

## Änderung in gemSpec\_Net

Das Kapitel 3.1.1.3 wird um die normativen Festlegungen für den neuen Anbindungstyp "SZZP-light-cloud" ergänzt.

Der SZZP-light-cloud ist eine modifizierte Variante des SZZP-light und setzt sich aus zentralen Komponenten sowie dem dezentralen virtuellen VPN-Anschlusspunkt zusammen. Deshalb wird im Abschnitt "Anbindungstyp SZZP-light" einige Anforderungen für den zentralen Anteil des SZZP-light um den SZZP-light-cloud ergänzt.

### 1.1.1.1 Anbindungen

#### Anbindungstyp SZZP-light

##### A\_14531-04 -zentrales Netz SZZP-light und SZZP-light-cloud, Redundanz pro zentralem Standort

Das zentrale Netz der TIMUSS die zentralen Komponenten des SZZP-light und SZZP-light-Cloud entweder an mindestens zwei Standorten als active/standby Cluster aus VPN-Konzentratoren und Paketfilter gemäß Abbildung "Abb\_VPN-Konzentrator\_und\_Paketfilter\_Redundanz" oder als stretched active/standby Cluster aus VPN-Konzentratoren und Paketfilter über zwei Standorte verteilt implementieren.

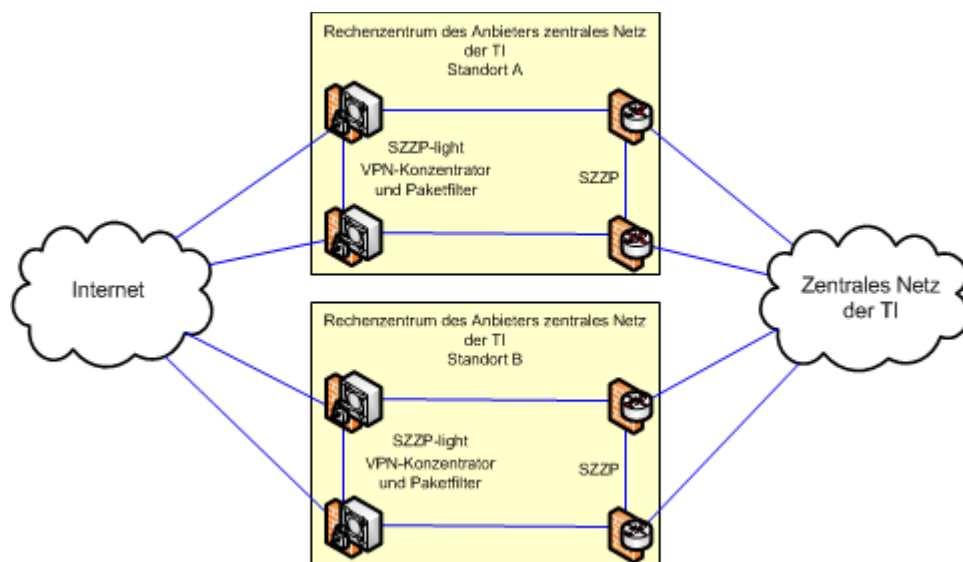


Abbildung 1: Abb\_VPN-Konzentrator\_und\_Paketfilter\_Redundanz

[<=]

##### A\_14533-04 -zentrales Netz SZZP-light und SZZP-light-cloud, Bandbreite der VPN-Anschlusspunkte

Das zentrale Netz der TI SOLL SZZP-light- und SZZP-light-cloud-Anschlüsse anbieten, die an den VPN-Anschlusspunkten eine Bandbreite (IPSec Verschlüsselungsleistung) von 100 Mbit/s bis 1 Gbit/s unterstützen.

[<=]

Der nachfolgende informativer Text zur obigen Festlegung wird modifiziert:

Die SZZP-light- und SZZP-light-cloud-Anschlüsse dürfen mit höherer Bandbreite angeboten werden.

#### A\_14534-04 -zentrales Netz SZZP-light und SZZP-light-cloud, Bandbreite zentral

Das zentrale Netz der TI MUSS die zentralen Komponenten der SZZP-light- und SZZP-light-cloud-Anschlüsse so dimensionieren und an sich ändernde Lastsituationen anpassen, dass

- die Auslastung an den Netzwerkschnittstellen der Komponenten VPN-Konzentrator und Paketfilter kleiner als 80% der Leistungsfähigkeit der jeweiligen Komponente ist.
- die Auslastung des Internetanschlusses kleiner als 80% seiner gesamten Bandbreite ist (Mittelwert über eine Stunde).

[<=]

#### A\_14536-04 -zentrales Netz SZZP-light und SZZP-light-cloud, Failover der VPN-Konzentratoren und der Paketfilter

Das zentrale Netz der TI MUSS die zentralen Komponenten der SZZP-light- und SZZP-light-cloud-Anschlüsse (VPN-Konzentratoren und Paketfilter) so implementieren, dass bei Ausfall einer aktiven Komponente ein Failover auf die Standby-Komponente erfolgt.

[<=]

Am Ende von Kapitel 3.1.1.3 wird der folgende Abschnitt eingefügt, der die spezifischen Festlegungen für den neuen Anbindungstypen "SZZP-light-cloud" enthält.

#### Anbindungstyp SZZP-light-cloud

Der SZZP-light-cloud ist ein Anbindungstyp für die Anbindung von Cloud Providern und den dort in Virtual PrivateCloud (VPC) betriebenen Produktinstanzen an das zentrale Netz der Telematikinfrastruktur.

Der SZZP-light-cloud besteht aus einem virtualisierten VPN-Anschlusspunkt (VPN-Router und Paketfilter) in einem eigenen VPC (Virtual Private Cloud) beim Cloud Provider sowie dem physischen VPN-Konzentrator und dem Paketfilter. Über das Internet wird ein IPSec-Tunnel vom virtuellen VPN-Anschlusspunkt zum VPN-Konzentrator aufgebaut. Über den nachfolgenden SZZP erfolgt die Anbindung an das Zentrale Netz der TI. Die virtualisierten Produktinstanzen werden beim Cloud Provider in eigenen VPCs bereitgestellt. Der VPC der virtualisierten Produktinstanzen wird direkt mit dem VPC des VPN-Anschlusspunktes verbunden (Peering). Dadurch wird eine 1 zu 1 Kommunikation zwischen den VPCs sichergestellt. Über den virtuellen Anschlusspunkt wird die Kommunikation in das zentrale Netz der TI ermöglicht. An der virtualisierte Firewall sowie am SZZP erfolgt die Kontrolle und Durchsetzung der erlaubten Kommunikationsbeziehungen.

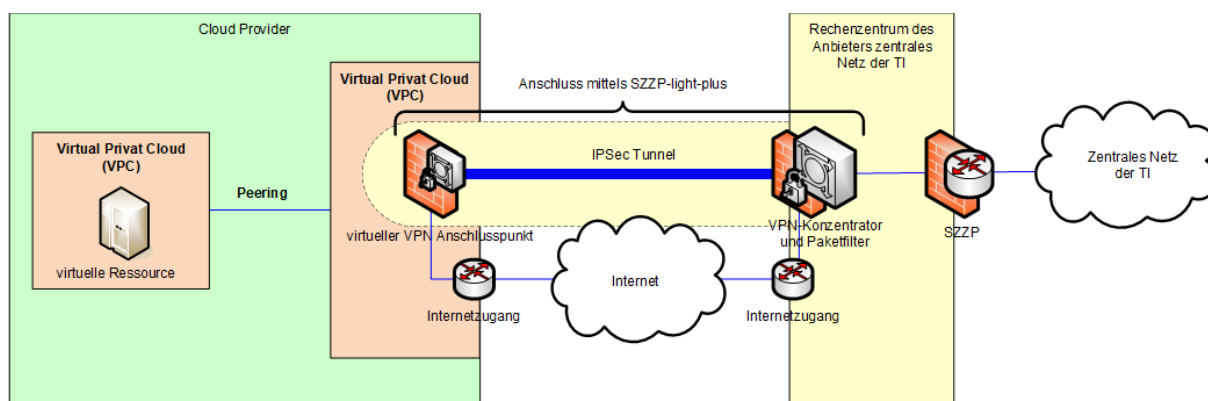


Abbildung 2: Abb\_zentrNetz\_SZZP-light-cloud

#### A\_24701 -zentrales Netz SZZP-light-cloud, Virtual Private Cloud

Das zentrale Netz der TI MUSS den virtualisierten VPN-Anschlusspunkt beim Cloud Provider in einer eigenen Virtual Private Cloud (VPC) bereitstellen. [≤]

#### **A\_24702 -zentrales Netz SZZP-light-cloud, logische Umgebungstrennung**

Das zentrale Netz der TI MUSS den virtualisierten VPN-Anschlusspunkt in seiner Virtual Private Cloud (VPC) so implementieren, dass die Zugänge zu den Umgebungen PU, TU und RU logisch getrennt bereitgestellt werden. [≤]

#### **A\_27670 -Zentrales Netz SZZP-light-cloud, Virtual Private Cloud Peering**

Das zentrale Netz der TI MUSS über das Peering-Verfahren seine Virtual Private Cloud (VPC) mit dem VPC des Mandanten verbinden. Dabei MUSS das Peering auf Grundlage der technischen Vorgaben des dabei genutzten Cloud Provider erfolgen. [≤]

*Die Anforderung A\_27670 durch den nachfolgenden informativen Text erläutert:*

Das Peering-Verfahren ist eine Netzwerktechnologie bei der zwei VPCs direkt miteinander verbunden werden. Dadurch wird sichergestellt, dass die Kommunikation über das interne Netzwerk des Cloud Providers geführt wird.

#### **A\_24713 -zentrales Netz SZZP-light-cloud, Virtual Private Cloud Verbindung**

Das zentrale Netz der TI MUSS die Verbindung mehrerer Virtual Private Clouds zu seiner Virtual Private Cloud (VPC) mit einem virtualisierten Anschlusspunkt innerhalb eines Cloud Providers unterstützen, wobei immer A\_27670-\* eingehalten wird. Jeder Mandant innerhalb eines Cloud Provider MUSS mit einem eigenen virtuellen Anschlusspunkt angebunden werden.

[≤]

#### **A\_24710 -zentrales Netz SZZP-light-cloud, Anschlussklassen**

Das zentrale Netz der TI MUSS die beim Cloud Provider in VPC virtualisierten Produktinstanzen entsprechend den Anschlussklassen gemäß Tabelle Tab\_zentrNetz\_Anschlussklassen über den im VPC bereitgestellten VPN-Anschlusspunkt anbinden. Jede Anschlussklasse ist über einen eigenen VPC anzubinden.

**Table 1: Tab\_zentrNetz\_Anschlussklassen**

Anschlussklasse	Beschreibung
Fachanwendung 1	Zur Anschlussklasse <<Fachanwendung 1>> zählen alle gesicherten Fachdienste.
Fachanwendung 2	Zur Anschlussklasse <<Fachanwendung 2>> zählen alle offenen Fachdienste.
andere Anwendungen des Gesundheitswesens	Zur Anwendungs-kategorie <<andere Anwendungen des Gesundheitswesens>> zählen WANDA Smart Anwendungen.
virtualisierte Konnektortypen	Zur Anwendungs-kategorie <<virtualisierte Konnektortypen>> zählt nur der Basis Consumer.

[≤]

*Die Anforderung A\_24710 wird durch den nachfolgenden informativen Text erläutert:*

Der Mandant bzw. der TI-Anschlussnehmer ist dafür verantwortlich, dass in einem VPC nicht zwei unterschiedliche Anschlussklassen realisiert werden. Es ist auch möglich, dass jede virtualisierte Produktinstanz einer Anschlussklasse in einem separaten VPC betrieben und angebunden wird. Jeder VPC der Mandanten wird an den VPC mit dem VPN Anschlusspunkt angebunden (Peering).

Zudem ist sicherzustellen, dass die Kommunikation zwischen den virtualisierten Produktinstanzen auch in einem VPC gemäß A\_21142 immer über den virtuellen VPN-Anschlusspunkt geführt wird.

Der TI-Anschlussnehmer kann gemäß IP-Adresskonzept TI-Netzwerke beantragen und diese in dem VPC verwenden. So wird sichergestellt, dass die TI-Netzwerke optimal genutzt werden und ein strukturiertes Routing pro VPC möglich ist.

#### **A\_27675 -zentrales Netz SZZP-light-cloud, Betrieb**

Das zentrale Netz MUSS den Mandanten einer SZZP-light-Cloud Anbindung für den Betrieb vertraglich zu den folgenden Vorgaben verpflichten.

- das Betriebssystem der VM ist mit Sicherheitspatches und Updates zu versorgen,
- regelmäßig (mindestens wöchentlich) eine Sicherung der VM vornehmen und die Wiederherstellung einer gesicherten VM ermöglichen,
- eine Containervirtualisierung unterstützen (z. B. Docker),
- die VM mittels Monitoring hinsichtlich der Verfügbarkeit der bereitgestellten Ressourcen überwachen und
- den reibungslosen Betrieb der VM sicherstellen.

[<=]

#### **A\_27677 -zentrales Netz SZZP-light-cloud, VPC Administration**

Das zentrale Netz MUSS den Mandanten einer SZZP-light-Cloud Anbindung zu den folgenden Optionen für den gesicherten Administrationszugang zu seinem VPC verpflichten:

- Über VPN Tunnel zum VPC.
- Über speziell abgesicherte Jump Hosts.
- Über Absicherung durch Zero Trust.

[<=]

Im Kapitel 2.6.3 werden die folgenden Festlegungen angepasst.

### **1.1.2 Platzierung von Sicherheitskomponenten**

#### **GS-A\_4062-02 -Sicherheitsanforderungen für Netzübergänge zu Fremdnetzen**

Zentrale Produkttypen MÜSSEN den Übergang zu Fremdnetzen mit niedrigerem oder unbekanntem Sicherheitsniveau, wie dem Internet mit einem vom BSI zertifizierten Sicherheitsgateway oder einem Sicherheitsgateway mit dreistufigem Aufbau, wie in [BSI ISI-LANA] beschrieben, sichern.

Die Produkttypen MÜSSEN Wechselwirkungen zwischen dem Fremdnetz und der TI verhindern, und dazu den Verkehr einschränken und kontrollieren.

Übergänge zum Transportnetz mittels SZZP-light, SZZP-light-cloud und Sicherheitsgateway Bestandsnetze sind von dieser Regelung ausgenommen.

[<=]

#### **A\_20574-03 -Beachtung der ISI-LANA für Übergänge zu Fremdnetzen**

Zentrale Produkttypen SOLLEN für Übergänge zu Fremdnetzen die Empfehlungen der [BSI ISI-LANA] befolgen.

Übergänge zum Transportnetz mittels SZZP-light, SZZP-light-cloud und Sicherheitsgateway Bestandsnetze sind von dieser Regelung ausgenommen.

[<=]

Im Kapitel 2.7 wird der folgende informative Text angepasst.

## 1.2 IP-Configuration-Management

Die Kommunikation innerhalb des zentralen Netzes der TI wird in den SZZPs, den VPN-Anschlusspunkten des SZZP-light und den virtuellen VPN-Anschlusspunkten des SZZP-light-cloud durch den Anbieter zentrales Netz der TI mittels Routingeinträgen und Firewallfreischaltungen kontrolliert. In