

Anbietertypsteckbrief

Prüfvorschrift

Proof of Patient Presence-Service

Anbietertyp Version:	2.0.0-0
Anbietertyp Status:	in Bearbeitung
Version:	1.0.0 CC
Revision:	1494658
Stand:	26.01.2026
Status:	zur Abstimmung freigegeben
Klassifizierung:	öffentlich_Entwurf
Referenzierung:	gemAnbT_PoPP_Service_ATV_2.0.0-0

Historie Anbietertypversion und Anbietertypsteckbrief

Historie Anbietertypversion

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

Anbietertypversion	Beschreibung der Änderung	Referenz
2.0.0-0	Initiale Erstellung für Umsetzungsstufe 2	gemAnbT_PoPP_Service_ATV_2.0.0-0

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 CC	26.01.2026		Umsetzungsstufe 2	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 funktionalen Eignung.....	8
3.1.1 Test Produkt/FA (Anwendung).....	8
3.1.2 Anbietererklärung funktionale Eignung.....	8
3.2 Festlegungen zur betrieblichen Eignung.....	10
3.2.1 Prozessprüfung betriebliche Eignung.....	10
3.2.2 Anbietererklärung betriebliche Eignung.....	12
3.2.3 Betriebshandbuch betriebliche Eignung.....	18
3.2.4 Test betriebliche Eignung.....	20
3.2.5 Dokumentenprüfung.....	21
3.3 Festlegungen zur sicherheitstechnischen Eignung.....	21
3.3.1 Sicherheitsgutachten.....	21
3.3.2 Anbietererklärung sicherheitstechnische Eignung.....	23
3.3.3 Prozessprüfung.....	25
4 Anhang - Verzeichnisse.....	26
4.1 Abkürzungen.....	26
4.2 Tabellenverzeichnis.....	26

1 Einführung

1.1 Zielsetzung und Einordnung des Dokumentes

Dieser Anbietertypsteckbrief verzeichnet verbindlich die normativen Festlegungen der gematik an den Anbieter des PoPP-Service zur Sicherstellung des Betriebes der von ihm 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 PoPP-Service
- 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 dem Fachportal der gematik (<https://fachportal.gematik.de/downloadcenter/zulassungs-bestaetigungsantraege-verfahrensbeschreibungen>) 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

Dokumenten Kürzel	Bezeichnung des Dokumentes	Version
gemF_PoPP_Online_Check-in	Feature Spezifikation PoPP Stufe 2 - Online Check-in	1.0.0 CC
gemKPT_Betr	Betriebskonzept Online-Produktivbetrieb	3.58.0
gemKPT_Test	Testkonzept der TI	3.3.0
gemRL_Betr_TI	Übergreifende Richtlinien zum Betrieb der TI	2.21.0
gemSpec_DS_Anbieter	Spezifikation Datenschutz- und Sicherheitsanforderungen der TI an Anbieter	2.1.0
gemSpec_IDP_FD	Spezifikation Identity Provider – Fachdienste	2.1.0
gemSpec_Krypt	Übergreifende Spezifikation Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur	2.43.0
gemSpec_OM	Übergreifende Spezifikation Operations und Maintenance	1.19.0
gemSpec_Perf	Übergreifende Spezifikation Performance und Mengengerüst TI-Plattform	2.73.0
gemSpec_PoPP_Service	Spezifikation Proof of Patient Presence-Service	1.0.0_RC
gemSpec_ZETA	Spezifikation Zero Trust Access (ZETA)	1.2.0

Weiterhin sind die in folgender Tabelle aufgeführten Dokumente und Web-Inhalte normativ und gelten mit.

Tabelle 2: Mitgeltende Dokumente und Web-Inhalte

Quelle	Herausgeber: Bezeichnung / URL	Version Branch / Tag
[api-popp] - Stufe 2	GitHub-Pfad zu den Schnittstellen-Beschreibungen https://github.com/gematik/api-popp/tree/US-2_CC1	US-2_CC1
[gemTI_SEC_Standard]	gematik: TI Security Standard https://gemospec.gematik.de/docs/gemTI/gemTI_SEC_Stan	1.0.0

	dard	
--	----------------------	--

Die Bestätigungs-/Zulassungsbedingungen für den Anbietertyp PoPP-Service 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	Versi on Branc h / Tag
[gemRL_PruefSichEig_DS]	gematik: Richtlinie zur Prüfung der Sicherheitseignung https://gemspec.gematik.de/docs/gemRL/gemRL_PruefSichEig_DS/latest/	latest

3 Normative Festlegungen

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

Hier werden gemeinsam gelistet:

- spezifische Festlegungen für den Anbieter eines PoPP-Service und
- allgemeine Festlegungen für Anbieter von TI-Diensten, die ZETA Guard nutzen.

3.1 Festlegungen zur funktionalen Eignung

3.1.1 Test Produkt/FA (Anwendung)

Sofern in diesem Abschnitt Festlegungen verzeichnet sind, werden deren Umsetzung und Beachtung zum Nachweis der funktionalen Eignung im Zuge von Zulassungstests durch die gematik geprüft.

Tabelle 4: Festlegungen zur funktionalen Eignung "Test Produkt/FA"

ID	Bezeichnung	Quelle (Referenz)
TIP1-A_6519	Eigenverantwortlicher Test: Hersteller und Anbieter	gemKPT_Test
A_28433	ZETA Guard, Bereitstellung externer Ingress	gemSpec_ZETA
A_28434	ZETA Guard, Verwendung externer Ingress	gemSpec_ZETA
A_28435	ZETA Guard, Ingress - Unterstützung Forwarded-Header	gemSpec_ZETA
A_28462	ZETA Guard, externer Ingress - TLS Terminierung	gemSpec_ZETA

3.1.2 Anbietererklärung funktionale Eignung

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

Tabelle 5: Festlegungen zur funktionalen Eignung "Anbietererklärung"

ID	Bezeichnung	Quelle (Referenz)
A_27294	PoPP-Service - Bereitstellung .well-known für PoPP-Service	gemF_PoPP_Online_Check-in

A_27294-01	PoPP-Service - Bereitstellung .well-known für PoPP-Service	gemF_PoPP_Online_Check-in
A_27295	PoPP-Service - Bereitstellung .well-known für PoPP-Service Resource Server	gemF_PoPP_Online_Check-in
A_27295-01	PoPP-Service - Bereitstellung oauth_resource im .well-known für den PoPP-Service	gemF_PoPP_Online_Check-in
A_23045-02	Registrierung des Fachdienstes	gemSpec_IDP_FD
A_23046	öffentlicher Schlüssel des Federation Master	gemSpec_IDP_FD
A_26539	PoPP-Service-Anbieter - Informationspflicht via Betriebshandbuch ZETA Guard Hersteller	gemSpec_PoPP_Service
A_26540	PoPP-Service - ZETA Guard - PoPP-Policy erstellen	gemSpec_PoPP_Service
A_26543	PoPP-Service - Kommunikation zu den Zero Trust Komponenten der gematik	gemSpec_PoPP_Service
A_27294	PoPP-Service - Bereitstellung .well-known für PoPP-Service	gemSpec_PoPP_Service
A_27295	PoPP-Service - Bereitstellung .well-known für PoPP-Service Resource Server	gemSpec_PoPP_Service
A_27296	PoPP-Service - Bereitstellung .well-known als Teilnehmer der TI-Föderation	gemSpec_PoPP_Service
A_28529	PoPP-Service - Rechtzeitige Ankündigung neuer PoPP-Token-Signaturschlüssel (Key-Rollover)	gemSpec_PoPP_Service
A_25655	PDP - Relying Party	gemSpec_ZETA
A_25773-02	ZETA Guard - Nutzung der von der gematik bereitgestellten Container Images	gemSpec_ZETA
A_25797-01	ZETA Guard-Komponenten - Health Check Schnittstelle für gematik Monitoring	gemSpec_ZETA
A_26105	ZETA Guard, Durchsetzung der Konfiguration	gemSpec_ZETA
A_28436	ZETA Guard, Endpunkte im Internet	gemSpec_ZETA
A_28526	ZETA Guard - Bereitstellung lokaler Artifact Registry	gemSpec_ZETA

3.2 Festlegungen zur betrieblichen Eignung

3.2.1 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 6: Festlegungen zur betrieblichen Eignung "Prozessprüfung"

ID	Bezeichnung	Quelle (Referenz)
A_27947	Nachweis der eingerichteten Probes	gemKPT_Betr
GS-A_3888	Incident Management - Verifikation vor Schließung eines übergreifenden Incident	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_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_3959	Problem Management - Prüfung auf übergreifendes Problem	gemRL_Betr_TI
GS-A_3964	Problem Management - Festlegung von Dringlichkeit und Auswirkung von 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	gemRL_Betr_TI

	übergreifenden Problems	
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_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_4125	Incident Management - TI-Notfallerkennung	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_4400-01	Change Management - Request for Change erstellen	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_5377	Problem Management - Durchführung einer Problemstornierung	gemRL_Betr_TI
GS-A_5400	Incident Management - Prüfung der Lösung durch den Melder eines übergreifenden Incidents	gemRL_Betr_TI
GS-A_5449	Incident Management - Typisierung eines übergreifenden Incidents als „sicherheitsrelevant“	gemRL_Betr_TI
GS-A_5450	Incident Management - Typisierung eines	gemRL_Betr_TI

	übergreifenden Incidents als „datenschutzrelevant“	
GS-A_5561	Bereitstellung 24/7-Kontaktpunkt	gemRL_Betr_TI
GS-A_5587	Incident Management - Ablehnung der Lösungsunterstützung bei einem übergreifenden Incident	gemRL_Betr_TI
GS-A_5593	Request Fulfillment - Schließung des Service Requests ohne Verifikation	gemRL_Betr_TI
GS-A_5597-01	Change Management - RfC (Sub-Changes) erstellen	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_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_26175	Performance - Selbstauskunft - Verpflichtung des Anbieters	gemSpec_Perf
A_26178	Performance - Selbstauskunft - Umsetzungszeit zur Änderung des Lieferintervalls	gemSpec_Perf

3.2.2 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 PoPP-Service deren Umsetzung und Beachtung durch eine Anbietererklärung bestätigen bzw. zusagen.

Tabelle 7: Festlegungen zur betrieblichen Eignung "Anbietererklärung"

ID	Bezeichnung	Quelle (Referenz)
A_18176-01	Unterstützung bei der Einrichtung und Betrieb von Probes	gemKPT_Betr
A_20218-01	Versionierung der Konfiguration von Produktinstanzen	gemKPT_Betr
A_20219-01	Versionierung bei Veränderungen der Konfiguration von Produktinstanzen	gemKPT_Betr
A_20220	Festlegung von Konfiguration durch die gematik	gemKPT_Betr

A_20221-01	Rückspielbarkeit bei Veränderungen der Konfiguration von Produktinstanzen	gemKPT_Betr
A_23664	Service Level - Kein Incident der Priorität 1 innerhalb 24 Stunden resultierend aus einem genehmigten Change	gemKPT_Betr
A_23665-01	Service Level - Störungsfreie Kommunikationsbeziehungen ohne resultierenden Incident	gemKPT_Betr
A_24981	Auskunfts-fähigkeit bei Verdacht einer Servicebeeinträchtigung im Verantwortungsbereich	gemKPT_Betr
A_26816	Reporting - Frist zur Übermittlung von Datenlieferungen	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_24800	Service Level Management - Auskunft Servicebedarf im Rahmen des Service Review	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_3876	Incident Management - Prüfung auf übergreifenden Incident	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	gemRL_Betr_TI

	Vorgangs	
GS-A_3917	Audit - Bereitstellung der ITSM-Dokumentation bei Audits	gemRL_Betr_TI
GS-A_3920-01	Koordinierung - Eskalationseinleitung durch den TI-ITSM-Teilnehmer	gemRL_Betr_TI
GS-A_3922	Koordinierung - Mitwirkung bei Taskforces	gemRL_Betr_TI
GS-A_3971	Problem Management - Verifikation vor Schließung eines übergreifenden Problems	gemRL_Betr_TI
GS-A_4085	Kommunikation - Etablierung von Kommunikationsschnittstellen durch die TI-ITSM-Teilnehmer	gemRL_Betr_TI
GS-A_4086	Kommunikation - Erreichbarkeit der Kommunikationsschnittstellen	gemRL_Betr_TI
GS-A_4090	Kommunikation - Kommunikationssprache	gemRL_Betr_TI
GS-A_4100	Service Level Management - Messung der Service Level	gemRL_Betr_TI
GS-A_4101	Service Level Management - Übermittlung der Service Level Messergebnisse	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_4117	Knowledge Management - Informationsbereitstellung durch TI-ITSM-Teilnehmer	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_4130	Notfall Management - Festlegung der Schnittstellen des EMC	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	gemRL_Betr_TI

	der Bewertung vom RfC	
GS-A_4419	Change Management - Nutzung der Testumgebung (RU/TU)	gemRL_Betr_TI
GS-A_4855-02	Audit - Auditierung von TI-ITSM-Teilnehmern	gemRL_Betr_TI
GS-A_5351	Request Fulfillment - Prüfung von Service Requests	gemRL_Betr_TI
GS-A_5352	Request Fulfillment - Lösung bzw. Bearbeitung des Service Requests	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_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_5588	Problem Management - Abbruch der Problembearbeitung	gemRL_Betr_TI
GS-A_5589	Problem Management - Prüfung auf Verantwortung zur Lösungsunterstützung	gemRL_Betr_TI
GS-A_5590	Request Fulfillment - Nutzung Business-Servicekatalog bei der Erfassung von Service Requests	gemRL_Betr_TI
GS-A_5591	Request Fulfillment - Verifikation des Service Requests	gemRL_Betr_TI
GS-A_5592	Request Fulfillment - Schließung des Service Requests	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_5607	Servicekatalog Management - Inhalte eines	gemRL_Betr_TI

	Servicekataloges der angebotenen TI-Services	
GS-A_5609	Servicekatalog Management - Abnahme des Servicekataloges	gemRL_Betr_TI
A_24607	Schlüsselwechsel Signaturschlüssel für Entity Statement	gemSpec_IDP_FD
GS-A_4542	Spezifikationsgrundlage für Produkte	gemSpec_OM
GS-A_5039-01	Änderung der Produktversion bei Änderungen der Produkttypversion	gemSpec_OM
GS-A_5040-01	Änderung der Produktversion bei Produktänderungen außerhalb von Produkttypänderungen	gemSpec_OM
A_20569	Performance - Standortredundanz	gemSpec_Perf
A_23347-01	Performance - Wartungsfenster - Durchführung	gemSpec_Perf
A_23618-01	Performance - Wartungsfenster und Ausfall - Verfügbarkeitsberechnung	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_27718	Telemetriedatenlieferung - Konnektivität zur gematik gewährleisten	gemSpec_Perf
A_27719	Telemetriedatenlieferung - Nutzung eines gültigen Client-Zertifikats	gemSpec_Perf
A_28220	Performance - Last- und Bearbeitungszeiten - Verpflichtung des Anbieters	gemSpec_Perf
GS-A_4095-02	Performance - Ad-hoc-Reports - Lieferverpflichtung	gemSpec_Perf
GS-A_5608-01	Performance - Ad-hoc-Reports - Format	gemSpec_Perf
A_26508	PoPP-Service - Vertrauenswürdige Uhrzeit	gemSpec_PoPP_Service
A_27390	Performance - PoPP-Service - Zugriff für den Nutzer	gemSpec_PoPP_Service
A_25797-01	ZETA Guard-Komponenten - Health Check Schnittstelle für gematik Monitoring	gemSpec_ZETA

A_27792	ZETA Guard - Verbot der Nutzung bestimmter ZETA Guard Versionen	gemSpec_ZETA
A_27793	ZETA Guard - Reguläre Aktualisierung von ZETA Guard	gemSpec_ZETA
A_27794	ZETA Guard - Prüfung auf neue ZETA Guard Versionen	gemSpec_ZETA
A_27795	ZETA Guard - Gewährleistung der Verbindung zu PIP/PAP	gemSpec_ZETA
A_27796	ZETA Guard - Gewährleistung der Verbindung zur Telemetriedatenlieferung der gematik	gemSpec_ZETA
A_28437	ZETA Guard, Registrierung bei der gematik	gemSpec_ZETA
A_28438	ZETA Guard, geo-redundanter Betrieb	gemSpec_ZETA

3.2.3 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 PoPP-Service 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 8: Festlegungen zur betrieblichen Eignung "Betriebshandbuch"

ID	Bezeichnung	Quelle (Referenz)
A_23551	Eigenmonitoring	gemKPT_Betr
A_23552	Verhalten bei Auffälligkeiten oder Anomalien	gemKPT_Betr
A_24799	Change Management - End-to-End-Funktionsprüfung nach Change	gemRL_Betr_TI
A_25903	Redundanz - Definition inhaltlicher Auszüge aus dem Redundanzkonzept	gemRL_Betr_TI
GS-A_3920-01	Koordinierung - Eskalationseinleitung durch den TI-ITSM-Teilnehmer	gemRL_Betr_TI
GS-A_4123	Notfall Management - Entwicklung und Pflege der TI-Notfallvorsorgedokumentation	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_4132	Notfall Management - Durchführung der	gemRL_Betr_TI

	Wiederherstellung und TI-Notfällen	
GS-A_4134	Notfall Management - Auswertungen von TI-Notfällen	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_4425-01	Change Management - Übermittlung von Optimierungsmöglichkeiten zur Umsetzung von genehmigten Changes	gemRL_Betr_TI
GS-A_5343-01	Betriebshandbuch - Definition inhaltlicher Auszüge aus dem Betriebshandbuch	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_5378	Change Management - Durchführung von Emergency-Changes durch TI-ITSM-Teilnehmer	gemRL_Betr_TI
GS-A_5597-01	Change Management - RFC (Sub-Changes) erstellen	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_5601-01	Change Management - Nachweis der	gemRL_Betr_TI

	Wirksamkeit eines Changes (Verifikation)	
GS-A_5602-01	Change Management - Nachweis der Wirksamkeit eines Changes in Auswirkung auf andere TI-Anwendungen (Verifikation)	gemRL_Betr_TI
GS-A_5606	Performance Management / Capacity - Unterstützung bei Definition von Kapazitätsanforderungen	gemRL_Betr_TI
GS-A_5610-03	Change Management - Vorlaufzeiten in der Bewertung von Changes	gemRL_Betr_TI
GS-A_5611	Change Management - Umsetzung von autorisierten RfC	gemRL_Betr_TI
A_26151-01	Redundanz - Lokale Redundanz	gemSpec_Perf
A_26152	Redundanz - Standortübergreifende Redundanz	gemSpec_Perf
A_26186	Redundanz - Wiederherstellungszeitraum - 5 Tage	gemSpec_Perf

3.2.4 Test betriebliche Eignung

Sofern in diesem Abschnitt Festlegungen mit Vorgaben zu organisatorischen Maßnahmen wie Prozessen und Strukturvorgaben verzeichnet sind, muss deren Erfüllung durch Teilnahme an GIT-TI in der RU nachgewiesen werden.

Tabelle 9: Festlegungen zur betrieblichen Eignung "Test"

ID	Bezeichnung	Quelle (Referenz)
A_27438	Durchführung der Generalprobe	gemKPT_Test
A_27815	Schnittstelle zur ZETA Guard - Funktionale Eignung - Shared Signals	gemKPT_Test
A_27829	Schnittstelle zur ZETA Guard - Konfigurierbarkeit - Umgebung	gemKPT_Test
A_27850	Generalprobe - Wartung ZETA Guard	gemKPT_Test
A_28336	Schnittstelle zur ZETA Guard - Systemanbindung	gemKPT_Test
A_28480	ZETA Guard, Integration optionaler Komponenten	gemSpec_ZETA

3.2.5 Dokumentenprüfung

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

Tabelle 10: Festlegungen zur sicherheitstechnischen Eignung "Dokumentenprüfung"

ID	Bezeichnung	Quelle (Referenz)
A_25903	Redundanz - Definition inhaltlicher Auszüge aus dem Redundanzkonzept	gemRL_Betr_TI

3.3 Festlegungen zur sicherheitstechnischen Eignung

3.3.1 Sicherheitsgutachten

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

Hinweis:

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

Abhängig von der konkreten Umsetzung können allerdings entsprechend [gemRL_PruefSichEig] Festlegungen, die nur für die Anbieter der zugehörigen Produkte relevant sind, vom Sicherheitsgutachter als „entbehrlich“ bewertet werden.

Weiterhin können Festlegungen, die zwar relevant sind, aber bereits vollständig vom Anbieter der zugehörigen Produkte erfüllt werden, vom Sicherheitsgutachter über Referenzieren der bestehenden Sicherheitsgutachten der Produkthanbieter als umgesetzt bewertet werden.

Tabelle 11: Festlegungen zur sicherheitstechnischen Eignung "Sicherheitsgutachten"

ID	Bezeichnung	Quelle (Referenz)
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_2158-01	Trennung von kryptographischen Identitäten und Schlüsseln in Produktiv- und Testumgebungen	gemSpec_Krypt
A_26495	PoPP-Service - PoPP-Token-Signatur-Identität	gemSpec_PoPP_Service
A_26496	PoPP-Service - APDU-Paket-Signatur-Zertifikat	gemSpec_PoPP_Service
A_26497	PoPP-Service - TLS-Server-Zertifikat an Client-Schnittstelle	gemSpec_PoPP_Service
A_26498	PoPP-Service - Schlüsselpaare und X.509-	gemSpec_PoPP_Service

	Zertifikate immer auf Basis P-256	
A_26539	PoPP-Service-Anbieter - Informationspflicht via Betriebshandbuch ZETA Guard Hersteller	gemSpec_PoPP_Service
A_26540	PoPP-Service - ZETA Guard - PoPP-Policy erstellen	gemSpec_PoPP_Service
A_26543	PoPP-Service - Kommunikation zu den Zero Trust Komponenten der gematik	gemSpec_PoPP_Service
A_26592	PoPP-Service - Rollentrennung zwischen Hersteller und Anbieter	gemSpec_PoPP_Service
A_26602	PoPP-Service - VAU - Prüfungsfunktionalität und Schlüsselmanagement im HSM	gemSpec_PoPP_Service
A_26616	PoPP-Service - TLS-Server-Zertifikate - Certificate Transparency	gemSpec_PoPP_Service
A_26623	PoPP-Service - VAU - Gemeinsame Zeremonie zur HSM-Einrichtung	gemSpec_PoPP_Service
A_26624	PoPP-Service - VAU - Sichere Erzeugung und Speicherung privater und geheimer Schlüssel der VAU	gemSpec_PoPP_Service
A_26625	PoPP-Service - VAU - Eingeschränkte HSM Administration	gemSpec_PoPP_Service
A_26626	PoPP-Service - VAU - Einsatz zertifizierter HSM	gemSpec_PoPP_Service
A_26627	PoPP-Service - VAU - Ausschluss von Manipulationen über physische Angriffe	gemSpec_PoPP_Service
A_26628	PoPP-Service - VAU - Physischer Zugriff auf Systeme der VAU nur im 4-Augen-Prinzip	gemSpec_PoPP_Service
A_26827	PoPP-Service - TLS-Server-Zertifikate - Certification Authority Authorization (CAA) Records	gemSpec_PoPP_Service
A_26828	PoPP-Service - Sichere Erzeugung und Speicherung Entity Statement-Signaturschlüssel	gemSpec_PoPP_Service
A_26954	PoPP-Service - Schlüsselpaare für CV-Zertifikate immer auf Basis von Brainpool	gemSpec_PoPP_Service
A_26968	PoPP-Service - VAU - Prozess für Vertrauensanker-Management	gemSpec_PoPP_Service
A_27041	PoPP-Service - VAU - Prozesse zur Regelmäßigen Erneuerung von Schlüsseln und Zertifikaten	gemSpec_PoPP_Service
A_27082	PoPP-Service - DDoS-Protection	gemSpec_PoPP_Service
A_27219	PoPP-Service - Absicherung Internet-	gemSpec_PoPP_Service

	Schnittstellen mit Paketfiltern	
A_27613	PoPP-Service - Maßnahmen gegen Datenverlust	gemSpec_PoPP_Service
A_25408-01	ZETA Guard - Verbot Profilbildung	gemSpec_ZETA
A_25413-01	ZETA Guard - Ordnungsgemäße IT-Administration	gemSpec_ZETA
A_25419-01	Security Monitoring - Erkennungsfähigkeit	gemSpec_ZETA
A_25420-01	Security Monitoring - Kommunikationsmerkmale signalisieren	gemSpec_ZETA
A_25608-01	ZETA Guard - Verarbeitung von Daten mit Schutzbedarf "sehr hoch"	gemSpec_ZETA
A_25747-01	ZETA Guard - Löschfristen Protokolle	gemSpec_ZETA
A_25763-01	Zero Trust-Komponenten - Private Schlüssel der Komponenten-Identitäten in einem HSM	gemSpec_ZETA
A_25764	Zero Trust-Komponenten - Sicherer Betrieb und Nutzung eines HSMs	gemSpec_ZETA
A_25765	Zero Trust-Komponenten - Einsatz zertifizierter HSM	gemSpec_ZETA
A_25775-01	PDP - Kontrolle des Audit-Logs	gemSpec_ZETA
A_26065-01	Nur zugelassene Images in Produktion	gemSpec_ZETA
A_26479-02	ZETA Guard - Ordnungsgemäße Änderung von Konfigurationen	gemSpec_ZETA
A_28462	ZETA Guard, externer Ingress - TLS Terminierung	gemSpec_ZETA

3.3.2 Anbietererklärung sicherheitstechnische Eignung

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

Tabelle 12: Festlegungen zur sicherheitstechnischen Eignung "Anbietererklärung"

ID	Bezeichnung	Quelle (Referenz)
TIP1-A_4191	Keine Echtdaten in RU und TU	gemKPT_Test
GS-A_5561	Bereitstellung 24/7-Kontaktpunkt	gemRL_Betr_TI
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_26533	PoPP-Service - Veröffentlichung der öffentlichen PoPP-Token-Verifikations-Schlüssel als signiertes JWKS	gemSpec_PoPP_Service
A_27546	PoPP-Service - VAU - Tägliche Übermittlung HSM-Protokoll an gematik	gemSpec_PoPP_Service

3.3.3 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 13: Festlegungen zur sicherheitstechnischen Eignung "Prozessprüfung"

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

4 Anhang - Verzeichnisse

4.1 Abkürzungen

Kürzel	Erläuterung
ID	Identifikation
CC	Common Criteria

4.2 Tabellenverzeichnis

Tabelle 1: Dokumente mit normativen Festlegungen.....	6
Tabelle 2: Mitgeltende Dokumente und Web-Inhalte.....	6
Tabelle 3: Informative Dokumente und Web-Inhalte.....	7
Tabelle 4: Festlegungen zur funktionalen Eignung "Test Produkt/FA".....	8
Tabelle 5: Festlegungen zur funktionalen Eignung "Anbietererklärung".....	8
Tabelle 6: Festlegungen zur betrieblichen Eignung "Prozessprüfung".....	10
Tabelle 7: Festlegungen zur betrieblichen Eignung "Anbietererklärung".....	12
Tabelle 8: Festlegungen zur betrieblichen Eignung "Betriebshandbuch".....	18
Tabelle 9: Festlegungen zur betrieblichen Eignung "Test".....	20
Tabelle 10: Festlegungen zur sicherheitstechnischen Eignung "Dokumentenprüfung".....	21
Tabelle 11: Festlegungen zur sicherheitstechnischen Eignung "Sicherheitsgutachten"....	21
Tabelle 12: Festlegungen zur sicherheitstechnischen Eignung "Anbietererklärung".....	23
Tabelle 13: Festlegungen zur sicherheitstechnischen Eignung "Prozessprüfung".....	25