

Elektronische Gesundheitskarte und Telematikinfrastruktur

# Anbietertypsteckbrief

## *Prüfvorschrift*

# TI-Gateway

Anbietertyp                    1.1.1  
Version:  
Anbietertyp Status:    freigegeben

Version:                    1.0.0  
Revision:                  857709  
Stand:                      05.03.2024  
Status:                    freigegeben  
Klassifizierung:        öffentlich  
Referenzierung:        gemAnbT\_TI\_Gateway\_ATV\_1.1.1

---

## 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_TI-Gateway_ATV_1.0.0
1.0.1	Anpassung durch Betr_Maintenance_23.3	gemAnbT_TI-Gateway_ATV_1.0.1
1.0.2	Anpassung durch HSK_23.5	gemAnbT_TI-Gateway_ATV_1.0.2
1.1.0	Anpassung durch TI-Gateway_23.1 und und HSK_23.6, gemF_Personalisierung_HSM	gemAnbT_TI-Gateway_ATV_1.1.0
1.1.1	Anpassung zu C_11631 (Zuordnung A_23551 und A_23552)	gemAnbT_TI-Gateway_ATV_1.1.1

### Historie Anbietertypsteckbrief

Die Dokumentenversion des Anbietertypsteckbriefs ändert sich mit jeder inhaltlichen oder redaktionellen Änderung des Anbietertypsteckbriefs und seinen referenzierten Dokumenten. Redaktionelle Änderungen haben keine Auswirkung auf die Anbietertypversion.

Version	Stand	Kap.	Grund der Änderung, besondere Hinweise	Bearbeiter
1.0.0	05.03.24		freigegeben	gematik

---

## Inhaltsverzeichnis

---

<b>1 Einführung .....</b>	<b>4</b>
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
<b>2 Dokumente .....</b>	<b>6</b>
<b>3 Normative Festlegungen .....</b>	<b>8</b>
<b>3.1 Festlegungen zur betrieblichen Eignung .....</b>	<b>8</b>
3.1.1 Prozessprüfung betriebliche Eignung.....	8
3.1.2 Anbietererklärung betriebliche Eignung .....	10
3.1.3 Betriebshandbuch betriebliche Eignung .....	17
3.1.4 Zuordnung der Festlegungen nach Anbieterkonstellation .....	19
3.1.4.1 Konstellation I (Normalfall).....	19
3.1.4.2 Konstellation II (Auslagerung Betrieb) .....	19
3.1.4.3 Konstellation III (Auslagerung Betrieb und UHD).....	19
<b>3.2 Festlegungen zur sicherheitstechnischen Eignung .....</b>	<b>20</b>
3.2.1 Sicherheitsgutachten .....	20
3.2.2 Sicherheitsgutachten Intermediär VSDM .....	24
3.2.3 Herstellererklärung Intermediär VSDM .....	26
3.2.4 Anbietererklärung sicherheitstechnische Eignung .....	28
<b>3.3 Anforderungen Betrieb Intermediär VSDM .....</b>	<b>29</b>
3.3.1 Prozessprüfung betriebliche Eignung.....	29
3.3.2 Anbietererklärung betriebliche Eignung .....	29
3.3.3 Betriebshandbuch betriebliche Eignung .....	30
<b>4 Anhang – Verzeichnisse .....</b>	<b>31</b>
4.1 Abkürzungen .....	31
4.2 Tabellenverzeichnis .....	31

---

## **1 Einführung**

---

### **1.1 Zielsetzung und Einordnung des Dokumentes**

Anbietertypsteckbriefe verzeichnen verbindlich die normativen Festlegungen der gematik an Anbieter 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
- die gematik im Rahmen der Zulassungsverfahren, Bestätigungsverfahren, Kooperationsverträge und Anbieterverfahren.

### **1.3 Geltungsbereich**

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

### **1.4 Abgrenzung des Dokumentes**

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

Dokumente zu den Zulassungsverfahren für den Anbietertyp sind nicht aufgeführt. Die geltenden Verfahren und Regelungen zur Beantragung und Durchführung von Zulassungsverfahren können 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
gemSpec_Intermediar_VSDM	Spezifikation Intermediär VSDM	1.14.0
gemF_Personalisierung_HSM	Feature Personalisierung SM-B mit HSM	1.0.0
gemSpec_PKI	Übergreifende Spezifikation – Spezifikation PKI	2.17.0
gemRL_TSL_SP_CP	Certificate Policy Gemeinsame Zertifizierungsrichtlinie für Teilnehmer der gematik-TSL	2.12.0
gemSpec_TSL	Spezifikation TSL-Dienst	1.20.0
gemSpec_Perf	Übergreifende Spezifikation Performance und Mengengerüst TI-Plattform	2.37.0
gemSpec_SST_VSDM	Schnittstellenspezifikation Transport VSDM	2.5.0
gemF_Highspeed-Konnektor	Feature Highspeed-Konnektor 2.0	1.4.0
gemKPT_Betr	Betriebskonzept Online-Produktivbetrieb	3.31.0
gemF_TI-Gateway	Feature TI-Gateway	1.3.0
gemSpec_SST_LD_BD	Spezifikation Logdaten und Betriebsdatenerfassung	1.6.0
gemSpec_OM	Übergreifende Spezifikation Operations und Maintenance	1.16.0
gemKPT_Test	Testkonzept der TI	2.9.0
gemSpec_Net	Übergreifende Spezifikation Netzwerk	1.27.0
gemSpec_DS_Anbieter	Spezifikation Datenschutz- und Sicherheitsanforderungen der TI an Anbieter	1.6.0
gemSpec_Krypt	Übergreifende Spezifikation Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur	2.28.1
gemRL_Betr_TI	Übergreifende Richtlinien zum Betrieb der TI	2.12.0

Weiterhin sind die in folgender Tabelle aufgeführten Dokumente und Web-Inhalte Gegenstand der Bestätigung/Zulassung. Details finden sich in den Bestätigungs-/Zulassungsbedingungen für das Bestätigung-/Zulassungsobjekt. Die Bestätigungs-

/Zulassungsbedingungen für den Anbietertyp *TI-Gateway* werden im Dokument [gemZul\_Anbieter] im Fachportal der gematik im Abschnitt Zulassung veröffentlicht.

**Tabelle 2: Mitgeltende Dokumente und Web-Inhalte**

Quelle	Herausgeber: Bezeichnung / URL	Version Branch / Tag
[gemRL_PruefSichEig_DS]	gematik: Richtlinie zur Prüfung der Sicherheitseignung	2.2.0
[gemZul_Anbieter]	gematik: Zulassungsverfahren für die Anbieter operativer Betriebsleistungen in der Telematikinfrastruktur	2.9.0

## 3 Normative Festlegungen

Die folgenden Abschnitte verzeichnen alle für den Anbiertypen 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)
GS-A_4085	Etablierung von Kommunikationsschnittstellen durch die TI-ITSM-Teilnehmer	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_5248	Konventionen zur Struktur von Prozessdaten	gemRL_Betr_TI
GS-A_5249	Reservierte Zeichen in den Prozessdaten	gemRL_Betr_TI
A_19174	Bereitstellung Übersicht Internet-Schnittstellen der TI	gemSpec_DS_Anbieter
A_20719	Weiterleitung erkannter Alarme an TI SIEM	gemSpec_DS_Anbieter
A_20720	Weiterleitung von Logdaten (Rohdaten) an TI SIEM	gemSpec_DS_Anbieter
A_21719	Weiterleitung von Reports TI SIEM	gemSpec_DS_Anbieter
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_20570	Performance – Standortübergreifende Redundanz	gemSpec_Perf
A_22057	Performance - Rohdaten - Verpflichtung des Anbieters (Rohdatenerfassung v.02)	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 4: Festlegungen zur betrieblichen Eignung "Anbietererklärung"**

ID	Bezeichnung	Quelle (Referenz)
A_23159	Prozess zum Erstellen und Löschen von HSK-Instanzen	gemF_Highspeed-Konnektor
A_25104	TSL Eintrag für TLS-Zertifikat Anbieter TI-Gateway	gemF_Personalisierung_HSM
A_25254	TLS-Zertifikat für Anbieter TI-Gateway	gemF_Personalisierung_HSM
A_18737-01	Sperrung von Zugängen zur TI	gemF_TI-Gateway
A_23237	Rollenausschluss Betreiber - DVO	gemF_TI-Gateway
A_23238	Rollenausschluss Hersteller - andere Rollen	gemF_TI-Gateway
A_23239	Rollenkombination Betreiber - Reseller	gemF_TI-Gateway
A_23261	Sperrbarkeit von Institutionen	gemF_TI-Gateway
A_23472	Auftragsverarbeitung bei weiteren Diensten	gemF_TI-Gateway
A_23487	Aktualisierbarkeit von VPN-Clients	gemF_TI-Gateway
A_24297	Probing TI-GW-Zugangsmodule	gemF_TI-Gateway
A_24541	TI-Gateway - Internetanbindung	gemF_TI-Gateway
A_24575	TI-Gateway, Umschaltzeiten am Internetzugang	gemF_TI-Gateway
A_24576	TI-Gateway, redundante Anbindung an die TI	gemF_TI-Gateway
A_24697	Prüfung TI-Gateway-Kompatibilität der Clientsysteme	gemF_TI-Gateway
A_18176	Mitwirkungspflichten bei der Einrichtung von Probes des Service Monitorings	gemKPT_Betr
A_18240	Reporting der technischen Service Level	gemKPT_Betr
A_19532-01	Erreichbarkeitszeiten im Anwendersupport (24/7)	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_23334	Bereitstellung Firewall-Konfigurationsdaten vom Anbieter TI-Gateway	gemKPT_Betr
A_23335	Verpflichtung zur Dokumentation von Service Levels im Anwendersupport des Anbieters TI-Gateway	gemKPT_Betr
A_23551	Eigenmonitoring	gemKPT_Betr
A_23552	Verhalten bei Auffälligkeiten oder Anomalien	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
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_7265-04	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_17764	Verwendung CI-ID	gemRL_Betr_TI
A_18363	Berechnung von Performance-Kenngrößen aus Rohdaten	gemRL_Betr_TI
A_18405	Erstellung einer Root Cause Analysis durch am Incident beteiligte TI-ITSM-Teilnehmer	gemRL_Betr_TI
A_18406	Nachlieferung zu einer Root Cause Analysis	gemRL_Betr_TI
A_18407	Unterstützung bei Change-Verifikation	gemRL_Betr_TI
A_24968	Probleme während Lösungsphase als "Pending" kennzeichnen	gemRL_Betr_TI
A_24983	Erstellung einer Root Cause Analysis im Incident - Prio 1 bis 2	gemRL_Betr_TI
A_24984	Erstellung einer Root Cause Analysis im Incident - Prio 3 bis 4	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_3889	Schließung eines übergreifenden Incidents	gemRL_Betr_TI
GS-A_3904	Annahme eines übergreifenden Incidents	gemRL_Betr_TI
GS-A_3905	Ablehnung eines übergreifenden Incidents	gemRL_Betr_TI
GS-A_3907	Lösung von übergreifenden Incidents	gemRL_Betr_TI
GS-A_3917	Bereitstellung der ITSM-Dokumentation bei Audits	gemRL_Betr_TI
GS-A_3922	Mitwirkung bei Taskforces	gemRL_Betr_TI
GS-A_3959	Prüfung auf übergreifendes Problem	gemRL_Betr_TI
GS-A_3971	Verifikation vor Schließung eines übergreifenden Problems	gemRL_Betr_TI
GS-A_3975	Prüfung auf Serviceverantwortung zum übergreifenden Problem	gemRL_Betr_TI
GS-A_3976	Ablehnung der Lösungsunterstützung	gemRL_Betr_TI
GS-A_3977	Annahme der Verantwortung zur Lösungsunterstützung	gemRL_Betr_TI
GS-A_3981	Annahme eines übergreifenden Problems	gemRL_Betr_TI
GS-A_3982	Ablehnung eines übergreifenden Problems	gemRL_Betr_TI
GS-A_3983	Ursachenanalyse eines übergreifenden Problems durch Serviceverantwortlichen	gemRL_Betr_TI
GS-A_3984	Service Request zur Bereitstellung der TI-Testumgebung (RU/TU)	gemRL_Betr_TI
GS-A_3986	Koordination bei übergreifenden 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_3991	WDB-Aktualisierung nach Schließung eines übergreifenden Problems	gemRL_Betr_TI

GS-A_4090	Kommunikationssprache	gemRL_Betr_TI
GS-A_4114	Bereitstellung von TI-Konfigurationsdaten	gemRL_Betr_TI
GS-A_4115	Datenänderung für TI-Konfigurationsdaten	gemRL_Betr_TI
GS-A_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_4125	TI-Notfallerkennung	gemRL_Betr_TI
GS-A_4126	Eskalation TI-Notfälle	gemRL_Betr_TI
GS-A_4127	Sofortmaßnahmen TI-Notfälle	gemRL_Betr_TI
GS-A_4128	Bewältigung der TI-Notfälle	gemRL_Betr_TI
GS-A_4129	Unterstützung bei TI-Notfällen	gemRL_Betr_TI
GS-A_4130	Festlegung der Schnittstellen des EMC	gemRL_Betr_TI
GS-A_4132	Durchführung der Wiederherstellung und TI-Notfällen	gemRL_Betr_TI
GS-A_4134	Auswertungen von TI-Notfällen	gemRL_Betr_TI
GS-A_4397	Teilnahme am Service Review	gemRL_Betr_TI
GS-A_4402	Mitwirkungspflicht bei der Bewertung vom Produkt-RfC	gemRL_Betr_TI
GS-A_4417	Stetige Aktualisierung des Change-Datensatzes im TI-ITSM-System	gemRL_Betr_TI
GS-A_4418	Übermittlung von Abweichungen vom Produkt-RfC	gemRL_Betr_TI
GS-A_4419	Nutzung der Testumgebung (RU/TU)	gemRL_Betr_TI
GS-A_4424	Umsetzung des Fallbackplans	gemRL_Betr_TI
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_5250	Ablehnung der Lösung eines übergreifenden Incidents	gemRL_Betr_TI
GS-A_5351	Prüfung von Service Requests	gemRL_Betr_TI
GS-A_5352	Lösung bzw. Bearbeitung des Service Requests	gemRL_Betr_TI
GS-A_5361	Durchführung von Emergency-Changes durch TI-ITSM-Teilnehmer bei Nichterreichbarkeit des Gesamtverantwortlichen TI	gemRL_Betr_TI
GS-A_5366	Mitwirkungspflicht der TI-ITSM-Teilnehmer bei der Festsetzung von Standard-Produkt-Changes	gemRL_Betr_TI
GS-A_5377	Durchführung einer Problemstornierung	gemRL_Betr_TI
GS-A_5378	Durchführung von Emergency-Changes durch TI-ITSM-Teilnehmer	gemRL_Betr_TI
GS-A_5400	Prüfung der Lösung durch den Melder eines übergreifenden Incidents	gemRL_Betr_TI
GS-A_5401-01	Verschlüsselte E-Mail-Kommunikation	gemRL_Betr_TI
GS-A_5402	Eigenverantwortliches Handeln bei Ausfall von Kommunikationsschnittstellen	gemRL_Betr_TI
GS-A_5449	Typisierung eines übergreifenden Incidents als „sicherheitsrelevant“	gemRL_Betr_TI
GS-A_5450	Typisierung eines übergreifenden Incidents als „datenschutzrelevant“	gemRL_Betr_TI
GS-A_5587	Ablehnung der Lösungsunterstützung bei einem übergreifenden Incident	gemRL_Betr_TI
GS-A_5588	Abbruch der Problembearbeitung	gemRL_Betr_TI
GS-A_5589	Prüfung auf Verantwortung zur Lösungsunterstützung	gemRL_Betr_TI
GS-A_5591	Verifikation des Service Requests	gemRL_Betr_TI
GS-A_5592	Schließung des Service Requests	gemRL_Betr_TI
GS-A_5593	Schließung des Service Requests ohne Verifikation	gemRL_Betr_TI
GS-A_5594	Identifikation von TI-Konfigurationsdaten	gemRL_Betr_TI
GS-A_5597	Produkt-RfC (Sub-Changes) erstellen	gemRL_Betr_TI
GS-A_5599	Beschreibung der Verifikation des Produkt-Changes im RfC	gemRL_Betr_TI

GS-A_5600	Beschreibung der Verifikation des Produkt-Changes in Auswirkung auf andere TI-Fachanwendungen im RFC	gemRL_Betr_TI
GS-A_5601	Nachweis der Wirksamkeit eines Changes	gemRL_Betr_TI
GS-A_5602	Nachweis der Wirksamkeit eines Changes in Auswirkung auf andere TI-Fachanwendungen	gemRL_Betr_TI
GS-A_5603	Eingangskanal für Informationen von TI-ITSM-Teilnehmern	gemRL_Betr_TI
GS-A_5604	Bewertung der Messergebnisse	gemRL_Betr_TI
GS-A_5606	Unterstützung bei Definition von Kapazitätsanforderungen	gemRL_Betr_TI
GS-A_5608	Übermittlung von CSV-Dateien	gemRL_Betr_TI
GS-A_5610-02	Bearbeitungsfristen in der Bewertung von Produkt-Changes	gemRL_Betr_TI
GS-A_5611	Umsetzung von autorisierten RFC	gemRL_Betr_TI
A_20570	Performance – Standortübergreifende Redundanz	gemSpec_Perf
A_22003-01	Performance - Rohdaten - Nachlieferung auf Anforderung (Rohdatenerfassung v.02)	gemSpec_Perf
A_22620	Performance - Rohdaten - Umsetzungszeit für Änderung der Lieferintervalle (Rohdatenlieferung v.02)	gemSpec_Perf
A_22996	Performance - Rohdaten - Zeitpunkte der Übermittlungen (Rohdatenerfassung v.02)	gemSpec_Perf
A_23347-01	Performance - Wartungsfenster - Durchführung	gemSpec_Perf
A_23431-01	Performance – TI-Gateway – Verfügbarkeit	gemSpec_Perf
A_23433-01	Performance - TI-Gateway - Skalierung	gemSpec_Perf
A_23615	Performance - Wartungsfenster und Ausfall - Ausnahme zur Verfügbarkeitsberechnung bei Wartung	gemSpec_Perf
A_23616	Performance - Verfügbarkeit - Anschluss an zentrales Netz - Hohe Verfügbarkeit	gemSpec_Perf
A_23988-01	Performance - Spezifika TI-Gateway - Bestandsdaten	gemSpec_Perf
A_23989-01	Performance - Spezifika TI-Gateway -	gemSpec_Perf



	Lieferweg und Format für Bestandsdaten	
A_24962	Performance - Servicezeiten des Anbieters basierend auf Produkttypen	gemSpec_Perf
A_17416-01	Schnittstelle Betriebsdatenerfassung Prüfung des TLS-Server-Zertifikats durch Fach- und zentrale Dienste	gemSpec_SST_LD_BD

Für den Betrieb des Intermediär sind zusätzlich die Festlegungen gemäß "Tabelle 5: Festlegungen zur betrieblichen Eignung "Anbietererklärung" für Betrieb Intermediär" nachzuweisen.

**Tabelle 5: Festlegungen zur betrieblichen Eignung "Anbietererklärung" für Betrieb Intermediär**

ID	Bezeichnung	Quelle(Referenz)
GS-A_5073	Performance – Intermediär VSDM – Skalierbarkeit	gemSpec_Perf
GS-A_5030	Performance – VSDM Intermediär – Verfügbarkeit	gemSpec_Perf
A_22057	Performance - Rohdaten - Verpflichtung des Anbieters (Rohdatenerfassung v.02)	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)
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_3976	Ablehnung der Lösungsunterstützung	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_4123	Entwicklung und Pflege der TI-Notfallvorsorgedokumentation	gemRL_Betr_TI
GS-A_4136	Statusinformation bei TI-Notfällen	gemRL_Betr_TI
GS-A_4137	Dokumentation im TI-Notfall-Logbuch	gemRL_Betr_TI
GS-A_4138	Erstellung des Wiederherstellungsberichts nach TI-Notfällen	gemRL_Betr_TI
GS-A_4398	Prüfung auf genehmigungspflichtige Produktänderung	gemRL_Betr_TI
GS-A_4399	Übermittlung von Produktdaten nach Abschluss von lokal autorisierten Produkt-Changes	gemRL_Betr_TI
GS-A_4400	Produkt-RfC (Master-Change) erstellen	gemRL_Betr_TI
GS-A_4407	Bereitstellung der Dokumentation des Change Managements für genehmigungspflichtige Produkt-Changes	gemRL_Betr_TI
GS-A_4417	Stetige Aktualisierung des Change-Datensatzes im TI-ITSM-System	gemRL_Betr_TI
GS-A_5343	Definition inhaltlicher Auszüge aus dem Betriebshandbuch	gemRL_Betr_TI
GS-A_5370	Prüfung auf Emergency Change	gemRL_Betr_TI
A_20714	Abstimmung der Maßnahmen im Security Monitoring mit gematik	gemSpec_DS_Anbieter
A_20715	kontinuierliche Verbesserung und Dokumentation des Security Monitorings	gemSpec_DS_Anbieter

A_23433-01	Performance - TI-Gateway - Skalierung	gemSpec_Perf
------------	---------------------------------------	--------------

### **3.1.4 Zuordnung der Festlegungen nach Anbieterkonstellation**

Der Anbieter TI-Gateway erfüllt in jedem Fall alle Festlegungen dieses Anbietertypsteckbriefes.

Der aufgeführten Konstellationen aus dem [gemKPT\_Betr] folgend ergeben sich die Zuordnungen der in diesem Anbietertypsteckbrief aufgeführten Festlegungen in folgenden 3 Konstellationen:

#### **3.1.4.1 Konstellation I (Normalfall)**

Der Anbieter TI-Gateway erbringt alle Festlegungen dieses Anbietertypsteckbriefes aus den Kapiteln 3.1.1 bis 3.2.2 selbst.

#### **3.1.4.2 Konstellation II (Auslagerung Betrieb)**

Der Anbieter TI-Gateway erbringt alle Festlegungen in Tabelle Tab\_KPT\_Betr\_TI\_007 selbst.

Der vom Anbieter TI-Gateway beauftragte Unterauftragnehmer vertritt den Anbieter und erbringt für diesen alle Festlegungen dieses oder einer anderen gültigen Version des Anbietertypsteckbriefes aus den Kapiteln 3.1.1 bis 3.2.2, mit der Ausnahme der in Tabelle Tab\_KPT\_Betr\_TI\_007 aufgeführten Festlegungen.

**Tabelle 7: Tab\_KPT\_Betr\_TI\_007 Liste der beim Anbieter verbleibenden Festlegungen Konstellation II**

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
TIP1-A_6388-02	Bereitstellung eines lokalen IT-Service-Managements durch Anbieter für ihre zu verantwortenden Servicekomponenten	gemKPT_Betr
A_19532-01	Erreichbarkeitszeiten im Anwendersupport (24/7)	gemKPT_Betr
TIP1-A_6389-02	Erreichbarkeit der 1st-Level (UHD), 2nd-Level (SPOCs) der Anbieter	gemKPT_Betr
TIP1-A_7266	Mitwirkungspflichten im TI-ITSM-System	gemKPT_Betr
GS-A_4088-01	Benennung von Ansprechpartnern	gemRL_Betr_TI

#### **3.1.4.3 Konstellation III (Auslagerung Betrieb und UHD)**

Der vom Anbieter TI-Gateway beauftragte Unterauftragnehmer vertritt den Anbieter und erbringt für diesen alle Festlegungen dieses oder einer anderen gültigen Version des Anbietertypsteckbriefes aus den Kapiteln 3.1.1 bis 3.2.2, inklusive der in Tabelle

Tab\_KPT\_Betr\_TI\_007 aufgeführten Festlegungen bis auf GS-A\_4088-01 aus gemRL\_Betr\_TI.

Beim Anbieter TI-Gateway verbleibt folgende Festlegung aus Tab\_KPT\_Betr\_TI\_008.

**Tabelle 8: Tab\_KPT\_Betr\_TI\_008 Liste der beim Anbieter verbleibenden Festlegungen  
Konstellation III**

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
GS-A_4088-01	Benennung von Ansprechpartnern	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.

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 mit einer entsprechenden Begründung 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 9: Festlegungen zur sicherheitstechnischen Eignung "Sicherheitsgutachten"**

ID	Bezeichnung	Quelle (Referenz)
A_21248-02	Anbieter HSK - Unabhängigkeit des Betreibers eines ePA-Aktensystems vom Betreiber eines HSK	gemF_Highspeed-Konnektor
A_23303	TLS mit Client-Authentisierung verpflichtend für Clientsystemanbindungen	gemF_Highspeed-Konnektor
A_23432	Verpflichtendes Auto-Update	gemF_Highspeed-Konnektor

A_25256	TSL Eintrag für TLS-Zertifikat Anbieter TI-Gateway löschen lassen bei Zertifikatsungültigkeit	gemF_Personalisierung_HSM
A_25257	Löschen C.FD.OSIG Zertifikat vom Konfigurationsinformations-Endpunkt bei Zertifikatsungültigkeit	gemF_Personalisierung_HSM
A_23237	Rollenausschluss Betreiber - DVO	gemF_TI-Gateway
A_23238	Rollenausschluss Hersteller - andere Rollen	gemF_TI-Gateway
A_23239	Rollenkombination Betreiber - Reseller	gemF_TI-Gateway
A_23248	DDoS-Protection	gemF_TI-Gateway
A_23249	Erkennung und Abwehr unberechtigter Zugriffe	gemF_TI-Gateway
A_23281	Schutz der privaten VPN-Schlüssel und initialer Passwörter bei zentraler Speicherung	gemF_TI-Gateway
A_23340	TI-Gateway Zugangsmodul - Beschreibung Authentifizierung & Verifikation HSK-Instanz	gemF_TI-Gateway
A_23352	Anforderungsabdeckung von zugekaufter Leistung	gemF_TI-Gateway
A_23361	TI-Gateway - Zulässige Produkttypversionen Highspeed-Konnektor	gemF_TI-Gateway
A_23362	TI-Gateway-Zugangsmodul - Kopplung HSK, Geschützter Import Clientsystem-Credentials	gemF_TI-Gateway
A_23382	TI-Gateway VPN-Client - Nutzerinformation	gemF_TI-Gateway
A_23392	Sperrung VPN-Zugänge bei detektierten Angriffen	gemF_TI-Gateway
A_23393	Prozesse zur schnellen Kommunikation und Entsperrung von VPN-Zugängen	gemF_TI-Gateway
A_23457	Weiterleitung gesammelter Informationen zu Bedrohungen an zentrales Security Monitoring	gemF_TI-Gateway
A_23494	4-Augen-Prinzip bei Wartung HSK	gemF_TI-Gateway
A_23496	Erkennen und Melden von Unregelmäßigkeiten bei physischem Zugriff auf HSK	gemF_TI-Gateway
GS-A_4847-01	Produkttyp TI-Gateway, DNSSEC im Namensraum Transportnetz	gemF_TI-Gateway
TIP1-A_4338-01	TI-GW-Zugangsmodul, Sicherung zum Transportnetz Internet durch Paketfilter	gemF_TI-Gateway

TIP1-A_4339-01	TI-GW-Zugangsmodule, Platzierung Paketfilters Internet	gemF_TI-Gateway
TIP1-A_4341-01	TI-Gateway, Erkennung von Angriffen	gemF_TI-Gateway
TIP1-A_4482-01	TI-Gateway, Kommunikation LE-Institutionen	gemF_TI-Gateway
A_21716	Unverzögliche Bewertung von Schwachstellen	gemSpec_DS_Anbieter
A_21717	Bereitstellung der Bewertung von Schwachstellen gegenüber der gematik	gemSpec_DS_Anbieter
A_21718	Umsetzen von Gegenmaßnahmen in Abhängigkeit der Kritikalität	gemSpec_DS_Anbieter
GS-A_2076-01	kDSM: Datenschutzmanagement nach BSI	gemSpec_DS_Anbieter
GS-A_2158-01	Trennung von kryptographischen Identitäten und Schlüsseln in Produktiv- und Testumgebungen	gemSpec_DS_Anbieter
GS-A_2214-01	kDSM: Anbieter müssen jährlich die Auftragsverarbeiter kontrollieren	gemSpec_DS_Anbieter
GS-A_2328-01	Pflege und Fortschreibung des Sicherheitskonzeptes und Notfallkonzeptes	gemSpec_DS_Anbieter
GS-A_2329-01	Umsetzung der Sicherheitskonzepte	gemSpec_DS_Anbieter
GS-A_2331-01	Sicherheitsvorfalls-Management	gemSpec_DS_Anbieter
GS-A_2332-01	Notfallmanagement	gemSpec_DS_Anbieter
GS-A_2345-01	regelmäßige Reviews	gemSpec_DS_Anbieter
GS-A_3078	Anbieter einer Schlüsselverwaltung: verpflichtende Migrationsstrategie bei Schwächung kryptographischer Primitive	gemSpec_DS_Anbieter
GS-A_3125	Schlüsselinstallation und Verteilung: Dokumentation gemäß Minimalitätsprinzip	gemSpec_DS_Anbieter
GS-A_3130	Krypto_Schlüssel_Installation: Dokumentation der Schlüsselinstallation gemäß Minimalitätsprinzip	gemSpec_DS_Anbieter
GS-A_3139	Krypto_Schlüssel: Dienst Schlüsselableitung	gemSpec_DS_Anbieter
GS-A_3141	Krypto_Schlüssel_Ableitung: Maßnahmen bei Bekanntwerden von Schwächen in der Schlüsselableitungsfunktion	gemSpec_DS_Anbieter
GS-A_3149	Krypto_Schlüssel_Archivierung: Dokumentation der Schlüsselarchivierung gemäß Minimalitätsprinzip	gemSpec_DS_Anbieter

GS-A_3737-01	Sicherheitskonzept	gemSpec_DS_Anbieter
GS-A_3753-01	Notfallkonzept	gemSpec_DS_Anbieter
GS-A_3772-01	Notfallkonzept: Der Dienstanbieter soll dem BSI-Standard 100-4 folgen	gemSpec_DS_Anbieter
GS-A_4980-01	Umsetzung der Norm ISO/IEC 27001	gemSpec_DS_Anbieter
GS-A_4981-01	Erreichen der Ziele der Norm ISO/IEC 27001 Annex A	gemSpec_DS_Anbieter
GS-A_4982-01	Umsetzung der Maßnahmen der Norm ISO/IEC 27002	gemSpec_DS_Anbieter
GS-A_4983-01	Umsetzung der Maßnahmen aus dem BSI-Grundschutz	gemSpec_DS_Anbieter
GS-A_4984-01	Befolgen von herstellerepezifischen Vorgaben	gemSpec_DS_Anbieter
GS-A_5551	Betriebsumgebung in einem Mitgliedstaat der EU bzw. des EWR	gemSpec_DS_Anbieter
GS-A_5557	Security Monitoring	gemSpec_DS_Anbieter
GS-A_5558	Aktive Schwachstellenscans	gemSpec_DS_Anbieter
GS-A_5626	kDSM: Auftragsverarbeitung	gemSpec_DS_Anbieter
A_20574-01	Beachtung der ISI-LANA für Übergänge zu Fremdnetzen	gemSpec_Net
GS-A_4057-01	Technische Anforderungen Sicherheitsgateways – Betriebssoftware	gemSpec_Net
GS-A_4062-01	Sicherheitsanforderungen für Netzübergänge zu Fremdnetzen	gemSpec_Net
GS-A_4777-01	Technische Anforderungen Sicherheitsgateways - Dokumentation Systemfunktion	gemSpec_Net
GS-A_4778-01	Technische Anforderungen Sicherheitsgateways - Verbindungen nach Erstinstallation	gemSpec_Net
GS-A_4808	Nameserver-Implementierungen, nichtautorisierte Zonentransfers	gemSpec_Net
GS-A_4879	DNSSEC, Zonen im Namensraum Internet mittels DNSSEC sichern	gemSpec_Net
GS-A_5089	Nameserver-Implementierungen, private Schlüssel sicher speichern	gemSpec_Net

### 3.2.2 Sicherheitsgutachten Intermediär VSDM

Die folgenden Anforderungen sind vom Anbieter nachzuweisen, wenn dieser mit seinem TI-Gateway auch einen Intermediär betreibt. Nutzt der Anbieter einen bestehenden Intermediär eines anderen Betreibers, sind diese Anforderungen entsprechend von diesem Betreiber nachzuweisen.

**Tabelle 10: Festlegungen zur sicherheitstechnischen Eignung "Sicherheitsgutachten" Intermediär VSDM**

ID	Bezeichnung	Quelle (Referenz)
GS-A_4330	Einbringung des Komponentenzertifikats	gemRL_TSL_SP_CP
A_21716	Unverzögliche Bewertung von Schwachstellen	gemSpec_DS_Anbieter
GS-A_2076-01	kDSM: Datenschutzmanagement nach BSI	gemSpec_DS_Anbieter
GS-A_2158-01	Trennung von kryptographischen Identitäten und Schlüsseln in Produktiv- und Testumgebungen	gemSpec_DS_Anbieter
GS-A_2214-01	kDSM: Anbieter müssen jährlich die Auftragsverarbeiter kontrollieren	gemSpec_DS_Anbieter
GS-A_2328-01	Pflege und Fortschreibung des Sicherheitskonzeptes und Notfallkonzeptes	gemSpec_DS_Anbieter
GS-A_2329-01	Umsetzung der Sicherheitskonzepte	gemSpec_DS_Anbieter
GS-A_2331-01	Sicherheitsvorfalls-Management	gemSpec_DS_Anbieter
GS-A_2332-01	Notfallmanagement	gemSpec_DS_Anbieter
GS-A_2345-01	regelmäßige Reviews	gemSpec_DS_Anbieter
GS-A_3078	Anbieter einer Schlüsselverwaltung: verpflichtende Migrationsstrategie bei Schwächung kryptographischer Primitive	gemSpec_DS_Anbieter
GS-A_3125	Schlüsselinstallation und Verteilung: Dokumentation gemäß Minimalitätsprinzip	gemSpec_DS_Anbieter
GS-A_3130	Krypto_Schlüssel_Installation: Dokumentation der Schlüsselinstallation gemäß Minimalitätsprinzip	gemSpec_DS_Anbieter
GS-A_3139	Krypto_Schlüssel: Dienst Schlüsselableitung	gemSpec_DS_Anbieter
GS-A_3141	Krypto_Schlüssel_Ableitung: Maßnahmen bei Bekanntwerden von Schwächen in der Schlüsselableitungsfunktion	gemSpec_DS_Anbieter
GS-A_3149	Krypto_Schlüssel_Archivierung:	gemSpec_DS_Anbieter



	Dokumentation der Schlüsselarchivierung gemäß Minimalitätsprinzip	
GS-A_3737-01	Sicherheitskonzept	gemSpec_DS_Anbieter
GS-A_3753-01	Notfallkonzept	gemSpec_DS_Anbieter
GS-A_3772-01	Notfallkonzept: Der Dienstanbieter soll dem BSI-Standard 100-4 folgen	gemSpec_DS_Anbieter
GS-A_4980-01	Umsetzung der Norm ISO/IEC 27001	gemSpec_DS_Anbieter
GS-A_4981-01	Erreichen der Ziele der Norm ISO/IEC 27001 Annex A	gemSpec_DS_Anbieter
GS-A_4982-01	Umsetzung der Maßnahmen der Norm ISO/IEC 27002	gemSpec_DS_Anbieter
GS-A_4983-01	Umsetzung der Maßnahmen aus dem BSI-Grundschutz	gemSpec_DS_Anbieter
GS-A_4984-01	Befolgen von herstellerepezifischen Vorgaben	gemSpec_DS_Anbieter
GS-A_5551	Betriebsumgebung in einem Mitgliedstaat der EU bzw. des EWR	gemSpec_DS_Anbieter
GS-A_5557	Security Monitoring	gemSpec_DS_Anbieter
GS-A_5558	Aktive Schwachstellenscans	gemSpec_DS_Anbieter
GS-A_5626	kDSM: Auftragsverarbeitung	gemSpec_DS_Anbieter
VSDM-A_2669	Intermediär VSDM: Zugriff nur für autorisierte Personen	gemSpec_Intermediaer_VSDM
VSDM-A_2748-01	Intermediär VSDM: Löschen von personenbeziehenden Daten in Protokollen innerhalb von 30 Tagen	gemSpec_Intermediaer_VSDM
A_17124-01	TLS-Verbindungen (ECC-Migration)	gemSpec_Krypt
A_18464	TLS-Verbindungen, nicht Version 1.1	gemSpec_Krypt
A_21275-01	TLS-Verbindungen, zulässige Hashfunktionen bei Signaturen im TLS-Handshake	gemSpec_Krypt
GS-A_4359-02	X.509-Identitäten für die Durchführung einer TLS-Authentifizierung	gemSpec_Krypt
GS-A_4367	Zufallszahlengenerator	gemSpec_Krypt
GS-A_4368	Schlüsselerzeugung	gemSpec_Krypt
GS-A_4384-01	TLS-Verbindungen	gemSpec_Krypt

GS-A_4385	TLS-Verbindungen, Version 1.2	gemSpec_Krypt
GS-A_4387	TLS-Verbindungen, nicht Version 1.0	gemSpec_Krypt
GS-A_4388	DNSSEC-Kontext	gemSpec_Krypt
GS-A_5035	Nichtverwendung des SSL-Protokolls	gemSpec_Krypt
GS-A_5131	Hash-Algorithmus bei OCSP/CertID	gemSpec_Krypt
GS-A_5322	Weitere Vorgaben für TLS-Verbindungen	gemSpec_Krypt
GS-A_4808	Nameserver-Implementierungen, nichtautorisierte Zonentransfers	gemSpec_Net
GS-A_4641	Initiale Einbringung TI-Vertrauensanker	gemSpec_PKI
GS-A_4748	Initiale Einbringung TSL-Datei	gemSpec_PKI
VSDM-A_2238	Intermediär VSDM: Nachrichten grundsätzlich nicht speichern	gemSpec_SST_VSDM

### 3.2.3 Herstellererklärung Intermediär VSDM

Die folgenden Anforderungen sind vom Anbieter nachzuweisen, wenn dieser mit seinem TI-Gateway auch einen Intermediär betreibt. Nutzt der Anbieter einen bestehenden Intermediär eines anderen Betreibers, sind diese Anforderungen entsprechend von diesem Betreiber nachzuweisen.

**Tabelle 11: Festlegungen zur sicherheitstechnischen Eignung "Herstellererklärung" Intermediär VSDM**

ID	Bezeichnung	Quelle (Referenz)
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_4526-01	Aufbewahrungsvorgaben an die Nachweise zu Sicherheitsmeldungen	gemSpec_DS_Anbieter
GS-A_4530-01	Maßnahmen zur Behebung von erheblichen Sicherheitsvorfällen und Notfällen	gemSpec_DS_Anbieter
GS-A_4532-01	Nachweis der Umsetzung von Maßnahmen in Folge eines erheblichen Sicherheitsvorfalls oder Notfalls	gemSpec_DS_Anbieter
GS-A_5324-01	Teilnahme des Anbieters an Sitzungen des kISMS	gemSpec_DS_Anbieter
GS-A_5324-02	kDSM: Teilnahme des Anbieters an Sitzungen des kDSM	gemSpec_DS_Anbieter
GS-A_5555	Unverzügliche Meldung von erheblichen Sicherheitsvorfällen und -notfällen	gemSpec_DS_Anbieter
GS-A_5556	Unverzügliche Behebung von erheblichen Sicherheitsvorfällen und -notfällen	gemSpec_DS_Anbieter
GS-A_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
GS-A_5566	kDSM: Sicherstellung der Datenschutzanforderungen in Unterbeauftragungsverhältnissen	gemSpec_DS_Anbieter
GS-A_5624-01	Auditrechte der gematik zur Informationssicherheit	gemSpec_DS_Anbieter
GS-A_5625	kDSM: Auditrechte der gematik zum Datenschutz	gemSpec_DS_Anbieter
A_17205	Signatur der TSL: Signieren und Prüfen (ECC-Migration)	gemSpec_Krypt

A_17206	XML-Signaturen (ECC-Migration)	gemSpec_Krypt
A_17322	TLS-Verbindungen nur zulässige Ciphersuiten und TLS-Versionen (ECC-Migration)	gemSpec_Krypt
A_18467	TLS-Verbindungen, Version 1.3	gemSpec_Krypt
A_21275-01	TLS-Verbindungen, zulässige Hashfunktionen bei Signaturen im TLS-Handshake	gemSpec_Krypt
A_23913	Intermediär: TLS, Kurven beim ephemeren ECDH (TLS-Handshake)	gemSpec_Krypt
GS-A_5527	TLS-Renegotiation-Indication-Extension Intermediär	gemSpec_Krypt
GS-A_5541	TLS-Verbindungen als TLS-Klient zur Störungssampel oder SM	gemSpec_Krypt
GS-A_5580-01	TLS-Klient für betriebsunterstützende Dienste	gemSpec_Krypt
GS-A_5581	"TUC vereinfachte Zertifikatsprüfung" (Komponenten-PKI)	gemSpec_Krypt
GS-A_4720	Verwendung registrierter Werte für subjectDN	gemSpec_PKI

### 3.2.4 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 12: Festlegungen zur sicherheitstechnischen Eignung "Anbietererklärung"**

ID	Bezeichnung	Quelle (Referenz)
A_19175	Zustimmung zu regelmäßigen Schwachstellenscans durch die gematik	gemSpec_DS_Anbieter
A_20716	Überwachung von Systemen	gemSpec_DS_Anbieter
A_20717	Zentrale Auswertung sicherheitsrelevanter Ereignisse	gemSpec_DS_Anbieter
A_20718	Reaktion auf detektierte Ereignisse	gemSpec_DS_Anbieter
A_21720	Beteiligung an Coordinated Vulnerability Disclosure	gemSpec_DS_Anbieter
GS-A_4526-01	Aufbewahrungsvorgaben an die Nachweise zu Sicherheitsmeldungen	gemSpec_DS_Anbieter

GS-A_5324-01	Teilnahme des Anbieters an Sitzungen des kISMS	gemSpec_DS_Anbieter
GS-A_5324-02	kDSM: Teilnahme des Anbieters an Sitzungen des kDSM	gemSpec_DS_Anbieter
GS-A_5566	kDSM: Sicherstellung der Datenschutzanforderungen in Unterbeauftragungsverhältnissen	gemSpec_DS_Anbieter
GS-A_5624-01	Auditrechte der gematik zur Informationssicherheit	gemSpec_DS_Anbieter
GS-A_5625	kDSM: Auditrechte der gematik zum Datenschutz	gemSpec_DS_Anbieter

### 3.3 Anforderungen Betrieb Intermediär VSDM

Die folgenden Anforderungen sind vom Anbieter TI-Gateway nachzuweisen, wenn dieser mit seinem TI-Gateway auch selbst einen Intermediär betreibt. Nutzt der Anbieter TI-Gateway einen bestehenden Intermediär eines anderen Betreibers, sind diese Anforderungen entsprechend von diesem Betreiber nachzuweisen.

#### 3.3.1 Prozessprüfung betriebliche Eignung

Für den Betrieb des Intermediärs sind die Festlegungen gemäß "Tabelle 3: Festlegungen zur betrieblichen Eignung "Prozessprüfung"" zusätzlich für den Scope Intermediär nachzuweisen.

#### 3.3.2 Anbietererklärung betriebliche Eignung

Für den Betrieb des Intermediär sind die Festlegungen gemäß "Tabelle 4: Festlegungen zur betrieblichen Eignung "Anbietererklärung"" nachzuweisen mit Ausnahme der in "Tabelle 13: nicht geltende Anforderungen für den Betrieb des Intermediär" aufgeführten Festlegungen.

**Tabelle 13: nicht geltende Anforderungen für den Betrieb des Intermediär**

ID	Bezeichnung	Quelle(Referenz)
A_23159	Prozess zum Erstellen und Löschen von HSK-Instanzen	gemF_HighspeedKonnektor
A_18737-01	Sperrung von Zugängen zur TI	gemF_TI-Gateway
A_23237	Rollenausschluss Betreiber - DVO	gemF_TI-Gateway

A_23238	Rollenausschluss Hersteller - andere Rollen	gemF_TI-Gateway
A_23239	Rollenkombination Betreiber - Reseller	gemF_TI-Gateway
A_23261	Sperrbarkeit von Institutionen	gemF_TI-Gateway
A_23472	Auftragsverarbeitung bei weiteren Diensten	gemF_TI-Gateway
A_23487	http-Forwarder - IP-Adresse	gemF_TI-Gateway
TIP1-A_4323-01	TI-Gateway, http-Forwarder - Verteilung	gemF_TI-Gateway

### 3.3.3 Betriebshandbuch betriebliche Eignung

Für den Betrieb des Intermediär sind die Festlegungen gemäß "Tabelle 6: Festlegungen zur betrieblichen Eignung "Betriebshandbuch"" nachzuweisen mit Ausnahme der in "Tabelle 14: nicht geltende Anforderungen für den Betrieb des Intermediär" aufgeführten Festlegungen.

**Tabelle 14: nicht geltende Anforderungen für den Betrieb des Intermediär**

ID	Bezeichnung	Quelle(Referenz)
A_23433	Performance - TI-Gateway - Skalierung	gemSpec_Perf

---

## 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 .....	7
Tabelle 3: Festlegungen zur betrieblichen Eignung "Prozessprüfung" .....	8
Tabelle 4: Festlegungen zur betrieblichen Eignung "Anbietererklärung" .....	10
Tabelle 5: Festlegungen zur betrieblichen Eignung "Anbietererklärung" für Betrieb Intermediär .....	17
Tabelle 6: Festlegungen zur betrieblichen Eignung "Betriebshandbuch" .....	17
Tabelle 7: Tab_KPT_Betr_TI_007 Liste der beim Anbieter verbleibenden Festlegungen Konstellation II .....	19
Tabelle 8: Tab_KPT_Betr_TI_008 Liste der beim Anbieter verbleibenden Festlegungen Konstellation III .....	20
Tabelle 9: Festlegungen zur sicherheitstechnischen Eignung "Sicherheitsgutachten" .....	20
Tabelle 10: Festlegungen zur sicherheitstechnischen Eignung "Sicherheitsgutachten" Intermediär VSDM .....	24
Tabelle 11: Festlegungen zur sicherheitstechnischen Eignung "Herstellererklärung" Intermediär VSDM .....	26
Tabelle 12: Festlegungen zur sicherheitstechnischen Eignung "Anbietererklärung" .....	28
Tabelle 13: nicht geltende Anforderungen für den Betrieb des Intermediär .....	29
Tabelle 14: nicht geltende Anforderungen für den Betrieb des Intermediär .....	30

