters	gemSpec_Perf
GS-A_5608-01	Performance - Ad-hoc-Reports - Format	gemSpec_Perf
TIP1-A_6437-01	Performance - Datenlieferungen - Aufbewahrungsfrist	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 6: Festlegungen zur betrieblichen Eignung "Betriebshandbuch"

ID	Bezeichnung	Quelle (Referenz)
A_25903	Redundanz - Definition inhaltlicher Auszüge aus dem Redundanzkonzept	gemRL_Betr_TI
GS-A_3876	Incident Management - Prüfung auf übergreifenden Incident	gemRL_Betr_TI
GS-A_3888	Incident Management - Verifikation vor Schließung eines übergreifenden Incident	gemRL_Betr_TI
GS-A_3920-01	Koordinierung - Eskalationseinleitung durch den TI-ITSM-Teilnehmer	gemRL_Betr_TI
GS-A_3958	Problem Management - Problemerkennung durch TI-ITSM-Teilnehmer	gemRL_Betr_TI
GS-A_3964	Problem Management - Festlegung von Dringlichkeit und Auswirkung von übergreifenden Problems	gemRL_Betr_TI

GS-A_4086	Kommunikation - Erreichbarkeit der Kommunikationsschnittstellen	gemRL_Betr_TI
GS-A_4100	Service Level Management - Messung der Service Level	gemRL_Betr_TI
GS-A_4117	Knowledge Management - Informationsbereitstellung durch TI-ITSM-Teilnehmer	gemRL_Betr_TI
GS-A_4123	Notfall Management - Entwicklung und Pflege der TI-Notfallvorsorgedokumentation	gemRL_Betr_TI
GS-A_4136	Notfall Management - Statusinformation bei TI-Notfällen	gemRL_Betr_TI
GS-A_4137	Notfall Management - Dokumentation im TI-Notfall-Logbuch	gemRL_Betr_TI
GS-A_4138	Notfall Management - Erstellung des Wiederherstellungsberichts nach TI-Notfällen	gemRL_Betr_TI
GS-A_4398-02	Change Management - Prüfung auf genehmigungspflichtige Änderung	gemRL_Betr_TI
GS-A_4400-01	Change Management - Request for Change erstellen	gemRL_Betr_TI
GS-A_4407-01	Change Management - Bereitstellung der Dokumentation des Change Managements für genehmigungspflichtige Changes	gemRL_Betr_TI
GS-A_4417-01	Change Management - Stetige Aktualisierung des Change-Datensatzes im TI-ITSM-System	gemRL_Betr_TI
GS-A_4418-01	Change Management - Übermittlung von Abweichungen vom RfC	gemRL_Betr_TI
GS-A_4424-01	Change Management - Umsetzung des Fallbackplans	gemRL_Betr_TI
GS-A_5597-01	Change Management - RfC (Sub-Changes) erstellen	gemRL_Betr_TI
GS-A_5601-01	Change Management - Nachweis der Wirksamkeit eines Changes (Verifikation)	gemRL_Betr_TI
GS-A_5602-01	Change Management - Nachweis der Wirksamkeit eines Changes in Auswirkung auf andere TI-Anwendungen (Verifikation)	gemRL_Betr_TI
GS-A_5610-03	Change Management - Vorlaufzeiten in der Bewertung von Changes	gemRL_Betr_TI

3.2 Festlegungen zur sicherheitstechnischen Eignung

3.2.1 Sicherheitsgutachten

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

Tabelle 7: Festlegungen zur sicherheitstechnischen Eignung "Sicherheitsgutachten"

ID	Bezeichnung	Quelle (Referenz)
GS-A_4191	Einsatz interoperabler Systeme durch einen externen Dienstleister	gemRL_TSL_SP_CP
GS-A_4230	Gewährleistung der Online-Verfügbarkeit von Sperrinformationen	gemRL_TSL_SP_CP
GS-A_4247	Obligatorische Vorgaben für das Rollenkonzept	gemRL_TSL_SP_CP
GS-A_4249	Standort für Backup-HSM	gemRL_TSL_SP_CP
GS-A_4255	Nutzung des HSM im kontrollierten Bereich	gemRL_TSL_SP_CP
GS-A_4259	Vorgaben für die informationstechnische Trennung sicherheitskritischer Bestandteile der Systemumgebung	gemRL_TSL_SP_CP
GS-A_4261	Vorgaben zur Betriebsumgebung für sicherheitskritische Bestandteile des Systems	gemRL_TSL_SP_CP
GS-A_4268	Anforderungen an den Einsatz freier Mitarbeiter	gemRL_TSL_SP_CP
GS-A_4270	Aufzeichnung von technischen Ereignissen	gemRL_TSL_SP_CP
GS-A_4271	Aufzeichnung von organisatorischen Ereignissen	gemRL_TSL_SP_CP
GS-A_4272	Aufbewahrungsfrist für sicherheitsrelevante Protokolldaten	gemRL_TSL_SP_CP
GS-A_4273	Schutz vor Zugriff, Löschung und Manipulation elektronischer Protokolldaten	gemRL_TSL_SP_CP
GS-A_4274	Archivierung von für den Zertifizierungsprozess relevanten Daten	gemRL_TSL_SP_CP
GS-A_4275	Dokumentationspflicht für Prozesse zum Schlüsselwechsel	gemRL_TSL_SP_CP
GS-A_4276	Aktionen und Verantwortlichkeit im Rahmen der Notfallplanung	gemRL_TSL_SP_CP

GS-A_4279	Fortbestand von Archiven und die Abrufmöglichkeit einer vollständigen Widerrufsliste	gemRL_TSL_SP_CP
GS-A_4284	Beachtung des betreiberspezifischen Sicherheitskonzepts bei der Erzeugung von Schlüsselpaaren	gemRL_TSL_SP_CP
GS-A_4285	Sicherheitsniveau bei der Generierung von Signaturschlüsseln	gemRL_TSL_SP_CP
GS-A_4287	Sichere Aufbewahrung des privaten Schlüssels einer CA	gemRL_TSL_SP_CP
GS-A_4288	Verwendung eines Backup-HSM zum Im-/Export von privaten Schlüsseln	gemRL_TSL_SP_CP
GS-A_4290	Generieren und Löschen von Schlüsselpaaren gemäß Vier-Augen-Prinzip	gemRL_TSL_SP_CP
GS-A_4291	Berechnungen mit dem privaten Schlüssel gemäß Vier-Augen-Prinzip	gemRL_TSL_SP_CP
GS-A_4292-01	Protokollierung der HSM-Nutzung	gemRL_TSL_SP_CP
GS-A_4294	Bedienung des Schlüsselgenerierungssystems	gemRL_TSL_SP_CP
GS-A_4295	Berücksichtigung des aktuellen Erkenntnisstands bei der Generierung von Schlüsseln	gemRL_TSL_SP_CP
GS-A_4304	Speicherung und Anwendung von privaten Schlüsseln	gemRL_TSL_SP_CP
GS-A_4305	Ordnungsgemäße Sicherung des privaten Schlüssels	gemRL_TSL_SP_CP
GS-A_4306	Verwendung von privaten Schlüsseln	gemRL_TSL_SP_CP
GS-A_4307	Vorgaben an HSM-Funktionalität	gemRL_TSL_SP_CP
GS-A_4308	Speicherung und Auswahl von Schlüsselpaaren im HSM	gemRL_TSL_SP_CP
GS-A_4309	Verwendung von zertifizierten kryptographischen Modulen	gemRL_TSL_SP_CP
GS-A_4310-01	Vorgaben an die Prüftiefe der Evaluierung eines HSM	gemRL_TSL_SP_CP
GS-A_4311	Hinterlegung des privaten Signaturschlüssels	gemRL_TSL_SP_CP
GS-A_4312	Aktivierung privater Schlüssel	gemRL_TSL_SP_CP
GS-A_4313	Deaktivierung privater Schlüssel	gemRL_TSL_SP_CP

GS-A_4314	Sichere Übermittlung von Aktivierungsdaten	gemRL_TSL_SP_CP
GS-A_4315	Konformität zum betreiberspezifischen Sicherheitskonzept	gemRL_TSL_SP_CP
GS-A_4316	Härtung von Betriebssystemen	gemRL_TSL_SP_CP
GS-A_4317	Obligatorische Sicherheitsmaßnahmen	gemRL_TSL_SP_CP
GS-A_4396	Speicherung hinterlegter Root- und CA-Schlüssel	gemRL_TSL_SP_CP
GS-A_4925	CP-Test, Keine Verwendung von Echtdaten	gemRL_TSL_SP_CP
GS-A_2076-01	kDSM: Datenschutzmanagement nach BSI	gemSpec_DS_Anbieter
GS-A_5551-01	Betriebsumgebung in einem Mitgliedstaat der EU bzw. des EWR oder der Schweiz	gemSpec_DS_Anbieter
GS-A_5626	kDSM: Auftragsverarbeitung	gemSpec_DS_Anbieter
GS-A_5079	Migration von Algorithmen und Schlüssellängen bei PKI-Betreibern	gemSpec_Krypt
GS-A_4641	Initiale Einbringung TI-Vertrauensanker	gemSpec_PKI
GS-A_4748	Initiale Einbringung TSL-Datei	gemSpec_PKI
A_17339-01	Signaturdienst - Speicherung privater Schlüssel mit einem HSM	gemSpec_SigD
A_17372	Signaturdienst - Schutz des Auftrags der Krankenkasse während des Transports	gemSpec_SigD
A_17375-03	Signaturdienst - P_Create_Identity	gemSpec_SigD
A_17382-01	Signaturdienst - Schutz gegen OWASP Top 10-Risiken	gemSpec_SigD
A_17528-01	Signaturdienst - Schutz der Verbindung zum Signaturdienst	gemSpec_SigD
A_17808-01	Signaturdienst - P_Delete_Identity	gemSpec_SigD
A_17853-02	Signaturdienst - Auskunft an Versicherten	gemSpec_SigD
A_18958	Sicherer Betrieb des Produkts nach Handbuch	gemSpec_SigD
A_19033	Schützenswerte Objekte	gemSpec_SigD
A_19037	Gesicherte interne Schnittstellen des Anbieters Signaturdienst	gemSpec_SigD
A_19038	Datenaustausch zwischen gematik und Anbieter Signaturdienst	gemSpec_SigD

A_19039	Gesicherte externe Schnittstellen des Anbieters Signaturdienst	gemSpec_SigD
A_19040	Eindeutige Verbindung Zertifikatsnehmer und privater Schlüssel	gemSpec_SigD
A_19041-01	Umsetzung Signaturdienst für Zertifikate	gemSpec_SigD
A_19042	Trennung der Signaturdienst-Betriebsumgebungen	gemSpec_SigD
A_19043	Datenschutzgerechte Antrags- und Sperrprozesse	gemSpec_SigD
A_19044	Löschung von Signaturdienst-Zertifikatstatusinformationen, Zertifikats- und Sperranträgen	gemSpec_SigD
A_19045	Fehlerprotokollierung	gemSpec_SigD
A_26271	Signaturdienst - Schutz vor DoS-Angriffen aus dem Internet	gemSpec_SigD

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 8: Festlegungen zur sicherheitstechnischen Eignung "Anbietererklärung"

ID	Bezeichnung	Quelle (Referenz)
A_27099	Audits und Sicherheitsanalysen	gemSpec_DS_Anbieter
GS-A_4980-02	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_5554	Aufrechterhaltung der Informationssicherheit	gemSpec_DS_Anbieter
A_28976	TLS-Verbindungen, TLS-Schnittstellen Internet-PKI	gemSpec_Krypt

3.2.3 Prozessprüfung

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

Tabelle 9: Festlegungen zur sicherheitstechnischen Eignung "Prozessprüfung"

ID	Bezeichnung	Quelle (Referenz)
A_27098-01	Verpflichtung zur Umsetzung des TI Security Standards	gemSpec_DS_Anbieter

4 Produktspezifische Merkmale

4.1 Optionale Ausprägungen

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

5 Anhang A – Verzeichnisse

5.1 Abkürzungen

Kürzel	Erläuterung
ID	Identifikation
CC	Common Criteria

5.2 Tabellenverzeichnis

Tabelle 1: Dokumente mit normativen Festlegungen 7
Tabelle 2: Mitgeltende Dokumente und Web-Inhalte 7
Tabelle 3: Informative Dokumente und Web-Inhalte 8
Tabelle 4: Festlegungen zur betrieblichen Eignung "Prozessprüfung" 9
Tabelle 5: Festlegungen zur betrieblichen Eignung "Anbietererklärung" 10
Tabelle 6: Festlegungen zur betrieblichen Eignung "Betriebshandbuch" 16
Tabelle 7: Festlegungen zur sicherheitstechnischen Eignung "Sicherheitsgutachten" 18
Tabelle 8: Festlegungen zur sicherheitstechnischen Eignung "Anbietererklärung".....21
Tabelle 9: Festlegungen zur sicherheitstechnischen Eignung "Prozessprüfung" 22