Elektronische Gesundheitskarte und Telematikinfrastruktur

Feature:
TI-Gateway

Version:	1.0.0 CC
Revision:	523942
Stand:	25.11.2022
Status:	zur Abstimmung freigegeben
Klassifizierung:	öffentlich_Entwurf
Referenzierung:	gemF_TI-Gateway

Dokumentinformationen

Änderungen zur Vorversion

Anpassungen des vorliegenden Dokumentes im Vergleich zur Vorversion können Sie der nachfolgenden Tabelle entnehmen.

Dokumentenhistorie

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
1.0.0 CC	25.11.22		Kommentierung	gematik

Inhaltsverzeichnis

1 Einordnung des Dokuments

Die Schnittstelle zwischen der zentralen Infrastruktur der TI und der dezentralen Umgebung bildet derzeit die dezentrale Komponente Konnektor, die eine gesicherte Verbindung zum VPN-Zugangsdienst der TI aufbaut. Um im Sinne der TI2.0 Komplexität aus der dezentralen Umgebung zu entfernen, wurde das Produkt TI-Gateway definiert, welches die Funktion von Zugangsdienst und Konnektor in einem Dienst zusammenfasst. Dieses Feature-Dokument beschreibt das TI-Gateway (Anbieter TI-Gateway, Produkt Zugangsmodul und Anpassungen am Produkt Highspeed-Konnektor) und beinhaltet Blattanforderungen, die nicht bereits Teil anderer Spezifikationen der gematik sind. Der vollständige Anforderungshaushalt ergibt sich aus den Steckbriefen für den Anbieter TI-Gateway und den Produkten, die Teil des TI-Gateway sind.

1.1 Zielsetzung

Dieses Dokument soll ein Verständnis für das TI-Gateway vermitteln und die Anforderungslage vervollständigen. Dadurch sollen Hersteller und Anbieter in die Lage versetzt werden, das Produkt herzustellen bzw. dessen Betrieb zu ermöglichen.

1.2 Zielgruppe

Hersteller, Anbieter, Nutzer und andere Stakeholder.

1.3 Abgrenzungen

Das Dokument beinhaltet nur neue bzw. geänderte Anforderungen. Die vollständige Anforderungslage für die Produkttypen des TI-Gateways und den Anbieter des TI-Gateways ergeben sich aus den Produkttypsteckbriefen, dem Anbietersteckbrief und den darin referenzierten Anforderungen.

1.4 Methodik Anforderungen

Anforderungen als Ausdruck normativer Festlegungen werden durch eine eindeutige ID sowie die dem RFC 2119 [RFC2119] entsprechenden, in Großbuchstaben geschriebenen deutschen Schlüsselworte MUSS, DARF NICHT, SOLL, SOLL NICHT, KANN gekennzeichnet.

Da in dem Beispielsatz „Eine leere Liste DARF NICHT ein Element besitzen.“ die Phrase „DARF NICHT“ semantisch irreführend wäre (wenn nicht ein, dann vielleicht zwei?), wird in diesem Dokument stattdessen „Eine leere Liste DARF KEIN Element besitzen.“ verwendet. Die Schlüsselworte werden außerdem um Pronomen in Großbuchstaben ergänzt, wenn dies den Sprachfluss verbessert oder die Semantik verdeutlicht.

Anforderungen werden im Dokument wie folgt dargestellt:
<AFO-ID> - <Titel der Afo>
Text / Beschreibung
[<=]

Dabei umfasst die Anforderung sämtliche zwischen Afo-ID und Textmarke [<=] angeführten Inhalte.

2 Einordnung in die Telematikinfrastruktur

Das TI-Gateway ist ein zentraler Dienst der Telematikinfrastruktur, der Leistungserbringern anstelle eines Konnektors ermöglicht,

- eHealth-Kartenterminals (und darüber TI-Smartcards) zu nutzen,
- Services zu nutzen, wie sie vom Anwendungskonnektor und den Fachmodulen des Konnektors angeboten werden und
- über das Netzwerk auf offene Fachdienste und WANDA zuzugreifen.

3 Technisches Konzept

Die Anbieterzulassung für das TI-Gateway setzt eine Produktzulassung Zugangsmodul und eine Produktzulassung Highspeed-Konnektor (HSK) voraus. Die Anbieterzulassung für das TI-Gateway kann erweitert werden auf die Produkte Intermediär-VSDM und OCSP-Proxy, wenn nicht auf bereits zugelassene Produkte dieser Produkttypen zugegriffen werden soll.

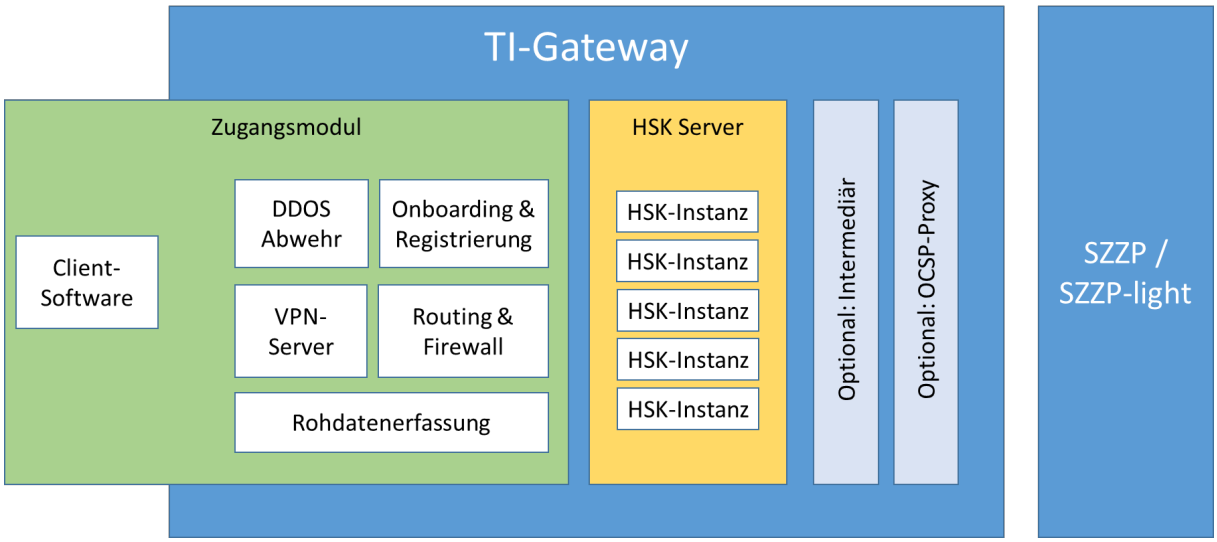


Abbildung 1: Anbindung TI-Gateway

Das Zugangsmodul ermöglicht und sichert

- den Zugriff für die fachliche Nutzung auf die HSK-Instanz
- den Zugriff für die Administration einer HSK-Instanz
- den Zugriff auf offene Fachdienste und WANDA der Telematikinfrastruktur

Der HSK stellt bereit

- die Basisdienste der Telematikinfrastruktur für LE-Umgebungen
- die Fachmodule
- die Kartenterminalintegration für die LE-Umgebung

Die Produkte Intermediär und OCSP-Proxy bieten Funktionalitäten, die bei Nutzung von Konnektoren durch den VPN-Zugangsdienst abgedeckt werden.

Die Anbindung an die Telematikinfrastruktur erfolgt über einen SZZP oder SZZP-light. Die Notwendigkeit einer kryptographischen Kopplung zwischen HSK und einem SZZP-light-plus, die bei einer Anbieterzulassung HSK vorgeschrieben ist, entfällt auf Grund der im Kontext der Anbieterzulassung TI-Gateway geprüften betrieblichen Sicherheit beim Anbieter.

4 Rollenkonzept TI-Gateway

Der Anbieter eines TI-Gateways vereint die Rollen des Infrastrukturbetreibers und des Resellers. Diese Aufteilung berücksichtigt, dass ein Anbieter bestimmte Leistungen für seinen Dienst zukauft. Da das TI-Gateway aus den Produkten Zugangsmodul und HSK aufgebaut ist, sind auch die Hersteller dieser Produkte für den Betrieb eines TI-Gateways zu berücksichtigen. Gesondert betrachtet wird der Hersteller HSK, wegen der Anforderungen an die VAU des HSK.

Auf der Anwenderseite wird der Leistungserbringer und der lokale Administrator unterschieden. Auch diese Rollen können auf unterschiedliche Akteure verteilt werden.

4.1 Infrastrukturbetreiber

Der Infrastrukturbetreiber verantwortet das Rechenzentrum, Zugangskontrolle, Strom, Klima, Hardware und die Sicherheitsinfrastruktur. Der Infrastrukturbetreiber administriert den HSK-Server (Basis-System), bis auf bestimmte Arbeiten am HSK, die nur der Hersteller des HSK vornehmen darf. Der Infrastrukturbetreiber hat keinen Zugriff auf den Inhalt und die Konfiguration der HSK-Instanzen und deren fachliche Logs und er hat ebenso keinen Zugriff auf medizinische Daten. Der Infrastrukturbetreiber betreibt und überwacht zudem das Zugangsmodul und ist für die Installation von Softwareupdates der betriebenen Komponenten zuständig.

Der Infrastrukturbetreiber kann technische Parameter wie die Ressourcenauslastung überwachen und technische Parameter wie die Ressourcenzuweisung für HSK-Instanzen ändern. Diese Aufgabe kann auch an den Reseller übertragen werden.

Das Zugangsmodul stellt die Anbindung für die LEI bereit und stellt sicher, dass eine LEI nur auf ihre zugeordnete HSK-Instanz zugreifen kann (Firewall, Routing und VPN). Das Zugangsmodul ist eine automatisierte, technische Lösung, die durch den Reseller bedient wird. Manuelle Eingriffe des Infrastrukturbetreibers werden unterbunden. (Infrastructure as code)

4.2 Reseller

Der Reseller steuert das Onboarding von LE-Institutionen inklusive dem Erzeugen von HSK-Instanzen im „Werkszustand" (automatisiert) über die Onboarding- & Registrierungskomponente des Zugangsmoduls. Zudem obliegt ihm das Speichern und Wiederherstellen von Backups von HSK-Instanzen sowie das Löschen von HSK-Instanzen.

Im Rahmen des Onboardings werden auch der Administrations-Zugang an den Leistungserbringer bzw. den von diesem beauftragen lokalen Administrator (DVO) vergeben und die HSK-Instanzen zugewiesen. In diesem Prozess sind Kontrollen einzubauen, damit der Reseller nicht vom Leistungserbringer unbemerkt einem Unberechtigten oder sich selbst den Administrationszugang zur HSK-Instanz vergeben kann. Der Wechsel des Administrators (DVO) ist als Anwendungsfall vorzusehen.

Der Reseller hat keinen Zugriff auf medizinische Daten oder die fachliche Konfiguration von HSK-Instanzen. Wenn vom Infrastrukturbetreiber dazu befähigt, kann er technische

Parameter wie die Ressourcenauslastung überwachen und technische Parameter wie die Ressourcenzuweisung für HSK-Instanzen ändern.

Die Rolle Reseller kann nur dann mit der Rolle des lokalen Administrators der HSK-Instanz kombiniert werden, wenn ausgeschlossen ist, dass der Reseller auch die Rolle Infrastrukturbetreiber inne hat, also bspw. Zugang zum Rechenzentrum hat.

Der Reseller beantragt die Anbieterzulassung von der gematik. Dabei kann er vorgeprüfte Unterlagen verwenden, welche Anforderungen an den Infrastrukturbetreiber betreffen, die vom Reseller nachgenutzt werden. Er muss aber in jedem Fall konkret nachweisen, welche Anforderungen vom Infrastrukturbetreiber erfüllt werden und das dies auch vertraglich eindeutig geregelt ist.

Der Reseller hat keine eigene Rolle am HSK, sondern nutzt diesen über das Zugangsmodul, welches selbst als technische Administrator-Rolle am HSK agiert.

4.3 Hersteller des HSK

Der Hersteller stellt Softwareupdates bereit und wird für 3rd-Level-Support/Debugging hinzugezogen.

Der Hersteller des HSK hat zudem eine Sonderrolle für Arbeiten innerhalb des HSK-Käfigs (physischer Schutz des HSK vor Zugriffen des Betreibers), dem Pairing von HSK-AK mit dem SZZP (sofern ein SZZP-light-plus verwendet wird) und dem HSM und der Personalisierung des HSM mit der Konnektoridendität.

Der Hersteller des HSK hat keinen Zugriff auf fachliche Logs. Wenn diese für den Support notwendig sind, müssen diese von einer Administrator-Rolle pseudonymisiert bereitgestellt werden.

4.4 „Lokaler" Administrator z.B. Dienstleister vor Ort (DVO)

Der Leistungserbringer steuert, ob der Zugang für die Rolle lokaler Administrator von ihm selber wahrgenommen wird oder an einen von ihm ausgewählten DVO delegiert wird. Der Leistungserbringer muss diese Zugänge jederzeit entziehen, suspendieren oder neu vergeben können.

Der lokale Administrator nimmt die initiale Anbindung der HSK-Instanz an die LEI vor (Pairing der KTs und Konfiguration der Primärsysteme, beidseitige Authentisierung). Auch ein späteres Hinzufügen von neuen Primärsystemen hat stets einen lokalen Anteil auf Grund der notwendigen Konfiguration in Clientsystem und HSK-Instanz für die beidseitige Authentisierung und Zugriffssteuerung (Infomodell). Durch Weiterentwicklung der Konfigurationsmechanismen kann diese Konfiguration unter Berücksichtigung der Sicherheitsvorgaben endbenutzertauglich gemacht werden (vergleichbar Pairingprozesse bei Consumerprodukten z.B. AppleWatch+iPhone).

Diese Rolle entspricht somit dem lokalen Administrator/DVO, wie er auch beim Einboxkonnektor agiert. Beauftragt durch den Leistungserbringer, administriert er die konkrete HSK-Instanz einer LEI, richtet das Primärsystemen ein, verbindet Kartenterminals und führt andere fachliche Einrichtungen durch. Der lokale Administrator hat keinen Zugriff auf medizinische Daten oder personenbezogene Daten von Versicherten (abgesehen von den spezifizierten Einträgen im VSDM-Protokoll).

Der lokale Administrator kann fachliche Logs der HSK-Instanz einsehen.

Da die LEI über ein VPN mit dem TI-Gateway verbunden ist, kann das TI-Gateway durch Netzwerkkonfiguration sicherstellen, dass der Zugriff auf fachliche Schnittstellen (SOAP, CETP, SICCT) und die Administrationsschnittstelle der HSK-Instanz nur aus dem Netz der LEI möglich ist. Eine zusätzliche Erreichbarkeit der Administrations-Schnittstelle der HSK-Instanz über ein DVO-Netz (ebenso per VPN angebunden) ist möglich, wenn der Nutzer (LEI) dies wünscht und freigibt. Eine Erreichbarkeit der fachlichen Schnittstellen (SOAP/LDAP) über ein DVO-Netz ist ausgeschlossen.

4.5 Remote-Administrator

Der Remote-Administrator übernimmt kontinuierliche Überwachungs- und Wartungsaufgaben. Der Remote-Administrator ist eine eingeschränkte Administrator-Rolle, die nicht über alle Rechte verfügt. Insbesondere kann der Remote-Administrator keine neuen Clients anlegen oder bestehende Client-Identitäten ändern. Dadurch ist ausgeschlossen, dass ein Remote-Administrator als Innentäter sich selbst als Client konfiguriert und somit dauerhaft remote mittels der Identität der jeweiligen LEI auf die TI und ihre Fachdienste zugreifen kann (bspw. ePA).

Der Remote-Administrator darf keinen Zugriff auf die SOAP/CETP-Schnittstellen haben (Ausschluss durch Netzwerk und/oder Authentifizierung)

Die Rolle entspricht dem bisherigen Remote-Administrator bei Einboxkonnektoren. Die Rolle ist optional.

4.6 Leistungserbringer

Fachlicher Nutzer einer konkreten HSK-Instanz, Inhaber einer SMC-B-Identität.

4.7 Rollenausschüsse

Rollenkombination und -ausschlüsse

nicht relevant	erlaubt	erlaubt mit Bedingungen	verboten

	Infrastruktur-betreiber	Reseller	Hersteller	lokaler Admin/ DVO	remote Admin	Leistungs-erbringer	
Infrastruktur-betreiber			im gleichen Unternehmen aber personell getrennt				Infrastruktur-betreiber
Reseller				wenn != Inf.str.betr. && zusätzliche Maßnahmen*			Reseller
Hersteller	im gleichen Unternehmen aber personell getrennt						Hersteller
lokaler Admin / DVO		wenn != Inf.str.betr. && zusätzliche Maßnahmen*					lokaler Admin / DVO
remote Admin							remote Admin
Leistungs-erbringer							Leistungs-erbringer
	Infrastruktur-betreiber	Reseller	Hersteller	lokaler Admin/ DVO	remote Admin	Leistungs-erbringer	

* Durchsetzen beim Infrastrukturbetreiber: Zugriff auf Admin-Schnittstelle nur über LEI-LAN

Abbildung 2 : Rollenkombination und -ausschlüsse

A_23237 - Rollenausschluss Infrastrukturbetreiber - DVO
Der Anbieter des TI-Gateways MUSS sicherstellen, dass der Infrastrukturbetreiber des TI-Gateways nicht als lokaler Administrator von HSK-Instanzen des TI-Gateway tätig wird.**[<=]**

A_23238 - Personelle Trennung Hersteller - Infrastrukturbetreiber
Der Anbieter des TI-Gateways MUSS sicherstellen, dass keine Personen sowohl in der Herstellung des HSK und/oder des Zugangsmoduls als auch im Betrieb der Infrastruktur arbeiten.**[<=]**

A_23239 - Zusätzliche Maßnahmen für Reseller als lokaler Administrator
Der Anbieter des TI-Gateway MUSS sicherstellen, dass der Reseller nur dann lokale Konfigurationsaufgaben (Administration von HSK-Instanzen) übernimmt, wenn

- die Rollen Reseller und Infrastrukturbetreiber von unterschiedlichen Firmen und Personen geleistet werden und
- der Infrastrukturbetreiber technisch durchsetzt, dass die lokale Administration nur aus dem Netz des Leistungserbringers erbracht werden kann.

[<=]

4.8 Umsetzung des Rollenmodells

Die Umsetzung des Rollenmodells muss durch das Zusammenwirken von technischen und organisatorischen Maßnahmen erreicht werden. Dabei werden folgende Ziele verfolgt:

(a) Der Leistungserbringer soll festlegen, wer sein System administriert. Er soll die Administrationsrechte auch einfach wieder entziehen können.

(b) Der Zugang zur Administration soll über zwei Stufen abgesichert werden

z.B. Netzwerkzugang (z.B. aus dem LE-LAN) + Authentifizierung des Administrators

Der Netzwerkzugang wird durch das TI-GW-Zugangsmodul gesteuert. Für die Authentifizierung des Administrators muss der Betreiberausschluss gewährleistet sein, z.B. indem sie direkt durch die HSK-Instanz durchgeführt wird.

(c) Der Betreiberausschluss muss auch für die Authentifizierungsdaten der Administratoren gewährleistet sein.

Für die technische Umsetzung sind unterschiedliche Ansätze möglich.

(1) Nutzung der Administratorauthentifizierung der HSK-Instanz. Ein Administrator verbindet sich aus dem LE-Netz direkt mit dem Administrationsendpunkt der zugeordneten HSK-Instanz, der Zugriff ist nur aus dem LE-Netz möglich. Der LE ermöglicht einem Dienstleister Zugriff, indem er ihm Zugang zu seinem Netz gewährt.

(2) Umsetzung des Berechtigungsmodells im Zugangsmodul. Die Administrations-GUI wird dabei im Zugangsmodul umgesetzt, welches auch die Zugriffsrechte durchsetzt. Das JSON-Administrationsinterface der HSK-Instanzen ist mit vollen Rechten mit dem Zugangsmodul verbunden, eine Administration ohne das Zugangsmodul ist ausgeschlossen. Zugang zum Administrationsinterface im Zugangsmodul ist ausschließlich über VPN aus dem LE-Netz oder über VPN aus dem Netz eines angeschlossenen Dienstleisters möglich. Der Leistungserbringer erteilt und entzieht den möglichen Zugang aus einem angeschlossenen DVO-Netz zu seiner Instanz über sein Portal. Die Administratorenauthentifizierung ist durch eine VAU vor dem Zugriff des Betreibers geschützt.

5 Spezifikation Zugangsmodul

5.1 Onboarding und Registrierung

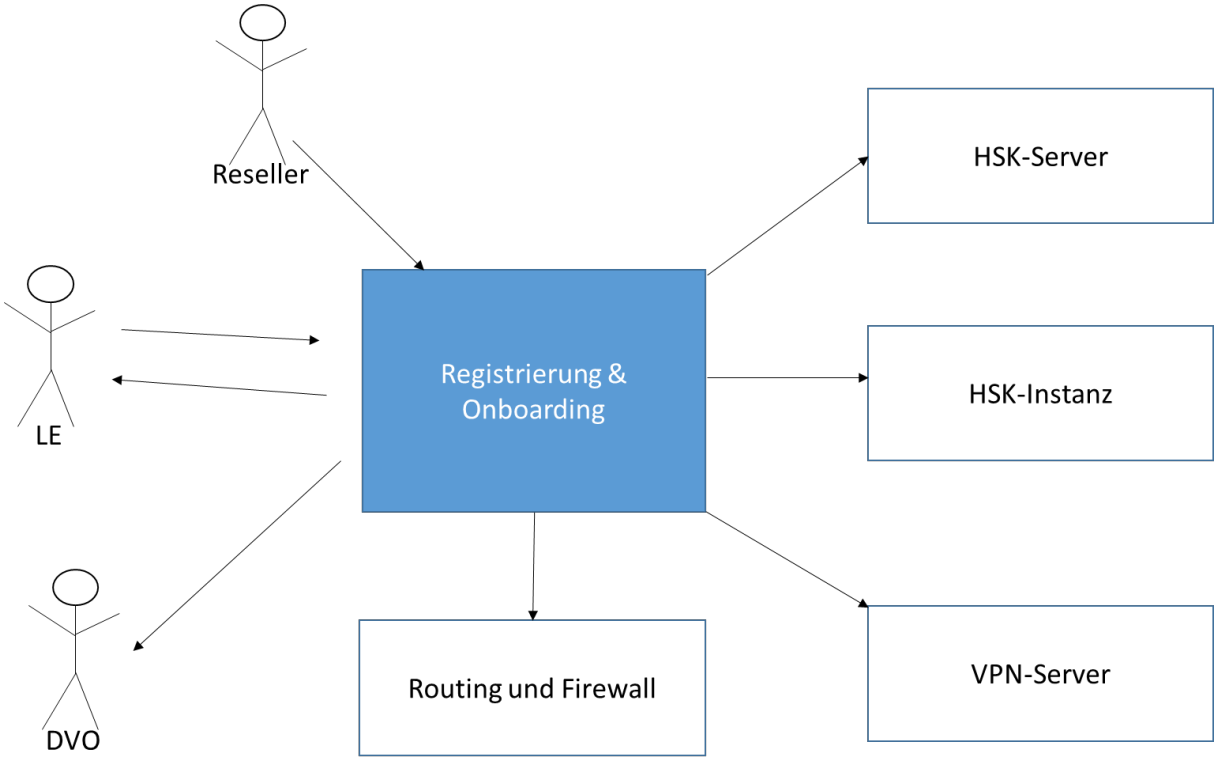


Abbildung 3 : Onboarding und Registrierung

Der Anwender soll von dem System durch den Registrierungs- und Onboardingprozess geführt werden. Der Prozess soll in der Regel ohne Intervention eines Administrators auf Seiten des TI-Gateways durchgeführt werden.

Der Reseller oder im Falle einer Selbstregistrierung der Leistungserbringer startet den Registrierungsprozess.

Der Leistungserbringer richtet eine Zwei-Faktor-Authentisierung (2FA) für seinen Zugang ein.

Nach erfolgreicher Registrierung erfolgt das Onboarding:

1. Das Onboarding-Modul löst am HSK-Server die Erzeugung einer HSK-Instanz aus. Darauf erhält das Onboarding-Modul die virtuelle IP-Adresse der HSK-Instanz und das initiale Admin-Passwort.

2. Das Onboarding-Modul generiert die benötigten VPN-Profile mit Credentials und der Inner-IP für die LE-Umgebung.

3. Das Onboarding-Modul konfiguriert den VPN-Server und das Routing für diese LE-Umgebung zu der zugehörigen HSK-Instanz. Wenn ein über VPN angeschlossener DVO auf die HSK-Instanz zugreifen soll, gibt der LE diesen Netzwerkzugriff frei.

4. Der Nutzer oder sein DVO lädt die Zugangsdaten für die initiale Einrichtung aus dem Onboarding-Modul. Er richtet die lokale Umgebung inkl. des VPN-Clients ein. Über den eingerichteten VPN-Kanal konfiguriert er die HSK-Instanz. Dabei prüft der DVO zunächst das HSK-AK.AUT-Zertifikat. Anschließend ändert der DVO das Passwort zum Administrations-Zugang der Instanz, prüft auf ein "sauberes" (= leeres) Informationsmodell und erzeugt oder importiert eine individuelle TLS-Identität für die Instanz, welche dann in den Clients verteilt wird. Somit kann später bei jeder Server-Authentifizierung konkret die Instanz der LEI verifiziert werden (statt nur der HSK). Ansätze zur Authentifizierung der konkreten HSK-Instanz über eigene AK.AUT-Identitäten pro Instanz sind ebenso zulässig. Der DVO richtet initial mindestens das Informationsmodell für ein Kartenterminal mit einer SMC-B ein.

5. Das Onboarding-Modul prüft die SMC-B (Nutzung SMC-B über KT und HSK-Instanz; ggf. lokale Onboarding-Softwarekomponente notwendig, welche die Aufrufe der Konnektor-Operation steuert). Im Falle einer gültigen SMC-B schaltet das Onboarding-Modul das Routing aus dem LE-Netz zu WANDA und offenen Fachdiensten frei.

5.1.1 Nutzerportal

A_23241 - Nutzer-Portal für Leistungserbringer
Das Zugangsmodul MUSS ein Nutzer-Portal zur Interaktion des Leistungserbringers mit dem TI-Gateway bereitstellen, welches über eine Verbindung mit prüfbarerer Authentizität des Servers und Schutz der Vertraulichkeit und Integrität erreicht wird. Wird das Nutzer-Portal über einen Web-Browser erreicht, MUSS es sich mit einem Extended Validation TLS-Zertifikat eines Herausgebers gemäß [CAB Forum] authentisieren und OCSP-Stapling [RFC-6066] umsetzen.**[**<=**]**

Das Zugangsmodul kann eine lokale Softwarekomponente umfassen. Das Zugangsmodul interagiert mit dem HSK über einen technischen User mit der Rolle Zugangsmodul.

A_23242 - TI-Gateway Zugangsmodul - Zwei-Faktor-Authentifizierung für Leistungserbringer
Das Zugangsmodul MUSS den Leistungserbringer mit zwei Faktoren authentifizieren.**[**<=**]**

Grundsätzlich gibt es keine Einschränkung bei den Verfahren, es sollen jedoch wann immer möglich, moderne Verfahren verwendet werden. So ist bspw. der Einsatz von SMS als zweiter Faktor aktuell nicht untersagt, kann jedoch ggf. zukünftig nicht mehr zulässig sein.

A_23338 - TI-Gateway Zugangsmodul - Schutz der Zugangsdaten
Das Zugangsmodul MUSS die Zugangsdaten/-faktoren der Nutzer (Leistungserbringer) geschützt vor unberechtigter Kenntnisnahme und Manipulation - auch von Administratoren - speichern und Änderungen dieser nur nach erfolgreicher Zwei-Faktor-Authentisierung zulassen.**[**<=**]**

A_23339 - TI-Gateway Zugangsmodul - Maßnahmen bei vergessenen oder verlorenen Zugangsfaktoren
Wenn das Zugangsmodul Maßnahmen zum Zurücksetzen von Zugangsfaktoren implementiert, DARF es NICHT die Sicherheit der Zwei-Faktor-Authentisierung aushebeln.**[**<=**]**

Dies kann bspw. über eine registriertes E-Mail-Konto des Nutzers geschehen, sofern dieses in dem Sinne als dritter Faktor fungiert, also nicht bereits in die 2FA eingebunden ist.

A_23363 - TI-Gateway Zugangsmodul - Freischaltung von HSK-Instanzen für Nutzer
Das Zugangsmodul MUSS durchsetzen, dass HSK-Instanzen erst erzeugt werden, wenn diesbezüglich ein Vertrag mit einem Reseller abgeschlossen wurde (Freigabe durch Reseller).**[<=]**

A_23353 - TI-Gateway Zugangsmodul - Erzeugung HSK-Instanz und VPN-Profil
Das Zugangsmodul MUSS für registrierte Nutzer folgendes erzeugen und für den Nutzer bereithalten:

- Eine oder mehrere HSK-Instanzen - entsprechend der Freigabe des Resellers - am HSK des TI-Gateway, wobei als Rückgabeparameter das initiale Passwort für den Instanz-Administrator und die Routinginformationen für die jeweilige Instanz erhalten wird.
- Ein VPN-Profil bestehend aus Daten, die für den Aufbau der VPN-Verbindung notwendig sind. (bspw. Client-Schlüssel und -Zertifikat, Informationen zu Adressierung und Routing, Vertrauensanker zur Authentifizierung des VPN-Konzentrators durch den Client).

[<=]

A_23281 - Schutz der privaten Schlüssel der VPN-Clientauthentifizierung und initialer Passwörter
Das Zugangsmodul MUSS das VPN-Profil eines Nutzers sowie das initiale Instanz-Administrator-Passwort ausschließlich an den authentifizierten Nutzer (Leistungserbringer) oder an den authentifizierten DVO, der vom Nutzer ausgewählt wurde, zustellen. Die privaten Schlüssel für die VPN-Clientauthentifizierung und das initiale Instanz-Administrator-Passwort MÜSSEN vor dem unberechtigten Zugriff und Manipulation - auch von Administratoren beim Zugangsmodul - geschützt sein, wobei dies neben organisatorischen Maßnahmen auch durch technische Maßnahmen unterstützt sein muss. So ist bspw. eine persistente Speicherung im Klartext und ohne Maßnahmen zum Erkennen von Änderungen unzulässig.**[<=]**

Es ist zulässig, dass DVOs über ein VPN an das TI-Gateway angeschlossen werden und nach Freigabe durch den LE als Administrator auf die HSK-Instanz des LE zugreifen. (Siehe 5.3 Routing und Firewall)

A_23385 - TI-Gateway Zugangsmodul - Sichere Übermittlung VPN-Profil an DVOs
Das Zugangsmodul MUSS das VPN-Profil eines DVOs vertraulich und integer an den authentifizierten DVO übermitteln. Dies muss jedoch nicht zwingend über das selbe Nutzerportal geschehen wie für Leistungserbringer.**[<=]**

A_23243 - Netzzugang zur TI nach SMC-B Prüfung
Das Zugangsmodul MUSS die SMC-B der LE-Institution inkl. Besitz des privaten Schlüssels und Online-Sperrstatus prüfen bevor es die Netzwerkverbindung zu WANDA und offenen Fachdiensten freigibt. Für diese Authentisierung wird die Identität HCI.AUT verwendet.**[<=]**

A_23340 - TI-Gateway Zugangsmodul - Beschreibung Authentifizierung HSK-Instanz
Der Anbieter TI-Gateway MUSS seinen Nutzern (Leistungserbringer bzw. deren DVO) Informationen zur Hand geben, dass beim Verbindungsaufbau zur HSK-Instanz deren Authentizität überprüft werden muss und wie dies möglich ist. Dies umfasst mindestens

- die technische Prüfung des Zertifikats C.AK.AUT des HSK auf Gültigkeit (inkl. Online-Sperrstatus) und gegen das entsprechende Komponenten-CA-Zertifikat [GEM.KOMP-CAX.der] vom TSL-Downloadpunkt (https://download.tsl.ti-dienste.de/SUB-CA/) bei Verbindungsaufbau für administrative Zugriffe,
- die organisatorische Prüfung, dass beim Download der TSL bzw. des Komponenten-CA-Zertifikats der Browser eine sichere Verbindung anzeigt und das TLS-Server-Zertifikat des TSL-Downloadpunkts auf die gematik GmbH ausgestellt ist,
- die Verifizierung, dass das Informationsmodell der HSK-Instanz leer/unkonfiguriert ist bei der Ersteinrichtung,
- Import der individuellen HSK-Instanz-Identität in die "Allowlist" der Clientsysteme
  - entweder durch die Erzeugung oder den Import einer HSK-Instanz-individuellen Server-Identität
  - oder durch die Nutzung der AK.AUT-Identitäten sofern diese HSK-Instanz-individuell sind, also genau eine AK.AUT-Identität immer genau einer HSK-Instanz zugeordnet ist.

[<=]

Die technische Prüfung des C.AK.AUT kann bei Nutzung eines Webbrowsers bspw. durch Import des Komponenten-CA-Zertifikats in den Browser und die Konfiguration einer zwingenden OCSP-Prüfung erreicht werden, wobei die Beschreibung deutlich darauf hinweisen soll, dass hierfür ein gesonderter Browser verwendet werden muss, also gerade keine Zertifikate aus anderen Vertrauensräumen in den Standard-Browser des Nutzers importiert werden sollen. Die Beschreibungen sollen zudem gerade nicht ein Nutzerverhalten des ständigen Akzeptierens von Ausnahmen/Sicherheitswarnungen erwirken.

A_23341 - TI-Gateway Zugangsmodul - Authentifizierung HSK-Instanz
Das Zugangsmodul MUSS, wenn es für die initiale Verbindung eines Nutzers zu seiner HSK-Instanz eine Client-Software bereitstellt, das Zertifikat C.AK.AUT des HSK auf Gültigkeit (inkl. Online-Sperrstatus) und gegen das entsprechende Komponenten-CA-Zertifikat GEM.KOMP-CAX. der vom TSL-Downloadpunkt (https://download.tsl.ti-dienste.de/SUB-CA/) in der Client-Software verifizieren lassen.**[<=]**

A_18733-02 - Prüfung zugelassener Produkte bei Verbindung zur TI
Das Zugangsmodul MUSS täglich prüfen, ob nicht zugelassene Produkte (eHealth-Kartenterminals) mit dem TI-Gateway verbunden sind.**[<=]**

Dieses kann über die Betriebsdaten der HSK-Instanz realisiert werden.

A_18734-01 - Informationspflicht zu Leistungserbringern
Der Anbieter TI-Gateway MUSS die jeweiligen über seinen Dienst angebundenen Leistungserbringer unverzüglich bei Verbindungen von nicht-zugelassenen Produkten schriftlich über den Sachverhalt informieren.**[<=]**

Die Information sollte so ausgestaltet werden, dass nachvollzogen werden kann, dass die Information den Nutzer auch erreicht hat. z.B. indem die Information über das Nutzer-Portal erfolgt und dort geprüft wird, ob der Nutzer die Information auch abgerufen hat.

5.1.2 Betriebsfunktionen für den Leistungserbringer

A_23302 - Anzeige Verfügbarkeit und Service Level

Der Produkttyp TI-Gateway-Zugangsmodul MUSS dem Leistungserbringer die aktuelle Verfügbarkeit des Services und die erreichten Werte für die Service-Level zur Verfügbarkeit anzeigen.**[**<=**]**

Umgesetzt werden kann diese Anforderung über das Nutzer-Portal oder über eine lokale Softwarekomponente. Bei einer lokalen Softwarekomponente muss die Internet-Verfügbarkeit mit überwacht werden, um nicht die Verfügbarkeit der TI-Gateway Services zu verzerren. Als Indikator für die Verfügbarkeit des TI-GW kann die Operation getRessourceInformation verwendet werden. Für die Anzeige des aktuellen Betriebsstatus sollte die Erreichbarkeit aller Kartenterminals und der Freischaltstatus der SMC-B mit einbezogen werden.

5.2 VPN

Der VPN-Service des TI-Gateway-Zugangsmoduls ermöglicht es Leistungserbringerumgebungen eine VPN-Verbindung zum TI-Gateway aufzubauen. Es sind unterschiedliche VPN-Lösungen und -Clients erlaubt, solange sie den folgenden Sicherheits-Mindestanforderungen genügen.

A_23351 - TI-Gateway-Zugangsmodul - Verbindungen ausschließlich über VPN
Das Zugangsmodul MUSS sicherstellen, dass Verbindungen zur Nutzung von HSK-Instanzen des HSK des TI-Gateways ausschließlich über einen VPN-Kanal akzeptiert werden.**[**<=**]**

A_23379 - TI-Gateway-Zugangsmodul - VPN - Protokoll
Das Zugangsmodul MUSS Nutzer mittels eines VPN-Kanals anbinden, welcher auf den Protokollen IPsec/IKEv2 oder WireGuard beruht und dafür VPN-Server und VPN-Client bereitstellen.**[**<=**]**

Als VPN-Protokolle sind aktuell IPsec/IKEv2 oder WireGuard vorgesehen. Andere Protokolle sind nicht grundsätzlich ausgeschlossen, müssen jedoch mit der gematik abgestimmt werden. In Bezug auf das WireGuard-Protokoll siehe auch:

- "Whitepaper Wire Guard" https://www.wireguard.com/papers/wireguard.pdf
- "Mechanised Cryptographic Proof" https://hal.inria.fr/hal-02100345v3/document

A_23375 - TI-Gateway-Zugangsmodul - VPN - Authentisierung
Das Zugangsmodul MUSS für den VPN-Kanal eine zwingende beidseitige Authentisierung am Server und Client durchsetzen, wobei jeweils sowohl die eigene Authentisierung als auch die Authentifizierung des Gegenübers mindestens anhand statischer asymmetrische Schlüsselpaare stattfinden muss und dabei für die Schlüsselpaare asymmetrische Algorithmen aus der Menge {RSA3072, ECC-NIST-P-256, ECC-Brainpool256r1, ECC-Curve25519} verwendet werden müssen.**[**<=**]**

A_23376 - TI-Gateway-Zugangsmodul - VPN - Transportschutz
Das Zugangsmodul MUSS für den VPN-Kanal am Server und am Client einen Transportschutz für alle übermittelte Daten bzgl. Vertraulichkeit und Integrität durchsetzen unter Verwendung symmetrischer Chiffren aus der Menge {AES128, AES256, ChaCha20Poly1305}.**[**<=**]**

A_23377 - TI-Gateway-Zugangsmodul - VPN - Ephemere Sitzungs-Schlüssel
Das Zugangsmodul MUSS für den VPN-Kanal Forward-Secrecy Server- und Client-seitig durchsetzen mit ephemeren ECDH-Schlüsseln aus der Menge {ECC-NIST-P-256, ECC-Brainpool256r1, ECC-Curve25519}.**[<=]**

A_23378 - TI-Gateway-Zugangsmodul - VPN - Hash-Funktionen
Das Zugangsmodul MUSS für alle im Rahmen des Aufbaus und Betriebs des VPN-Kanals notwendigen Hashwertberechnungen Hashfunktionen aus der Menge {SHA256, BLAKE2s} im Server und im Client verwenden.**[<=]**

A_23380 - TI-Gateway-Zugangsmodul - VPN - Prüfung Sperrstatus Clients
Das Zugangsmodul MUSS bei der Client-Authentifizierung durch den Server im Rahmen des VPN-Verbindungsaufbau den Sperrstatus der Client-Identität prüfen (Vergleich A_23261*).**[<=]**

A_23381 - TI-Gateway-Zugangsmodul - VPN - Abbruch Verbindungsaufbau im Fehlerfall
Das Zugangsmodul MUSS durchsetzen, dass sowohl im Server als auch im Client, wenn Fehler im Rahmen der beidseitigen Authentisierung oder des Schlüsselaustauschs auftreten, jeweils ein Abbruch des Verbindungsaufbaus stattfindet.**[<=]**

A_23364 - TI-Gateway-Zugangsmodul - VPN-Client - Server-Authentifizierung
Der VPN-Client eines TI-Gateway-Zugangsmoduls MUSS den VPN-Server gegen eine ihm vorliegende Prüfbasis authentifizieren.**[<=]**

A_23365 - TI-Gateway-Zugangsmodul - VPN-Client - VPN-Protokoll
Der Hersteller des VPN-Client eines TI-Gateway-Zugangsmoduls MUSS das VPN-Protokoll im Client entsprechend A_23375*, A_23376*, A_23377*, A_23378*, A_23379* und A_23381* umsetzen und dies im Rahmen des Sicherheitsnachweis (Produktgutachten) mindestens durch entsprechende Tests inkl. Negativ-Testfälle im Blackbox-Ansatz verifizieren lassen.**[<=]**

Idealer Weise können bestehende Sicherheitsnachweis zum VPN-Client nachgenutzt werden.

A_23382 - TI-Gateway VPN-Client - Nutzerinformation
Der Anbieter des TI-Gateways MUSS seine Nutzer verständlich zum sicheren Umgang mit den privaten VPN-Client-Schlüsseln und zur korrekten Installation und Nutzung des VPN-Clients informieren.**[<=]**

A_23245 - VPN-Server Konfiguration durch Onboarding-Modul
Der VPN-Server des Zugangsmoduls MUSS ausschließlich Verbindungen annehmen, für die er vom Onboarding-Modul ein VPN-Profil erhalten hat.**[<=]**

5.3 Routing und Firewall

A_23246 - Routing zur zugewiesenen HSK-Instanz

Das TI-GW-Zugangsmodul MUSS sicherstellen, dass eine LE-Institution nur die Interfaces der ihr zugewiesenen HSK-Instanz erreichen kann.**[<=]**

A_23370 - Routing zum Administrationsinterface einer HSK-Instanz
Das TI-GW-Zugangsmodul MUSS sicherstellen, dass das Administrationsinterface einer HSK-Instanz nur aus dem Netz der zugeordneten LE-Institution und einem möglicherweise vom Leistungserbringer freigegebenen DVO-Netz möglich ist.**[<=]**

A_23394 - Routing zum fachlichen Interface einer HSK-Instanz
Das TI-GW-Zugangsmodul MUSS sicherstellen, dass das fachliche Interface (SOAP, LDAP, CETP) einer HSK-Instanz nur aus dem Netz der zugeordneten LE-Institution möglich ist - also auch explizit nicht aus einem möglicherweise vom Leistungserbringer für die Administration freigegebenen DVO-Netz.**[<=]**

A_23371 - DVO-Netzzugang entziehen
Das TI-GW-Zugangsmodul MUSS es einem Leistungserbringer ermöglichen, den Zugang zum Administrationsinterface aus einem DVO-Netz auch wieder zu entziehen.**[<=]**

5.4 Sicherheit & Datenschutz

TIP1-A_5389-01 - TI-GW-Zugangsmodul, zyklische Prüfung der C.HCI.AUT Zertifikate
Das Zugangsmodul MUSS die Gültigkeit (inkl. Online-Sperrstatus) aller bei ihm im Rahmen der Registrierung (siehe A_23243*) verwendeten C.HCI.AUT (SM-B-AUT-Zertifikat) einmal täglich prüfen.
[<=]

TIP1-A_5390-01 - TI-GW-Zugangsmodul, gesperrtes C.HCI.AUT Zertifikat
Das Zugangsmodul MUSS, wenn die zyklische Prüfung ergeben hat, dass das C.HCI.AUT (SM-B-AUT-Zertifikat) nicht mehr gültig ist, das mit diesen Zertifikaten assoziierten Routing zu offenen Fachdiensten und Wanda unverzüglich entfernen und den Leistungserbringer benachrichtigen. Die Anzahl der auf diese Weise gesperrten Zugänge muss an die gematik reported werden.**[<=]**

A_23248 - DDOS-Protection
Das TI-GW-Zugangsmodul MUSS Angriffe auf die Verfügbarkeit des TI-Gateways an seinen Schnittstellen zum Internet abwehren.**[<=]**

A_23249 - Abwehr unberechtigter Zugriffe
Das TI-GW-Zugangsmodul MUSS Maßnahmen zur Abwehr unberechtigter Zugriffe aus dem Internet sowie aus angeschlossenen LEI- und DVO-Netzen umsetzen (IDS/IPS).**[<=]**

Auch aus per VPN angeschlossenen Netzen von Leistungserbringerinstitutionen sowie ggf. DVOs dürfen nur erlaubte Kommunikationen/Protokolle/Funktionen möglich sein. Insbesondere kann vor der Prüfung der SMC-B nicht sicher davon ausgegangen werden, dass tatsächlich Leistungserbringer über einen VPN-Kanal mit dem TI-Gateway interagieren.

A_23392 - Sperrung VPN-Zugänge bei detektierten Angriffen
Das TI-GW-Zugangsmodul MUSS, wenn über Netze von angeschlossenen Nutzern (LEI/DVO) Angriffe detektiert werden, Maßnahmen bis hin zur Sperrung der betroffenen VPN-Zugänge umsetzen und die Nutzer dieser Zugänge unverzüglich darüber informieren.**[<=]**

A_23393 - Prozesse zur schnellen Kommunikation und Entsperrung von VPN-Zugängen
Der Anbieter TI-Gateway MUSS Prozesse zur Behandlung und Klärung erkannter Angriffe aus Nutzer-Netzen etablieren, sodass eine schnelle Kommunikation mit betroffenen Kunden sowie ggf. Entsperrung der Zugänge möglich ist, sofern keine sicherheitstechnischen Bedenken mehr bestehen.**[<=]**

TIP1-A_4338-01 - TI-GW-Zugangsmodul, Sicherung zum Transportnetz Internet durch Paketfilter
Das TI-GW-Zugangsmodul MUSS das TI-Gateway zum Transportnetz Internet durch einen zustandslosen Paketfilter (ACL) absichern, welcher ausschließlich die erforderlichen Protokolle weiterleitet. Der Paketfilter MUSS frei konfigurierbar sein auf der Grundlage von Informationen aus OSI Layer 3 und 4, das heißt Quell- und Zieladresse, IP-Protokoll sowie Quell- und Zielport.**[<=]**

TIP1-A_4339-01 - TI-GW-Zugangsmodul, Platzierung Paketfilters Internet
Der Paketfilter des TI-GW-Zugangsmoduls zum Schutz der VPN-Konzentratoren in Richtung Transportnetz Internet DARF NICHT auf den VPN-Konzentratoren implementiert werden.**[<=]**

A_23342 - TI-GW-Zugangsmodul - Richtlinien für den Paketfilter zum Internet
Der Paketfilter des TI-GW-Zugangsmoduls MUSS die Weiterleitung von IP-Paketen an der Schnittstelle zum Internet auf genau die Protokolle beschränken, die für die verwendete VPN-Technologie zwingend erforderlich sind. Ein Verbindungsaufbau aus dem TI-GW-Zugangsmodul in Richtung Internet MUSS unterbunden werden.**[<=]**

TIP1-A_4292-01 - TI-GW-Zugangsmodul, Härtung des VPN-Konzentrators
Die VPN-Konzentratoren des Zugangsmoduls MÜSSEN so konfigurieren werden, dass ausschließlich die erforderlichen Netzwerkprotokolle und kryptographischen Methoden akzeptiert werden.**[<=]**

A_23343 - TI-GW-Zugangsmodul - Kein direkter Zugriff auf zentrale Dienste und gesicherte Fachdienste
Das TI-GW-Zugangsmodul MUSS einen direkten Zugriff aus dem Internet und den Netzen angeschlossener Nutzer auf gesicherte Fachdienste und zentrale Dienste verhindern.
[<=]

A_23344 - TI-GW-Zugangsmodul - Verbindungen bei Komponentenausfall beenden
Das TI-GW-Zugangsmodul MUSS sicherstellen, dass alle bestehenden VPN-Verbindungen beendet werden und keine neuen Verbindungen zugelassen werden, wenn nachgelagerte Komponenten vollständig ausgefallen sind und dadurch die Nutzung des TI-Gateways nicht mehr möglich ist.**[<=]**

A_23345 - TI-GW-Zugangsmodul - Härtung Zugänge
Das TI-GW-Zugangsmodul MUSS sicherstellen, dass es ausschließlich definierte und gehärtete Schnittstellen anbietet - auch für die Administration - ohne Low-Level-Zugänge mit Systemrechten.**[<=]**

A_23366 - TI-GW-Zugangsmodul - Nutzung HSM

Das TI-GW-Zugangsmodul MUSS geheime Schlüssel in einem nach FIPS 140-2 Level 3 oder Common Criteria EAL 4 zertifizierten HSM erzeugen und dort so vor Zugriff geschützt speichern, dass nur das TI-GW-Zugangsmodul selbst die Schlüssel nutzen kann. Dies bezieht sich mindestens auf folgende Schlüssel:

- Private Schlüssel von VPN-Konzentratoren
- Geheime Schlüssel zur Authentisierung gegenüber dem HSK
- Schlüssel zum Schutz von Vertraulichkeit und Integrität persistent gespeicherter Daten

[<=]

A_23390 - TI-Gateway-Zugangsmodul - Eigene HSK-Instanz pro Kunde
Das TI-GW-Zugangsmodul MUSS jedem Nutzer seine eigene virtuelle HSK-Instanz zuweisen, sodass nie unterschiedliche Nutzer die selbe HSK-Instanz verwenden.**[<=]**

Möchten Leistungserbringer bspw. in Gemeinschaftspraxen oder MVZ bewusst eine einzige HSK-Instanz verwenden, müssen die verschiedenen LEI als ein Nutzer ggü. dem TI-GW auftreten, wie dies heute bereits bei der Verwendung eines Konnektors durch mehrere LEI ggü. dem VPN-Zugangsdienst notwendig ist. Die Nutzung mehrerer Instanzen durch einen einzigen Nutzer ist problemlos, solange die Nutzung jeder Instanz entsprechend A_23390* exklusiv durch diesen Nutzer stattfindet.

A_23354 - TI-Gateway-Zugangsmodul - Kopplung HSK, Prüfung I.AK.AUT des HSK
Das Zugangsmodul in einem TI-Gateway MUSS bei der beidseitigen Authentisierung mit dem HSK die Identität I.AK.AUT des HSK prüfen und seine eigenen Client-Credentials hinsichtlich Vertraulichkeit und Integrität geschützt speichern.**[<=]**

A_23355 - TI-Gateway-Zugangsmodul - Kopplung HSK, Geschützte Speicherung Client-Credentials
Das Zugangsmodul in einem TI-Gateway MUSS seine eigenen Client-Credentials hinsichtlich Vertraulichkeit und Integrität geschützt speichern.**[<=]**

A_23362 - TI-Gateway-Zugangsmodul - Kopplung HSK, Geschützter Import Client-Credentials
Der Anbieter TI-Gateway MUSS einen sicheren Prozess zur Erzeugung und/oder Import der Client-Credentials des Zugangsmoduls für die Verbindung zum HSK etablieren, der die Vertraulichkeit und Integrität der Client-Credentials wahrt und gewährleistet, dass Client-Credentials nicht dauerhaft außerhalb des Zugangsmoduls oder HSK vorliegen.**[<=]**

Die Administration des Zugangsmoduls lässt somit nur den Import der Client-Credentials zu, nicht jedoch das Auslesen dieser.

A_23261 - Sperrbarkeit von Institutionen
Der Anbieter TI-Gateway und das Zugangsmodul MÜSSEN über organisatorische und technische Maßnahmen verfügen, um einzelne angeschlossene Institutionen vom Zugang zur TI auszuschließen, unter anderem auch auf Weisung der gematik.**[<=]**

Die gematik muss den Zugang von Leistungserbringerinstitutionen bspw. für den Fall der Verwendung veralteter, schwachstellenbehafteter Versionen anderer TI-Komponenten sperren lassen können, da solche Komponenten eine Bedrohung für die gesamte TI darstellen können.

TIP1-A_5048-01 - TI-GW-Zugangsmodul, Schlüssel sicher speichern
Das TI-GW-Zugangsmodul MUSS geheime Schlüssel sicher speichern und unberechtigte Zugriffe darauf verhindern.**[<=]**

5.5 Rohdaten-Performance-Reporting

in [gemSpec_Perf#2.5.2] Rohdaten-Performance-Reporting (Rohdatenerfassung v.02)

Tabelle 1 : Tab_gemSpec_Perf_Produkte_Rohdatenerfassung_Version_v02

PDT	Produkttyp
PDT72	TI-Gateway-Zugangsmodul

Die Zuweisungen der Anforderungen zu dem Produkttypen TI-Gateway-Zugangsmodul sowie zu dem entsprechenden Anbietertypen werden wie folgt vorgenommen:

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

hinzufügen der Zuordnung zu Anbietertyp: Anb_TI_Gateway - org./betriebl. Eignung: Prozessprüfung

A_22482 - Performance - Rohdaten - Erfassung von Rohdaten (Rohdatenerfassung v.02)

hinzufügen der Zuordnung zu Produkttyp: TI-Gateway-Zugangsmodul - funkt. Eignung: Test Produkt/FA

5.5.1 Umfang

A_22002 - Performance - Rohdaten - Übermittlung (Rohdatenerfassung v.02)

hinzufügen der Zuordnung zu Produkttyp: TI-Gateway-Zugangsmodul - funkt. Eignung: Test Produkt/FA

A_22000 - Performance - Rohdaten - zu liefernde Dateien (Rohdatenerfassung v.02)

hinzufügen der Zuordnung zu Produkttyp: TI-Gateway-Zugangsmodul - funkt. Eignung: Test Produkt/FA

A_22429 - Performance - Rohdaten - Inhalt der Selbstauskunft (Rohdatenerfassung v.02)

hinzufügen der Zuordnung zu Produkttyp: TI-Gateway-Zugangsmodul - funkt. Eignung: Test Produkt/FA

A_22004 - Performance - Rohdaten - Korrektheit (Rohdatenerfassung v.02)

hinzufügen der Zuordnung zu Produkttyp: TI-Gateway-Zugangsmodul - funkt. Eignung: Test Produkt/FA

A_22005 - Performance - Rohdaten - Frist für Nachlieferung (Rohdatenerfassung v.02)

hinzufügen der Zuordnung zu Produkttyp: TI-Gateway-Zugangsmodul - funkt. Eignung: Herstellererklärung

A_22003-01 - Performance - Rohdaten - Nachlieferung auf Anforderung (Rohdatenerfassung v.02)

hinzufügen der Zuordnung zu Anbietertyp: Anb_TI_Gateway - org.-betr.: Anbietererklärung

A_22996 - Performance - Rohdaten - Zeitpunkte der Übermittlungen (Rohdatenerfassung v.02)

hinzufügen der Zuordnung zu Anbietertyp: Anb_TI_Gateway - org.-betr.: Anbietererklärung

5.5.2 Lieferintervalle

A_21976 - Performance - Rohdaten - Konfigurierbarkeit der Lieferintervalle (Rohdatenerfassung v.02)

hinzufügen der Zuordnung zu Produkttyp: TI-Gateway-Zugangsmodul - funkt. Eignung: Test Produkt/FA

A_22047 - Performance - Rohdaten - Änderung der Konfiguration der Lieferintervalle (Rohdatenerfassung v.02)

hinzufügen der Zuordnung zu Produkttyp: TI-Gateway-Zugangsmodul - funkt. Eignung: Test Produkt/FA

A_22620 - Rohdaten - Umsetzungszeit für Änderung der Lieferintervalle

hinzufügen der Zuordnung zu Anbietertyp: Anb_TI_Gateway - org.-betr.: Anbietererklärung

A_21978 - Performance - Rohdaten - Trennung der Lieferintervalle (Rohdatenerfassung v.02)

hinzufügen der Zuordnung zu Produkttyp: TI-Gateway-Zugangsmodul - funkt. Eignung: Herstellererklärung

A_21975 - Performance - Rohdaten - Default-Werte für Lieferintervalle (Rohdatenerfassung v.02)

hinzufügen der Zuordnung zu Produkttyp: TI-Gateway-Zugangsmodul - funkt. Eignung: Test Produkt/FA

A_21979 - Performance - Rohdaten - Bezug der Lieferverpflichtung (Rohdatenerfassung v.02)

hinzufügen der Zuordnung zu Produkttyp: TI-Gateway-Zugangsmodul - funkt. Eignung: Herstellererklärung

A_21980 - Performance - Rohdaten - Leerlieferung (Rohdatenerfassung v.02)

hinzufügen der Zuordnung zu Produkttyp: TI-Gateway-Zugangsmodul - funkt. Eignung: Test Produkt/FA

5.5.3 Format

A_22001-01 - Performance - Rohdaten - Name der Berichte (Rohdatenerfassung v.02)

hinzufügen der Zuordnung zu Produkttyp: TI-Gateway-Zugangsmodul - funkt. Eignung: Test Produkt/FA

A_21981-02 - Performance - Rohdaten - Format des Rohdaten-Performance-Berichtes (Rohdatenerfassung v.02)

hinzufügen der Zuordnung zu Produkttyp: TI-Gateway-Zugangsmodul - funkt. Eignung: Test Produkt/FA

A_22500-01 - Performance - Rohdaten - Status-Block (Rohdatenerfassung v.02)

hinzufügen der Zuordnung zu Produkttyp: TI-Gateway-Zugangsmodul - funkt. Eignung: Test Produkt/FA

A_21982-01 - Performance - Rohdaten - Message-Block (Rohdatenerfassung v.02)

hinzufügen der Zuordnung zu Produkttyp: TI-Gateway-Zugangsmodul - funkt. Eignung: Test Produkt/FA

A_22513-01 - Performance - Rohdaten - Message-Block im Fehlerfall - JSON (Rohdatenerfassung v.02)

hinzufügen der Zuordnung zu Produkttyp: TI-Gateway-Zugangsmodul- funkt. Eignung: Test Produkt/FA

Neue Anforderungen in Kapitel "3.x.2.2 Format"

A_23269 - Performance - Rohdaten - TI-Gateway-Zugangsmodul - Duration (Rohdatenerfassung v.02)
Der Produkttyp TI-Gateway-Zugangsmodul MUSS bei Rohdaten-Performance-Berichten bzgl. der "duration_in_ms"-Felder die Hinweise der Spalte "Duration" aus Tabelle Tab_gemSpec_Perf_Berichtsformat_TI-Gateway-Zugangsmodul berücksichtigen.**[<=]**

Zuordnung zu Produkttyp: TI-Gateway-Zugangsmodul - Prüfverfahren funkt. Eignung: Test Produkt/FA

A_23270 - Performance - Rohdaten - TI-Gateway-Zugangsmodul - Operation (Rohdatenerfassung v.02)
Der Produkttyp TI-Gateway-Zugangsmodul MUSS bei Rohdaten-Performance-Berichten bzgl. der "operation"-Felder die Angabe der Spalte "Operation/Usecase" aus Tabelle Tab_gemSpec_Perf_Berichtsformat_TI-Gateway-Zugangsmodul berücksichtigen.**[<=]**

Zuordnung zu Produkttyp: TI-Gateway-Zugangsmodul - Prüfverfahren funkt. Eignung: Test Produkt/FA

Tabelle 2 : Tab_gemSpec_Perf_Berichtsformat_TI-Gateway-Zugangsmodul

Operation / Usecase	Duration
I_Secure_Channel_Tunnel::connect	Bei Aufruf der Operation beginnt die Messung mit Annahme der Aufrufnachricht an der Außenschnittstelle

	des Produkttyps und endet mit dem vollständigen Versenden der Antwortnachricht.
I_Secure_Channel_Tunnel::disconnect	-''-
I_DNS_Name_Resolution::get_IP_Address	-''-

809

5.6 Lastanforderungen

811 **GS-A_5545-01 - Performance – TI-Gateway-Zugangsmodul – VPN**
812 **Konfigurationseinstellungen**
813 Der Produkttyp TI-Gateway-Zugangsmodul DARF den VPN-Durchsatz pro
814 Leistungserbringerumgebung auf die vertraglich vereinbarte Bandbreite reduzieren.**[<=]**

6 Änderungen am Highspeed-Konnektor

Es sind Anpassungen am Produkt Highspeed-Konnektor notwendig, damit dieses innerhalb eines TI-Gateways verwendet werden kann. Entsprechend ist nachzuweisen, dass eine für die Verwendung im TI-Gateway vorgesehene Produkttypversion durch die genutzten HSKs umgesetzt ist.

A_23361 - TI-Gateway - Zulässige Produkttypversionen Highspeed-Konnektor
Der Anbieter TI-Gateway MUSS eine Highspeed-Konnektor-Version einsetzen, die für die Verwendung im TI-Gateway zugelassen ist.**[<=]**

Es sind Anpassungen an den Administratorrollen des HSK notwendig. Konkret ersetzt die folgende beiden Anforderung die Anforderungen A_21882 und A_21883 [gemF_Highspeed-Konnektor] für einen HSK, der innerhalb eines TI-Gateway genutzt wird.

A_23359 - Administration des HSK-Basis Systems
Der Highspeed-Konnektor MUSS ein Administrationsinterface für das Basissystem bereitstellen und folgende separate Administratoren-Rollen umsetzen:

- Hersteller (HSK-Basis)
  - Aktivierung der kryptographischen Kopplung zum SZZP-light-plus
  - Konfiguration des Schlüssels für die Verbindung zum SZZP-light-plus
  - Konfiguration der Kopplung zum HSM und Management HSM
  - Leserechte auf das Logging des Basissystems ohne die Logs der HSK-Instanzen
  - Nutzer mit Rolle "Hersteller" erzeugen/ändern/löschen
- Basissystem-Administrator
  - Verwaltung der instanzenübergreifenden HSK-Konfigurationen inkl. Einspielen Updates
  - Ressourcenkonfiguration von HSK-Instanzen
  - Leserechte auf das Logging des Basissystems ohne die Logs der HSK-Instanzen
  - Backup/Restore von HSK-Instanzen
  - Löschen von HSK-Instanzen
  - Nutzer mit Rolle "HSK-Admin" erzeugen/ändern/löschen
  - im technisch unterstützten 4 Augenprinzip Nutzer mit Rolle "Zugangsmodul" erzeugen/ändern/löschen
- Zugangsmodul (technischer user)
  - Erzeugen und löschen von HSK-Instanzen
  - Zuordnen von IP-Adressen zu Konnektor-Instanzen
  - Backup/Restore von HSK-Instanzen
  - Ressourcenkonfiguration von HSK-Instanzen

[<=]

TIP1-A_4810-02 - Benutzerverwaltung der Managementschnittstelle
HSK-Instanzen MÜSSEN eine Benutzerverwaltung für die Managementschnittstelle enthalten, in der anmeldeberechtigte Administratoren-Benutzer definiert werden können. Die Benutzerverwaltung MUSS die Administrator-Rollen Lokaler-Administrator, Remote-Administrator und Super-Administrator unterstützen.
Die Benutzerverwaltung kann weitere Rollen unterstützen.
Den Administrator-Rollen MÜSSEN folgende Rechte zugewiesen sein:

- Lokaler-Administrator:
  - ausschließlicher Zugriff über lokalen Endpunkt der Managementschnittstelle
  - Verwaltung aller Konfigurationsdaten und Durchführung aller Administratoraktionen mit Ausnahme von:
    - Benutzerverwaltung gemäß Tabelle TAB_KON_655
- Remote-Administrator:
  - ausschließlicher Zugriff über remote-Endpunkt der Managementschnittstelle
  - Verwaltung aller Konfigurationsdaten und Durchführung aller Administratoraktionen mit Ausnahme von:
    - Benutzerverwaltung gemäß Tabelle TAB_KON_655
    - Konfigurationseinstellungen und Administratoraktionen gemäß Tabelle TAB_KON_851
- Super-Administrator:
  - ausschließlicher Zugriff über lokalen Endpunkt der Managementschnittstelle
  - Benutzerverwaltung gemäß Tabelle TAB_KON_655
  - Verwaltung aller Konfigurationsdaten und Durchführung aller Administratoraktionen

Tabelle 3: TAB_KON_655 Konfigurationen der Benutzerverwaltung (Super-Administrator)

ReferenzID	Belegung	Bedeutung und Administrator-Interaktion
MGM_USER_LIST	Liste von Benutzernamen und deren Kontaktdaten	Liste von Benutzern und deren Kontaktdaten. Benutzerkonten MÜSSEN angelegt, geändert und gelöscht werden können. Das Passwort eines Benutzerkontos MUSS neu gesetzt werden können.
MGM_ADMIN_RIGHTS	Liste von Zugriffsrechten eines Benutzers	i. Eindeutige Zuordnung eines Benutzerkontos zu einer Rolle. Die Benutzerverwaltung MUSS sicherstellen, dass zu jeder Zeit mindestens ein Benutzerkonto mit der Rolle Super-Administrator vorhanden ist. Gewähren/Entziehen von Rechten für Benutzerkonten: ii. Zugriffsrechte bezüglich der Konfigurationsbereiche. iii. Recht zum Aufbau einer Remote-Management-Session und/oder zur

		Konfiguration des Remote-Management gemäß TAB_KON_663 (USER_INIT_REMOTESESSION). iv. Recht für einen Werksreset (USER_RESET_PERMISSION)

Die Benutzerverwaltung MUSS es jedem Benutzer ermöglichen Konfigurationsänderungen gemäß Tabelle TAB_KON_656 vorzunehmen:

Tabelle 4: TAB_KON_656 Konfigurationen der Benutzerverwaltung

ReferenzID	Belegung	Bedeutung und Administrator-Interaktion
MGM_USER_INFO	Kontaktdaten	Der angemeldete Benutzer MUSS seine Kontaktdaten ändern können. Der Benutzername DARF NICHT änderbar sein.

[<=]

A_23395 - Backup & Restore von Instanzen (Konfigurationsdaten)
Der Highspeed-Konnektor MUSS ein Backup und Restore der Konfigurationen seiner Instanzen ermöglichen, wobei die Backups entweder den HSK (und seine VAU) nicht verlassen oder mit Schlüsselmaterial des HSK hinsichtlich Vertraulichkeit und Integrität so geschützt sind, dass diese nicht unberechtigt eingesehen oder geändert werden dürfen. Unberechtigt ist jeder außer der Inhaber der Instanz (LEI) und der ggf. von ihm berechtigte DVO.**[<=]**

A_23397 - Sicherung und Wiederherstellung HSK-Basissystem
Der HSK MUSS eine Möglichkeit bieten, die Konfiguration des Basissystems zu sichern und wieder herzustellen.
[<=]

A_23360 - TI-Gateway - Kopplung Zugangsmodul und HSK
Der HSK in einem TI-Gateway MUSS das Zugangsmodul (bzw. Clients in der Rolle "Zugangsmodul") mittels eines beidseitig authentisierten und hinsichtlich Vertraulichkeit und Integrität geschützten Kanals anbinden, wobei der HSK seine Identität I.AK.AUT zur Server-Authentisierung nutzt.**[<=]**

A_23258 - Rollenausschlüsse Highspeedkonnektor
Der Highspeed-Konnektor MUSS folgende Einschränkungen bei der Zuordnung von Rollen zu Nutzern durchsetzen:

- Ein Nutzer mit der Rolle Hersteller darf keine andere Rolle haben.
- Ein Nutzer mit der Rolle Zugangsmodul darf keine andere Rolle haben.

[<=]

A_21853-01 - Feste Kopplung von Konnektor und SZZP
Der Konnektor MUSS eine kryptographische Kopplung mit dem SZZP light plus unterstützen, durch die ausschließlich der Konnektor - und explizit nicht der Administrator der Betriebsumgebung - über die Schnittstellen des SZZP light plus Zugang in die geschützten Bereiche der TI bekommen. Die Kopplung muss aktiviert sein, wenn der Highspeed-Konnektor unter einer Anbieterzulassung Highspeed-Konnektor betrieben wird. Die Kopplung kann deaktiviert sein, wenn der Highspeed-Konnektor unter einer

Anbieterzulassung TI-Gateway betrieben wird. Die Konfiguration MUSS durch den Hersteller erfolgen.**[<=]**

A_23303 - TLS mit Client-Authentisierung verpflichtend für Clientanbindungen
Der Highspeed-Konnektor in einem TI-Gateway MUSS im Modus [ANCL_ TLS_ MANDATORY = enabled] und [ANCL_ CAUT_ MANDATORY = enabled] und [ANCL_ CAUT_ MODE = CERTIFICATE] betrieben werden, was global am Basissystem des HSK durch die Rolle "Hersteller" im Rahmen der Inbetriebnahme konfiguriert werden muss und nicht durch andere Administrator-Rollen (Basissystem-Administrator, Zugangsmodul, Administratoren von HSK-Instanzen) deaktivierbar sein darf.
[<=]

7 Anforderungshaushalt TI-Gateway

Dem Anbietertyp TI-Gateway sind Betriebliche Anforderungen aus den Spezifikationen gemSpec_DS_Anbieter, gemRL_Betr_TI, gemKPT_Betr, gemKPT_Test, gemSpec_Perf, gemSpec_Krypt und gemSpec_Net zugewiesen.

7.1 Neue Anforderungen

7.1.1 Anbietererklärung

A_18737-01 - Sperrung von Zugängen zur TI
Der Anbieter TI-Gateway MUSS nach Weisung der gematik Zugänge zur TI sperren.**[<=]**

7.1.2 Sicherheitsgutachten

Es sind wie beschrieben Konstellationen möglich und zulässig, bei denen ein Anbieter TI-Gateway nicht selbst alle Anforderungen erfüllt, sondern in der Zusammenarbeit zwischen Reseller und Infrastrukturbetreiber Anforderungen von einer Partei erfüllt und nachgewiesen werden und von der anderen Partei dies im Rahmen der Anbieterzulassung nachgenutzt wird. Es muss jedoch stets nachgewiesen werden, dass in Summe alle Anforderungen erfüllt sind und keine Lücken durch gegenseitige Verweise auf die Verantwortung des anderen entstehen.

A_23352 - Anforderungsabdeckung von zugekaufter Leistung
Der Anbieter des TI-Gateways MUSS, wenn er zur Erfüllung von Anforderungen Leistungen einer andern Partei (Infrastrukturbetreiber oder Reseller) erwirbt bzw. nachnutzt, nachweisen, dass diese Anforderungen für ihn von der anderen Partei erfüllt werden, was mindestens einen Verweis auf den bestehenden Nachweis der anderen Partei zur Erfüllung der nachgenutzten Anforderung und die vertragliche Regelung zur Erbringung eben dieser Leistung durch die andere Partei für den Zulassungsnehmer beinhalten muss.**[<=]**

TIP1-A_4482-01 - TI-Gateway, Kommunikation LE-Institutionen
Der Anbieter des TI-Gateways MUSS sicherstellen, dass eine direkte Netzwerkkommunikation zwischen LE-Institutionen über das TI-Gateway nicht möglich ist.**[<=]**

TIP1-A_4341-01 - TI-Gateway, Erkennung von Angriffen
Der Anbieter des TI-Gateways MUSS durch technische und organisatorische Maßnahmen sicherstellen, dass Angriffe aus dem Internet auf den VPN-Zugangsdienst erkannt werden.
Als geeignete Maßnahmen werden angesehen:

- Auswertung von Logfiles
- Auswertung von Netflow
- Intrusion Detection Systeme (IDS)

[<=]

Der Anbieter muss dabei berücksichtigen, dass ein Neukunde, dessen SMC-B noch nicht geprüft wurde, möglicherweise ein Angreifer ist.

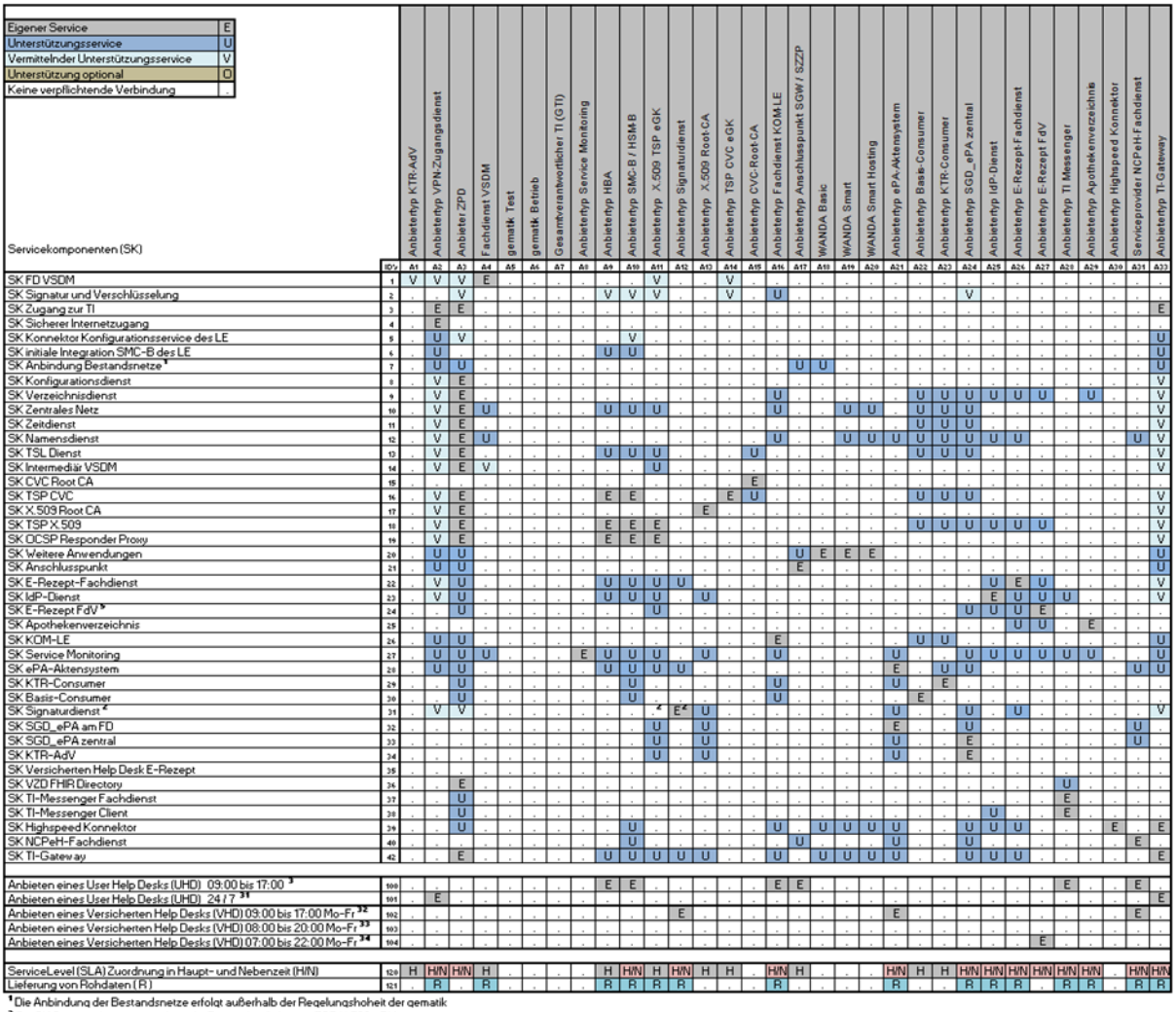
GS-A_4847-01 - Produkttyp TI-Gateway, DNSSEC im Namensraum Transportnetz
Anbieter des TI-Gateways MÜSSEN den Namensraum Transportnetz per DNSSEC sichern.**[<=]**

GS-A_5037-01 - TI-Gateway, Prozess zur Verteilung des DNSSEC Trust Anchor im Namensraum Transportnetz
Der Anbieter TI-Gateway MUSS bei Verwendung eines vom Internet verschiedenen Transportnetzes einen Prozess implementieren, der es ermöglicht den Hash des DNSSEC Trust Anchor für den Namensraum Transportnetz an Betreiber von Konnektoren zu verteilen.**[<=]**

Der Hersteller muss die für sein Produkt erforderlichen Protokolle angeben wie in TIP1-A_4340-01.

7.2 Betrieb

7.2.1 Servicezerlegung



Eigener Service	E
Unterstützungsservice	U
Vermittelnder Unterstützungsservice	V
Unterstützung optional	O
Keine verpflichtende Verbindung	

Servicekomponenten (SK)	ID's	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10	A11	A12	A13	A14	A15	A16	A17	A18	A19	A20	A21	A22	A23	A24	A25	A26	A27	A28	A29	A30	A31	A33
		Anbietertyp KTR-AdV	Anbietertyp VPN-Zugangsdienst	Anbieter ZPD	Fachdienst VSDM	gematik Test	gematik Betrieb	Gesamtverantwortlicher TI (GTI)	Anbietertyp Service Monitoring	Anbietertyp HBA	Anbietertyp SMC-B / HSM-B	Anbietertyp X.509 TSP eGK	Anbietertyp Signaturdienst	Anbietertyp X.509 Root CA	Anbietertyp TSP CVC eGK	Anbietertyp CVC-Root-CA	Anbietertyp Fachdienst KOM-LE	Anbietertyp Anschlusspunkt SGW / SZZP	WANDA Basic	WANDA Smart	WANDA Smart Hosting	Anbietertyp ePA-Aktensystem	Anbietertyp Basis-Consumer	Anbietertyp KTR-Consumer	Anbietertyp SGD_ePA zentral	Anbietertyp IdP-Dienst	Anbietertyp E-Rezept-Fachdienst	Anbietertyp E-Rezept FdV	Anbietertyp TI Messenger	Anbietertyp Apothekenverzeichnis	Anbietertyp Highspeed Konnektor	Serviceprovider NCPeH-Fachdienst	Anbietertyp TI-Gateway
SK FD VSDM	1	V	V	V	E							V			V																		
SK Signatur und Verschlüsselung	2			V						V	V	V			V		U							V								
SK Zugang zur TI	3		E	E																													E
SK Sicherer Internetzugang	4		E																														
SK Konnektor Konfigurationsservice des LE	5		U	V							V																						U
SK initiale Integration SMC-B des LE	6		U							U	U																						U
SK Anbindung Bestandsnetze [1]	7		U	U														U	U														U
SK Konfigurationsdienst	8		V	E																													V
SK Verzeichnisdienst	9		V	E													U						U	U	U	U	U	U		U			V
SK Zentrales Netz	10		V	E	U					U	U	U					U			U	U		U	U	U								V
SK Zeitdienst	11		V	E																			U	U	U								V
SK Namensdienst	12		V	E	U												U			U	U	U	U	U	U	U	U					U	V
SK TSL Dienst	13		V	E						U	U	U				U							U	U	U								V
SK Intermediär VSDM	14		V	E	V							U																					V
SK CVC Root CA	15															E																	
SK TSP CVC	16		V	E						E	E				E	U							U	U	U								V
SK X.509 Root CA	17		V	E										E																			V
SK TSP X.509	18		V	E						E	E	E											U	U	U	U	U	U					V
SK OCSP Responder Proxy	19		V	E						E	E	E																					V
SK Weitere Anwendungen	20		U	U														U	E	E	E												U
SK Anschlusspunkt	21		U	U														E															U
SK E-Rezept-Fachdienst	22		V	U						U	U	U	U														U	E	U					V
SK IdP-Dienst	23		V	U						U	U	U		U												E	U	U	U				V
SK E-Rezept FdV [5]	24			U								U														U	U	U	E				
SK Apothekenverzeichnis	25																											U	U		E		
SK KOM-LE	26		U	U													E						U	U									U
SK Service Monitoring	27		U	U	U				E	U	U	U		U			U					U			U	U	U	U	U	U			U
SK ePA-Aktensystem	28		U	U						U	U	U	U									E		U	U							U	U
SK KTR-Consumer	29			U							U						U					U		E									
SK Basis-Consumer	30			U							U						U						E										
SK Signaturdienst [4]	31		V	V								[4]	E[4]	U								U			U		U						V
SK SGD_ePA am FD	32											U		U								E			U							U	
SK SGD_ePA zentral	33											U		U								U			E							U	
SK KTR-AdV	34											U		U								U			E								
SK Versicherten Help Desk E-Rezept	35																																
SK VZD FHIR Directory	36			E																									U				
SK TI-Messenger Fachdienst	37			U																									E				
SK TI-Messenger Client	38			U																						U			E				
SK Highspeed Konnektor	39			U							U						U		U	U	U	U			U	U	U				E		E
SK NCPeH-Fachdienst	40										U							U				U			U							E	
SK TI-Gateway	42			E						U	U	U	U	U			U		U	U	U	U			U	U	U						E
Anbieten eines User Help Desks (UHD) 09:00 bis 17:00 [3]	100									E	E						E	E											E		E		
Anbieten eines User Help Desks (UHD) 24 / 7 [31]	101		E																														E
Anbieten eines Versicherten Help Desks (VHD) 09:00 bis 17:00 Mo-Fr [32]	102												E									E										E	
Anbieten eines Versicherten Help Desks (VHD) 08:00 bis 20:00 Mo-Fr [33]	103																																
Anbieten eines Versicherten Help Desks (VHD) 07:00 bis 22:00 Mo-Fr [34]	104																											E					
ServiceLevel (SLA) Zuordnung in Haupt- und Nebenzeit (H/N)	120	H	H/N	H/N	H					H	H/N	H	H/N	H	H		H/N	H				H/N	H	H	H/N	H/N	H/N	H/N	H/N	H/N		H/N	H/N
Lieferung von Rohdaten (R)	121		R		R					R	R	R	R				R					R			R	R	R		R	R		R	R

[1] Die Anbindung der Bestandsnetze erfolgt außerhalb der Regelungshoheit der gematik
[2] Die SK Signaturdienst neu nicht mehr Option des Anbieters TSP X.509 eGK
[3] siehe AFO TIP1-A_7260-01
[31] siehe AFO A_19532-01
[32] siehe AFO A_16217-01
[33] siehe AFO A_20734-01
[34] siehe AFO A_20733-03
[5] Die SK E-Rezept FdV enthält auch die SK E-Rezept AdV.

7.2.2 Mitwirkungsverpflichtung im TI-ITSM gemäß [gemRL_Betr_TI]

Tab_KPT_Betr_TI_003 Mitwirkungsverpflichtung im TI-ITSM

Mitwirkung in den TI-ITSM-Prozessen:	INC	PRO	CHG	SKM	SLM	RF	Perf	CapM	KM	CSI	CM	NM

Anbieter TI-Gateway	A/E	A/E	A/E	.	A/E	A	A	A	A/E	.	A/E	A/E

Legende:

INC: Incident Management

PRO: Problem Management

CHG: Change Management

SKM: Servicekatalog Management

SLM: Service Level Management

RF: Request Fulfillment

Perf: Perfomance Management

CapM: Capacity Management

KM: Knowledge Management

CSI: Continual Service Improvement

CM: Configuration Management

NF: Notfall Management

A: Auslöser in INC, PRO, CHG

Auslöser (A) ist, wer Incidents, Problems oder Changes eröffnet.

E: Empfänger von INC, PRO, CHG

Empfänger (E) ist wer Incidents, Problems oder Changes zugewiesen bekommt und dessen vollständige Mitarbeit gewährleistet ist.

Auslöser und Empfänger im SKM

Auslöser (A) ist, wer Änderungen im Service Katalog Management einbringt.

Empfänger (E) ist, wer Änderungen im Service Katalog Management aufnimmt.

Portalanbieter (P) ist, wer das TI-Service-Portal zur Verfügung stellt und selbst Nutzer ist.

A/E: Auslöser und Empfänger im SLM

Auslöser (A) ist, wer Änderungen im Servicelevel Management einbringt.

Empfänger (E) ist, wer im Servicelevel Management an Servicelevel-Reviews teilnimmt.

A/E: Auslöser und Empfänger im RF

Auslöser (A) ist, wer Services bei anderen Anbietern abruft.

Empfänger (E) ist, wer einen Servicekatalog führt und Services anbietet.

A/E: Auslöser und Empfänger im Perf

Auslöser (A) ist, wer Performancereports bzw. Rohdaten-Performance-Berichte sendet.

Empfänger (E) ist die gematik.

A/E: Auslöser und Empfänger im CapM

Auslöser (A) ist, wer Kapazitätspläne führt und reportet.
Empfänger (E) ist die gematik (GTI).

A/E: Auslöser und Empfänger im KM

Auslöser (A) ist, wer Artikel in der Wissensdatenbank einstellt.

Empfänger (E) ist, wer Artikel aus der Wissensdatenbank bezieht.

A/E: Auslöser und Empfänger im CSI

Auslöser (A) ist, wer ein CSI-Register führt und reportet.
Empfänger (E) ist die gematik (GTI).

A/E: Auslöser und Empfänger im CM

Auslöser (A) ist, wer Reports sendet, in denen die Konfigurationen der verwendeten Produkte dargestellt werden.

Empfänger (E) ist, wer Konfigurationsvorgaben und deren Umsetzung dar z.B. im Zuge eines CRs oder Changes empfängt und umsetzt.

A/E: Auslöser und Empfänger im NM

Aktiv (A) ist, wer im Notfall zuarbeiten und unterstützen muss.

Empfänger (E) stellen einen Notfall-Ansprechpartner bereit.

7.2.3 Spezifische Ausprägungen und Verpflichtungen einzelner Rollen

Tab_KPT_Betr_Betriebliche Rolle_Anbieterkonstellationen

Spezifische Ausprägung der Rolle	Zulässige Anbieterkonstellationen	Bemerkung
Anbieter TI-Gateway	<I / II / III>	

Anbieter TI-Gateway

Für die Anbieter TI-Gateway gelten die Konstellationen gemäß [gemKPT_Betrieb#3.4.4] abschließend. Der Anbieter kann sich zwischen diesen Konstellationen entscheiden und den Betrieb entweder selbst organisieren und alle Anforderungen des Anbietertypsteckbriefes selbst erfüllen. Alternativ kann er sich bereits im Zulassungsverfahren durch einen Unterauftragnehmer vertreten lassen und sich somit für die Konstellation II oder III entscheiden. Mit Abschluss des Zulassungsvertrages/Zulassungsbescheides verpflichtet sich dann der Anbieter sicherzustellen, dass sein Unterauftragnehmer gegenüber der gematik zur Abgabe aller erforderlichen Erklärungen sowie zur Durchführung aller tatsächlichen Handlungen berechtigt und verpflichtet ist, soweit diese zur Erbringung der Betriebsleistung erforderlich sind.

A_23334 - Bereitstellung Firewall-Konfigurationsdaten vom Anbieter TI-Gateway
Der Anbieter TI-Gateway MUSS alle für die Registrierung und den Verbindungsaufbau zur TI notwendigen Netzwerkinformationen (IP-Zieladressen und Ports) veröffentlichen und dem Gesamtverantwortlichen der TI bereitstellen. Der Anbieter TI-Gateway MUSS diese veröffentlichten Informationen stets aktuell halten**[<=]**

Die Veröffentlichung dieser Informationen durch den Anbieter kann über unterschiedliche Portale erfolgen, wie z.B. eigene Support-Portale oder die TI-Wissensdatenbank. Zielgruppe für die veröffentlichten Informationen sind sowohl die Leistungserbringer selbst als auch deren betreuende IT-Dienstleister.
Mit diesen Informationen sollen die lokalen Firewalls in den dezentralen Umgebungen der Leistungserbringer möglichst restriktiv konfiguriert werden können. Zeitgleich soll damit eine fehlerfreie Kommunikation von dezentral mit der TI über Ihr TI-Gateway sichergestellt werden.

7.2.4 Supportkonzept

7.2.4.1 Spezifische Ausprägungen

Tab_KPT_Betr_TI_Anbieter_UHD/VHD

	UHD (Anwender)	VHD (Versicherte)**
Anbieter TI-Gateway	Mo - So 0:00 bis 24:00 Uhr (24/7)	

Der Anbieter VPN-Zugangsdienst stellt seinen Anwendern (Leistungserbringern) einen UHD zur Verfügung.

Spezifische Ausprägungen Anbieter TI-Gateway

A_23335 - Verpflichtung zur Dokumentation von Service Levels im Anwendersupport des Anbieters TI-Gateway
Der Anbieter TI-Gateway MUSS alle Service Levels im Anwendersupport im Rahmen der Zulassung dokumentieren und die gematik über Änderungen informieren. Hierbei MUSS der Anbieter TI-Gateway eine Einteilung in eine oder mehrere verschiedene Serviceklassen (logische Gruppierungen von Service Levels in einer definierten Servicequalität, z. B. Gold, Silber, Bronze) vornehmen.**[<=]**

7.2.4.2 Organisatorische Service Level

Tabelle x: Tab_gemKPT_Betr_OrgSL_Serviceleistung_Zeiten

Serviceleistung	zu Haupt- und Nebenzeit (TIP1-A_7265)	zu Hauptzeit (A_13573)
Anbieter TI-Gateway	x	

Sind SL nur der Hauptzeit (H) zugeordnet, so kann die Bearbeitung in der Nebenzeit unterbrochen werden und wieder in der Hauptzeit aufgenommen werden. Die Einhaltung dieses SL wird nur in der Hauptzeit gemessen.

7.2.4.3 Technische Service Level / Performance-Kenngrößen

Anwendung Anwendung TI-Gateway-Zugangsmodul (PDT72)

Schnittstellen::Operation bzw. Anwendungsfall

Tab_gemKPT_Betr_TI-Gateway-Zugangsmodul_Operationen/Anwendungsfälle

Produkttyp / Anwen-dungstyp	S/A-ID	Schnittstellen::Operation / Anwendungsfall	Beschreibung	Berichtsformat-Alias (sofern von Schnittstellen::Operation bzw. Anwendungsfall abweichend)
PDT72	S01	I*		
PDT72	S02	I_Secure_Channel_Tunnel::connect		
PDT72	S03	I_Secure_Channel_Tunnel::disconnect		
PDT72	S04	I_DNS_Name_Resolution::get_IP_Address		

Performance-Kenngrößen / SL-Werte

Der Erfassungszeitraum für die aufgeführten Soll-Werte beträgt ein Kalendermonat.

<< Standardsatz von Performance-Kenngrößen. Nicht verwendete bitte streichen. >>

Tab_gemKPT_Betr_TI-Gateway-Zugangsmodul_Performance-Kenngroessen

Performance-Kenngröße (PKG-ID)	Beschreibung	berechnet aus (Rohdaten-BDE, Probing)	SL-Wert (Soll-Wert)	min / max	Normative Referenz
TI-Gateway-Zugangsmodul - PDT72 - I*					
PDT72-S01-D3-G12	Relative Verfügbarkeit im Erfassungszeitraum exkl. Wartung. [%*1000]	Probing			
PDT72-S01-D3-G14	Relative Verfügbarkeit im Erfassungszeitraum zur Hauptzeit exkl. Wartung. [%*1000]	Probing			
PDT72-S01-D3-G16	Relative Verfügbarkeit im Erfassungszeitraum zur Nebenzeit exkl. Wartung. [%*1000]	Probing			

PDT72-S01-D1-G05	Anzahl der bestehenden VPN-Tunnel	Rohdaten-BDE			
TI-Gateway-Zugangsmodul - PDT72 - I_Secure_Channel_Tunnel::connect					
PDT72-S02-D1-G01	Anzahl der Aufrufe im Erfassungszeitraum. [Stück]	Rohdaten-BDE			
PDT72-S02-D3-G12	Relative Verfügbarkeit im Erfassungszeitraum exkl. Wartung. [%*1000]	Probing			
PDT72-S02-D3-G14	Relative Verfügbarkeit im Erfassungszeitraum zur Hauptzeit exkl. Wartung. [%*1000]	Probing			
PDT72-S02-D3-G16	Relative Verfügbarkeit im Erfassungszeitraum zur Nebenzeit exkl. Wartung. [%*1000]	Probing			
TI-Gateway-Zugangsmodul - PDT72 - I_Secure_Channel_Tunnel::disconnect					
PDT72-S03-D1-G01	Anzahl der Aufrufe im Erfassungszeitraum. [Stück]	Rohdaten-BDE			
PDT72-S03-D3-G12	Relative Verfügbarkeit im Erfassungszeitraum exkl. Wartung. [%*1000]	Probing			
PDT72-S03-D3-G14	Relative Verfügbarkeit im Erfassungszeitraum zur Hauptzeit exkl. Wartung. [%*1000]	Probing			
PDT72-S03-D3-G16	Relative Verfügbarkeit im Erfassungszeitraum zur Nebenzeit exkl. Wartung. [%*1000]	Probing			
TI-Gateway-Zugangsmodul - PDT72 - I_DNS_Name_Resolution::get_IP_Address					

PDT72-S04-D1-G01	Anzahl der Aufrufe im Erfassungszeitraum. [Stück]	Rohdaten-BDE			
PDT72-S04-D2-G08	Mittlere Bearbeitungszeit im Erfassungszeitraum. [msec]	Rohdaten-BDE			
PDT72-S04-D2-G30	Maximale Bearbeitungszeit im Erfassungszeitraum. [msec]	Rohdaten-BDE			
PDT72-S04-D2-G31	Anteil Bearbeitungen innerhalb der Bearbeitungszeitvorgabe im Erfassungszeitraum. [%]	Rohdaten-BDE			
PDT72-S03-D3-G12	Relative Verfügbarkeit im Erfassungszeitraum exkl. Wartung. [%*1000]	Probing			
PDT72-S04-D3-G14	Relative Verfügbarkeit im Erfassungszeitraum zur Hauptzeit exkl. Wartung. [%*1000]	Probing			
PDT72-S04-D3-G16	Relative Verfügbarkeit im Erfassungszeitraum zur Nebenzeit exkl. Wartung. [%*1000]	Probing			

7.2.5 gemKPT_Betr: Anhang A

Tab_gemKPT_Betr_Produkttypen

ID	Produkttyp / Anwendungstyp	Produkttyp-Name / Anwendungsname
PDT72	gemProdT_TI-Gateway-Zugangsmodul	TI-Gateway-Zugangsmodul

7.2.6 gemSpec_Perf#5.2 Verfügbarkeit

GS-A_4155-01 - Performance – TI-Gateway – Verfügbarkeit
Die Anbieter des TI-Gateways MÜSSEN zur Hauptzeit eine Verfügbarkeit von 99,9% und zur Nebenzeit von 99% für alle Operationen der technischen Schnittstellen aufweisen. Wartungsfenster dürfen nur in der Nebenzeit liegen. Genehmigte Wartungsfenster werden nicht als Ausfallzeit gewertet.

Hauptzeit ist Montag bis Freitag von 6 bis 22 Uhr sowie Samstag und Sonntag von 6 bis 20 Uhr. Alle übrigen Stunden der Woche sind Nebenzeit. Bundeseinheitliche Feiertage werden wie Sonntage behandelt, alle übrigen Feiertage wie Werktage.
Der Anschluss an das zentrale Netz muss über die Anschlussoption „redundante Anbindung" erfolgen.
[<=]

Messung der Verfügbarkeit:

Die Messung könnte z.B. durch eine lokale Softwarekomponente des Zugangsmoduls erfolgen. Für Testaufrufe muss sich eine solche Probe authentifizieren und korrekte Context-Parameter verwenden.

- Das TI-Gateway als ganzes gilt als verfügbar, wenn 90 % der HSK-Instanzen auf getRessourceInformation mit get RessourceInformationResponse antworten.
- Das TI-Gateway gilt für den Leistungserbringer als verfügbar, wenn bei verfügbarem Internet der Intermediär-VSDM erreichbar ist.

8 Anhang A – Verzeichnisse

8.1 Abkürzungen

Kürzel	Erläuterung

8.2 Referenzierte Dokumente

8.2.1 Dokumente der gematik

Die nachfolgende Tabelle enthält die Bezeichnung der in dem vorliegenden Dokument referenzierten Dokumente der gematik zur Telematikinfrastruktur. Der mit der vorliegenden Version korrelierende Entwicklungsstand dieser Konzepte und Spezifikationen wird pro Release in einer Dokumentenlandkarte definiert; Version und Stand der referenzierten Dokumente sind daher in der nachfolgenden Tabelle nicht aufgeführt. Deren zu diesem Dokument jeweils gültige Versionsnummern sind in der aktuellen, von der gematik veröffentlichten Dokumentenlandkarte enthalten, in der die vorliegende Version aufgeführt wird.

[Quelle]	**Herausgeber: Titel**
[gemGlossar]	gematik: Glossar der Telematikinfrastruktur