

## Elektronische Gesundheitskarte und Telematikinfrastruktur

# Feature: TI-Gateway

Version:	1.45.0
Revision:	101978521980
Stand:	13.0622.10.2024
Status:	freigegeben
Klassifizierung:	öffentlich
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	15.02.202 3		freigegeben	gematik
1.1.0	04.08.202 3		Übernahme von Inhalten gemF_TI- Gateway --> gemSpec_Perf, gemKPT_Betr, gemF_Highspeed- Konnektor; redaktionelle Anpassungen	gematik
1.2.0	12.12.202 3	6.1.2	Einarbeitung HSK_23.5	gematik
1.3.0	23.02.202 4		Änderungsliste HSK_Maintenance_23.6 und TI-Gateway_23.1	gematik
1.4.0	13.06.202 4		Änderungsliste TI-Gateway_24.1	gematik
<a href="#">1.5.0</a>	<a href="#">22.10.202 4</a>		<a href="#">Änderungsliste TI-Gateway_24.2</a>	<a href="#">gematik</a>

---

## Inhaltsverzeichnis

---

<b>1 Einordnung des Dokuments.....</b>	<b>5</b>
1.1 Zielsetzung.....	5
1.2 Zielgruppe.....	5
1.3 Abgrenzungen.....	5
1.4 Methodik Anforderungen.....	5
<b>2 Einordnung in die Telematikinfrastuktur.....</b>	<b>7</b>
<b>3 Technisches Konzept.....</b>	<b>8</b>
<b>4 Rollenkonzept TI-Gateway.....</b>	<b>9</b>
4.1 Reseller.....	9
4.2 Betreiber.....	10
4.3 Hersteller des HSK.....	10
4.4 HSK-Instanz Administrator z.B. Dienstleister vor Ort (DVO).....	10
4.5 Remote-Administrator.....	11
4.6 Kunde – Leistungserbringer.....	11
4.7 Rollenkombinationen & Rollenausschlüsse.....	12
<b>5 Spezifikation Zugangsmodul.....</b>	<b>14</b>
5.1 Onboarding und Registrierung.....	14
5.1.1 Nutzerportal.....	15
5.1.2 Initiale Authentifizierung der HSK-Instanz.....	17
5.1.3 Betriebsfunktionen für den Leistungserbringer.....	20
5.2 VPN.....	20
5.3 Routing und Firewall.....	22
5.4 Sicherheit & Datenschutz.....	23
5.5 Rohdaten-Performance-Reporting.....	26
5.5.1 Umfang.....	26
5.5.2 Lieferintervalle.....	26
5.5.3 Format.....	26
5.6 Lastanforderungen.....	27
5.7 Anforderungen an den Hersteller.....	27
<b>6 Anforderungshaushalt TI-Gateway.....</b>	<b>28</b>
6.1 Neue Anforderungen.....	28
6.1.1 Anbietererklärung.....	28
6.1.1.1 Anbindung an das Transportnetz Internet.....	28
6.1.1.2 Anbindung an die TI.....	29

6.1.2 Sicherheitsgutachten.....	29
<b>6.2 Betrieb.....</b>	<b>31</b>
6.2.1 Servicezerlegung.....	31
6.2.2 Mitwirkungsverpflichtung im TI-ITSM gemäß [gemRL_Betr_TI].....	31
6.2.3 Spezifische Ausprägungen und Verpflichtungen einzelner Rollen.....	31
6.2.4 Supportkonzept.....	31
6.2.4.1 Spezifische Ausprägungen.....	31
6.2.4.2 Organisatorische Service Level.....	31
6.2.4.3 Technische Service Level / Performance-Kenngrößen.....	31
6.2.5 gemKPT_Betr: Anhang A.....	31
6.2.6 gemSpec_Perf#3.x.1 Leistungsanforderungen TI-Gateway.....	32
6.2.6.1 gemSpec_Perf#3.x.1.1 Lastmodell TI-Gateway.....	32
6.2.6.2 gemSpec_Perf#3.x.1.2 Bearbeitungszeiten TI-Gateway.....	32
6.2.6.3 gemSpec_Perf#3.x.1.3 Performancevorgaben TI-Gateway.....	32
6.2.7 Zugang und Verfügbarkeit.....	32
<b>7 Änderungen an gemILF_PS.....</b>	<b>33</b>
<b>8 Beispiele und Referenzimplementierungen.....</b>	<b>34</b>
<b>9 Anhang A – Verzeichnisse.....</b>	<b>35</b>
9.1 Abkürzungen.....	35
9.2 Referenzierte Dokumente.....	35
9.2.1 Dokumente der gematik.....	35
9.2.2 Weitere Dokumente.....	35
<b>1 Einordnung des Dokuments.....</b>	<b>7</b>
1.1 Zielsetzung.....	7
1.2 Zielgruppe.....	7
1.3 Abgrenzungen.....	7
1.4 Methodik Anforderungen.....	7
<b>2 Einordnung in die Telematikinfrastuktur.....</b>	<b>9</b>
<b>3 Technisches Konzept.....</b>	<b>10</b>
<b>4 Rollenkonzept TI-Gateway.....</b>	<b>12</b>
4.1 Vertrieb.....	13
4.2 Betreiber.....	14
4.3 Hersteller des HSK.....	14
4.4 HSK-Instanz Administrator z.B. Dienstleister vor Ort (DVO).....	15
4.5 Remote-Administrator.....	15
4.6 Kunde - Nutzer.....	15
4.7 Rollenkombinationen & Rollenausschlüsse.....	16

<b>5 Spezifikation Zugangsmodul.....</b>	<b>19</b>
<b>5.1 Onboarding und Registrierung.....</b>	<b>19</b>
5.1.1 Nutzerportal.....	20
5.1.2 Initiale Authentifizierung der HSK-Instanz.....	23
5.1.3 Betriebsfunktionen für den Nutzer des TI-Gateways.....	26
<b>5.2 VPN.....</b>	<b>26</b>
<b>5.3 Routing und Firewall.....</b>	<b>28</b>
<b>5.4 Sicherheit &amp; Datenschutz.....</b>	<b>29</b>
<b>5.5 Rohdaten-Performance-Reporting.....</b>	<b>32</b>
5.5.1 Umfang.....	32
5.5.2 Lieferintervalle.....	32
5.5.3 Format.....	32
<b>5.6 Lastanforderungen.....</b>	<b>33</b>
<b>5.7 Anforderungen an den Hersteller.....</b>	<b>33</b>
<b>6 Anforderungshaushalt TI-Gateway.....</b>	<b>34</b>
<b>6.1 Neue Anforderungen.....</b>	<b>34</b>
6.1.1 Anbietererklärung.....	34
6.1.1.1 Anbindung an das Transportnetz Internet.....	34
6.1.1.2 Anbindung an die TI.....	35
6.1.2 Sicherheitsgutachten.....	35
<b>6.2 Betrieb.....</b>	<b>37</b>
6.2.1 Servicezerlegung.....	37
6.2.2 Mitwirkungsverpflichtung im TI-ITSM gemäß [gemRL_Betr_TI].....	38
6.2.3 Spezifische Ausprägungen und Verpflichtungen einzelner Rollen.....	38
6.2.4 Supportkonzept.....	38
6.2.4.1 Spezifische Ausprägungen.....	38
6.2.4.2 Organisatorische Service Level.....	38
6.2.4.3 Technische Service Level / Performance-Kenngrößen.....	38
6.2.5 gemKPT_Betr: Anhang A.....	38
6.2.6 gemSpec_Perf#3.x.1 Leistungsanforderungen TI-Gateway.....	38
6.2.6.1 gemSpec_Perf#3.x.1.1 Lastmodell TI-Gateway.....	38
6.2.6.2 gemSpec_Perf#3.x.1.2 Bearbeitungszeiten TI-Gateway.....	38
6.2.6.3 gemSpec_Perf#3.x.1.3 Performancevorgaben TI-Gateway.....	38
6.2.7 Zugang und Verfügbarkeit.....	38
<b>6.3 Netzanbindung TI-Gateway.....</b>	<b>39</b>
6.3.1 Netzdelegation.....	39
6.3.2 Verwendung der Netzbereiche.....	39
6.3.3 IP-Adressvergabe und Netzfreeschaltungen.....	40
6.3.3.1 Aufbau 1 - Eigenständige Systemdienste.....	41
6.3.3.1.1 Front-Zone.....	41
6.3.3.1.2 Back-Zone.....	42
6.3.3.1.3 Intermediär.....	43
6.3.3.2 Aufbau 2 - Systemdienste in den HSK-Servern.....	44
6.3.3.3 Aufbau 3 - Durchleitung offene Fachdienste / WANDA durch den HSK.....	44
<b>7 Änderungen an gemILF_PS.....</b>	<b>46</b>

<b>8 Beispiele und Referenzimplementierungen.....</b>	<b>47</b>
<b>9 Anhang A - Verzeichnisse.....</b>	<b>48</b>
<b>9.1 Abkürzungen.....</b>	<b>48</b>
<b>9.2 Referenzierte Dokumente.....</b>	<b>48</b>
9.2.1 Dokumente der gematik.....	48
9.2.2 Weitere Dokumente.....	48

---

## 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 Teilfunktionen des Konnektors 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 und an anderen Nutzern der Telematikinfrastruktur 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.

Anbieter des TI-Gateways können darüber hinaus ihren Kunden weitere Services anbieten, müssen dann jedoch transparent machen, dass diese nicht Teil des zugelassenen TI-Gateways sind. (siehe A\_23472)

Durch die Verschiebung der Funktionalitäten, die heute vom Konnektor im lokalen Netz des Nutzers bereitgestellt werden, in einen im Rechenzentrum betriebenen Dienst stehen zwangsläufig gewisse Funktionen nicht mehr zur Verfügung. Dies sind konkret:

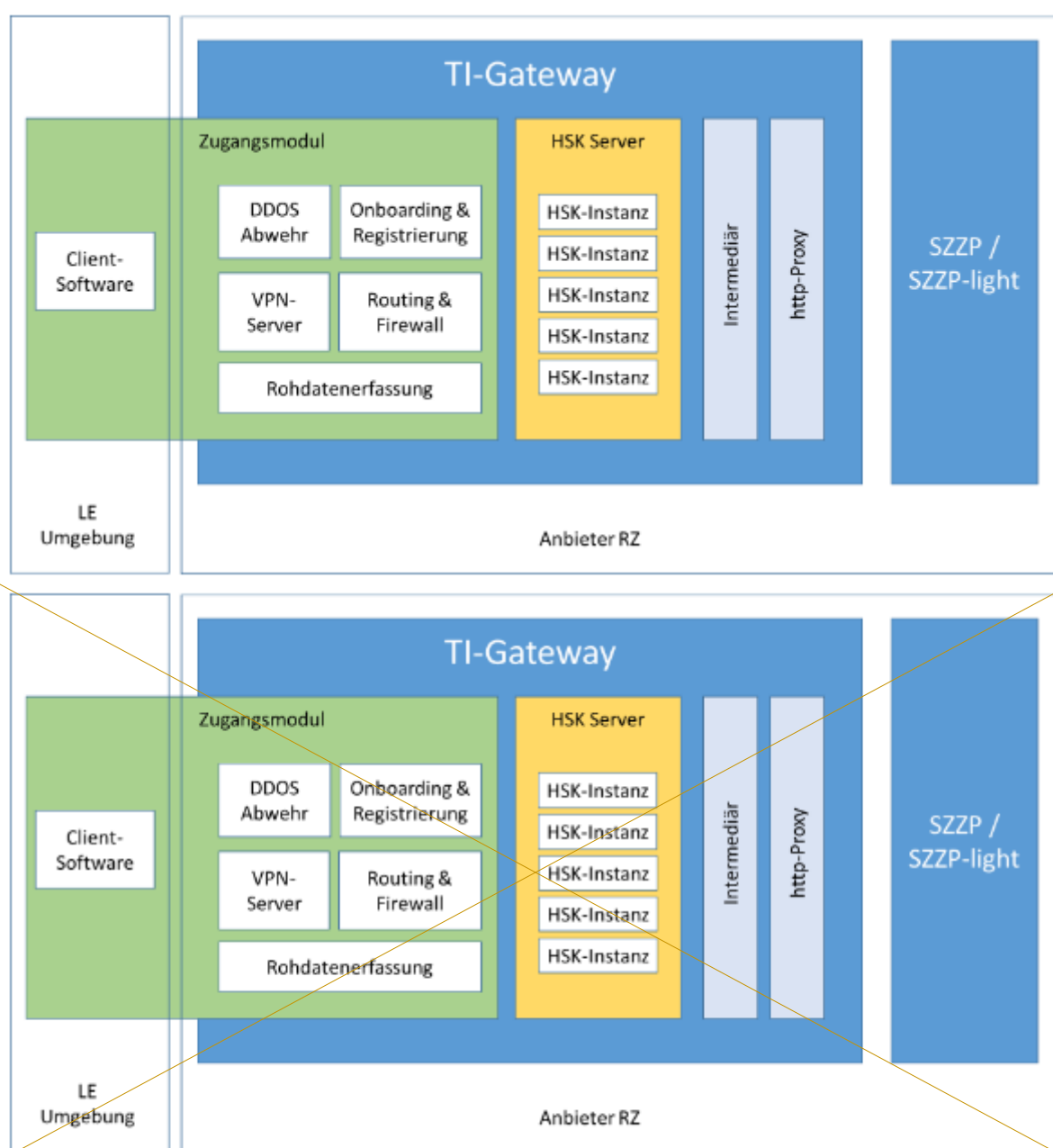
- Schutz des lokalen Netzes des Nutzers gegenüber Angriffen aus dem Internet (bei Konnektor ausschließlich bei Anbindung "in Reihe" gegeben)
- Sicherer Internet Service (SIS)
- Zeitdienst für das lokale Netz
- DHCP Server für das lokale Netz
- VSDM im Offline-Betrieb
- VSDM im Standalone-Betrieb (nur bei Nutzung von zwei Konnektoren gegeben)

Nutzer bzw. die von ihnen beauftragten IT-Dienstleister (DVO) müssen entsprechend alternative Lösungen für die Funktionen umsetzen, die zuvor über den Konnektor genutzt wurden (sofern die Funktionen benötigt werden). Dies gilt insbesondere für die Absicherung des lokalen Netzes gegen das Internet, falls vor der Nutzung des TI-Gateway ein Konnektor in Anbindungsart "in Reihe" installiert war.

### 3 Technisches Konzept

Die Anbieterzulassung für das TI-Gateway setzt eine Produktzulassung Zugangsmodul und eine Produktzulassung Highspeed-Konnektor (HSK) voraus. Die Komponente http-Proxy ist als Teil des Produkttyps HSK umzusetzen. Die Anbieterzulassung für das TI-Gateway umfasst die Produkte Intermediär-VSDM, wobei e. Zwar kann ein in bereits unter der Anbieterzulassung VPN-Zugangsdienst der TI durch einen Dritten betriebener Intermediär nachmitgenutzt werden kann.

, der Anbieter bleibt jedoch für den anforderungskonformen Betrieb verantwortlich.



### 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 http-Proxy bieten Funktionalitäten, die bei Nutzung von Konnektoren durch den VPN-Zugangsdienst abgedeckt werden.

Die Anbindung an die Telematikinfrastruktur erfolgt über einen SZZP. Die Anbindung über ein SZZP-light-plus, die bei einer Anbieterzulassung HSK vorgeschrieben ist, wird für das TI-Gateway nicht unterstützt.

---

## 4 Rollenkonzept TI-Gateway

---

Die gematik lässt ein Unternehmen als Anbieter des TI-Gateways zu. Der Anbieter erbringt Betriebsleistung und Service unter Verwendung zugelassener Produkte. Der Anbieter kann dazu Unterauftragnehmer beauftragen (siehe auch gemKPT\_Betr.) Die Beziehungen der Firmen untereinander wird im Rollenkonzept nicht betrachtet.

Damit Mitarbeiter des Anbieters oder seiner Unterauftragnehmer nicht auf medizinische Informationen oder unberechtigt auf personenbezogene Daten zugreifen, werden die betrieblichen Tätigkeit in verschiedenen Rollen zugeordnet und es wird geregelt, welche Rollen ein Mitarbeiter innehaben kann.

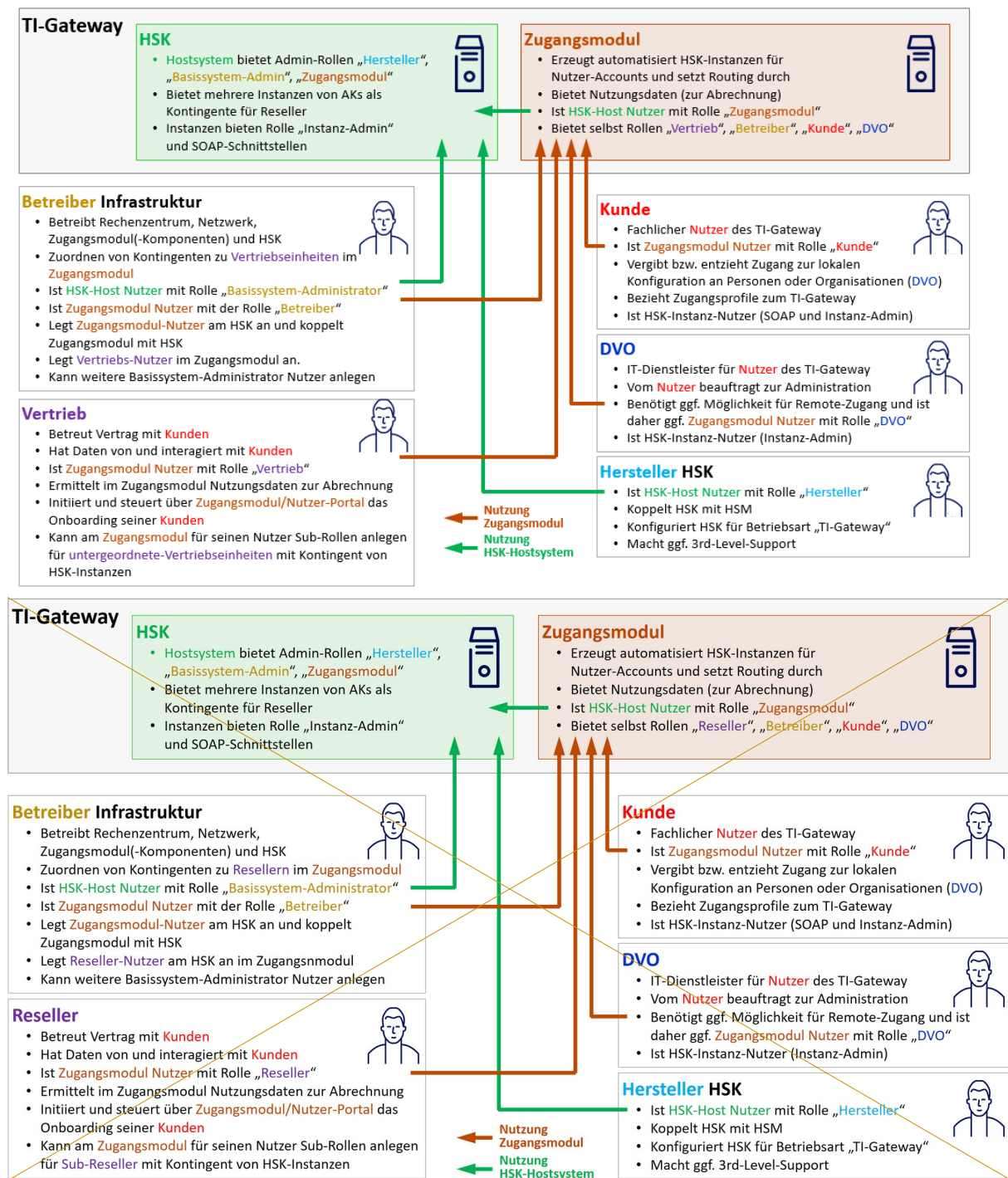


Abbildung 2: Übersicht Rollen und Komponenten

## 4.1 ResellerVertrieb

Der **ResellerVertrieb** betreut den Kunden kaufmännisch und qualifiziert einen Neukunden bevor im Onboardingprozess dem Kunden einen HSK-Instanz erzeugt/zugeordnet wird.

Der **ResellerVertrieb** steuert das Onboarding von **LE-Institutionen Nutzern des TI-Gateways** inklusive dem Erzeugen von HSK-Instanzen im „Werkzustand“ (automatisiert) über die

| Onboarding- & Registrierungskomponente des Zugangsmoduls. Der ResellerVertrieb beauftragt die Löschung von HSK-Instanzen durch den Infrastrukturbetreiber (4-Augen-Prinzip).

| Im Rahmen des Onboardings werden auch automatisiert der Administrations-Zugang an den LeistungserbringerNutzer des TI-Gateways bzw. den von diesem beauftragen lokalen Administrator (DVO) vergeben (Zugangsdaten abrufbar über das Nutzer-Portal) und die HSK-Instanzen zugewiesen. Der ResellerVertrieb hat auf diese Daten keinen Zugriff. Dieser Prozess ist automatisiert und erfordert keinen manuellen Eingriff des ResellersVertriebs oder Betreibers.

| Der ResellerVertrieb hat keinen Zugriff auf medizinische Daten oder die fachliche Konfiguration von HSK-Instanzen.

| Der ResellerVertrieb kann am Zugangsmodul abrechnungsrelevante Information einsehen bzw. abrufen.

| Der ResellerVertrieb hat keinen Zugriff auf das HSK-Basissystem oder die HSK-Instanzen.

## 4.2 Betreiber

Der Betreiber überwacht und steuert technische Komponenten des TI-Gateways inkl. der RZ-Infrastruktur darum.

Der Betreiber greift auf das HSK-Basissystem über die Admin-Rolle "Basissystem-Admin" zu. Dazu gehört die Installation von Softwareupdates und das Erzeugen und Wiederherstellen von Backups der HSK-Instanzen (Snapshots). Dabei hat der Betreiber 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 führt die Löschaufträge des ResellersVertriebs von HSK-Instanzen aus.

Der Betreiber überwacht und administriert das Zugangsmodul.

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 ResellerVertrieb für dessen jeweiliges Kontingent von HSK-Instanzen übertragen werden.

## 4.3 Hersteller des HSK

Der Hersteller interagiert mit dem HSK-Basissystem mit der Rolle Hersteller. In dieser Funktion konfiguriert er den HSK für die Betriebsart "TI-Gateway" und koppelt den HSK mit dem HSM.

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

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

#### 4.4 HSK-Instanz Administrator z.B. Dienstleister vor Ort (DVO)

Die Administration der HSK-Instanz wird vom LeistungserbringerNutzer des TI-Gateways oder einem von ihm beauftragten Dienstleister durchgeführt (DVO). Diese Rolle entspricht somit dem lokalen Administrator, wie er auch beim Inboxkonnektor agiert.

Der DVO greift aus der LeistungserbringerNutzerumgebung oder über einen eigenständigen Zugang auf die Administrationsschnittstelle der HSK-Instanz zu. Im Fall des eigenständigen Zugangs steuert der LENutzer über das Nutzer-Portal des Zugangsmoduls welche Person/Organisation(DVO) auf seine Instanz zugreifen kann. Der DVO authentifiziert sich in jedem Fall direkt am Admin-Interface der HSK-Instanz.

Der LE/DVO nimmt die initiale Anbindung der HSK-Instanz an die LE+Nutzerumgebung 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).

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

Die Erreichbarkeit der Administrations-Schnittstelle der HSK-Instanz muss für den LENutzer von seinen Systemen aus jederzeit gegeben sein. Dabei müssen zwei unabhängige Sicherungsschichten umgesetzt werden, eine für den Zugang zum Administrations-Interface und eine durch Authentisierung an der HSK-Instanz. Eine Erreichbarkeit der fachlichen Schnittstellen (SOAP, LDAP, CETP, SICCT) über ein anders Netz bzw. einen anderen Zugang als den VPN-Zugang ist ausgeschlossen. Der Nutzer kann einem DVO den Zugriff auf die Administrationsschnittstelle seine HSK-Instanz auch jederzeit wieder über das Nutzer-Portal entziehen.

#### 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 Clientsysteme anlegen oder bestehende Clientsystem-Identitäten ändern. Dadurch ist ausgeschlossen, dass ein Remote-Administrator als Innentäter sich selbst als Clientsystem konfiguriert und somit dauerhaft remote mittels der Identität der fs jeweiligen LE+Nutzers 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 Inboxkonnektoren. Die Rolle ist optional.

#### 4.6 Kunde - LeistungserbringerNutzer

Der Kunde, also der Leistungserbringer ist oder ein anderer Nutzer der Telematikinfrastruktur ist der Nutzer der fachlichen Schnittstellen(SOAP, LDAP, CETP, SICCT) einer konkreten HSK-Instanz und Inhaber einer SMC-B-Identität. Der Kunde hat Administrativen Zugang zu seiner HSK-Instanz.

Der Nutzer des Zugangsmoduls mit der Rolle Kunde

- bezieht ein Zugangsprofile zum TI-Gateway und

- vergibt/entzieht den Remote-Zugang zum Admin-Interface seiner HSK-Instanz für DVO.

Der Kunde hat einen Vertrag mit dem Anbieter des TI-Gateway und beauftragt ggf. einen DVO.

### Weitere Rollen

Die Hersteller von anderen Komponenten (Intermediär, Zugangsmodul) haben abgesehen von ggf. Support für die von ihnen entwickelten Komponenten keine Rolle im Betrieb.

## 4.7 Rollenkombinationen & Rollenausschlüsse

Durch die Beschränkung der Rollen, die ein Mitarbeiter eines Anbieters TI-Gateway und seiner Unterauftragnehmer innehat, soll der Zugang zu medizinischen und personenbezogenen Versichertendaten verhindert werden.

Personen können mehrere der oben genannten Rollen ausführen. Folgende Rollen können dabei kombiniert werden

### Erlaubte Rollenkombination

Rollen Szenario						
	Betreiber	Vertrieb	Hersteller	lokaler Admin/ DVO	remote Admin	Leistungs- erbringer
Vertrieb und DVO	✗	✓	✗	✓	✗	✗
Vertrieb und Support	✗	✓	✗	✗	✓	✗
Kunde als Admin	✗	✗	✗	✓	✗	✓
Betreiber mit Support	✓	✗	✗	✗	✓	✗
Vertrieb und Betreiber	4-Augen Prinzip für Löschen von Instanz	4-Augen Prinzip für Löschen von Instanz	✗	✗	✗	✗

erlaubt

erlaubt mit  
Bedingungen

### Erlaubte Rollenkombination

Rollen Szenario						
	Betreiber	Reseller	Hersteller	lokaler Admin/ DVO	remote Admin	Leistungs- erbringer
Reseller mit DVO	✗	✓	✗	✓	✗	✗
Reseller mit Support	✗	✓	✗	✗	✓	✗
LE als Admin	✗	✗	✗	✓	✗	✓
Betreiber mit Support	✓	✗	✗	✗	✓	✗
Reseller und Betreiber	4-Augen Prinzip für Löschen von Instanz	4-Augen Prinzip für Löschen von Instanz	✗	✗	✗	✗

erlaubt

erlaubt mit  
Bedingungen



Abbildung 3: Szenarien mit erlaubten Rollenkombinationen

**A\_23237 - Rollenausschluss Betreiber - DVO**

Der Anbieter des TI-Gateways MUSS sicherstellen, dass Personen aus dem Betrieb des TI-Gateways (Rolle Betreiber) nicht zeitgleich als lokale Administratoren von HSK-Instanzen des TI-Gateway (Rolle DVO) tätig werden und dass entsprechende Prozesse definiert und etabliert sind, die dies dauerhaft gewährleisten und eine regelmäßige Validierung der Umsetzung durchsetzen. Die Umsetzung des Rollenausschluss MUSS die Weisungsbefugnis von Vorgesetzten berücksichtigen. Das heißt, dass kein Vorgesetzter direkte Weisungsbefugnis sowohl für Personen mit der Rolle Betreiber als auch für Personen mit der Rolle DVO innehaben darf (ausgenommen ist das Management des Unternehmens). [Anb\_TI\_Gateway, organ./betriebl. Eignung: Anbietererklärung, Sich.techn. Eignung: Gutachten (Anbieter), <=]

**34721A\_23238-01 - Rollenausschluss Hersteller - andere Rollen**

Der Anbieter des TI-Gateways MUSS sicherstellen, dass keine Personen, die in der Herstellung (Entwicklung/Implementierung) des HSK und/oder des Zugangsmoduls tätig ist, Aufgaben eines Betreibers, Resellerdes Vertriebs oder eines DVOs übernimmt und dass entsprechende Prozesse definiert und etabliert sind, die dies dauerhaft gewährleisten und eine regelmäßige Validierung der Umsetzung durchsetzen. [Anb\_TI\_Gateway, organ./betriebl. Eignung: Anbietererklärung, Sich.techn. Eignung: Gutachten (Anbieter), <=]

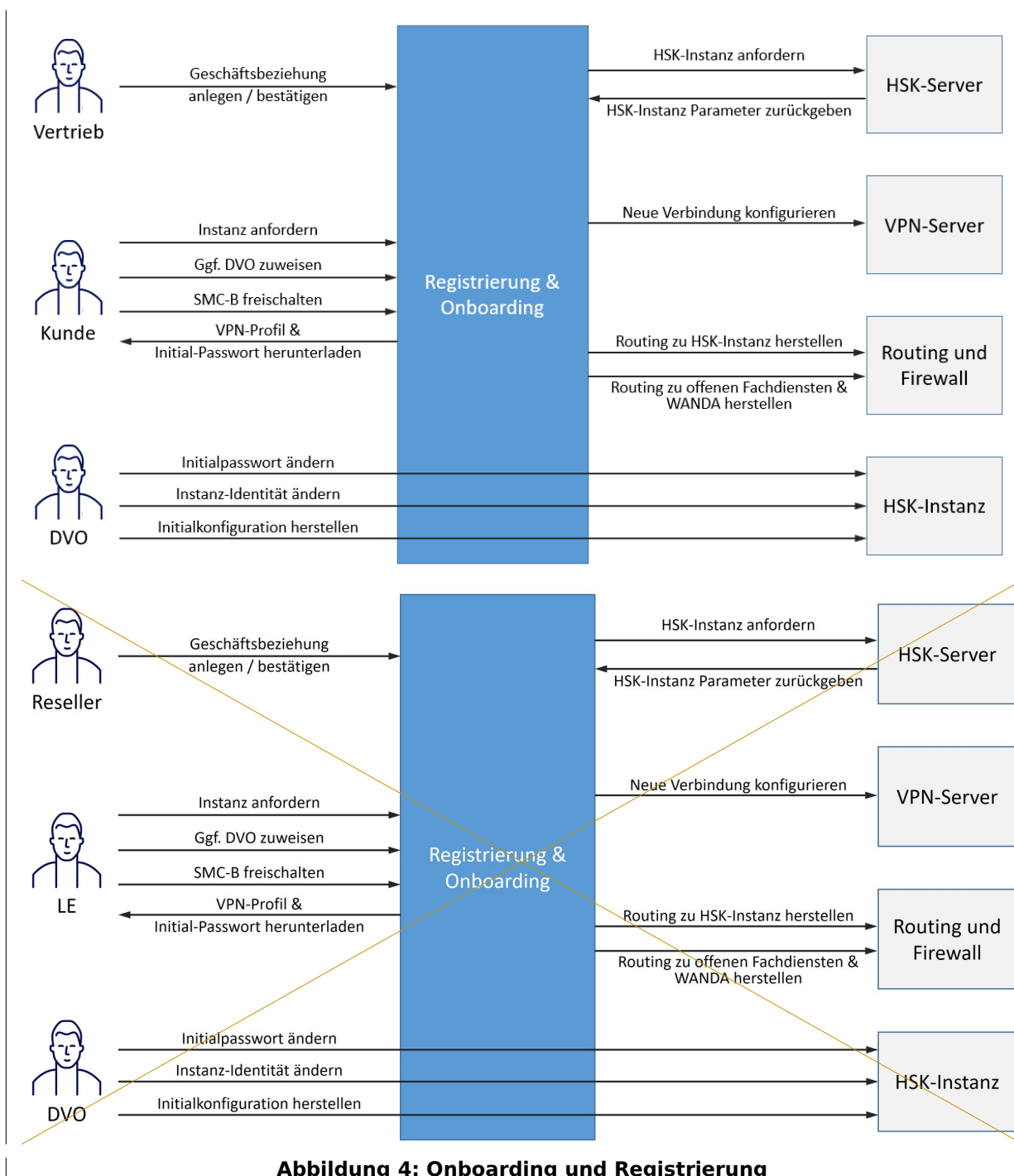
Die Einschränkung aus den obigen Anforderung muss vertraglich zwischen Anbieter und seinen Unterauftragnehmern festgelegt werden. Die Unterauftragnehmer müssen diese Einschränkung vertraglich mit ihren Mitarbeitern festlegen.

**34722A\_23239-01 - Rollenkombination Betreiber - ResellerVertrieb**

Der Anbieter des TI-Gateway MUSS sicherstellen, dass für das Löschen von HSK-Instanzen ein 4-Augen-Prinzip unter Mitwirkung des ResellerVertriebs zur Anwendung kommt. [Anb\_TI\_Gateway, organ./betriebl. Eignung: Anbietererklärung, Sich.techn. Eignung: Gutachten (Anbieter), <=]

## 5 Spezifikation Zugangsmodul

### 5.1 Onboarding und Registrierung



**Abbildung 4: 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. Im Folgenden wird der Prozess exemplarisch beschrieben. Die Konkrete Umsetzung darf davon abweichen, solange die formulierten Anforderungen erfüllt werden. Die Automatisierung manueller Schritte ist ausdrücklich erwünscht.

Der **ResellerVertrieb** oder im Falle einer Selbstregistrierung der **LeistungserbringNutzer** startet den Registrierungsprozess.

Der **LeistungserbringerNutzer** 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-Profilen mit Credentials und der Inner-IP für die **LE-Nutzer** Umgebung. Der **LE-Nutzer** wählt, ob er ein VPN-Profil für ein VPN-Gateway, mehrere VPN-Profilen für Software-VPN-Clients auf verschiedenen Rechnern oder separate VPN-Profilen für Kartenterminals benötigt.
3. Das Onboarding-Modul konfiguriert den VPN-Server und das Routing für diese **LE-Nutzer** Umgebung zu der zugehörigen HSK-Instanz. Wenn ein über VPN angeschlossener DVO auf die HSK-Instanz zugreifen soll, gibt der **LE-Nutzer** 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 einen VPN-Kanal konfiguriert der DVO 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 Clientsystemen verteilt wird. Somit kann später bei jeder Server-Authentifizierung konkret die Instanz der **LEs Nutzers** 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-NetzNetz des Nutzers** zu WANDA und offenen Fachdiensten frei.

### 5.1.1 Nutzerportal

MainlineIn den nachfolgende Anforderungen genannten Leistungserbringer stehen exemplarisch für die Nutzer des TI-Gateways und schließen andere Nutzer des TI-Gateways ein.

#### **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 prüfbarer 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. [TI\_GW\_Zugangsmodul, Sich.techn. Eignung: Produktgutachten, funkt. Eignung: Test Produkt/FA, <=]

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 für den Zugang zum Nutzer-Portal mit zwei Faktoren authentifizieren und dabei sowohl durchsetzen, dass die Faktoren aus verschiedenen Kategorien stammen:

- Wissen: Passwort (ORP.4.A22 des BSI-Grundschutzkompendiums ist zu beachten), PIN (min. 6-stellig);
- Besitz: Chipkarte, TAN-Generator, pushTAN, hardwaregebundenes kryptographische Token;
- Biometrie: Android: Biometric Class 3 (ehemals "Strong") oder äquivalent, iOS: Face-ID, Fingerabdruck;

als auch, dass die Faktoren nicht unabhängig voneinander angreifbar sind.

[TI\_GW\_Zugangsmodul, Sich.techn. Eignung: Produktgutachten, funkt. Eignung: Test Produkt/FA, <=]

Informationen zu Biometrie-Klassen unter Android sind unter <https://source.android.com/docs/compatibility/cdd> zu finden.

### **A\_23338 - TI-Gateway Zugangsmodul - Schutz der Zugangsdaten**

Das Zugangsmodul MUSS die Nutzer-Portal-Zugangsdaten/-faktoren der Nutzer geschützt vor unberechtigter Kenntnisnahme und Manipulation - auch von Administratoren - speichern. Das Zugangsmodul MUSS Änderungen von Zugangsdaten/-faktoren von Nutzern mit zwei Faktor Authentisierung nur nach erfolgreicher Zwei-Faktor-Authentisierung zulassen.[TI\_GW\_Zugangsmodul, Sich.techn. Eignung: Produktgutachten, <=]

### **A\_23339 - TI-Gateway Zugangsmodul - Maßnahmen bei vergessenen oder verlorenen Zugangsfaktoren**

Wenn das Zugangsmodul Maßnahmen zum Zurücksetzen von Zugangsfaktoren für das Nutzer-Portal implementiert, DARF es NICHT die Sicherheit der Zwei-Faktor-Authentisierung aushebeln.[TI\_GW\_Zugangsmodul, Sich.techn. Eignung: Produktgutachten, <=]

Dies kann bspw. über ein registriertes E-Mail-Konto des Nutzers geschehen, sofern dieses in dem Sinne als dritter Faktor fungiert, also nicht bereits in die 2FA eingebunden ist und jeweils nur ein Faktor zurückgesetzt werden kann, also nicht beide gleichzeitig.

### **35421A\_23363-01 - TI-Gateway Zugangsmodul - Freischaltung von HSK-Instanzen für Nutzer**

Das Zugangsmodul MUSS durchsetzen, dass HSK-Instanzen erst erzeugt werden, wenn diesbezüglich ein Vertrag abgeschlossen wurde (Freigabe durch [ResellersVertrieb](#)). [TI\_GW\_Zugangsmodul, Sich.techn. Eignung: Produktgutachten, <=]

Die obige Anforderung zielt darauf ab, dass neue Nutzer vertrieblich qualifiziert werden, bevor sie Zugang zu einer HSK-Instanz bekommen. Damit soll ausgeglichen werden, dass die technische Berechtigungsprüfung mit der SMC-B erst später im Onboardingprozess erfolgen kann.

### **35376A\_23353-01 - 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 [ResellersVertriebs](#) - 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).

[TI\_GW\_Zugangsmodule, funkt. Eignung: Test Produkt/FA, <=]

Als Variante zur Zustellung des VPN-Profiles über das Nutzerportal kann auch ein Provisionierungssystem angebunden werden, wenn z.B. vorkonfigurierte VPN-Gateway-Hardware zum Einsatz kommt.

Für den Fall, dass seine VPN-Schlüssel korrumpiert wurden, gilt:

#### **A\_23439 - TI-Gateway Zugangsmodule - Wechsel von VPN-Profilen**

Das TI-GW-Zugangsmodule MUSS dem LE ermöglichen, bestehende VPN-Profile zu deaktivieren und neue VPN-Profile zu generieren.

[TI\_GW\_Zugangsmodule, funkt. Eignung: Test Produkt/FA, <=]

#### **A\_23281 - Schutz der privaten VPN-Schlüssel und initialer Passwörter bei zentraler Speicherung**

Das Zugangsmodule MUSS das VPN-Profil eines Nutzers sowie das initiale Instanz-Administrator-Passwort ausschließlich dem authentifizierten Nutzer (Leistungserbringer) oder dem authentifizierten DVO, der vom Nutzer ausgewählt wurde, zugänglich machen. Die privaten Schlüssel für die VPN-Clientauthentisierung, die VPN-Serverauthentisierung und das initiale Instanz-Administrator-Passwort MÜSSEN bei der zentralen Speicherung vor unberechtigtem Zugriff und Manipulation - auch von Administratoren beim Zugangsmodule - 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 (siehe dazu auch A\_23366\*). [TI\_GW\_Zugangsmodule, Anb\_TI\_Gateway, Sich.techn. Eignung: Produktgutachten, Sich.techn. Eignung: Gutachten (Anbieter), <=]

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 Zugangsmodule - Sichere Übermittlung VPN-Profil an DVOs**

Das Zugangsmodule 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. [TI\_GW\_Zugangsmodule, Sich.techn. Eignung: Produktgutachten, <=]

#### **A\_23243 - Netzzugang zur TI nach SMC-B Prüfung**

Das Zugangsmodule 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.

[TI\_GW\_Zugangsmodule, Sich.techn. Eignung: Produktgutachten, funkt. Eignung: Test Produkt/FA, <=]

### **5.1.2 Initiale Authentifizierung der HSK-Instanz**

Im Rahmen der Ersteinrichtung der HSK-Instanz muss sich der Nutzer bzw. der vom Nutzer beauftragte DVO bei der ersten Verbindung mit der Management-Schnittstelle davon überzeugen, dass er tatsächlich mit einem echten TI-Highspeed-Konnektor kommuniziert. Dafür muss die Authentizität des HSK über dessen TI-Identitäten (AK.AUT)

geprüft werden. Hierbei kann eine HSK-weit genutzte Identität verwendet werden, diese muss also nicht Instanz-individuell sein. Erst nach dem Etablieren dieser Vertrauensbeziehung können nachfolgende Prüfschritte und die Ersteinrichtung stattfinden, wobei dann bspw. auch individuelle Identitäten und Zertifikate für spätere Verbindungen zur SOAP- und Management-Schnittstelle erzeugt werden.

Der einfachste Fall - wie er auch bei Inbox-Konnektoren vorliegt - ist eine über den Webbrowser bediente Administrations-GUI. Diese hat für die Zertifikatsprüfung den Nachteil, dass Webbrowser keine TI-Zertifikate positiv validieren. Im Falle von Inboxkonnektoren können entsprechende Warnungen des Browsers durch die manuelle Prüfung von im Browser anzeigbaren Zertifikatsdaten sowie vor allem die gleichzeitige Kontrolle über Konnektor, Netzwerk und Client akzeptiert werden. Dies ist beim TI-Gateway nicht möglich. Es ist ein essentieller Schritt bei der ersten Verbindung die Authentizität technisch vollständig zu prüfen.

Allein mit einem Webbrowser ist dies also beim TI-Gateway nicht möglich (oder nur höchst umständlich). Daher ist ein zusätzlicher Software-Client notwendig, der mindestens die Prüfung des TI-Zertifikats übernimmt und entweder weiter gefasst ist und auch die Management-GUI umfasst oder zumindest eine Validierung des anschließend im Browser mit einer Warnung angezeigten Zertifikats ermöglicht (Abgleich von Fingerprint des im Software-Client geprüften Zertifikats gegen den im Browser anzeigbaren Fingerprint). Letztere Variante ermöglicht anschließend eine Nutzung des Browsers für die Administration. In der Minimal-Version ist der Software-Client ein Kommandozeilen-Tool.

Sofern ein Browser involviert ist, sind die dadurch gegebenen Implikationen von Herstellern und Anbietern zu berücksichtigen, wie die in Webbrowsern nicht vorhandene Unterstützung von Zertifikaten und Schlüsseln, die auf Brainpool-Kurven basieren. Auch wenn nur einmalig bei der initialen Verbindung das C.AK.AUT in Zusammenspiel mit einem Webbrowser verwendet werden soll (weil anschließend Instanz-individuelle self-signed-Zertifikate erzeugt oder importiert werden), ist dies technisch nicht möglich, wenn das C.AK.AUT auf Brainpool-Kurven basiert.

Die geschilderte Prüfung der Authentizität gegen eine TI-Identität muss lediglich einmalig als initialer Schritt stattfinden. Über die so gebildete Vertrauensbeziehung ist die Erzeugung oder der Import individueller Nicht-TI-Identitäten möglich, wie es auch Inbox-Konnektoren heute schon unterstützen. Diese Identitäten können dann in Form von Allow-Listen in die genutzten Clientsysteme importiert werden, sodass spätere Authentifizierungen gegen diese Prüfbasis durchgeführt werden. Erzeugung und Import individueller Nicht-TI-Identitäten kann für eine einfache Handhabung in das Tool integriert werden.

Grundsätzlich ergibt sich somit initial folgender Ablauf:

- Nutzer bzw. DVO (im Folgenden nur DVO) hat VPN-Profil, Initial-Passwort und Software-Client heruntergeladen
- DVO hat den VPN-Client installiert / eingerichtet und den VPN-Tunnel aufgebaut
- DVO kennt IP-Adresse seiner HSK-Instanz und kann diese von seinem Clientsystem aus über den VPN-Tunnel erreichen
- DVO nutzt den Software-Client, welcher parametrisiert mit der IP-Adresse der HSK-Instanz einen TLS-Verbindungsaufbau zur Management-Schnittstelle der Instanz durchführt und das C.AK.AUT prüft
- Der Software-Client gibt im Positiv-Fall das Prüfergebnis sowie den SHA-256 Wert des geprüften C.AK.AUT aus
- DVO verbindet sich über Webbrowser mit der HSK-Instanz
- Der Webbrowser gibt eine Warnung zur unsicheren Verbindung aus



- DVO lässt sich über die weiteren Informationen das Zertifikat und dort den SHA-256 Wert anzeigen
- DVO vergleicht die SHA-256 Werte und akzeptiert im Positiv-Fall die Verbindung im Browser
- Es findet die Ersteinrichtung unter Berücksichtigung weiterer Prüfungen im Webbrowser statt (siehe A\_23340\*).

Da der Software-Client die Zertifikatsprüfung durchführt, muss genau dieser Aspekt durch einen Gutachter technisch geprüft werden (A\_23341\*).

Für den Highspeed-Konnektor ist in diesem Zusammenhang A\_23469\* und A\_23470\* in [gemF\_Highspeed-Konnektor] zu beachten.

### **35357A\_23341-01 - TI-Gateway Zugangsmodul - Client-Software für Prüfung HSK-TLS-Zertifikat**

Das TI-GW-Zugangsmodul MUSS eine Client-Software umfassen, welche unter Angabe der IP-Adresse der HSK-Instanz einen TLS-Verbindungsaufbau zur Management-Schnittstelle dieser Instanz durchführt, dabei das C.AK.AUT Zertifikat des HSK wie folgt prüft:

- Prüfung der Signatur des Zertifikats gegen ein aktuell gültiges Komponenten-CA-Zertifikat [GEM.KOMP-CAX.der] vom TSL-Downloadpunkt <https://download.tsl.ti-dienste.de/SUB-CA/>,
  - Prüfung auf zeitliche Gültigkeit des Zertifikats,
  - Prüfung auf die Zertifikatstyp-OID oid\_ak\_aut,
  - Prüfung auf Sperrstatus "good" mittels des OCSP-Responders der Komponenten-CA im Internet
- (~~R~~**S**aktuelle URLs: **RS**A: <http://download.crl.ti-dienste.de/ocsp> | ECC: <http://download.crl.ti-dienste.de/ocsp/ec>),

ein entsprechend aussagekräftiges Prüfergebnis ausgibt und im Positiv-Fall zusätzlich den SHA-256 Wert des Zertifikats ausgibt, mit dem sich das Admin-Interface der HSK-Instanz bei nachfolgenden Verbindungen identifiziert (C.AK.AUT oder ggf. über Client-SW bereits importiertes oder erzeugtes individuelles Zertifikat).

[TI\_GW\_Zugangsmodul, Sich.techn. Eignung: Produktgutachten, <=]

Die Internet-Schnittstelle des OCSP-Responders für Zertifikate der Kogematik-eHealth-CA finden sich in den jeweiligen Zertifikaten.

Die Internet-Schnittstelle des OCSP-Responders der TI-Komponenten-CA für die RU/TU finden sich hier:

- RSA: <http://download-testref.crl.ti-dienste.de/ocsp>
- ECC: <http://download-testref.crl.ti-dienste.de/ocsp/ec>

### **A\_26629 - TI-Gateway Zugangsmodul - Verifikation Prüfbarkeit HSK-TLS-Zertifikat durch Hersteller Zugangsmodul**

Der Hersteller des TI-GW-Zugangsmoduls MUSS regelmäßig prüfen, dass die C.AK.AUT-Zertifikate der über sein Zugangsmodul zugänglichen Highspeed-Konnektoren mit der von ihm bereitgestellten Client-Software vollständig prüfbar sind, was insbesondere die Prüfung des Sperrstatus via OCSP umfasst. Dies gilt für alle Umgebungen (RU, TU und PU).[TI\_GW\_Zugangsmodul, Sich.techn. Eignung: Herstellererklärung, <=]

### **A\_23340 - TI-Gateway Zugangsmodul - Beschreibung Authentifizierung & Verifikation HSK-Instanz**

Der Anbieter TI-Gateway MUSS seinen Nutzern (Leistungserbringer bzw. deren DVO) Informationen zur Hand geben, dass beim initialen Verbindungsaufbau zur

Administrationsschnittstelle der HSK-Instanz deren Authentizität überprüft werden muss und wie dies möglich ist. Dies umfasst mindestens

- die technische Prüfung des TLS-Zertifikats C.AK.AUT des HSK mittels des Software-Clients (siehe A\_23341\*)
- Bei Verwendung eines Webbrowsers zur Administration:
  - der Abgleich des SHA-256 Werts des im Browser bei der Verbindung zur Management-Schnittstelle der HSK-Instanz mit einer Sicherheitswarnung angezeigten Zertifikats gegen den durch den Software-Client angezeigten SHA-256 Wert
- die Verifikation, dass die HSK-Instanz zur Änderung des Passworts für den Admin-Account auffordert,
- die Änderung des Passworts des Admin-Accounts,
- die Verifikation, dass keine weiteren Admin-Nutzer in der HSK-Instanz angelegt sind,
- die Verifikation, dass das Informationsmodell der HSK-Instanz leer/unkonfiguriert ist bei der Ersteinrichtung,
- Import der individuellen HSK-Instanz-Identität in die "Allowlist" der Clientsysteme und den ggf. für die Administration genutzten Webbrowser
  - 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.

Zudem MUSS der Nutzer darauf hingewiesen werden im Nutzer-Portal zu prüfen, dass initial keine Freischaltung für Remote-Zugänge zur HSK-Instanz aus DVO-Netzen konfiguriert sind.

**[Anb\_TI\_Gateway, Sich.techn. Eignung: Gutachten (Anbieter), <=]**

Die oben in A\_23340\* dargestellten Prüfungen sind wie bereits zu Beginn des Abschnitts geschildert einmalig beim initialen Verbindungsaufbau durchzuführen. Anschließend Zertifikats-Prüfungen erfolgen gegen eine Allowlist wie im letzten Punkt von A\_23340\* beschrieben.

### 5.1.3 Betriebsfunktionen für den **LeistungserbringerNutzer des TI-Gateways**

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. Verfügbarkeitsdaten werden vom HSK ermittelt und dem Zugangsmodul bereitgestellt (siehe A\_23446).

#### **A\_23302-01 - 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. Hierzu zählen auch die Dienste für eRezept und der verwendete KIM-Dienst, sowie die vom HSK über A\_23446\* bereitgestellten Informationen.

**[TI\_GW\_Zugangsmodul, funkt. Eignung: Test Produkt/FA, <=]**



## 5.2 VPN

Der VPN-Service des TI-Gateway-Zugangsmoduls ermöglicht es Leistungserbringer Nutzer umgebungen 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. [TI\_GW\_Zugangsmodul, Sich.techn. Eignung: Produktgutachten, <=]

### **A\_23379-01 - TI-Gateway-Zugangsmodul - VPN - Protokoll**

Das Zugangsmodul MUSS Nutzer mittels eines VPN-Kanals anbinden, welcher auf den Protokollen IPsec/IKEv2, TLS oder WireGuard beruht und dafür VPN-Server und VPN-Client bereitstellen. [TI\_GW\_Zugangsmodul, Sich.techn. Eignung: Produktgutachten, <=]

ABei Verwendung der von TIs Protokolle sind aktuell zur Erfüllung von A\_23379-\* gilt bzgl. kryptographischer Vorgaben [gemSpec\_Krypt#A\_24779\*]. Die folgenden Anforderungen beziehen sich auf IPsec/IKEv2, TLS und WireGuard-vorgesehen.

#### **Hinweis bzgl. WireGuard**

*Das WireGuard-Protokoll und die darin genutzten kryptographischen Algorithmen befinden sich derzeit noch in einer detaillierteren Sicherheitsbewertung, weshalb diese aktuell noch mit einem Vorbehalt versehen sind.*

*Dies betrifft die Anforderungen*

- ~~A\_23379\* (Protokoll),~~
- ~~A\_23375\* und A\_23377\* (Curve25519),~~
- ~~A\_23376\* (ChCha20Poly1305) und~~
- ~~A\_23378\* (BLAKE2s).~~

.

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>

Es kann für eine LEI sowohl eine VPN-Verbindung zu einem VPN-Router aufgebaut werden, als auch mehrere VPN-Verbindungen zu einzelnen Rechnern und Kartenterminals. Dabei müssen unterschiedliche VPN-Client-Identitäten zum Einsatz kommen.

### **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 asymmetrischer 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.

[TI\_GW\_Zugangsmodul, Sich.techn. Eignung: Produktgutachten, <=]

### **A\_23376 - TI-Gateway-Zugangsmodul - VPN - Transportschutz**

Das Zugangsmodul MUSS für den VPN-Kanal am Server und am Client einen Transportschutz für alle übermittelten Daten bzgl. Vertraulichkeit und Integrität

durchsetzen unter Verwendung symmetrischer Chiffren aus der Menge {AES128, AES256, ChaCha20Poly1305}.[TI\_GW\_Zugangsmodule, Sich.techn. Eignung: Produktgutachten, <=]

### **A\_23377 - TI-Gateway-Zugangsmodule - VPN - Ephemere Sitzungs-Schlüssel**

Das Zugangsmodule 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}.[TI\_GW\_Zugangsmodule, Sich.techn. Eignung: Produktgutachten, <=]

### **A\_23378 - TI-Gateway-Zugangsmodule - VPN - Hash-Funktionen**

Das Zugangsmodule 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.[TI\_GW\_Zugangsmodule, Sich.techn. Eignung: Produktgutachten, <=]

### **A\_23380 - TI-Gateway-Zugangsmodule - VPN - Prüfung Sperrstatus Clients**

Das Zugangsmodule MUSS bei der Client-Authentifizierung durch den Server im Rahmen des VPN-Verbindungsaufbaus den Sperrstatus der Client-Identität prüfen (Vergleich A\_23261\*).[TI\_GW\_Zugangsmodule, Sich.techn. Eignung: Produktgutachten, <=]

### **A\_23381 - TI-Gateway-Zugangsmodule - VPN - Abbruch Verbindungsaufbau im Fehlerfall**

Das Zugangsmodule 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.

[TI\_GW\_Zugangsmodule, Sich.techn. Eignung: Produktgutachten, funkt. Eignung: Test Produkt/FA, <=]

### **A\_23364 - TI-Gateway-Zugangsmodule - VPN-Client - Server-Authentifizierung**

Der VPN-Client eines TI-Gateway-Zugangsmoduls MUSS den VPN-Server gegen eine ihm vorliegende Prüfbasis authentifizieren.[TI\_GW\_Zugangsmodule, Sich.techn. Eignung: Produktgutachten, <=]

Die Prüfbasis hängt vom gewählten Authentifizierungsverfahren ab: Schlüssel, Zertifikat, CA-Zertifikat...

### **35422A\_23365-01 - TI-Gateway-Zugangsmodule - VPN-Client - VPN-Protokoll**

Der Hersteller des VPN-Client eines TI-Gateway-Zugangsmoduls MUSS das VPN-Protokoll im Client-entsprechend A\_23364\*, 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.[TI\_GW\_Zugangsmodule, Sich.techn. Eignung: Produktgutachten, <=]

Idealer Weise können bestehende Sicherheitsnachweise 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.[Anb\_TI\_Gateway, Sich.techn. Eignung: Gutachten (Anbieter), <=]

### **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.

[TI\_GW\_Zugangsmodule, Sich.techn. Eignung: Produktgutachten, funkt. Eignung: Test Produkt/FA, <=]

## 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. [TI\_GW\_Zugangsmodul, Sich.techn. Eignung: Produktgutachten, <=]

Einem Kunden können mehrere HSK-Instanzen zugewiesen werden, aber eine HSK-Instanz kann nur einem Kunden zugewiesen sein. Siehe auch A\_23390

### A\_23370 - Zugang 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.

[TI\_GW\_Zugangsmodul, Sich.techn. Eignung: Produktgutachten, <=]

Für den Zugang zum Administrationsinterface sind zwei unabhängige Sicherungsschichten umzusetzen. Eine Schicht kontrolliert den Zugang zum Administrationsinterface, die zweite Schicht ist die Authentisierung an der HSK-Instanz.

### ~~35500~~A\_23394-01 - Routing zum fachlichen Interface einer HSK-Instanz

Das TI-GW-Zugangsmodul MUSS sicherstellen, dass das fachliche Interface (SOAP, LDAP, CETP), SICCT 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. [TI\_GW\_Zugangsmodul, Sich.techn. Eignung: Produktgutachten, <=]

### 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.

[TI\_GW\_Zugangsmodul, funkt. Eignung: Test Produkt/FA, <=]

## 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 aktiven C.HCI.AUT (SM-B-AUT-Zertifikat) einmal täglich prüfen.

[TI\_GW\_Zugangsmodul, funkt. Eignung: Test Produkt/FA, <=]

### TIP1-A\_5390-01 - TI-GW-Zugangsmodul, gesperrtes C.HCI.AUT Zertifikat

Das Zugangsmodul MUSS, wenn die zyklische Prüfung ergeben hat, dass eine HSK-Instanz keinen Zugriff auf ein gültiges C.HCI.AUT (SM-B-AUT-Zertifikat) hat, das mit dieser Instanz assoziierte 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. [TI\_GW\_Zugangsmodul, funkt. Eignung: Test Produkt/FA, <=]

Die eigentliche Gültigkeitsprüfung der SM-B wird durch den HSK durchgeführt (A\_23444). Die Freischaltung der offenen Fachdienste und Wanda wird durch A\_23243\* geregelt.

### A\_23248 - DDoS-Protection

Das TI-GW-Zugangsmodul und der Anbieter des TI-Gateway MÜSSEN Angriffe auf die Verfügbarkeit des TI-Gateways (DDoS) an seinen Schnittstellen zum Internet abwehren und dabei die Empfehlungen des BSI sowie, wenn ein qualifizierter Dienstleister zum Schutz vor DDoS-Angriffen beauftragt wird, die Kriterien des BSI zur

Auswahl qualifizierter Dienstleister berücksichtigen. [TI\_GW\_Zugangsmodul, Anb\_TI\_Gateway, Sich.techn. Eignung: Produktgutachten, Sich.techn. Eignung: Gutachten (Anbieter), <=]

Empfehlungen des BSI zur Abwehr von DDoS-Angriffen sind unter [https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Gefahren/DDoS/ddos\\_node.html](https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Gefahren/DDoS/ddos_node.html) und Kriterien für entsprechende Dienstleister sind unter [https://www.allianz-fuer-cybersicherheit.de/Webs/ACS/DE/Informationen-und-Empfehlungen/Informationen-und-weiterfuehrende-Angebote/Qualifizierte-Dienstleister/qualifizierte-dienstleister\\_node.html](https://www.allianz-fuer-cybersicherheit.de/Webs/ACS/DE/Informationen-und-Empfehlungen/Informationen-und-weiterfuehrende-Angebote/Qualifizierte-Dienstleister/qualifizierte-dienstleister_node.html) zu finden.

#### **A\_23249 - Erkennung und Abwehr unberechtigter Zugriffe**

Das TI-GW-Zugangsmodul MUSS Maßnahmen zum Erkennen und zur Abwehr unberechtigter Zugriffe aus dem Internet sowie aus angeschlossenen LEI- und DVO-Netzen umsetzen (bspw. durch Paketfilter, Netflow, IDS/IPS, ALG). [TI\_GW\_Zugangsmodul, Anb\_TI\_Gateway, Sich.techn. Eignung: Produktgutachten, Sich.techn. Eignung: Gutachten (Anbieter), <=]

Auch aus per VPN angeschlossenen Netzen von [Leistungserbringerinstitutionen Nutzern des TI-Gateways](#) 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 [Leistungserbringberechtigte Nutzer](#) 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, die Nutzer dieser Zugänge unverzüglich darüber informieren und Maßnahmen bis hin zur Sperrung der betroffenen VPN-Zugänge umsetzen. Eine vollständige Sperrung des Zugangs muss dabei immer das letzte Mittel sein. [TI\_GW\_Zugangsmodul, Anb\_TI\_Gateway, Sich.techn. Eignung: Produktgutachten, Sich.techn. Eignung: Gutachten (Anbieter), <=]

#### **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 und eine Klärung der Situation möglich ist und eine Sperrung möglichst, vermieden werden kann, sofern dies sicherheitstechnisch vertretbar ist. Ebenso müssen Situationen, die zu einer Sperrung geführt haben, schnellst möglich geklärt werden können um den Zugang wieder zu entsperren. [Anb\_TI\_Gateway, Sich.techn. Eignung: Gutachten (Anbieter), <=]

#### **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. [TI\_GW\_Zugangsmodul, Anb\_TI\_Gateway, Sich.techn. Eignung: Produktgutachten, Sich.techn. Eignung: Gutachten (Anbieter), <=]

#### **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. [TI\_GW\_Zugangsmodul, Anb\_TI\_Gateway, Sich.techn. Eignung: Produktgutachten, Sich.techn. Eignung: Gutachten (Anbieter), <=]

#### **A\_23342 - TI-GW-Zugangsmodul - Richtlinien für den Paketfilter zum Internet**

Der Paketfilter des TI-GW-Zugangsmodus MUSS die Weiterleitung von IP-Paketen an der Schnittstelle zum Internet auf genau die Protokolle beschränken, die für die verwendete VPN-Technologie und das Nutzer-Portal zwingend erforderlich sind. Ein Verbindungsaufbau aus dem TI-GW-Zugangsmodus in Richtung Internet MUSS unterbunden werden. Ausnahmen davon bspw. für die Erreichbarkeit von Update-Servern sind mit dem Gutachter abzustimmen, von diesem zu bewerten und im Falle der Abnahme (positiven Bewertung) durch den Gutachter nachvollziehbar im Gutachten zu dokumentieren. [TI\_GW\_Zugangsmodus, Sich.techn. Eignung: Produktgutachten, <=]

#### **A\_23457 - Weiterleitung gesammelter Informationen zu Bedrohungen an zentrales Security Monitoring**

Der Anbieter TI-Gateway MUSS die Informationen über potenzielle Bedrohungen, die durch die Umsetzung von A\_23248\*, A\_23249\*, A\_23342\* und TIP1-A\_4338\* gesammelt werden an ein zentrales Security Monitoring (siehe GS-A\_5557\* und A\_20719\*) zur übergreifenden Erkennung und Analyse weiterleiten. [Anb\_TI\_Gateway, Sich.techn. Eignung: Gutachten (Anbieter), <=]

#### **TIP1-A\_4292-01 - TI-GW-Zugangsmodus, Härtung des VPN-Konzentrators**

Die VPN-Konzentratoren des Zugangsmodus MÜSSEN so konfigurier~~ent~~ werden, dass ausschließlich die erforderlichen Netzwerkprotokolle und kryptographischen Methoden akzeptiert werden. [TI\_GW\_Zugangsmodus, Sich.techn. Eignung: Produktgutachten, <=]

#### **A\_23343 - TI-GW-Zugangsmodus - Kein direkter Zugriff auf zentrale Dienste und gesicherte Fachdienste**

Das TI-GW-Zugangsmodus MUSS einen direkten Zugriff aus dem Internet und den Netzen angeschlossener Nutzer auf gesicherte Fachdienste und zentrale Dienste verhindern. [TI\_GW\_Zugangsmodus, Sich.techn. Eignung: Produktgutachten, <=]

#### **~~35363~~A\_23344-01 - TI-GW-Zugangsmodus - ~~Verbindungen~~Sicherer Zustand bei Komponentenausfall beenden**

Das TI-GW-Zugangsmodus MUSS sicherstellen, dass ~~alle bestehend~~beim Ausfall von ~~sicherheitsrelevanten VPN-Verbindung~~Komponenten beendet werden und ~~des Zugangsmodus oder des Highspeed-Konnektors~~ keine ~~neuen Verbindu~~Zugriffe aus ~~angen~~ zugelassen werden, wenn ~~nachgelagertes~~geschlossenen Netzen auf TI-Gateway-Services, für ~~die die ausgefallenen~~ Komponenten ~~vollständig~~ausgefallen sind, ~~mehr möglich sind~~ und ~~da, bspw. in dem alle Zugriffe durch die Nutzung des TI-Gate~~eine Fireways nicht mehr ~~möglich ist~~ blockiert oder alle VPN-Verbindungen getrennt werden.

[TI\_GW\_Zugangsmodus, Sich.techn. Eignung: Produktgutachten, funkt. Eignung: Test Produkt/FA, <=]

#### **A\_23345 - TI-GW-Zugangsmodus - Härtung Zugänge**

Das TI-GW-Zugangsmodus MUSS sicherstellen, dass es ausschließlich definierte und gehärtete Schnittstellen anbietet - auch für die Administration - ohne Low-Level-Zugänge mit Systemrechten. [TI\_GW\_Zugangsmodus, Sich.techn. Eignung: Produktgutachten, <=]

#### **A\_23366 - TI-GW-Zugangsmodus - Nutzung HSM**

Das TI-GW-Zugangsmodus MUSS für die Erzeugung von Zufallszahlen und Schlüsseln ein nach FIPS 140-2 Level 3 oder Common Criteria EAL 4 zertifiziertes HSM verwenden und geheime Schlüssel in diesem HSM vor Zugriff geschützt speichern, so dass nur das TI-GW-Zugangsmodus selbst die Schlüssel nutzen kann. Dies bezieht sich mindestens auf folgende Schlüssel:

- Geheime Schlüssel zur Authentisierung gegenüber dem HSK
- Schlüssel zum Schutz von Vertraulichkeit und Integrität persistent gespeicherter Daten (bspw. die privaten Schlüssel von VPN-Konzentratoren)

[TI\_GW\_Zugangsmodus, Sich.techn. Eignung: Produktgutachten, <=]

#### **A\_23473 - TI-GW-Zugangsmodus - Nachnutzung HSM des HSK**



Das TI-GW-Zugangsmodule KANN das HSM des Highspeed-Konnektors nachnutzen, sofern der Highspeed-Konnektor dies entsprechend A\_23474\* und A\_23475\* zulässt. HSM-Administrator bleibt in diesem Fall jedoch der Hersteller des HSK.

[TI\_GW\_Zugangsmodule, Sich.techn. Eignung: Produktgutachten, <=]

### **A\_23390 - TI-Gateway-Zugangsmodule - Eigene HSK-Instanz pro Kunde**

Das TI-GW-Zugangsmodule MUSS jedem Nutzer seine eigene virtuelle HSK-Instanz zuweisen, sodass nie unterschiedliche Nutzer die selbe HSK-Instanz verwenden.

[TI\_GW\_Zugangsmodule, Sich.techn. Eignung: Produktgutachten, <=]

Es ist weiterhin möglich, dass **LeistungserbringerNutzer** bspw. in Gemeinschaftspraxen oder einem MVZ eine einzige HSK-Instanz gemeinsam verwenden. In diesem Fall treten die Leistungserbringer gegenüber dem TI-Gateway-Anbieter als ein einziger Nutzer auf. Dies ist analog zur Nutzung eines Inbox-Konnektors mit einem VPN-Zugang durch mehrere Leistungserbringer, wobei diese ebenso gegenüber dem VPN-Zugangsdienst-Anbieter als ein Nutzer erscheinen.

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-Zugangsmodule - Kopplung HSK, Prüfung Identität des HSK**

Das Zugangsmodule in einem TI-Gateway MUSS bei der beidseitigen Authentisierung mit dem HSK die Identität (I.AK.AUT) des HSK prüfen und seine eigenen Clientsystem-Credentials hinsichtlich Vertraulichkeit und Integrität geschützt speichern.

[TI\_GW\_Zugangsmodule, Sich.techn. Eignung: Produktgutachten, <=]

### **A\_23362 - TI-Gateway-Zugangsmodule - Kopplung HSK, Geschützter Import Clientsystem-Credentials**

Der Anbieter TI-Gateway MUSS einen sicheren Prozess zur Erzeugung und/oder Import der Clientsystem-Credentials des Zugangsmoduls für die Verbindung zum HSK etablieren, der die Vertraulichkeit und Integrität der Clientsystem-Credentials wahrt und gewährleistet, dass Clientsystem-Credentials nicht dauerhaft außerhalb des Zugangsmoduls oder HSK vorliegen. [Anb\_TI\_Gateway, Sich.techn. Eignung: Gutachten (Anbieter), <=]

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

### **A\_23261 - Sperrbarkeit von Institutionen**

Der Anbieter TI-Gateway und das Zugangsmodule MÜSSEN über organisatorische und technische Maßnahmen verfügen, um einzelne angeschlossene Institutionen vom Zugang zur TI auszuschließen, unter anderem auch auf Weisung der gematik.

[TI\_GW\_Zugangsmodule, Anb\_TI\_Gateway, Sich.techn. Eignung: Produktgutachten, organ./betriebl. Eignung: Anbietererklärung, <=]

Die gematik muss den Zugang von **LeistungserbringerinstitutioneNutzern** 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.

### **A\_23490 - TI-Gateway-Zugangsmodule - Keine Unterbrechung TLS-Kanal zur HSK-Instanz-Administration**

Das TI-GW-Zugangsmodule DARF NICHT die TLS-Verbindung des Nutzers bzw. DVOs zur Management-Schnittstelle der jeweiligen HSK-Instanz unterbrechen. Die Verbindung ist immer Ende-zu-Ende vom Nutzer bzw. DVO, der sich somit auch immer direkt an der HSK-Instanz authentisiert. [TI\_GW\_Zugangsmodule, Sich.techn. Eignung: Produktgutachten, <=]

## 5.5 Rohdaten-Performance-Reporting

verschoben nach [gemSpec\_Perf::2.5.2 Rohdaten-Performance-Reporting (Rohdatenerfassung v.02)]

### 5.5.1 Umfang

verschoben nach [gemSpec\_Perf::2.5.2.1 Umfang]

### 5.5.2 Lieferintervalle

verschoben nach [gemSpec\_Perf::2.5.2.2 Lieferintervalle]

### 5.5.3 Format

verschoben nach [gemSpec\_Perf::2.5.2.3 Format]

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

verschoben nach [gemSpec\_Perf::2.5.2.2 Format]

## 5.6 Lastanforderungen

verschoben nach [gemSpec\_Perf::3.10.1.3 Performancevorgaben TI-Gateway]

## 5.7 Anforderungen an den Hersteller

### 54927A\_25899-01 - Dauerhafte Bereitstellung Zugangsmodul-in-, HSK und Intermediär in RU

Der Hersteller eines TI-Gateway-Zugangsmoduls MUSS das Zugangsmodul mit angeschlossenem HSK und Intermediär\_VSDM in der jeweils letzten zugelassenen Version in der RU für die Dauer der produktiven Nutzung -Primärsystemherstellern gegen Aufwandsentschädigung anbieten. ~~Der Hersteller des Zugangsmodul kann diesen Service an einen dritten (Anbieter TI-Gateway) delegieren. [TI\_GW\_Zugangsmodul, funkt. Eignung: und dafür eine Kontaktadresse (E-Mail) bereitstellen, über die Primärsystem~~ Herstellererklärung, <=]

Mainline\_OPB1/ML-154926A\_25898 - Dauerhafte Informationen zum Service und den Bereitstellung Zugangsmodul in TU  
möglichkeiten bekommen. Der Hersteller eines TI-Gateway-Zugangsmoduls MUSS das Zugangsmodul mit angeschlossenem HSK in der TU dauerhaft betreiben und der gematik kostenfrei zur Verfügung stellen.  
 Der Hersteller MUSS der gematik ein kann diesen Service an einen Dritten Ansprechpartn (Anbieter für die Behebung von Störungen benenn TI-Gateway) delegieren. [TI\_GW\_Zugangsmodul, funkt. Eignung: Herstellererklärung, <=]

---

## 6 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.

### 6.1 Neue Anforderungen

#### 6.1.1 Anbietererklärung

##### **A\_18737-01 - Sperrung von Zugängen zur TI**

Der Anbieter TI-Gateway MUSS nach Weisung der gematik Zugänge zur TI sperren.

[Anb\_TI\_Gateway, organ./betriebl. Eignung: Anbietererklärung, <=]

##### **A\_23472 - Auftragsverarbeitung bei weiteren Diensten**

Der Anbieter TI-Gateway MUSS für weitere Services, bei denen medizinische oder personenbezogene Daten verarbeitet werden, einen Vertrag zur Auftragsverarbeitung mit seinen Kunden schließen und diesen transparent machen, dass solche Services nicht im Rahmen der Anbieterzulassung des TI-Gateways geprüft wurden.

[Anb\_TI\_Gateway, organ./betriebl. Eignung: Anbietererklärung, <=]

Auf Grund der Informationsflüsse ist es sinnvoll das KIM-Clientmodul in das TI-Gateway zu integrieren.

##### **A\_23487 - Aktualisierbarkeit von VPN-Clients**

Der Anbieter des TI-Gateways MUSS Maßnahmen umsetzen, um die Aktualität der eingesetzten VPN-Clients und weiterer ggf. ausgelieferter Client-Software sicherzustellen.

[Anb\_TI\_Gateway, [organ./betriebl.Sich.techn.](#) Eignung: [AnGutachten](#) (Anbietererklärung), <=]

##### **A\_24697 - Prüfung TI-Gateway-Kompatibilität der Clientsysteme**

Der Anbieter TI-Gateway MUSS anhand der Angaben des Nutzers prüfen, ob die eingesetzten Primärsysteme, KIM-Clientmodule und andere Clientmodule mit dem TI-Gateway kompatibel sind. Dafür ist mindestens zu prüfen, dass die notwendigen Voraussetzungen zum TLS-Verbindungsaufbau durch die Clients erfüllt werden. Der Anbieter muss den Nutzer über das Ergebnis der Prüfung informieren und im Negativ-Fall mögliche Maßnahmen zur Erreichung der Kompatibilität aufzeigen (z.B. Update).

[Anb\_TI\_Gateway, organ./betriebl. Eignung: Anbietererklärung, <=]

##### **A\_25684 - VSDM-Intermediärsleistung für TI-Gateway**

Ein Anbieter TI-Gateway KANN einen Intermediär als Service von einem anderen Anbieter einkaufen. Der Anbieter TI-Gateway bleibt dennoch gegenüber der gematik für den Betrieb dieses Intermediärs verantwortlich. Das beinhaltet im Besonderen, dass der Anbieter TI-Gateway den Intermediär im Konfigurationsmanagement der gematik (ZIS) auf seine Organisation registriert und die für den Intermediär geforderten Rohdaten an die gematik übermittelt. [Anb\_TI\_Gateway, organ./betriebl. Eignung: Anbietererklärung, <=]

#### 6.1.1.1 Anbindung an das Transportnetz Internet

##### **A\_24541 - TI-Gateway - Internetanbindung**



Der Anbieter TI-Gateway MUSS das TI-Gateway Zugangsmodul über einen redundanten Zugang an das Internet anbinden. Hierzu sind mindestens zwei vollständig unabhängige Leitungsführungen zwischen dem Standort und dem IP-Backbone sowie unabhängige Zugangsrouten erforderlich. [Anb\_TI\_Gateway, organ./betriebl. Eignung: Anbietererklärung, <=]

### **A\_24575 - TI-Gateway, Umschaltzeiten am Internetzugang**

Der Anbieter TI-Gateway MUSS sicherstellen, dass die Umschaltzeit vom Ausfall einer Verbindung zwischen TI-Gateway Zugangsmodul und Internet-Router oder beim Ausfall eines Internet-Routers bis zur Wiederherstellung des Internetzugangs unter einer Sekunde liegt.

[Anb\_TI\_Gateway, organ./betriebl. Eignung: Anbietererklärung, <=]

### **6.1.1.2 Anbindung an die TI**

#### **A\_24576 - TI-Gateway, redundante Anbindung an die TI**

Der Anbieter TI-Gateway MUSS die Standorte des TI-Gateway redundant an das Zentrale Netz der TI anbinden.

[Anb\_TI\_Gateway, organ./betriebl. Eignung: Anbietererklärung, <=]

Der SZSP übernimmt die Sicherheitsleistung für diese Anbindung (siehe [gemSpec\_Net]).

### **6.1.2 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 mit Unterauftragnehmern 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.

#### **35374A\_23352-02 - Anforderungsabdeckung von zugekaufter Leistung**

Der Anbieter des TI-Gateways MUSS, wenn er zur Erfüllung von Anforderungen Leistungen einer anderen Partei (z.B. Infrastrukturbetreiber oder Reseller, Betreiber Intermediär) 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. [Anb\_TI\_Gateway, Sich.techn. Eignung: Gutachten (Anbieter), <=]

#### **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. [Anb\_TI\_Gateway, Sich.techn. Eignung: Gutachten (Anbieter), <=]

Die geeignete und robuste technische Umsetzung obliegt dem Anbieter (Firewalls, VLANs).

#### **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 das TI-Gateway erkannt werden. Als geeignete Maßnahmen werden angesehen:

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

[Anb\_TI\_Gateway, Sich.techn. Eignung: Gutachten (Anbieter), <=]

Der Anbieter muss dabei berücksichtigen, dass sowohl Bestandskunden, als auch Neukunden, deren SMC-B noch nicht geprüft wurde, möglicherweise ein Angreifer sind.

### **GS-A\_4847-01 - Produkttyp TI-Gateway, DNSSEC im Namensraum Transportnetz**

Anbieter des TI-Gateways MÜSSEN den Namensraum Transportnetz per DNSSEC sichern.

[TI\_GW\_Zugangsmodule, Anb\_TI\_Gateway, funkt. Eignung: Test Produkt/FA, Sich.techn. Eignung: Gutachten (Anbieter), <=]

Der Hersteller muss die für sein Produkt erforderlichen Protokolle angeben wie in TIP1-A\_4340-01.

### **A\_23494 - 4-Augen-Prinzip bei Wartung HSK**

Der Anbieter des TI-Gateway MUSS Zugriffe auf den HSK (vgl. gemF\_Highspeed-Konnektor#5.2.1.4) auf Wartungsarbeiten in Notfällen beschränken, ein striktes 4-Augen-Prinzip für diese Zugriffe etablieren und durchsetzen sowie solche Zugriffe protokollieren. Zugriffe auf den HSK durch den Anbieter sind ausschließlich für Wartungsarbeiten beim Ausfall von Hardware-Komponenten wie Netzteilen vorgesehen - sofern solche Wartungen beim eingesetzten HSK überhaupt für den Betreiber möglich sind -, welche zum Ausfall des HSK und zu einer verringerten Verfügbarkeit oder Performance des TI-Gateway führen.[Anb\_TI\_Gateway, Sich.techn. Eignung: Gutachten (Anbieter), <=]

### **A\_23496 - Erkennen und Melden von Unregelmäßigkeiten bei physischem Zugriff auf HSK**

Der Anbieter des TI-Gateway MUSS Prozesse definieren und etablieren, die Unregelmäßigkeiten bzgl. physischer Zugriffe auf den HSK erkennen lassen. Dies umfasst die Prüfung von Protokollen des HSK bzgl. des Auslösens von Alarmen zum physischen Zugang (vgl. A\_23495\*) und dem Herunterfahren des HSK. Erkannte Unregelmäßigkeiten sind als erheblicher Sicherheitsvorfall zu werten und im Rahmen von GS-A\_5555\* an die gematik zu melden.[Anb\_TI\_Gateway, Sich.techn. Eignung: Gutachten (Anbieter), <=]

### **A\_24295 - Zusätzliche Betreiber-Rolle bei physischem Zugang bei laufender Verarbeitung**

Der Anbieter TI-Gateway MUSS, wenn ein von ihm verwendetes HSK-Produkt physischen Zugang zur Hardware bei laufender Datenverarbeitung durch berechnete Mitarbeiter des Anbieters entsprechend A\_17354-\* Punkt b zulässt, eine Rollentrennung zwischen dem Personal, dass den HSK administriert und wartet ("HSK-Betreiber"), und dem Personal, dass das Rechenzentrum betreibt ("RZ-Betreiber"), umsetzen, so dass

- der HSK-Betreiber keinen Zutritt zum HSK hat, ohne den RZ-Betreiber,
- der RZ-Betreiber keinen Zugang zur Hardware des HSK hat, ohne den HSK-Betreiber,
- der RZ-Betreiber die Wartungsarbeiten des HSK-Betreibers überwacht und durchsetzt, dass sich diese auf die in den Vorgaben des Herstellers (bspw. "Secure User Guidance") definierten Wartungsarbeiten und deren Maximaldauer beschränken (siehe A\_24294).

Der Anbieter MUSS entsprechende Prozesse definieren und etablieren, die dies dauerhaft gewährleisten und eine regelmäßige Validierung der Umsetzung durchsetzen. Die Umsetzung des Rollenausschluss MUSS die Weisungsbefugnis von Vorgesetzten berücksichtigen. Das heißt, dass keine Person direkter Vorgesetzter sowohl von Personal der Rolle HSK-Betreiber als auch von Personal der Rolle RZ-Betreiber sein darf. Der Anbieter TI-Gateway SOLL weitere Schutz-/Überwachungsmaßnahmen, die unberechtigte Zugriffe/Manipulationen der HW erkennbar machen und durch den RZ-Betreiber durchgesetzt werden, umsetzen, wie bspw. Video-Überwachung. Werden keine zusätzlichen Maßnahmen umgesetzt, ist dies durch den Gutachter im Sicherheitsgutachten zu begründen.

[Anb\_Konn\_Highspeed, Sich.techn. Eignung: Gutachten (Anbieter), <=]

### **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. [Anb\_TI\_Gateway, Sich.techn. Eignung: Gutachten (Anbieter), <=]

## 6.2 Betrieb

### 6.2.1 Servicezerlegung

#### verA 26630 - Technische Prüfung von Produktanforderungen auch bei Umsetzung durch den Anbieter

Der Anbieter TI-Gateway und der Hersteller des Zugangsmoduls MÜSSEN, wenn Anforderungen, die grundsätzlich dem Produkt und dort dem Produktgutachten zugeordnet sind, nicht im Produkt, sondern durch den Anbieter umgesetzt werden, im Rahmen des Sicherheitsgutachtens des Anbieters oder im Rahmen des Produktgutachtens des Herstellers, den technischen Nachweis (Prüfmethoden eines Produktgutachtens) zur Umsetzung dieser Anforderungen erbringen. Dieser Nachweis ist relevant für die Produktzulassung, welche dann nur anbieterspezifisch erteilt werden kann. [TI\_GW\_Zugangsmodul, Anb\_TI\_Gateway, Sich.techn. Eignung: Produktgutachten, Sich.techn. Eignung: Gutachten (Anbieter), <=]

Grundsätzlich sind dem Produkt zugeordnete Anforderungen auch im Produkt umzusetzen. Das in der vorhergehenden Anforderung beschriebene Szenario stellt somit eine Ausnahme dar. In solchen Fällen muss der Hersteller für die Produktzulassungen benennen, welche Anforderungen nicht durch das Produkt, sondern durch die Betriebsumgebung des Anbieters zu erfüllen sind. Dafür muss dann der Nachweis der Umsetzung durch technische Prüfungen am Gesamtsystem (Produkt + Betriebsumgebung des Anbieters) erfolgen und mittels Gutachten bereitgestellt werden. Die Produktzulassung kann dementsprechend erst erteilt werden, wenn ein bestätigendes Gutachten vorgelegt wurde. Die Produktzulassung ist dann beschränkt auf die Betriebsumgebung, für die auch der Nachweis erbracht wurde und den zugehörigen Anbieter dieser Umgebung. Entsprechend müssen Änderungen an Komponenten der Betriebsumgebung wie Änderungen am Produkt behandelt werden. Sollten zu einem späteren Zeitpunkt weitere Anbieter das Produkt verwenden wollen, muss auch für deren Betriebsumgebung der technische Nachweis erbracht werden und die Produktzulassung würde dann im Positivfall auf diese Anbieter und deren Betriebsumgebung erweitert werden.

## 6.3 Betrieb

### 6.3.1 Servicezerlegung

verschoben nach [gemKPT\_Betr::3.5.2 Servicezerlegung]

### 6.3.2 Mitwirkungsverpflichtung im TI-ITSM gemäß [gemRL\_Betr\_TI]

verschoben nach [gemKPT\_Betr::3.5.3 Mitwirkungsverpflichtung im TI-ITSM gemäß [gemRL\_Betr\_TI]]

### **6.3.3 Spezifische Ausprägungen und Verpflichtungen einzelner Rollen**

verschoben nach [gemKPT\_Betr::3.4.4 Spezifische Ausprägungen und Verpflichtungen einzelner Rollen]

### **6.3.4 Supportkonzept**

#### **6.3.4.1 Spezifische Ausprägungen**

verschoben nach [gemKPT\_Betr::3.6.3 Spezifische Ausprägungen]

#### **6.3.4.2 Organisatorische Service Level**

verschoben nach [gemKPT\_Betr::5.2.2 Spezifische Ausprägungen]

#### **6.3.4.3 Technische Service Level / Performance-Kenngrößen**

verschoben nach [gemKPT\_Betr::5.3.2.13 TI-Gateway-Zugangsmodule (PDT72)]

### **6.3.5 gemKPT\_Betr: Anhang A**

verschoben nach [gemKPT\_Betr::7.1.1 Produkttypen (PDT-IDs)]

### **6.3.6 gemSpec\_Perf#3.x.1 Leistungsanforderungen TI-Gateway**

#### **6.3.6.1 gemSpec\_Perf#3.x.1.1 Lastmodell TI-Gateway**

verschoben nach [gemSpec\_Perf::3.10.1.3.1 Lastmodell TI-Gateway]

#### **6.3.6.2 gemSpec\_Perf#3.x.1.2 Bearbeitungszeiten TI-Gateway**

verschoben nach [gemSpec\_Perf::3.10.1.3 Bearbeitungszeiten TI-Gateway]

#### **6.3.6.3 gemSpec\_Perf#3.x.1.3 Performancevorgaben TI-Gateway**

verschoben nach [gemSpec\_Perf::3.10.1.3 Performancevorgaben TI-Gateway]

### **6.3.7 Zugang und Verfügbarkeit**

Für die Ermittlung der Verfügbarkeit des Anbieter TI-Gateway ist es erforderlich, dass die gematik eine Möglichkeit zum Probing des TI-Gateways erhält. Das Probing wird realisiert durch den Abruf der connectors.sds einer für diesen Zwecke bereitgestellten virtuellen HSK-Instanz alle 5min. Diese vHSK-Instanz wird nicht mittels einer SMC-B für den Zugang zur TI freigeschaltet.

#### **A\_24297 - Probing TI-GW-Zugangsmodule**

Der Anbieter TI-Gateway MUSS der gematik einen VPN-Zugang über das TI-GW-Zugangsmodule zu einer virtuelle HSK-Instanz für das Probing der connector.sds zur Verfügung stellen.[Anb\_TI\_Gateway, organ./betriebl. Eignung: Anbietererklärung, <=]

#### **A\_25977 - Probing VPN-Anbindung**

Der Anbieter TI-Gateway MUSS der gematik eine softwarebasierte Lösung für die Anbindung an das TI-Gateway Zugangsmodul zur Installation in einer virtuellen Maschine bereit stellen.

Die Anbindung MUSS über die gleiche VPN-Serverstruktur, wie die Anbindung einer Leistungserbringer-Institution an das TI-Gateway-Zugangsmodul erfolgen.

[Anb\_TI\_Gateway, organ./betriebl. Eignung: Anbietererklärung, <=]

#### Änderungen an gemILFA\_26379 - Softwareclient zum Probing

Das TI-Gateway-Zugangsmodul MUSS einen Softwareclient und eine virtuelle Instanz in RU/TU zum Probing durch die gematik bereitstellen. Der Softwareclient MUSS die gleiche VPN-Konzentrator-Infrastruktur nutzen wie die Anbindung von Leistungserbringer-Institutionen.[TI\_GW\_Zugangsmodul, funkt. Eignung: Test Produkt/FA, <=]

## **6.4 Netzanbindung TI-Gateway**

### **6.4.1 Netzdelegation**

Ein Anbieter TI-Gateway muss sich drei IP-Adressbereiche delegieren lassen:

- Für TI-Gateway eigene Dienste aus dem Bereich "TI-Gateway"
- Für virtuelle Konnektorinstanzen und den Zugriff auf WANDA und offene Fachdienste aus dem Bereich "Konnektoren, Consumer und Highspeed-Konnektoren"
- Für Intermediäre aus dem Bereich "Gesicherte Fachdienste"

Die Bereiche sind definiert in gemSpec\_Net:

- GS-A\_4029-08 - IPv4-Adresskonzept Produktivumgebung.
- GS-A\_4850-06 - IPv4-Adresskonzept Testumgebung.

Zusätzlich kann das TI-Gateway den Netzbereich "TI-Gateway (intern)" für interne Kommunikation verwenden, wobei IP-Adresskonflikte mit Diensten in der TI ausgeschlossen sind. Eine Delegation ist für diesen Bereich nicht notwendig.

Die Komponenten des TI-Gateways können direkt an den SZPP oder über ein Transfernetz angeschlossen werden. Da die IP-Adressen des Transfernetzes nur von lokaler Relevanz sind, sollten sie dem privaten IP-Adressbereich entnommen werden (RFC 1918#Kap.3.) und der genaue IP-Bereich und Netzmaske mit dem Anbieter Zentraler Plattformdienste (AZPD = Arvato) abgestimmt werden. Alternativ können delegierte IP-Adressen aus dem IP-Adressbereich "TI-Gateway" verwendet werden.

### **6.4.2 Verwendung der Netzbereiche**

#### **Netzbereich "Konnektoren, Consumer und Highspeed Konnektoren":**

Kommunikation der HSK-Instanzen zu den offenen und gesicherten Fachdiensten sowie zu den weiteren Anwendungen im Gesundheitswesen.

#### **Netzbereich "TI-Gateway":**

Kommunikation der Systemdienste im TI-Gateway zu den zentralen Diensten der TI, z.B. Namens- und Zeitdienst oder den OCSP-Responder der Komponenten PKI.

#### **Netzbereich "Gesicherte Fachdienste":**

Kommunikation des Intermediär zu den zentralen Diensten sowie Erreichbarkeit für die HSK.

#### **Netzbereich "TI-Gateway (intern)":**

Kommunikation innerhalb des TI-Gateways z.B. zwischen dem VPN-Client in der Leistungserbringerumgebung und der zugehörigen HSK-Instanz oder zwischen den HSK-Instanzen und den Systemdiensten.

### 6.4.3 IP-Adressvergabe und Netzfreisaltungen

Die Registrierung der Systemdienste und die daraus resultierende Freischaltung erfolgt durch den AZPD über die folgenden TINA-Schnittstellen.

Der Netzbereich "TI-Gateway" ist für die Registrierung der folgenden Schnittstellen zu nutzen:

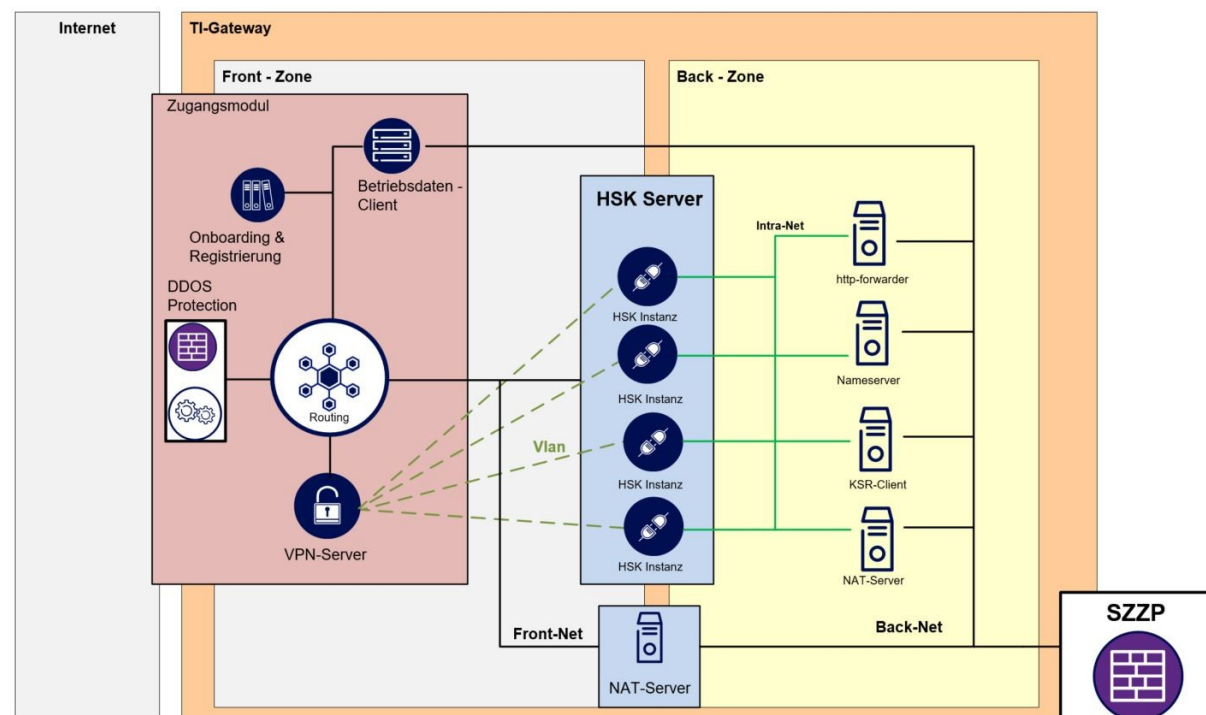
- TI-Gateway C201 TI-Gate-Caching Nameserver
- TI-Gateway C202 TI-Gate-NTP Server
- TI-Gateway C203 TI-Gate-http-forwarder
- TI-Gateway C204 TI-Gate-KSR-Client
- TI-Gateway C205 TI-Gate-Betriebsdaten-Client

Der Netzbereich "Konnektoren, Consumer und Highspeed-Konnektoren" ist für die Registrierung der folgenden Schnittstellen zu nutzen:

- TI-Gateway C210 TI-Gate-HSK-NAT-Server - zentrale Dienst & gesicherte Fachdienste
- TI-Gateway C211 TI-Gate-Proxy-Server - offene Fachdienste & WANDA

Die Registrierung erfolgt für eine IP-Adresse oder einen IP-Adresspool und genau eine Schnittstelle. Die Registrierung einer IP-Adresse für mehrere Schnittstellen ist nur für spezifizierte Ausnahmen gestattet, z.B. für alle Systemdienste in einem HSK-Server.

#### 6.4.3.1 Aufbau 1 - Eigenständige Systemdienste



**Abbildung 5 Aufbau 1 - Eigenständige Systemdienste**

Das TI-Gateway unterteilt sich in eine Front-Zone und eine Back-Zone.

### 6.4.3.1.1 Front-Zone

Die Front-Zone besteht aus:

- Zugangsmodule mit VPN-Server, Betriebsdaten-Client usw.
- NAT-Server für offene Fachdienste & WANDA (C211)
- HSK-Server / HSK-Instanzen

Die Netzwerkkonzeption für das Zugangsmodule und die Front-Zone obliegt dem Anbieter des TI-Gateway. Prinzipiell kann der Betreiber TI-Gateway in der Front-Zone IP-Adressen aus dem Netzbereich TI-Gateway (intern) verwenden, sofern die Komponenten nicht mit der TI kommunizieren. Der Betreiber TI-Gateway muss die IP-Verwaltung für diesen Netzwerkbereich eigenständig durchführen.



## 7\_PS

### Zertifikatsbasierte Clients **A\_26387 - Verwendung IP-Adressen TI-Gateway (intern)**

Der Anbieter TI-Gateway DARF IP-Adressen aus dem Netzbereich "TI-Gateway (intern)" NICHT für die Kommunikation in die TI verwenden.

[Anb\_TI\_Gateway, organ./betriebl. Eignung: Anbietererklärung, <=]

#### 7.1.1.1.1 Back-Zone

Die Back-Zone besteht aus:

- HSK-Server / HSK-Instanzen
- Systemdiensten: Caching-Nameserver, http-forwarder, NTP-Server, KSR-Client
- NAT Server für Zentrale TI und gesicherte Fachdienste (C210)
- NAT Server für offene Fachdienste und WANDA (C211)

Die IP-Adressen für die interne Kommunikation zwischen HSK bzw. den HSK-Instanzen mit den Systemdiensten im TI-Gateway können ebenfalls dem Netzbereich "TI-Gateway (intern)" entnommen werden.

Die NAT Server verwenden als Netzmaske mindesten /26 idealerweise /24 und arbeiten im Source-NAT.

**Hinweis:** Die NAT-Server können auch mit den IP-Adressen aus dem NAT-Bereich an den SZZP angeschlossen werden.

In diesem Aufbau sind Caching-Nameserver, NTP-Server, http-forwarder, und KSR-Client separate Dienste mit eigener IP-Adresse, die einzeln für die zugehörige Schnittstelle freigeschaltet werden.

### **A\_26386 - Freischaltung Systemauthentiendienste des TI-Gateways**

Der Anbieter TI-Gateway MUSS folgenden Diensten IP-Adressen aus dem Bereich "TI-Gateway" zuordnen und für die entsprechende Schnittstelle registrieren

<b>Dienst</b>	<b>Schnittstelle</b>
<u>Caching Nameserver</u>	<u>C201</u>
<u>NTP-Server</u>	<u>C202</u>
<u>http-Forwarder</u>	<u>C203</u>
<u>KSR-Client</u>	<u>C204</u>

[Anb\_TI\_Gateway, organ./betriebl. Eignung: Anbietererklärung, <=]

### **A\_26384 - fizierung muss-reischaltung virtuelle HSK-Instanzen**

Der Anbieter TI-Gateway MUSS für den NAT-Server, über den die virtuellen HSK-Instanzen mit zentralen Diensten und gesicherten Fachdiensten kommunizieren, einen IP-Adresspool aus dem Bereich "Konnektoren, Consumer und Highspeed-Konnektoren" verwenden und auf die Schnittstelle C210 registrieren.

[Anb\_TI\_Gateway, organ./betriebl. Eignung: Anbietererklärung, <=]



**A\_26385 - Freischaltung offene Fachdienste & WANDA**

Der Anbieter TI-Gateway MUSS für den NAT-Server, über den Nutzer mit offenen Fachdiensten und WANDA kommunizieren, einen IP-Adresspool aus dem Bereich "Konnektoren, Consumer und Highspeed-Konnektoren" verwenden und auf die Schnittstelle C211 registrieren. [Anb\_TI\_Gateway, organ./betriebl. Eignung: Anbietererklärung, <=]

**A\_26414 - Freischaltung Betriebsdaten-Client**

Der Anbieter TI-Gateway MUSS für den Betriebsdaten-Client des Zugangsmoduls eine dedizierte IP-Adresse aus dem Bereich "TI-Gateway" verwenden, und für die Schnittstelle C205 registrieren. [Anb\_TI\_Gateway, organ./betriebl. Eignung: Anbietererklärung, <=]

Weitere Funktionen, die aus den virtuellen Instanzen im Basissystem des HSK zentralisiert werden (z.B. TSL-Client) müssen eine dedizierte IP-Adresse aus dem Bereich "Konnektoren, Consumer und Highspeed Konnektoren" verwenden, die für die Schnittstelle C210 registriert wird.

**7.1.1.1.2 Intermediär**

Nach [gemSpec\_Net#GS-A\_4782, GS-A\_5076] muss bei Nutzung eines gemeinsamen SZZP-Anschluss die Kommunikation über diesen geführt werden.

- Separate Anbindung an den SZZP
- Keine direkte Kommunikation zum TI-Gateway

Der Intermediär ist ein gesicherter Fachdienst. Damit benötigt der Anbieter TI-Gateway IP-Adressen aus dem Netzbereich "gesicherte Fachdienste".

Für den Intermediär müssen zwei Registrierungen/Freischaltungen erfolgen:

- Registrierung einer Host-IP für Intermediär als Client mit Schnittstelle C091
- Registrierung einer Host-IP für Intermediär als Dienst mit Dienst-SST 201

### 7.1.1.2 Aufbau 2 - Systemdienste in den HSK-Servern

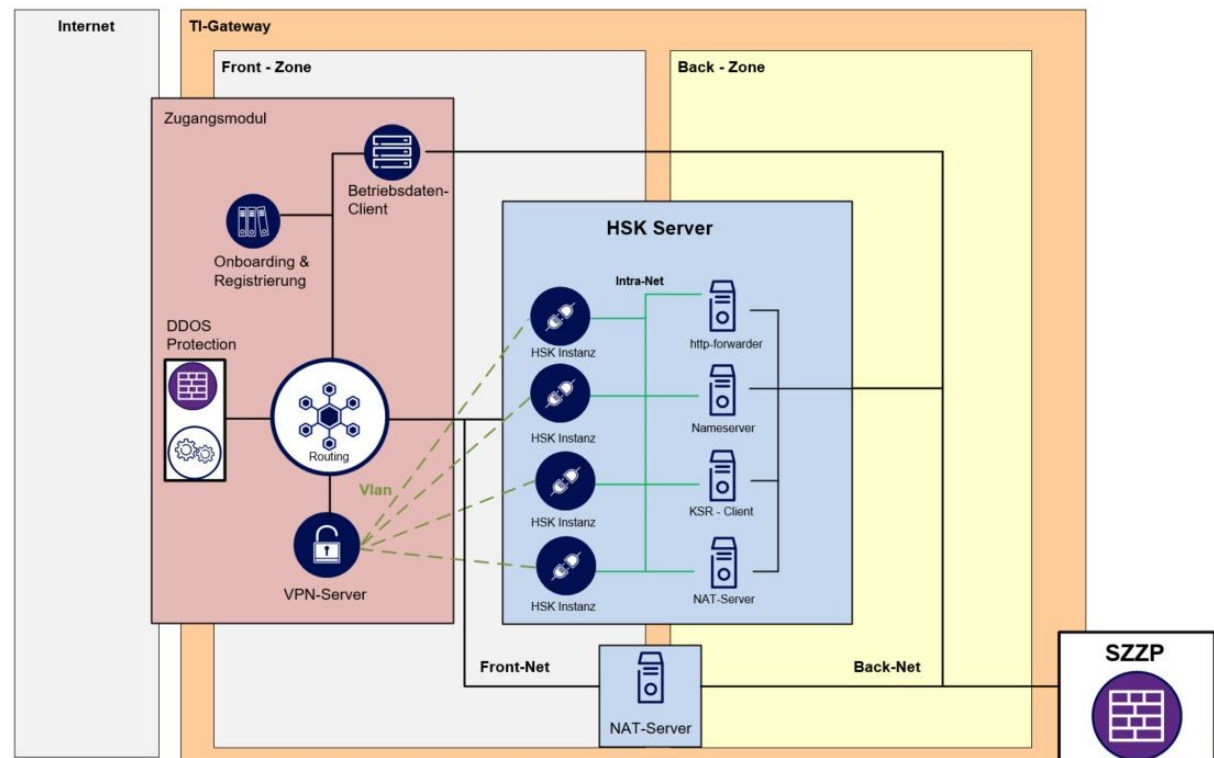


Abbildung 6 Aufbau 2 - Systemdienste in den HSK-Servern

#### A\_26388 - Zusammenfassung der Schnittstellen für Systemdienste

Der Anbieter TI-Gateway SOLL, wenn die Systemdienste Caching-Nameserver, NTP-Server, http-Forwarder und KSR-Client in den HSK-Server integriert sind, pro Server eine IP-Adressen für die Schnittstellen C201-C204 verwenden und diese IP-Adresse für alle diese Schnittstellen zusammen registrieren. [Anb\_TI\_Gateway, organ./betriebl. Eignung: Anbietererklärung, <=]

Jeder HSK-Server braucht somit TI-seitig mindestens eine IP-Adresse aus dem Bereich TI-Gateway für C201-C204 und mindestens eine IP-Adresse für den NAT-Server C210. Wenn mehrere HSK-Server eingesetzt vom Primärs werden, bekommen diese jeweils eigene IP-Adressen.

Die Kommunikation zu offenen Fachdiensten und WANDA erfolgt wie in Aufbau 1 über einen separaten NAT-Server, der für C211 freigeschaltet ist.

### 7.1.1.3 Aufbau 3 - Durchleitung offene Fachdienste / WANDA durch den HSK

Wenn der HSK-Server nicht nur die Gateway-Dienste wie in Aufbau 2, sondern auch die Durchleitung von offenen Fachdiensten & Wanda übernimmt, so braucht er TI-seitig mindestens drei IP-Adressen:

- Gateway-Dienste C201-C204
- zentrale Dienste und gesicherte Fachdienste C210
- offene Fachdienste & WANDA C211

Wie bei den anderen Aufbauten wird der Betriebsdaten-Client an den HSK-Servern vorbei mit dem SZZP verbunden.

---

## 8 Änderungen an gemILF\_PS

---

Zertifikatsbasierte Clientsystem-Authentifizierung muss jetzt vom Primärsystem unterstützt werden.

### **TIP1-A\_4962-01 - Nutzung von TLS-Authentisierungsmethoden**

Das Primärsystem MUSS die TLS-Authentisierungsmethoden der Stufen 2 und 4 aus Tabelle Tab\_ILF\_PS\_Konfigurationsvarianten\_HTTP und Stufe 2 aus Tabelle Tab\_ILF\_PS\_Konfigurationsvarianten\_CETP unterstützen, d. h. TLS mit Server-Authentisierung mit bzw. ohne Client-Authentisierung.

Das PS MUSS für TLS-gesicherte Verbindungen mindestens TLS-Version 1.2 verwenden, es KANN auch TLS Version 1.3 verwenden.

**[PS\_E-Rezept\_abgebend, PS, PS\_E-Rezept\_verordnend, funkt. Eignung: Herstellererklärung, <=]**

---

## 9 Beispiele und Referenzimplementierungen

---

*<Optional: Beispiele für Aufrufsequenzen, ausgetauschte Daten, etc. zur Unterstützung der Implementierung>*

---

## 10 Anhang A - Verzeichnisse

---

### 10.1 Abkürzungen

Kürzel	Erläuterung

### 10.2 Referenzierte Dokumente

#### 10.2.1 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

#### 10.2.2 Weitere Dokumente

[Quelle]	Herausgeber (Erscheinungsdatum): Titel