
Inhaltsverzeichnis

1 Änderung in gemF_TI-Gateway

Neues Kapitel:

1.1 Netzanbindung TI-Gateway

1.1.1 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 SZZP 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.

1.1.2 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.

1.1.3 IP-Adressvergabe und Netzfreeschaltungen

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.

1.1.3.1 Aufbau 1 - Eigenständige Systemdienste

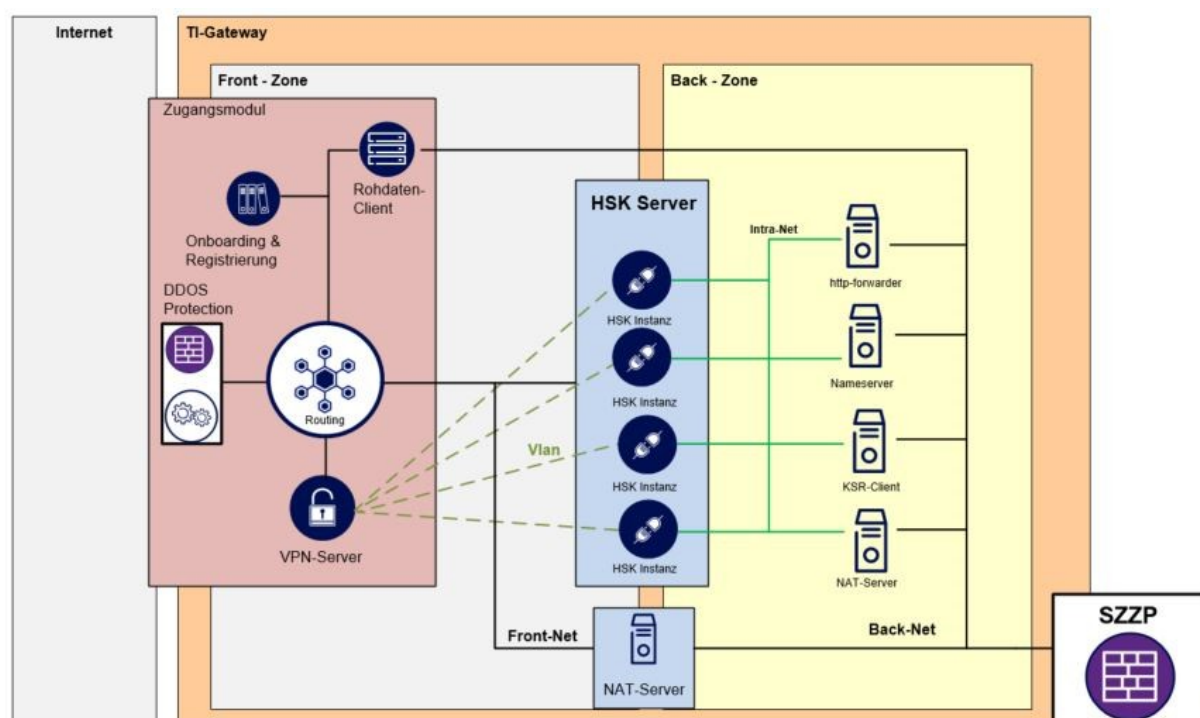


Abbildung 1 Aufbau 1 - Eigenständige Systemdienste

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

1.1.3.1.1 Front-Zone

Die Front-Zone besteht aus:

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

Die Netzwerkkonzeption für das Zugangsmodul 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 Netzbereich eigenständig durchführen.

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]

1.1.3.1.2 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 Systemdienste des TI-Gateways

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

Dienst	Schnittstelle
Caching Nameserver	C201
NTP-Server	C202
http-Forwarder	C203
KSR-Client	C204

[<=, Anb_TI_Gateway, organ./betriebl. Eignung: Anbietererklärung]

A_26384 - Freischaltung 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.

1.1.3.1.3 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

1.1.3.2 Aufbau 2 - Systemdienste in den HSK-Servern

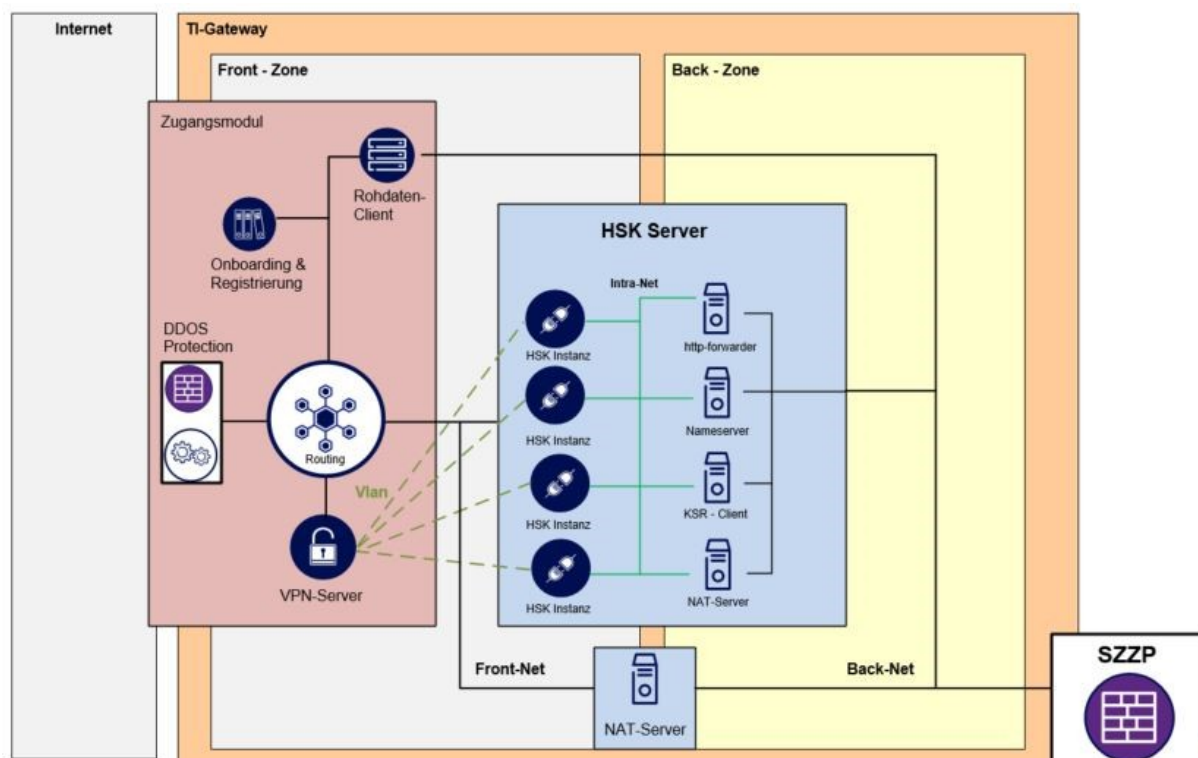


Abbildung 2 Aufbau 2 - Systemdienste in den HSK-Servern

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 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.

1.1.3.3 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.