Einführung der Gesundheitskarte

Spezifikation

VPN-Zugangsdienst

|  |  |
| --- | --- |
| Version: | 1.10.0 |
| Revision: | \main\rel\_online\rel\_ors1\rel\_opb1\rel\_ors2\11 |
| Stand: | 18.12.2017 |
| Status: | freigegeben |
| Klassifizierung: | öffentlich |
| Referenzierung: | [gemSpec\_VPN\_ZugD] |

Dokumentinformationen

Änderungen zur Vorversion

Einarbeitung der Errata 1.6.4-1 und 1.6.4-2

Dokumentenhistorie

| **Version** | **Stand** | **Kap./ Seite** | **Grund der Änderung, besondere Hinweise** | **Bearbeitung** |
| --- | --- | --- | --- | --- |
| 0.5.0 | 08.08.12 |  | zur Abstimmung freigegeben | PL P77 |
| 1.0.0 | 15.10.12 |  | Einarbeitung der Kommentare | P77 |
| 1.1.0 | 12.11.12 |  | Einarbeitung Kommentare aus der übergreifenden Konsistenzprüfung | P77 |
| 1.2.0 | 06.06.13 |  | Überarbeitung anhand interner Änderungsliste (Fehlerkorrekturen, Inkonsistenzen) | P77 |
| 1.3.0 | 15.08.13 |  | Einarbeitung lt. Änderungsliste vom 08.08.13 | P77 |
| 1.4.0 | 21.02.14 |  | Losübergreifende Synchronisation | P77 |
| 1.5.0 | 17.06.14 |  | Ersetzen HTTP durch HTTPS, Streichung nicht notwendiger Ablaufschritte, Aktualisierung Netztopologier gemäß P11-Änderungsliste | P77 |
| 1.6.0 | 24.08.16 |  | Anpassungen zum Online-Produktivbetrieb (Stufe 1) | gematik |
| 1.7.0 | 28.10.16 |  | Einarbeitung lt. Änderungsliste | gematik |
|  |  |  | Einarbeitung lt. Änderungsliste |  |
| 1.8.0 | 06.02.17 |  | freigegeben | gematik |
| 1.9.0 | 20.04.17 |  | Einarbeitung lt. Änderungsliste | gematik |
|  | 07.12.17 |  | Überarbeitung Online-Produktivbetrieb (Stufe 2.1) | gematik |
| 1.10.0 | 18.12.17 |  | freigegeben | gematik |

Inhaltsverzeichnis

[1 Einordnung des Dokumentes 7](#_Toc501718139)

[1.1 Zielsetzung 7](#_Toc501718140)

[1.2 Zielgruppe 7](#_Toc501718141)

[1.3 Geltungsbereich 7](#_Toc501718142)

[1.4 Abgrenzung 7](#_Toc501718143)

[1.5 Methodik 8](#_Toc501718144)

[2 Systemüberblick 9](#_Toc501718145)

[2.1 Funktion 9](#_Toc501718146)

[2.2 Netzaufbau 9](#_Toc501718147)

[3 Zerlegung des Produkttyps 11](#_Toc501718148)

[3.1 VPN-Konzentratoren 12](#_Toc501718149)

[3.1.1 Funktion 12](#_Toc501718150)

[3.1.2 Topologie 12](#_Toc501718151)

[3.1.3 Standorte des VPN-Zugangsdienstes 13](#_Toc501718152)

[3.1.4 Anbindung an das Transportnetz Internet 14](#_Toc501718153)

[3.1.5 Anbindung an die TI 15](#_Toc501718154)

[3.1.6 Anbindung an den SIS 15](#_Toc501718155)

[3.1.7 Service-Zone des Standortes TI 15](#_Toc501718156)

[3.1.8 Redundanz 15](#_Toc501718157)

[3.1.9 Konfiguration 16](#_Toc501718158)

[3.1.10 Adressierung 17](#_Toc501718159)

[3.1.10.1 VPN-Konzentratoren zum Transportnetz Internet 17](#_Toc501718160)

[3.1.10.2 VPN-Konzentratoren TI zum Zentralen Netz 18](#_Toc501718161)

[3.1.10.3 VPN-Konzentratoren SIS zum Internet 18](#_Toc501718162)

[3.1.11 DNS 18](#_Toc501718163)

[3.1.12 Performance 19](#_Toc501718164)

[3.2 Nameserver Internet 20](#_Toc501718165)

[3.2.1 Funktion 20](#_Toc501718166)

[3.2.2 Verteilung 20](#_Toc501718167)

[3.2.3 Redundanz 21](#_Toc501718168)

[3.2.4 Konfiguration 21](#_Toc501718169)

[3.2.5 Adressierung 22](#_Toc501718170)

[3.3 Nameserver TI 23](#_Toc501718171)

[3.3.1 Funktion 23](#_Toc501718172)

[3.3.2 Verteilung 23](#_Toc501718173)

[3.3.3 Redundanz 23](#_Toc501718174)

[3.3.4 Konfiguration 23](#_Toc501718175)

[3.3.5 Adressierung 24](#_Toc501718176)

[3.4 Nameserver SIS 24](#_Toc501718177)

[3.4.1 Funktion 24](#_Toc501718178)

[3.4.2 Verteilung 24](#_Toc501718179)

[3.4.3 Redundanz 24](#_Toc501718180)

[3.4.4 Konfiguration 24](#_Toc501718181)

[3.4.5 Adressierung 25](#_Toc501718182)

[3.5 Registrierungsserver 25](#_Toc501718183)

[3.5.1 Funktion 25](#_Toc501718184)

[3.5.2 Verteilung 25](#_Toc501718185)

[3.5.3 Redundanz 25](#_Toc501718186)

[3.5.4 Konfiguration 25](#_Toc501718187)

[3.5.5 Adressierung 25](#_Toc501718188)

[3.6 Autorisierungsserver 26](#_Toc501718189)

[3.6.1 Funktion 26](#_Toc501718190)

[3.6.2 Verteilung 27](#_Toc501718191)

[3.6.3 Redundanz 27](#_Toc501718192)

[3.6.4 Konfiguration 27](#_Toc501718193)

[3.6.5 Adressierung 27](#_Toc501718194)

[3.7 hash&URL-Server 27](#_Toc501718195)

[3.7.1 Funktion 28](#_Toc501718196)

[3.7.2 Verteilung 28](#_Toc501718197)

[3.7.3 Redundanz 28](#_Toc501718198)

[3.7.4 Konfiguration 28](#_Toc501718199)

[3.7.5 Adressierung 28](#_Toc501718200)

[3.8 http-Forwarder 29](#_Toc501718201)

[3.8.1 Funktion 29](#_Toc501718202)

[3.8.2 Verteilung 29](#_Toc501718203)

[3.8.3 Redundanz 29](#_Toc501718204)

[3.8.4 Konfiguration 29](#_Toc501718205)

[3.8.5 Adressierung 30](#_Toc501718206)

[3.9 NTP-Server TI 30](#_Toc501718207)

[3.9.1 Funktion 30](#_Toc501718208)

[3.9.2 Verteilung 31](#_Toc501718209)

[3.9.3 Redundanz 31](#_Toc501718210)

[3.9.4 Konfiguration 31](#_Toc501718211)

[3.9.5 Adressierung 32](#_Toc501718212)

[3.10 Secure Internet Service 32](#_Toc501718213)

[3.10.1 Funktion 32](#_Toc501718214)

[3.10.2 Verteilung 32](#_Toc501718215)

[3.10.3 Redundanz 32](#_Toc501718216)

[3.10.4 Konfiguration 32](#_Toc501718217)

[3.10.5 Adressierung 33](#_Toc501718218)

[4 Übergreifende Festlegungen 34](#_Toc501718219)

[4.1 Sicherheit 34](#_Toc501718220)

[4.1.1 Kommunikation zwischen Service-Zonen und Zugangszonen 34](#_Toc501718221)

[4.1.2 Übergang der VPN-Konzentratoren zum Transportnetz Internet 35](#_Toc501718222)

[4.1.3 Übergang der VPN-Konzentratoren zur TI 36](#_Toc501718223)

[4.1.4 Sicherheitsleistung des Secure Internet Service 36](#_Toc501718224)

[4.1.5 Kommunikation zwischen Konnektoren 37](#_Toc501718225)

[4.1.6 Durchsetzung der Zugangsberechtigung 37](#_Toc501718226)

[4.2 Protokollanforderungen 39](#_Toc501718227)

[4.2.1 IPsec 39](#_Toc501718228)

[4.2.2 IKEv2 39](#_Toc501718229)

[4.2.3 Verschlüsselung 40](#_Toc501718230)

[4.2.4 Kompression 40](#_Toc501718231)

[4.2.5 Verbindungszustand 40](#_Toc501718232)

[4.2.6 Fragmentierung von IKE-Paketen 41](#_Toc501718233)

[4.3 Netzanforderungen 41](#_Toc501718234)

[4.3.1 Routing 41](#_Toc501718235)

[4.3.1.1 VPN-Zugangsdienst 41](#_Toc501718236)

[4.3.1.2 Konnektor 42](#_Toc501718237)

[4.3.2 Behandlung gemäß DiffServ-Architektur 42](#_Toc501718238)

[4.3.2.1 VPN-Konzentratoren zum Transportnetz Internet 43](#_Toc501718239)

[4.3.2.2 VPN-Konzentratoren zu Konnektoren 43](#_Toc501718240)

[4.3.2.3 VPN-Zugangsdienst zur TI 44](#_Toc501718241)

[4.3.2.4 Alternatives Zugangsnetz 44](#_Toc501718242)

[4.3.2.5 SIS zum Internet 44](#_Toc501718243)

[5 Funktionsmerkmale 45](#_Toc501718244)

[5.1 Schnittstelle I\_Secure\_Channel\_Tunnel 46](#_Toc501718245)

[5.1.1 Operation connect 47](#_Toc501718246)

[5.1.1.1 Umsetzung 47](#_Toc501718247)

[5.1.1.2 Nutzung 48](#_Toc501718248)

[5.1.1.3 Verbindungsaufbau 51](#_Toc501718249)

[5.1.1.4 Adressierung 51](#_Toc501718250)

[5.1.2 Operation disconnect 52](#_Toc501718251)

[5.1.3 Operation send\_secure\_IP\_Packet 52](#_Toc501718252)

[5.2 Schnittstelle I\_Secure\_Internet\_Tunnel 52](#_Toc501718253)

[5.2.1 Operation connect 53](#_Toc501718254)

[5.2.1.1 Umsetzung 53](#_Toc501718255)

[5.2.1.2 Nutzung 54](#_Toc501718256)

[5.2.2 Operation disconnect 57](#_Toc501718257)

[5.3 Schnittstelle I\_Registration\_Service 57](#_Toc501718258)

[5.3.1 Operation registerKonnektor 57](#_Toc501718259)

[5.3.1.1 Umsetzung 61](#_Toc501718260)

[5.3.1.2 Nutzung 61](#_Toc501718261)

[5.3.2 Operation deregisterKonnektor 61](#_Toc501718262)

[5.3.2.1 Umsetzung 63](#_Toc501718263)

[5.3.2.2 Nutzung 63](#_Toc501718264)

[5.3.3 Operation registerStatus 64](#_Toc501718265)

[5.3.3.1 Umsetzung 65](#_Toc501718266)

[5.3.3.2 Nutzung 65](#_Toc501718267)

[5.3.4 Registrierungsserver Fehlermeldungen 66](#_Toc501718268)

[5.4 Schnittstelle I\_DNS\_Name\_Resolution (Namensraum TI) 66](#_Toc501718269)

[5.5 Schnittstelle I\_DNS\_Name\_Resolution (Namensraum Internet) 67](#_Toc501718270)

[5.6 Schnittstelle I\_DNS\_Name\_Resolution (Namensraum SIS) 67](#_Toc501718271)

[5.7 Schnittstelle I\_NTP\_Time\_Information 67](#_Toc501718272)

[5.8 Prozess Änderung der Sicherheitsleistungen des SIS 67](#_Toc501718273)

[5.9 Prozess zum Abschluss, Ändern und Auflösen des Vertragsverhältnisses 67](#_Toc501718274)

[6 Anhang A – Verzeichnisse 69](#_Toc501718275)

[6.1 A1 – Abkürzungen 69](#_Toc501718276)

[6.2 A2 – Glossar 71](#_Toc501718277)

[6.3 A3 – Abbildungsverzeichnis 71](#_Toc501718278)

[6.4 A4 – Tabellenverzeichnis 71](#_Toc501718279)

[6.5 A5 – Referenzierte Dokumente 72](#_Toc501718280)

[6.5.1 A5.1 – Dokumente der gematik 72](#_Toc501718281)

[6.5.2 A5.2 – Weitere Dokumente 72](#_Toc501718282)

# Einordnung des Dokumentes

## Zielsetzung

Die vorliegende Spezifikation definiert die Anforderungen zu Herstellung, Test und Betrieb des Produkttyps VPN-Zugangsdienst.

## Zielgruppe

Das Dokument ist maßgeblich für Hersteller und Anbieter von VPN-Zugangsdiensten der TI sowie Hersteller und Anbieter von Produkttypen, die hierzu eine Schnittstelle besitzen.

## Geltungsbereich

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

**Schutzrechts-/Patentrechtshinweis**

Die nachfolgende Spezifikation ist von der gematik allein unter technischen Gesichtspunkten erstellt worden. Im Einzelfall kann nicht ausgeschlossen werden, dass die Implementierung der Spezifikation in technische Schutzrechte Dritter eingreift. Es ist allein Sache des Anbieters oder Herstellers, durch geeignete Maßnahmen dafür Sorge zu tragen, dass von ihm aufgrund der Spe­zifikation angebotene Produkte und/oder Leistungen nicht gegen Schutzrechte Dritter verstoßen und sich ggf. die erforderlichen Erlaubnisse/Lizenzen von den betroffenen Schutz­rechts­inhabern einzuholen. Die gematik GmbH übernimmt insofern keinerlei Gewähr­leistungen.

## Abgrenzung

Spezifiziert werden in dem Dokument die von dem Produkttyp bereitgestellten (angebo­tenen) Schnittstellen. Benutzte Schnittstellen werden dagegen in der Spezifikation des­jenigen Produkttypen beschrieben, der diese Schnittstelle bereitstellt. Auf das entsprech­ende Dokument wird referenziert (siehe Anhang A5).

Die vollständige Anforderungslage für den Produkttyp ergibt sich aus weiteren Konzept- und Spezifikationsdokumenten, diese sind in dem Produkttypsteckbrief des Produkttyps VPN-Zugangsdienst verzeichnet.

## Methodik

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

Sie werden im Dokument wie folgt dargestellt:

**⌦ TIP1-A\_xxxx <Titel der Afo>**

Text/Beschreibung

**⌫**

Dabei umfasst die Anforderung sämtliche innerhalb der Textmarken angeführten Inhalte.

# 

# Systemüberblick

## Funktion

Der VPN-Zugangsdienst ermöglicht den Leistungserbringern den Zugang zur Telematik­infrastruktur (TI) und zum Secure Internet Service (SIS). Für Leistungs­erbringer ist die Nutzung des SIS optional. Als Trans­portinfrastruktur zwischen dem Netz des Leistungs­erbringers auf der einen Seite und dem VPN-Zugangsdienst auf der anderen Seite wird in der Regel das öffent­liche Internet genutzt. Durch diese Infrastruktur werden ge­sicherte Ver­bindungen von den Konnektoren der Leistungserbringer zu einer Anzahl zentraler VPN-Konzentratoren auf­gebaut. Der Zugang ist durch beidseitige, zertifikatsbasierte Authentisierung gesichert. Die Ver­trau­lichkeit und Integrität der über­tragenen Daten wird durch den Einsatz kryptographischer Maßnahmen sicher­ge­stellt.

## Netzaufbau

Das Zugangsnetz wird auf Grundlage einer „Hub-and-Spoke“-Architektur aufgebaut. Als „Hubs“ dienen regionale Zugangspunkte, die vom Anbieter des VPN-Zugangsdienstes bereitgestellt werden. An den Zugangspunkten sind VPN-Konzentratoren für den Zugang zur TI und zum SIS installiert.

Als Außenstellen („Spokes“) fungieren die Konnektoren. Sie initiieren den Verbindungs­aufbau zu den VPN-Konzentratoren. Über diesen sicheren Kanal ist die Nutzung von Diensten der TI und der Bestandsnetze möglich. Eine direkte Netzwerkkommunikation zwischen Konnektoren über die VPN-Konzentratoren ist nicht erlaubt.

In der Abbildung 1 werden auf logischer Ebene die im VPN-Zugangsdienst bereitzustel­lenden Komponenten und System und deren Einbindung in die TI dargestellt, deren detaillierte Beschreibung im Kapitel 3 erfolgt.



Abbildung 1: Netztopologie VPN-Zugangsdienst (logisch)

Als Transportnetz kommt nicht nur das öffentliche Internet in Frage, sondern eine beliebi­ge Zugangstechnik. Es steht dem Anbieter des VPN-Zugangsdienstes grundsätzlich frei, Zu­gänge z. B. per Festverbindung oder über ein geeignetes privates IP-basiertes Netz an­zu­bieten. In jedem Fall erfolgt der Zugang zur TI und zum SIS über VPN-Konzen­tratoren der TI.

In diesem Dokument wird als Transportnetz ausschließlich das öffentliche Internet be­trachtet. Anbindungsvarianten mit anderen Transportnetzen und dafür ggf. notwendige Ergänzungen sind bei Bedarf fallbezogen zu beschreiben.

# 

# Zerlegung des Produkttyps

Die folgende Abbildung stellt die einzelnen Komponenten des VPN-Zugangsdienstes dar.



Abbildung 2: Zerlegung des VPN-Zugangsdienstes

Die grün dargestellten Komponenten werden ausschließlich für den Zugang zur TI ver­wendet. Die blau dargestellten Komponenten werden ausschließlich für die Nutzung des Sicheren Internetzugangs genutzt. Die rosa dargestellten Komponenten haben Schnittstellen in Richtung Internet.

In der Abbildung 3 werden die Komponenten des VPN-Zugangsdienstes logischen Zonen zugeordnet, die für eine Adressierung von funktionalen und nichtfunktionalen Anforde­rungen genutzt werden.



Abbildung 3: Übersicht VPN-Zugangsdienst (Zonen)

Der Registrierungsserver und der hash&URL-Server haben eine Schnittstelle zum Internet. Der hash&URL-Server wird bei Bedarf für den VPN-Verbindungsaufbau TI und SIS genutzt.

## VPN-Konzentratoren

### Funktion

Der Anbieter VPN-Zugangsdienst verwendet für die Bereitstellung des VPN-Zugangs­dienstes auf IPsec basierende VPN-Konzentratoren. Die VPN-Konzentratoren stellen die Schnittstellen I\_Secure\_Channel\_Tunnel und I\_Secure\_Internet\_Tunnel im Transportnetz (Internet und ggf. zusätzlichen Transportnetzen) bereit.

Als VPN-Konzentratoren kommen dedizierte Geräte zum Einsatz, oder geeignete Hard­warecluster, welche eine gemeinsame Identität haben. Unabhängig von der gewählten Implementation werden diese Funktionseinheiten im Folgenden als VPN-Konzentratoren bezeichnet.

### Topologie

Die Konnektoren bauen IPsec-Tunnel zu einem VPN-Konzentrator auf, der ihnen Zugang zur TI gewährt. Optional bauen die Konnektoren auch gleichzeitig einen weiteren Tunnel zu einem anderen VPN-Konzentrator auf, der den Zugang zum SIS ermöglicht.

**⌦ TIP1-A\_4277 VPN-Zugangsdienst, Physische Trennung der VPN-Konzen­tra­toren**

Der Anbieter des VPN-Zugangsdienstes MUSS zwischen den VPN-Konzentratoren, welche für den Zugang zur TI verwendet werden, und den VPN-Konzentratoren für den Zugang zum SIS eine physische Trennung der Hardware gewährleisten.

**⌫**

### Standorte des VPN-Zugangsdienstes

Bei der Auswahl der Standorte soll die Nähe zu einer Vielzahl von Leistungserbringern berücksichtigt werden. Sie sollen daher möglichst zentral in den größten Ballungsräumen eingerichtet werden; zusätzlich sollen sie geografisch ver­teilt werden.

**⌦ TIP1-A\_4278 VPN-Zugangsdienst, Geografische Verteilung der VPN-Konzen­tratoren**

Der Anbieter des VPN-Zugangsdienstes MUSS die Standorte seiner VPN-Konzen­tra­toren geografisch in seinem Einzugsgebiet verteilen, so dass die durch­schnitt­liche Distanz und Laufzeit von den Netzen der Leistungserbringer zu den VPN-Konzentratoren optimiert wird.

**⌫**

Durch die Bereitstellung von mindestens zwei geografisch getrennten Standorten soll auch bei kleinen regionalen Anbietern sichergestellt werden, dass der gleichzeitige Aus­fall beider Standorte durch dasselbe Ereignis (z.B. Naturereignis, Stromausfall) unwahr­scheinlich ist.

**⌦ TIP1-A\_4279 VPN-Zugangsdienst, Mindestanzahl Standorte VPN-Konzentrator**

Der Anbieter des VPN-Zugangsdienstes MUSS VPN-Konzentratoren an mindes­tens zwei geografisch getrennten Standorten betreiben.

**⌫**

**⌦ TIP1-A\_5418 VPN-Zugangsdienst, Standorte VPN-Konzentrator RU und TU**

Der Anbieter des VPN-Zugangsdienstes KANN für den Nachweis der standortüber­grei­fenden Redundanzfunktionen in der Referenz- und der Testumgebung die VPN-Konzentratoren an einer Lokation betreiben.

**⌫**

Für einen bundesweiten VPN-Zugangsdienst werden folgende Standorte als besonders geeignet und notwendig angesehen:

* Frankfurt
* Hamburg
* München
* Berlin
* Köln, Düsseldorf, Bonn
* Ruhrgebiet (Dortmund, Essen)

Folgende Standorte werden zusätzlich als besonders geeignet angesehen, wenn der Betreiber eine weitere Flächendeckung erreichen will:

* Stuttgart
* Nürnberg
* Saarbrücken
* Leipzig/Dresden
* Hannover
* Bremen

Der Anbieter VPN-Zugangsdienst kann an jedem Standort eine beliebige Zahl von VPN-Konzentratoren zur Bereitstellung des Dienstes einsetzen.

### Anbindung an das Transportnetz Internet

**⌦ TIP1-A\_4281 VPN-Zugangsdienst, NAT an der Schnittstelle zum Internet**

Der Anbieter des VPN-Zugangsdienstes DARF NICHT zwischen der internet­seitigen Schnittstelle der VPN-Konzentratoren und dem Internet NAT-Verfahren einsetzen.

**⌫**

**⌦ TIP1-A\_4282 VPN-Zugangsdienst, Eindeutiger FQDN für VPN-Konzentratoren**

Der Anbieter des VPN-Zugangsdienstes MUSS jeden VPN-Konzentrator mit einem eindeutigen FQDN versehen.

**⌫**

**⌦ TIP1-A\_4284 VPN-Zugangsdienst, Redundanter Internetzugang**

Der Anbieter des VPN-Zugangsdienstes MUSS die VPN-Konzentratoren über einen redundanten Zugang an das Internet anbinden. Hierzu sind mindestens zwei vollständig unabhängige Leitungsführungen zwischen dem Standort und dem IP-Backbone sowie unabhängige Zugangsrouter erforderlich.

**⌫**

**⌦ TIP1-A\_4285 VPN-Zugangsdienst, Umschaltzeiten am Internetzugang**

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

**⌫**

### Anbindung an die TI

**⌦ TIP1-A\_4288 VPN-Zugangsdienst, redundante Anbindung an die TI**

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

**⌫**

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

### Anbindung an den SIS

Die VPN-Konzentratoren für den SIS-Zugang werden redundant an ein dreistufiges Sicher­heitsgateway angebunden, welches sich in Kolokation mit den VPN-Konzentra­toren befin­det.

Der grundlegende Schutz der angebundenen Teilnehmer vor dem öffentlichen Internet wird über eine Application-Level-Gateway-Paketfilter-Struktur (P-A-P) entsprechend den Vor­ga­ben des BSI zur Konzeption von Sicherheitsgateways [BSI-SiGw] gewährleistet.

### Service-Zone des Standortes TI

**⌦ TIP1-A\_4289 VPN-Zugangsdienst, Service-Zone TI**

Der Anbieter des VPN-Zugangsdienstes MUSS an jedem Standort in Kolokation eine eigene Service-Zone TI bereitstellen. Die Service-Zone TI besteht aus einem logisch getrennten Netzwerksegment. In dieser Service-Zone TI werden Proxy-Server, Nameserver TI, NTP-Server und andere Backend-Systeme aufgestellt.

**⌫**

Der Anbieter des VPN-Zugangsdienstes erhält einen Adressblock aus dem Adressbereich TI\_Zentral (siehe [gemSpec\_Net#3.3] IP-Adresskonzept der TI).

**⌦ TIP1-A\_4472 VPN-Zugangsdienst, Adressierung der Service-Zone TI**

Der Anbieter des VPN-Zugangsdienstes MUSS der Service-Zone TI einen aus­reichend großen Adressraum aus dem Adressbereich TI\_Zentral zuweisen.

**⌫**

### Redundanz

Die Anforderungen zur Verfügbarkeit ergeben sich aus [gemSpec\_Perf#4.2]. Die Ver­fügbar­keit wird hergestellt durch Anzahl, Verteilung und Konfiguration der VPN-Kon­zen­tratoren. In diesem Dokument werden zusätzliche Redundanzanforderungen spe­zifiziert, wenn die Anforderungen in [gemSpec\_Perf] zur Verfügbarkeit nicht ausreichen.

Die Auswahl der VPN-Konzentratoren wird durch die Konnektoren aus einer durch DNS übermittelten Liste vorgenommen. Auf die Auswahl des VPN-Konzentrators durch den Konnektor kann der Anbieter des VPN-Zugangsdienstes durch die Konfiguration und An­passung der DNS-Einträge Einfluss nehmen. Die Verfügbarkeit ist hergestellt, wenn jeder Konnektor die Möglichkeit zum Verbindungsaufbau hat.

Eine hardwaretechnische Hochverfügbarkeit der einzelnen VPN-Konzentratoren ist über grundlegende Maßnahmen, wie redundante Netzteile hinaus nicht erforderlich. Es steht dem Anbieter jedoch frei, zur Sicherstellung der Verfügbarkeitsanforderungen technische Lösungen, wie z. B. Load-Balancer und Stateful Failover innerhalb von Clustern einzuset­zen, so dass jeder einzelne VPN-Konzentrator im Ergebnis eine höhere Verfügbarkeit oder Leistungsfähigkeit besitzt.

**⌦ TIP1-A\_4290 VPN-Zugangsdienst, Redundanz der VPN-Konzentratoren im VPN-Konzentrator-Standort**

Der Anbieter des VPN-Zugangsdienstes MUSS sicherstellen, dass bei Ausfall eines von mehreren VPN-Konzentratoren die verbleibenden VPN-Konzentratoren in dem­selben Standort den Datenverkehr aller Kunden des ausgefallenen VPN-Kon­zen­trators zusätzlich übernehmen können. Die Anforderungen an die Dauer der Authentisierung sind in diesem Fall einzuhalten.

**⌫**

Für den Fall, dass ein ganzer VPN-Zugangsdienststandort ausfällt oder nicht erreichbar ist, wird der Konnektor einen Verbindungsaufbau zu einem anderen nahegelegenen Standort versuchen. Der Anbieter muss daher an dem anderen Standort ausreichende Kapazitäten vorhalten, um die zusätzliche Netzlast übernehmen zu können.

**⌦ TIP1-A\_4291 VPN-Zugangsdienst, standortübergreifende Redundanz der VPN-Konzentratoren**

Der Anbieter des VPN-Zugangsdienstes MUSS sicherstellen, dass bei Ausfall eines Stand­ortes ein anderer, vorzugsweise der geografisch nächste Standort, den Da­ten­verkehr des ausgefallenen Standortes übernehmen kann.

**⌫**

**⌦ TIP1-A\_5451 VPN-Zugangsdienst, IPsec-Verbindungen bei Komponentenausfall beenden**

Der Anbieter des VPN-Zugangsdienstes MUSS alle bestehenden IPsec-Ver­bin­dungen auf den VPN-Konzentratoren TI beenden und darf keine neuen Verbin­dungen zulassen, wenn am jeweiligen VPN-Zugangsdienst-Standort eine Kompo­nen­te der Service-Zone TI oder eine an der Weiterleitung der Daten vom VPN-Kon­zentrator TI zum SZZP beteiligte Komponente ausfällt und dadurch die Nutzung der Fachanwendungsspezifischen Dienste sowie der Zentralen Dienste der TI-Plattform nicht mehr möglich ist. Hiervon ausgenommen sind die NTP-Server der Service-Zone TI.

**⌫**

### Konfiguration

**⌦ TIP1-A\_4292 VPN-Zugangsdienst, Härtung des VPN-Konzentrators**

Der Anbieter des VPN-Zugangsdienstes MUSS die VPN-Konzentratoren so konfi­gu­rieren, dass ausschließlich die erforderlichen Netzwerkprotokolle und krypto­graphischen Methoden akzeptiert werden.

**⌫**

Die erforderlichen Netzwerkprotokolle werden in Kapitel 4 und die kryptographischen Methoden in [gemSpec\_Krypt] definiert.

**⌦ TIP1-A\_4473 VPN-Zugangsdienst, Verhalten der Konzentratoren bei Vollaus­lastung**

Der Anbieter des VPN-Zugangsdienstes MUSS die VPN-Konzentratoren so konfi­gu­rieren, dass bei Vollauslastung der Systemressourcen keine weiteren Ver­bin­dungen angenommen werden.

**⌫**

Durch die Zurückweisung von Verbindungen wird sichergestellt, dass der Konnektor einen Verbindungsaufbau mit einem anderen Konzentrator versucht, bei dem die erfor­derlichen Ressourcen zur Verfügung stehen.

**⌦ TIP1-A\_4286 VPN-Zugangsdienst, keine TI-Tunnel bei fehlender TI-Ver­bindung**

Der Anbieter des VPN-Zugangsdienstes MUSS sicherstellen, dass die VPN-Kon­zen­tratoren TI eines Standortes des VPN-Zugangsdienstes keine IPsec-Ver­bin­dungen von Konnektoren annehmen, während an diesem Standort der Zugang in das zentrale Netz der TI gestört ist. Aktive Verbindungen der Konnek­toren zu den VPN-Konzentratoren TI MÜSSEN gemäß [RFC 7296] abgebaut werden.

**⌫**

Durch die Zurückweisung von Verbindungen wird sichergestellt, dass der Konnektor einen Verbindungsaufbau mit einem anderen Konzentrator versucht, bei dem die Ver­bindung in die TI zur Verfügung steht.

**⌦ TIP1-A\_4287 VPN-Zugangsdienst, keine SIS-Tunnel bei fehlender SIS-Internet­verbindung**

Der Anbieter des VPN-Zugangsdienstes MUSS sicherstellen, dass die VPN-Konzentratoren SIS keine IPsec-Verbindungen annehmen, während der Übergang durch den SIS in das Internet gestört ist. Aktive Verbindungen der Konnektoren zu den VPN-Konzentratoren SIS MÜSSEN gemäß [RFC7296] abgebaut werden.

**⌫**

### Adressierung

#### VPN-Konzentratoren zum Transportnetz Internet

**⌦ TIP1-A\_4293 VPN-Zugangsdienst, IPv4-Adressierung der Internetschnitt­stellen der VPN-Konzentratoren**

Der Anbieter des VPN-Zugangsdienstes MUSS jedem VPN-Konzentrator genau eine öffentliche IPv4-Adresse zuweisen. Diese Adresse MUSS auf der physischen Schnittstelle zum Internet konfiguriert werden. Die öffentlichen IP-Adressen der VPN-Konzentratoren MÜSSEN vom Anbieter des VPN-Zugangsdienstes zur Verfügung gestellt werden.

**⌫**

**⌦ TIP1-A\_4474 IPv6-Adressierung der Internetschnittstellen der VPN-Konzen­tratoren**

Der Anbieter des VPN-Zugangsdienstes SOLL jedem VPN-Konzentrator eine IPv6-Adresse zuweisen. Diese Adresse wird auf der physischen Schnittstelle zum Inter­net konfiguriert. Die öffentlichen IPv6-Adressen der VPN-Konzentratoren werden vom Anbieter des VPN-Zugangsdienstes zur Verfügung gestellt.

**⌫**

#### VPN-Konzentratoren TI zum Zentralen Netz

Die Adressen der VPN-Konzentratoren am Übergang zur TI werden vom Anbieter des Zentralen Netzes aus dem Adressblock TI\_Zentral zugewiesen.

#### VPN-Konzentratoren SIS zum Internet

**⌦ TIP1-A\_4294 VPN-Zugangsdienst, Adressen des SIS zum Internet**

Der Anbieter des VPN-Zugangsdienstes MUSS eine ausreichende Anzahl öffent­licher IP-Adressen zum Betrieb des SIS zur Verfügung stellen.

**⌫**

### DNS

**⌦ TIP1-A\_4295 VPN-Zugangsdienst, eigene Domain für VPN-Konzentrator-FQDN**

Der Anbieter VPN-Zugangsdienst MUSS für die FQDN der VPN-Konzentratoren eine eigene Domain oder Subdomain im Namensraum Internet einrichten und betreiben**.**

**⌫**

Der Anbieter des VPN-Zugangsdienstes kann die Hostnamen der VPN-Konzentratoren im Rah­men der Zweckmäßigkeit frei wählen.

Bei einem Verbindungsaufbau durch den Konnektor verwendet dieser zur Auswahl des VPN-Konzentrators einen lokal konfigurierten SRV-Record-Bezeichner. Dieser Bezeich­ner wird verwendet, um über eine DNS-Abfrage eine VPN-Konzentratorliste (SRV-Record) abzufragen. Der SRV-Record enthält die FQDN aller aktiven VPN-Konzen­tra­toren mit einer jeweils zugewiesenen Priorität und Gewichtung. Der Kon­nektor berück­sichtigt gemäß [RFC2782] zunächst die Einträge mit der höchsten Priorität, und wählt aus diesen einen Eintrag zufällig aus, wobei die Wahrscheinlichkeit der Aus­wahl proportional zur Gewichtung ist. Den so gewonnenen FQDN benutzt der IKEv2-Initiator im Konnektor dann, um einen Verbindungsaufbau zu versuchen. Dazu löst der Konnektor den Eintrag als A-Record auf.

Bei einem gescheiterten Verbindungsaufbau versucht der Konnektor einen Verbindungs­aufbau in entsprechender Reihenfolge mit allen anderen Einträgen des SRV-Records, welche dieselbe Priorisierung haben. Danach werden die Einträge mit niedrigerer Priori­sierung entsprechend berücksichtigt.

Dieses Verhalten des Konnektors kann der Anbieter des VPN-Zugangsdienstes nutzen, um die Belastung seiner VPN-Konzentratoren entsprechend ihrer Leistungsfähigkeit zu ver­teilen. Durch die Priorisierung im SRV-Record wird eine Ausfallsicherheit verwirklicht, die auf Fehler der beteiligten intermediären Systeme, des VPN-Konzentrator-Standortes und der VPN-Konzentratoren reagieren kann.

Die TTL aller DNS-Records ist zweckmäßig zu wählen.

**⌦ TIP1-A\_4296 VPN-Zugangsdienst, Namensauflösung durch SRV-Record**

Der Anbieter des VPN-Zugangsdienstes MUSS die FQDN der VPN-Konzentratoren über DNS SRV-Records in den Nameservern Internet gemäß [RFC2782] bereit­stellen. Die DNS-SRV-Records MÜSSEN alle dem Kunden zugeordneten VPN-Kon­zentratoren enthalten. Jeder DNS-SRV-Record MUSS eine Priorisierung und Gewichtung der VPN-Konzentratoren vornehmen, wobei der den Kunden nächst­gelegene Standort die höchste Priorität erhält, der oder die Backup-Standorte eine nachrangige Priorität.

**⌫**

**⌦ TIP1-A\_4297 VPN-Zugangsdienst, Nutzung der SRV-Records zu betrieblichen Zwecken**

Der Anbieter des VPN-Zugangsdienstes MUSS die DNS-SRV-Records betrieb­lichen Erfordernissen anpassen. Dies beinhaltet mindestens:

* Abschaltung existierender oder Inbetriebnahme neuer Standorte
* Wartungsarbeiten oder Störungen an einzelnen VPN-Gateways
* Gegenmaßnahmen bei Ereignissen, welche einen Standort unbrauchbar machen
* Gegenmaßnahmen bei unvorhergesehener Überlast
* Optimierung der Systemperformance

**⌫**

### Performance

**⌦ TIP1-A\_4300 VPN-Zugangsdienst, Performance Authentisierung/Autori­sierung**

Der Anbieter des VPN-Zugangsdienstes MUSS das Authentisierungs- und Auto­risierungs­system so dimensionieren, dass die Authentisierungs- und Authorisierungsanfragen pro Tag, die durch einen IKEv2-Verbindungsaufbau ausge­löst wird, innerhalb von 2 s bearbeitet werden. Bearbeitungszeiten durch Systeme außerhalb des VPN-Zugangsdienstes sind hiervon ausgenommen.

**⌫**

Die Anforderung bezieht sich auf die Performance der Authentisierung beim Anbieter des VPN-Zugangsdienstes.

Es wird bei den LE eine stehende Internetverbindung voraus­ge­setzt. Diese wird vom IAG aufgebaut. In der Standardeinstellung des Konnektors wird die Verbindung nach dem IKEv2-Verbindungsaufbau, auch wenn keine Daten trans­por­tiert werden müssen, aufrechterhalten. ISDN (mit Einwahlverbindung) wird als Aus­nahmefall betrachtet.

**⌦ TIP1-A\_4475 VPN-Zugangsdienst, Performance Authentisierung/Auto­risierung bei Standortausfall**

Der Anbieter des VPN-Zugangsdienstes MUSS das Authentisierungs- und Autori­sierungs­system so dimensionieren, dass bei Ausfall eines Standortes ein anderer Standort alle dort zusätzlich ankommenden Verbindungsanfragen innerhalb von 5 Minuten abarbeiten kann.

**⌫**

**⌦ TIP1-A\_4301 VPN-Zugangsdienst, Durchsatz Verbindung zum Transportnetz Internet**

Der Anbieter des VPN-Zugangsdienstes MUSS den Internetzugang so dimen­sio­nieren, dass innerhalb eines Zeitraums von 5 Minuten die Auslastung nicht länger als insgesamt 15 Sekunden über 90% liegt.

**⌫**

**⌦ TIP1-A\_4476 VPN-Zugangsdienst, Durchsatz Verbindung zum Zentralen Netz TI**

Der Anbieter VPN-Zugangsdienst MUSS den Zugang zum Zentralen Netz TI so dimen­sionieren, dass innerhalb eines Zeitraums von 5 Minuten die Auslastung nicht länger als insgesamt 15 Sekunden über 90% liegt.

**⌫**

## Nameserver Internet

### Funktion

Der Nameserver Internet löst die Namen auf, die der Konnektor zum Aufbau der Tunnel zur TI und zum SIS sowie zur Registrierung benötigt.

### Verteilung

Die Nameserver Internet stehen in keiner Sicherheitszone der TI. Sie müssen auch nicht in Kolokation mit dem VPN-Zugangsdienst aufgestellt werden. Der Anbieter kann vorhan­dene Nameserver nutzen, sofern dies zweckmäßig ist.

**⌦ TIP1-A\_4302 VPN-Zugangsdienst, Nameserver mit rekursiver Funktion im Namensraum Internet**

Der Anbieter des VPN-Zugangsdienstes MUSS an mindestens drei verschiedenen, in Deutschland geografisch verteilten Orten, Nameserver im Namensraum Internet betreiben, welche rekursive DNS-Anfragen der Konnektoren beantworten.

Um die Sicherheit der Nameserver zu erhöhen, können die abfragbaren Domains per Whitelist auf die fachlich erforderlichen Domains eingeschränkt werden.

**⌫**

**⌦ TIP1-A\_4303 VPN-Zugangsdienst, Nameserver mit autoritativer Funktion im Namensraum Internet**

Der Anbieter des VPN-Zugangsdienstes MUSS an mindestens drei verschiedenen, in Deutschland geografisch verteilten Orten, autoritative Nameserver im Namens­raum Internet betreiben, welche DNS-Anfragen zur Auflösung von FQDNs der VPN-Konzentratoren beantworten.

**⌫**

Der VPN-Zugangsdienst darf die autoritative und die rekursive DNS-Funktion auf denselben Geräten bereitstellen**.**

### Redundanz

Die hierfür geltenden Anforderungen zur Verfügbarkeit werden in [gemSpec\_Perf#4.2] defi­niert.

### Konfiguration

Die Nameserver Internet sind mit dem Internet verbunden, welches als Transportnetz dient. Die Nameserver werden konfiguriert, um Anfragen aus dem öffentlichen Internet zu beantworten.

**⌦ TIP1-A\_5103 VPN-Zugangsdienst, Resource Records im Nameserver Internet**

Der Anbieter des VPN-Zugangsdienstes MUSS in den Nameservern Internet die Resource Records gemäß Tabelle Tab\_ZD\_Nameserver\_Int\_RR verwalten. Dazu müssen je Standort dedizierte Subdomänen verwendet werden.

Tabelle 1: Tab\_ZD\_Nameserver\_Int\_RR

| **Resource Record Bezeichner** | **Beschreibung** |
| --- | --- |
| \_isakmp.\_udp.ti-extern.<DNS\_DOMAIN\_VPN\_ZUGD\_INT> | SRV Resource Record zur Ermittlung der FQDN und Ports sowie der Priorität und Gewichtung der VPN-Konzentratoren TI |
| \_isakmp.\_udp.sis-extern.<DNS\_DOMAIN\_VPN\_ZUGD\_INT> | SRV Resource Record zur Ermittlung der FQDN und Ports sowie der Priorität und Gewichtung der VPN-Konzentratoren SIS |
| \_hashandurl.\_tcp.<DNS\_DOMAIN\_VPN\_ZUGD\_INT> | SRV Resource Record zur Ermittlung der URL des hash&URL-Servers |
| \_regserver.\_tcp.<DNS\_DOMAIN\_VPN\_ZUGD\_INT> | SRV Resource Record zur Ermittlung des FQDN und Ports des Registrierungsservers des VPN-Zugangsdienstes |
| REGISTRIERUNGSSERVER\_FQDN | A Resource Records zur Namensauflösung des FQDN des Registrierungsservers in IP-Adressen |
| HASH\_AND\_URL\_SERVER\_FQDN | A Resource Records zur Namensauflösung des FQDN des hash&URL Servers in IP-Adressen |
| VPN\_KONZENTRATOR\_TI\_FQDN | A Resource Records zur Namensauflösung von FQDN der VPN-Konzentratoren TI in IP-Adressen |
| VPN\_KONZENTRATOR\_TI\_FQDN | TXT Resource Records zur Ermittlung der IP-Adressen der Nameserver TI (DNS\_SERVERS\_TI) sowie die Domainnamen der Service Zone TI (DOMAIN\_SRVZONE\_TI) des VPN-Zugangsdienstes.  Die key/value Paare der TXT-Records haben folgende Struktur (die spitzen Klammern dienen der Abgrenzung eines Wertes):  "txtvers=1"  "NameserverTI=<IP-Adresse1>,<IP-Adresse2>[,<weitere IP-Adressen>]"  "DomainSrvTI=<Domainname der Servicezone TI des VPN-Zugangsdienstes>"  Beispiel für einen Zonendateieintrag:  vpnk1.ham.ti-vpn-zugd.anbieter.de. 3600 IN TXT "txtvers=1"  "NameserverTI=100.97.20.13,100.97.20.14"  "DomainSrvTI=ti-sz.ham.anbieter.vpn-zugd.telematik" |
| VPN\_KONZENTRATOR\_SIS\_FQDN | A Resource Records zur Namensauflösung von FQDN der VPN-Konzentratoren SIS in IP-Adressen |
| VPN\_KONZENTRATOR\_SIS\_FQDN | TXT Resource Records zur Ermittlung der IP-Adressen der Nameserver SIS (DNS\_SERVERS\_SIS) sowie die Domainnamen der Service Zone SIS (DOMAIN\_SRVZONE\_SIS) des VPN-Zugangsdienstes.  Die key/value Paare der TXT-Records haben folgende Struktur (die spitzen Klammern dienen der Abgrenzung eines Wertes):  "txtvers=1"  "NameserverSIS=<IP-Adresse1>,<IP-Adresse2>[,<weitere IP-Adressen>]"  "DomainSrvSIS=<Domainname der Servicezone SIS des VPN-Zugangsdienstes>"  Beispiel für einen Zonendateieintrag:  vpnk1.ham.sis-vpn-zugd.anbieter.de. 3600 IN TXT "txtvers=1"  "NameserverSIS=100.97.20.13,100.97.20.14"  "DomainSrvSIS=sis-sz.ham.anbieter.vpn-zugd.telematik" |

**⌫**

### Adressierung

**⌦ TIP1-A\_4305 VPN-Zugangsdienst, Nameserver Internet Adressierung**

Der Anbieter des VPN-Zugangsdienstes MUSS jedem der drei Nameserver Internet genau eine öffentliche IP-Adresse zuweisen.

**⌫**

## Nameserver TI

### Funktion

Der Nameserver TI löst die FQDN im Namensraum der TI auf. Er optimiert die Performance der Namensauflösung durch Caching.

**⌦ TIP1-A\_4306 VPN-Zugangsdienst, Nameserver Namensraum TI**

Der VPN-Zugangsdienst MUSS mindestens zwei Nameserver TI (full service resolver) bereitstellen, die rekursive DNS-Anfragen der Konnektoren zur Auflösung von Namen im Namensraum TI beantworten, und Antworten entsprechend der TTL zwischenspeichern (Caching).

**⌫**

### Verteilung

**⌦ TIP1-A\_4307 VPN-Zugangsdienst, Bereitstellung Nameserver TI**

Der Anbieter des VPN-Zugangsdienstes MUSS die Nameserver TI in Kolokation mit jedem Standort des VPN-Zugangsdienstes aufstellen. Sie MÜSSEN sich netzwerktechnisch in der Service-Zone TI des Standortes befinden.

**⌫**

### Redundanz

Die hierfür geltenden Anforderungen zur Verfügbarkeit werden in [gemSpec\_Perf#4.2] defi­niert.

### Konfiguration

Der Nameserver TI erlaubt rekursive Anfragen. Er leitet die Anfragen an die autoritativen Nameserver der TI weiter.

**⌦ TIP1-A\_5104 VPN-Zugangsdienst, Resource Records im Nameserver TI**

Der Anbieter des VPN-Zugangsdienstes MUSS in den Nameservern TI die Resource Records gemäß Tabelle Tab\_ZD\_Nameserver\_TI\_RR verwalten. Dazu müssen je Standort dedizierte Subdomänen verwendet werden.

Tabelle 2: Tab\_ZD\_Nameserver\_TI\_RR

| **Resource Record Bezeichner** | **Beschreibung** |
| --- | --- |
| \_ntp.\_udp.<DOMAIN\_SRVZONE\_TI> | SRV Resource Record zur Ermittlung der FQDN und Ports der NTP-Server TI des VPN-Zugangsdienstes |
| NTP\_SERVER\_ADDR | A Resource Records zur Namensauflösung von FQDN der NTP-Server TI in IP-Adressen |
| \_ocsp.\_tcp.<DOMAIN\_SRVZONE\_TI> | SRV Resource Record zur Ermittlung des FQDN und Ports des http-Forwarders des VPN-Zugangsdienstes |
| CERT\_OCSP\_FORWARDER\_ADDRESS | A Resource Records zur Namensauflösung des FQDN des http-Forwarders in IP-Adressen |

**⌫**

### Adressierung

**⌦ TIP1-A\_4308 VPN-Zugangsdienst, Adressierung des Nameservers TI**

Der Anbieter des VPN-Zugangsdienstes MUSS jedem Nameserver TI eine IP-Adresse aus der Service-Zone TI des Standortes zuweisen.

**⌫**

## Nameserver SIS

### Funktion

Der Nameserver SIS löst die FQDN im Adressraum Internet auf. Er optimiert die Performance der Namensauflösung durch Caching.

**⌦ TIP1-A\_4309 VPN-Zugangsdienst, Nameserver im Namensraum SIS**

Der VPN-Zugangsdienst MUSS mindestens zwei Nameserver SIS (full service resolver) bereitstellen, die rekursive DNS-Anfragen der Konnektoren, zur Auflösung von Namen im Namensraum Internet, beantworten und Antworten entsprechend der TTL zwischenspeichern (Caching).

**⌫**

### Verteilung

**⌦ TIP1-A\_4310 VPN-Zugangsdienst, Bereitstellung Nameserver SIS**

Der Anbieter des VPN-Zugangsdienstes MUSS pro Standort mindestens einen Nameserver SIS bereitstellen. Die Nameserver SIS MÜSSEN sich netzwerktechnisch in der Servicezone SIS des Standortes befinden.

**⌫**

### Redundanz

Die hierfür geltenden Anforderungen zur Verfügbarkeit werden in [gemSpec\_Perf#4.2] defi­niert.

### Konfiguration

Der Nameserver SIS erlaubt rekursive Anfragen. Er löst diese Anfragen über das öffentliche DNS-System im Internet auf.

### Adressierung

**⌦ TIP1-A\_4311 VPN-Zugangsdienst, Adressierung Nameserver SIS**

Der Anbieter des VPN-Zugangsdienstes MUSS jedem Nameserver SIS eine öffentliche IP-Adresse zuweisen.

**⌫**

## Registrierungsserver

### Funktion

Der Registrierungsserver ist ein http-Server, welcher Anfragen des Konnektors zur Regis­trierung des Konnektors durch den LE beim Anbieter ent­gegennimmt und bearbeitet. Er kommuniziert mit der Kundendatenbank des Anbieters.

Der Registrierungsvorgang ist im Kapitel 5.3 dieses Dokuments funktional beschrieben.

### Verteilung

**⌦ TIP1-A\_4312 VPN-Zugangsdienst, Bereitstellung Registrierungsserver**

Der Anbieter des VPN-Zugangsdienstes MUSS an mindestens einem Standort einen Registrierungsserver in der Zugangszone TI mit einer Schnittstelle zum Internet bereitstellen und diesen in einer DMZ betreiben.

**⌫**

### Redundanz

Die hierfür geltenden Anforderungen zur Verfügbarkeit werden in [gemSpec\_Perf#4.2] defi­niert.

### Konfiguration

Der Registrierungsserver nimmt http-Anfragen aus dem Internet ent­gegen.

**⌦ TIP1-A\_5713 VPN-Zugangsdienst, Härtung des Registrierungsservers**

Der Anbieter des VPN-Zugangsdienstes MUSS den Registrierungsserver so konfi-gurieren, dass an der Schnittstelle zum Internet ausschließlich https-Anfragen akzeptiert werden.

**⌫**

### Adressierung

**⌦ TIP1-A\_4314 VPN-Zugangsdienst, Adressierung des Registrierungsservers**

Der Anbieter VPN-Zugangsdienst MUSS jedem Registrierungsserver mindestens eine öffentliche IP-Adresse zuweisen.

**⌫**

## Autorisierungsserver

Der Autorisierungsserver ist Teil des AAA-Systems (Authentication, Authorisation, Ac­counting).

### Funktion

Der Autorisierungsserver erhält Autorisierungsanfragen per RADIUS oder DIAMETER vom VPN-Konzentrator.

Beim Verbindungsaufbau generiert der VPN-Konzentrator eine AAA-Anfrage an den Au­torisierungsserver. Dazu verarbeitet er den Aussteller und die Seriennummer sowie weitere Felder des Zertifikats C.NK.VPN, zu einer eindeutigen Kundenidentifikation. Die Kundenidentifikation wird in der Autorisierungsanfrage verwendet. Anhand der ein­deutigen Kundenidentifikation wird der Vertragsstatus des Kunden durch den RADIUS- oder DIAMETER-Server aus einer Kundendatenbank (z.B. LDAP, SQL) des VPN-Zu­gangsdienstanbieters abgefragt.

In Abhängigkeit vom Status des Kunden bzw. Zertifikats in der Kundendatenbank wird der Verbindung ein entsprechendes Profil zugewiesen. Insbesondere wird dem Tunnel eine IP-basierte ACL zugewiesen, welche dem Konnektor im Netzwerk des VPN-Zu­gangs­dienstes einen Vollzugriff auf die TI oder einen Vollzugriff auf TI und SIS ermöglicht.

**⌦ TIP1-A\_4315 VPN-Zugangsdienst, Bildung von AAA-Zugangsdaten aus Zertifikaten**

Die VPN-Konzentratoren des VPN-Zugangsdienstes MÜSSEN die Bildung von AAA-Zugangsdaten (Credentials) aus Aussteller und Seriennummer des Kon­nektorzertifikats C.NK.VPN unterstützen.

**⌫**

**⌦ TIP1-A\_4316 VPN-Zugangsdienst, Autorisierung über Protokoll**

Die VPN-Konzentratoren des VPN-Zugangsdienstes MÜSSEN die Weiterleitung der AAA-Zugangsdaten über ein standardisiertes Authentisierungsprotokoll (RADIUS oder DIAMETER) an einen gesonderten Autorisierungsserver unter­stützen.

**⌫**

**⌦ TIP1-A\_4317 VPN-Zugangsdienst, Profilzuweisung durch Autorisierungs­server**

Der Autorisierungsserver des VPN-Zugangsdienstes MUSS die Rückgabe eines Profilwertes unterstützen, der vom VPN-Konzentrator zur Zuweisung einer Policy genutzt werden kann.

**⌫**

**⌦ TIP1-A\_4318 VPN-Zugangsdienst, ACL-Zuweisung**

Die VPN-Konzentratoren des VPN-Zugangsdienstes MÜSSEN die Zuweisung von spe­zifischen Benutzerprofilen entsprechend der zugewiesenen Policy an die Ver­bindungen zu den Konnektoren aufgrund der Autorisierung durch den Autori­sierungs­server unterstützen. Insbesondere MUSS die Zuweisung einer IP-basierten ACL zu jedem IPsec-Tunnel möglich sein. Die IP-basierte ACL MUSS die Filterung von Datenverkehr auf OSI Layer 3 und 4 durch eine Regel ermöglichen. Die Regel beinhaltet Einträge von Quell- und Zieladresse, Protokoll sowie Quell- und Zielport.

**⌫**

### Verteilung

**⌦ TIP1-A\_4319 VPN-Zugangsdienst, Verteilung des Autorisierungsservers**

Der Anbieter des VPN-Zugangsdienstes MUSS die Autorisierungsserver in Kolo­kation mit jedem Standort des VPN-Zugangsdienstes aufstellen. Sie MÜSSEN sich jeweils netzwerktechnisch in der Zugangszone TI bzw. Zugangszone SIS des Standortes befinden.

**⌫**

### Redundanz

Die hierfür geltenden Anforderungen zur Verfügbarkeit werden in [gemSpec\_Perf#4.2] defi­niert.

### Konfiguration

Der Autorisierungsserver nimmt Autorisierungsanfragen der VPN-Konzentratoren entge­gen.

### Adressierung

**⌦ TIP1-A\_4321 VPN-Zugangsdienst, IP-Adresse des Autorisierungsservers**

Der Anbieter des VPN-Zugangsdienstes MUSS dem Autorisierungsserver eine IP-Adresse aus dem Adressbereich der jeweiligen Zugangszone TI bzw. Zugangszone SIS des Standortes zuweisen.

**⌫**

## hash&URL-Server

Der hash&URL-Server ist ein http-Server, der die zur gegenseitigen Authentifizierung von Konnektoren und VPN-Konzentratoren genutzten Zertifikate gemäß [RFC7296] zum Download bereitstellt.

### Funktion

**⌦ TIP1-A\_5709 VPN-Zugangsdienst, bereitgestellte Zertifikate**

Der Anbieter des VPN-Zugangsdienstes MUSS die Zertifikate

* der VPN-Konzentratoren TI C.VPNK.VPN
* der VPN-Konzentratoren SIS C.VPNK.VPN-SIS
* der registrierten Konnektoren C.NK.VPN

im hash&URL-Server bereitstellen.

Der Anbieter des VPN-Zugangsdienstes muss sicherstellen, dass die bereitgestellten Zertifikate gültig sind. Ungültige Zertifikate müssen gelöscht werden.

**⌫**

### Verteilung

**⌦ TIP1-A\_5710 VPN-Zugangsdienst, Verteilung des hash&URL-Servers**

Der Anbieter des VPN-Zugangsdienstes MUSS an mindestens einem Standort einen hash&URL-Server in der Zugangszone TI mit einer Schnittstelle zum Internet bereitstellen und diesen in einer DMZ betreiben.

**⌫**

### Redundanz

Die hierfür geltenden Anforderungen zur Verfügbarkeit werden in [gemSpec\_Perf#4.2] defi­niert.

### Konfiguration

**⌦ TIP1-A\_5711 VPN-Zugangsdienst, Härtung des hash&URL-Servers**

Der Anbieter des VPN-Zugangsdienstes MUSS den hash&URL-Server so konfi­gu­rieren, dass an der Schnittstelle zum Internet ausschließlich http-Anfragen akzeptiert werden.

**⌫**

### Adressierung

**⌦ TIP1-A\_5712 VPN-Zugangsdienst, IP-Adresse des hash&URL-Servers**

Der Anbieter des VPN-Zugangsdienstes MUSS dem hash&URL-Server mindestens eine öffentliche IP-Adresse zuweisen.

**⌫**

## http-Forwarder

### Funktion

Der http-Forwarder dient zur Erschwerung einer Profilbildung unter Ausnutzung von Infor­mationen aus OCSP-Anfragen und der IP-Adresse des Konnektors. Hierfür fungiert diese Komponente in der Funktion eines http-Forwarding-Proxy, der an ihn gerichtete OCSP-Anfragen an die entsprechenden OCSP-Responder weiterleitet sowie die zurückge­lieferten OCSP-Antworten an den Absender sendet.

**⌦ TIP1-A\_4322 VPN-Zugangsdienst, http-Forwarder - Bereitstellung**

Der Anbieter des VPN-Zugangsdienstes MUSS einen http-Forwarder bereitstellen, der an ihn gerichtete http-Anfragen in der Funktion eines Forwarding-Proxy weiterleitet und die zurückgelieferten http-Antworten an den Absender sendet.

Alle Anfragen, deren Ziel nicht im Namensraum der TI liegt, MÜSSEN an den OCSP-Proxy der TI-Plattform mit einer neu gebildeten Ziel-URL weitergeleitet werden. Die Ziel-URL ist nach folgendem Schema zu bilden:

<URL des OCSP-Proxy>/<bisherige Ziel URL des OCSP Requests>

**⌫**

Die URL des OCSP-Proxy kann bei der gematik erfragt werden.

### Verteilung

**⌦ TIP1-A\_4323 VPN-Zugangsdienst, http-Forwarder - Verteilung**

Der Anbieter des VPN-Zugangsdienstes MUSS pro Standort mindestens einen http-Forwarder bereitstellen, der sich netzwerktechnisch in der Service-Zone TI befin­det.

**⌫**

### Redundanz

Die hierfür geltenden Anforderungen zur Verfügbarkeit werden in [gemSpec\_Perf#4.2] defi­niert.

### Konfiguration

**⌦ TIP1-A\_4325 VPN-Zugangsdienst, http-Forwarder - Absenderadresse**

Der Anbieter des VPN-Zugangsdienstes MUSS sicherstellen, dass die http-An­fragen mit der IP-Adresse des http-Forwarders als Absenderadresse weitergeleitet werden.

**⌫**

**⌦ TIP1-A\_4326 VPN-Zugangsdienst, http-Forwarder - kein Cache**

Der Anbieter des VPN-Zugangsdienstes MUSS sicherstellen, dass der über den http-Forwarder geleiteten Datenverkehr nicht in einem Cache zwischengespeichert wird.

**⌫**

**⌦ TIP1-A\_5117 Anonymisierung**

Der Anbieter des VPN-Zugangsdienstes MUSS sicherstellen, dass die über ihn weiter­geleitetem http-Anfragen anonymisiert sind; insbesondere DARF die IP-Adresse des ursprünglichen http-Klienten NICHT in der weitergeleiteten Anfrage enthalten sein.

**⌫**

### Adressierung

**⌦ TIP1-A\_4327 VPN-Zugangsdienst, http-Forwarder - IP-Adresse**

Der Anbieter des VPN-Zugangsdienstes MUSS jedem http-Forwarder eine IP-Adresse aus dem Adressbereich der Service-Zone des Standortes zuweisen.

**⌫**

## NTP-Server TI

### Funktion

Die Stratum-2-NTP-Server des VPN-Zugangsdienstes erhalten die Zeitinformation von den Stratum-1-NTP-Servern des Zeitdienstes und stellen die Zeitinformation den Kon­nek­toren bereit.

**⌦ TIP1-A\_4477 VPN-Zugangsdienst, Synchronisierung der Komponenten mit den Stratum-2-NTP-Servern**

Der VPN-Zugangsdienst MUSS folgende Komponenten mit seinen Stratum-2-NTP-Servern synchronisieren:

* + Registrierungsserver
  + Nameserver (TI)
  + VPN-Konzentrator (TI)
  + http-Forwarder
  + Autorisierungsserver

**⌫**

**⌦ TIP1-A\_4478 VPN-Zugangsdienst, Synchronisierung der Komponenten mit Ersatzverfahren**

Der VPN-Zugangsdienst MUSS folgende Komponenten mit einem Ersatzverfahren synchronisieren, das sicherstellt, dass die maximale Abweichung von der gesetzlichen Zeit nicht größer als eine Sekunde ist:

* + VPN-Konzentrator (SIS)
  + Sicherheitsgateway (SIS)
  + Autorisierungsserver (SIS)
  + Nameserver (SIS)
  + Packet Filter (SIS)
  + Packet Filter (TI)

Die Stratum-1- und 2-NTP-Server für die TI dürfen dazu nicht verwendet werden.

**⌫**

### Verteilung

**⌦ TIP1-A\_4328 VPN-Zugangsdienst, Anzahl der Stratum-2-NTP-Server**

Der Anbieter des VPN-Zugangsdienstes MUSS pro Standort mindestens zwei aktive Stratum-2-NTP-Server bereitstellen, die mit den Stratum-1-NTP-Servern des Zeitdienstes synchronisiert sind. Sie MÜSSEN sich netzwerktechnisch in der Service-Zone TI des Standortes befinden.

**⌫**

**⌦ TIP1-A\_4479 VPN-Zugangsdienst, maximale Zeitabweichung der Stratum-2-NTP-Server**

Der Anbieter des VPN-Zugangsdienstes MUSS gewährleisten, dass die Zeitab­weichung zwischen den Stratum-2-NTP-Servern eines Standortes nicht mehr als 330ms beträgt.

**⌫**

### Redundanz

Die hierfür geltenden Anforderungen zur Verfügbarkeit werden in [gemSpec\_Perf#4.2] defi­niert.

### Konfiguration

**⌦ TIP1-A\_4330 VPN-Zugangsdienst, Synchronisierung der Konnektoren**

Der Anbieter des VPN-Zugangsdienstes MUSS gewährleisten, dass sich die über die VPN-Konzentratoren TI verbundenen Konnektoren mit den Stratum-2-NTP-Servern des Standortes synchronisieren können.

**⌫**

Die NTP-Server nehmen NTP-Anfragen aller an der Diensterbringung beteiligten Kom­po­nen­ten des Standortes entgegen.

### Adressierung

**⌦ TIP1-A\_4331 VPN-Zugangsdienst, Adressierung der NTP-Server**

Der Anbieter des VPN-Zugangsdienstes MUSS jedem Stratum-2-NTP-Server eine IP-Adresse aus dem Adressbereich der Service-Zone TI des Standortes zu­weisen.

**⌫**

## Secure Internet Service

### Funktion

Der SIS bietet einen gesicherten Zugang zu Diensten im Inter­net und besteht aus den Komponenten VPN-Konzentrator SIS und einem oder mehreren Sicher­heitsgateways.

Der grundlegende Schutz der angebundenen Teilnehmer vor dem öffentlichen Internet wird über eine Application-Level-Gateway-Paketfilter-Struktur (P-A-P) entsprechend den Vor­ga­ben des BSI zur Konzeption von Sicherheitsgateways [BSI-SiGw] gewährleistet. Über dort angebundene dedizierte DMZ können weitere Sicherheitsleistungen bereit­ge­stellt werden.

### Verteilung

**⌦ TIP1-A\_4332 VPN-Zugangsdienst, Verteilung des SIS**

Der Anbieter des VPN-Zugangsdienstes MUSS den SIS in jedem Standort des VPN-Zugangsdienstes bereitstellen. Die Service-Zone SIS MUSS als DMZ ausgelegt werden.

**⌫**

### Redundanz

Die hierfür geltenden Anforderungen zur Verfügbarkeit werden in [gemSpec\_Perf#4.2] defi­niert.

### Konfiguration

**⌦ TIP1-A\_4480 VPN-Zugangsdienst,**

Der VPN-Zugangsdienst MUSS ermöglichen, dass die Sicherheitsleistungen des SIS anpassbar sind.

**⌫**

### Adressierung

**⌦ TIP1-A\_4334 VPN-Zugangsdienst, Adressierung des SIS**

Der Anbieter des VPN-Zugangsdienstes MUSS in der Service-Zone SIS öffentliche IP-Adressen verwenden.

**⌫**

**⌦ TIP1-A\_4335 VPN-Zugangsdienst, Bereitstellung der öffentlichen Adressen**

Der Anbieter des VPN-Zugangsdienstes MUSS die öffentlichen IP-Adressen für die Service-Zone SIS bereitstellen.

**⌫**

# 

# Übergreifende Festlegungen

## Sicherheit

### Kommunikation zwischen Service-Zonen und Zugangszonen

**⌦ TIP1-A\_4481 VPN-Zugangsdienst, Kommunikation zwischen Service-Zonen und Zugangszonen**

Der Anbieter des VPN-Zugangsdienstes MUSS sicherstellen, dass die Netzwerkkommunikation der Konnektoren über

• die Zugangszone TI und anschließend über die Service-Zone TI in die TI oder

• die Zugangszone SIS und anschließend über die Service-Zone SIS in das Internet

erfolgt.

**⌫**

**⌦ TIP1-A\_5046 VPN-Zugangsdienst, Sichere Speicherung des Vertrauensankers der PKI**

Die Komponenten VPN-Konzentrator und Registrierungsserver des VPN-Zugangs­dienstes MÜSSEN den Vertrauensanker der PKI in Form TSL-Signer-CA-Zertifikat in aktueller Version enthalten und sicher im Trust Store speichern.

**⌫**

**⌦ TIP1-A\_5047 VPN-Zugangsdienst, Gültigkeitsprüfung und Speicherung der TSL-Inhalte in lokalem Trust Store**

Die Komponenten VPN-Konzentrator und Registrierungsserver des VPN-Zugangs­dienstes MÜSSEN die Inhalte der TSL nach erfolgreicher Prüfung der TSL gemäß [gemSpec\_PKI#TUC\_PKI\_019] in einem Trust Store sicher speichern. Ist das Prüfungsergebnis "VALIDITY\_WARNING\_1" oder "VALIDITY\_WARNING\_2" dürfen keine Inhalte der TSL in den Trust Store übernommen werden und bestehende Einträge im Trust Store müssen gelöscht werden.

Die Komponenten VPN-Konzentrator und Registrierungsserver des VPN-Zugangs­dienstes MÜSSEN die Inhalte der TSL nach erfolgreicher Vertrauensraum- und syntaktischer Prüfung in einem Trust Store sicher speichern.

**⌫**

**⌦ TIP1-A\_5048 VPN-Zugangsdienst, Schlüssel sicher speichern**

Die Komponenten VPN-Konzentrator und Registrierungsserver des VPN-Zugangs­dienstes MÜSSEN Schlüssel sicher speichern und ihr Auslesen verhindern.

**⌫**

### Übergang der VPN-Konzentratoren zum Transportnetz Internet

**⌦ TIP1-A\_4337 VPN-Zugangsdienst, Physisch getrennte Schnittstellen**

Die VPN-Konzentratoren des VPN-Zugangsdienstes MÜSSEN für die Anbindung an das Transportnetz Internet und für die Anbindung an die TI und den SIS physisch getrennte Schnittstellen nutzen.

**⌫**

**⌦ TIP1-A\_4338 VPN-Zugangsdienst, Sicherung zum Transportnetz Internet durch Paketfilter**

Die VPN-Konzentratoren des VPN-Zugangsdienstes MÜSSEN zum Transportnetz Internet durch einen zustandslosen Paketfilter (ACL) gesichert werden, welcher ausschließlich die erforderlichen Protokolle weiterleitet. Der Paketfilter MUSS frei konfigurierbar sein auf der Grundlage von Informationen aus OSI Layer 3 und 4, das heißt Quell- und Zieladresse, IP-Protokoll sowie Quell- und Zielport.

**⌫**

**⌦ TIP1-A\_4339 VPN-Zugangsdienst, Platzierung Paketfilters Internet**

Der Paketfilter des VPN-Zugangsdienstes zum Schutz der VPN-Konzentratoren in Richtung Transportnetz Internet DARF NICHT auf den VPN-Konzentratoren implementiert werden.

**⌫**

**⌦ TIP1-A\_4340 VPN-Zugangsdienst, Richtlinien für den Paketfilter zum Internet**

Der Paketfilter des VPN-Zugangsdienstes MUSS die Weiterleitung von IP-Paketen auf die nachfolgenden Protokolle beschränken:

* ESP
* IKEv2: UDP Port 500
* IPsec NAT-T: UDP Port 4500
* ICMP Unreachable (Type 3)
* ICMP Echo Request (Type 8)/Echo Replay (Type 0)
* DNS (wenn ein Nameserver Internet hinter dem Paketfilter implementiert ist)
* http (wenn ein Hash\_and\_URL Server hinter dem Paketfilter implementiert ist)
* https (wenn ein Registrierungsserver hinter dem Paketfilter implementiert ist)

**⌫**

**⌦ TIP1-A\_4341 VPN-Zugangsdienst, Erkennung von Angriffen**

Der Anbieter des VPN-Zugangsdienstes MUSS durch technische Maßnahmen sicherstellen, dass Angriffe aus dem Internet auf den VPN-Zugangsdienst erkannt werden.

Als geeignete Maßnahmen werden angesehen:

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

**⌫**

### Übergang der VPN-Konzentratoren zur TI

Die Schnittstelle zur TI ist der Sichere Zentrale Zugangspunkt (SZZP). Der SZZP ist mit einem Sicherheitsgateway versehen. Die Sicherheitsfunktion bei der Anbindung der VPN-Konzentratoren an die TI wird daher durch den SZZP erbracht.

### Sicherheitsleistung des Secure Internet Service

**⌦ TIP1-A\_4344 VPN-Zugangsdienst SIS, Maßnahmen gegen Schadsoftware**

Der VPN-Zugangsdienst MUSS im SIS bei der Übertragung von Daten über unverschlüsselte Protokolle Maßnahmen zum Schutz vor Schadsoftware umsetzen.

**⌫**

**⌦ TIP1-A\_4345 VPN-Zugangsdienst SIS, Application Layer Gateway**

Der VPN-Zugangsdienst MUSS im SIS Application Level Gateways/An­wen­dungsproxies zur Kontrolle des Datenverkehrs für folgende Protokolle bereitstellen:

* + - * HTTP und HTTPS
      * FTP
      * SMTP und SMTPS
      * IMAP und IMAPS
      * POP3 und POP3S

Eine Erweiterung um zusätzliche Application Level Gateways/ Anwendungsproxies für Standardprotokolle MUSS möglich sein.

**⌫**

**⌦ TIP1-A\_4346 VPN-Zugangsdienst SIS, Paketfilter**

Der VPN-Zugangsdienst MUSS im SIS Paketfilter mit Stateful-Inspection-Funktion bereitstellen.

**⌫**

**⌦ TIP1-A\_4347 VPN-Zugangsdienst SIS, Filter für aktive Inhalte**

Der VPN-Zugangsdienst MUSS im SIS für unverschlüsselte Protokolle Contentfilter für aktive Inhalte bereitstellen.

**⌫**

**⌦ TIP1-A\_4348 VPN-Zugangsdienst SIS, URL-Filter**

Der VPN-Zugangsdienst MUSS im SIS URL-Filterfunktion bereitstellen.

**⌫**

**⌦ TIP1-A\_5155 VPN-Zugangsdienst SIS, Verhinderung Verbindungsaufbau aus dem Internet**

Der VPN-Zugangsdienst MUSS im SIS jeden Verbindungsaufbau aus Richtung Internet verhindern.

**⌫**

**⌦ TIP1-A\_5156 VPN-Zugangsdienst SIS, Erkennung von Angriffen aus dem Internet**

Der VPN-Zugangsdienst MUSS im SIS durch technische Maßnahmen sicherstellen, dass Angriffe aus dem Internet erkannt werden können.

Als geeignete Maßnahmen werden angesehen:

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

**⌫**

### Kommunikation zwischen Konnektoren

**⌦ TIP1-A\_4482 VPN-Zugangsdienst, Kommunikation zwischen Konnektoren**

Der Anbieter des VPN-Zugangsdienstes MUSS sicherstellen, dass eine direkte Netzwerkkommunikation zwischen Konnektoren über den VPN-Konzentratoren nicht möglich ist.

**⌫**

### Durchsetzung der Zugangsberechtigung

Nur zugelassene Geräte in berechtigten Institutionen des Gesundheitswesens dürfen auf die TI zugreifen. Die Prüfung der Berechtigung erfolgt über die Geräteidentität des Kon­nektors C.NK.VPN (SMC-K-Zertifikat) und die Rolle der Institutionen des Gesundheits­wesens C.HCI.OSIG (SM-B-OSIG-Zertifikat). Durch die Registrierung des Konnektors beim Anbieter des VPN-Zugangsdienstes erfolgt eine initiale Prüfung dieser Identitäten.

Bei jedem IPsec-Verbindungsaufbau erfolgt die gegenseitige Authentifizierung über die Geräteidentität des Konnektors und des VPN-Konzentrators. Darüber hinaus wird anhand einer zyklischen Zertifikatsprüfung von C.NK.VPN (SMC-K-Zertifikat) und C.HCI.OSIG (SM-B-OSIG-Zertifikat) geprüft, ob die Berechtigung für den Zugang zur TI noch besteht.

**⌦ TIP1-A\_5389 VPN-Zugangsdienst, zyklische Prüfung der C.NK.VPN und C.HCI.OSIG Zertifikate**

Der VPN-Zugangsdienst MUSS die Gültigkeit aller bei ihm im Rahmen von Kon­nektor­registrierungen verwendeten C.NK.VPN (SMC-K-Zertifikat) und C.HCI.OSIG (SM-B-OSIG-Zertifikat) gemäß TUC\_PKI\_002 und TUC\_PKI\_006 einmal täglich prüfen.

Die Prüfung der Zertifikate muss gleichmäßig verteilt über das Prüfintervall erfolgen.

**⌫**

**⌦ TIP1-A\_5390 VPN-Zugangsdienst, gesperrtes C.HCI.OSIG oder ge­sperrtes C.NK.VPN Zertifikat**

Wenn die zyklische Prüfung ergeben hat, dass das C.HCI.OSIG (SM-B-OSIG-Zertifikat) oder das C.NK.VPN (gSMC-K-Zertifikat) nicht mehr gültig ist, MUSS der VPN-Zugangsdienst die mit diesen Zertifikaten assoziierten IPsec-Verbindungen unverzüglich trennen und den zugehörigen Eintrag im Autorisierungsserver auf "on hold" setzen. Einträge im Autorisierungsserver, die auf "on hold" gesetzt sind, dürfen maximal 2 Tage (oder nach einer vom GBV vorgegebenen Frist) in diesem Zustand verbleiben. Wenn die Statusprüfung des C.HCI.OSIG oder das C.NK.VPN nach Ablauf der Frist immer noch den Status ungültig ergibt, muss der Eintrag im Autorisierungsserver entfernt werden.

Der Anbieter des VPN-Zugangsdienstes muss bei einem massenhaften Auftreten von Fehlern bei der zyklischen Prüfung den GBV informieren und den wahrscheinlichen Verursacher der Störung (z. B. TSL-Aussteller oder TSP X.509, Anbieter Zentrales Netz) zur Behebung auffordern.

Die sich aus der Prüfung ergebenden Änderungen an den Einträgen im Auto­risierungs­server müssen protokolliert werden und die protokollierten Daten dem betroffenen Anwender oder der gematik auf Anforderung zur Verfügung gestellt werden.

**⌫**

**⌦ TIP1-A\_5391 VPN-Zugangsdienst, Unterstützung von Än­derungen der Registrierung**

Der Anbieter des VPN-Zugangsdienstes MUSS geeignete organisatorische und/oder technische Maßnahmen vorsehen, die den Anwender bei Änderungen der Registrierung des Konnektors unterstützen.

Hierzu gehören insbesondere:

* Information des Anwenders über den bevorstehenden Ablauf der Gültigkeit von zur Registrierung genutzten Zertifikaten
* Rechtzeitige Bereitstellung der zur Neuregistrierung erforderlichen Informationen
* Aktualisierung existierender Einträge im Registrierungsserver durch die Verwendung eines gültigen SMC-B-Zertifikates.

**⌫**

## Protokollanforderungen

### IPsec

Die Verbindung zwischen dem Konnektor und dem VPN-Konzentrator des VPN-Zu­gangs­dienstes wird im Ipsec-Tunnel-Mode hergestellt. Es kommt das ESP-Protokoll gemäß [RFC4303] zum Einsatz.

**⌦ TIP1-A\_4349 VPN-Zugangsdienst und Konnektor, IPsec-Protokoll**

Konnektor und VPN-Konzentrator des VPN-Zugangsdienstes MÜSSEN die „Security Architecture for the Internet Protocol“ gemäß [RFC4301] unterstützen.

**⌫**

**⌦ TIP1-A\_4350 VPN-Zugangsdienst und Konnektor, ESP**

Konnektor und VPN-Konzentrator des VPN-Zugangsdienstes MÜSSEN das ESP-Protokoll (Encapsulating Security Payload) gemäß [RFC4303] unterstützen.

**⌫**

**⌦ TIP1-A\_4351 VPN-Zugangsdienst und Konnektor, Auswertung der Sequenz­nummern**

Der Konnektor und der VPN-Konzentrator des VPN-Zugangsdienstes MÜSSEN er­mög­lichen, dass die Auswertung der Sequenznummern zur Unterstützung der Fehlersuche empfängerseitig abschaltbar ist.

**⌫**

**⌦ TIP1-A\_4352 VPN-Zugangsdienst und Konnektor, Fenster für die Auswertung der Sequenznummern**

Der Konnektor und der VPN-Konzentrator des VPN-Zugangsdienstes MÜSSEN er­möglichen, dass das Fenster für die Auswertung der Sequenznummern im Rahmen des Anti Replay Service empfängerseitig konfigurierbar ist.

**⌫**

### IKEv2

**⌦ TIP1-A\_4353 VPN-Zugangsdienst und Konnektor, Internet Key Exchange Version 2**

Der Konnektor und der VPN-Konzentrator des VPN-Zugangsdienstes MÜSSEN den Aufbau von Security Associations (SA) zwischen ihnen, entsprechend dem Internet Key Exchange Protocol Version 2 (IKEv2) gemäß [RFC 7296] und [RFC7427], durchführen.

**⌫**

**⌦ TIP1-A\_4354 VPN-Zugangsdienst und Konnektor, NAT-Traversal**

Der Konnektor und der VPN-Konzentrator des VPN-Zugangsdienstes MÜSSEN in ihren IKEv2-Implementationen NAT-Traversal (NAT-T) gemäß [RFC 7296] unterstützen.

**⌫**

Durch “Dynamic Address Update” wird bewirkt, dass der VPN-Tunnel zwischen Kon­nek­tor und VPN-Konzentrator erhalten bleibt, wenn sich die Internetadresse des Internet-Routers (IAG) beim Leistungserbringer ändert. Dies wird unter anderem durch die soge­nannte Zwangstrennung von DSL Anschlüssen auftreten.

**⌦ TIP1-A\_4355 VPN-Zugangsdienst und Konnektor, Dynamic Address Update**

Der Konnektor und der VPN-Konzentrator des VPN-Zugangsdienstes MÜSSEN in ihren IKEv2-Implementationen “Dynamic Address Update”, wie in [RFC 7296#Abs.2.23] beschrieben, unterstützen.

**⌫**

### Verschlüsselung

Für Schlüsselaustausch, Verschlüsselung und Hashing im Zusammenhang mit IKEv2 und IPsec kommen die in [gemSpec\_Krypt] spezifizierten Algorithmen und Parameter zum Einsatz.

### Kompression

**⌦ TIP1-A\_4356 VPN-Zugangsdienst und Konnektor, IP Payload Compression Protocol**

Der Konnektor und der VPN-Konzentrator des VPN-Zugangsdienstes MÜSSEN in ihren IPsec-Implementationen das IP Payload Compression Protocol (IPComp) gemäß [RFC3173] unterstützen.

**⌫**

### Verbindungszustand

**⌦ TIP1-A\_4357 VPN-Zugangsdienst und Konnektor, Peer Liveness Detection**

Der Konnektor und der VPN-Konzentrator des VPN-Zugangsdienstes MÜSSEN in ihren IPsec-Implementationen den Liveness Check gemäß [RFC 7296] unterstützen.

**⌫**

**⌦ TIP1-A\_4358 Konnektor, Liveness Check Konnektor Zeitablauf**

Der Konnektor MUSS ermöglichen, dass die Dauer in Sekunden, bis seine IKEv2-Implementation die Verbindung als beendet betrachtet (Liveness Check), über die Management­schnittstelle konfigurierbar ist.

**⌫**

**⌦ TIP1-A\_4359 Konnektor, NAT-Keepalives**

Der Konnektor MUSS NAT-Keepalives unterstützen.

**⌫**

**⌦ TIP1-A\_4360 Konnektor, Konfiguration der NAT-Keepalives im Konnektor**

Der Zeitabstand in Sekunden zwischen zwei NAT-Keepalives MUSS im Konnektor über die Managementschnittstelle konfigurierbar sein. Die Keepalives MÜSSEN über die Managementschnittstelle abschaltbar sein.

**⌫**

### Fragmentierung von IKE-Paketen

Bei der Aushandlung der IKE-SA werden die Zertifikate zwischen Konnektor und VPN-Kon­zentrator über UDP übertragen. Aufgrund der genutzten Zertifikatsprofile und Schlüssellängen können die ISAKMP-Pakete größer als die MTU des Transportnetzes werden, so dass diese fragmentiert werden müssen. Hierbei kann es potentiell zu Proble­men mit auf der Übertragungsstrecke liegenden Netzwerkkomponenten kommen, die frag­mentierte UDP-Pakete nicht weiterleiten.

## Netzanforderungen

### Routing

#### VPN-Zugangsdienst

**⌦ TIP1-A\_4484 Routing VPN-Zugangsdienst TI**

Der VPN-Zugangsdienst MUSS IP-Pakete, die vom Konnektor über den IPsec-Tun­nel des VPN-Konzentrators TI zu fachanwendungsspezifischen Diensten, zen­tralen Diensten der TI-Plattform gesendet werden, zu den entsprechenden Diensten der TI weiterleiten.

Zur jeweiligen Kommunikationsbeziehung zugehörige IP-Pakete der Gegenrichtung müssen zum Konnektor weitergeleitet werden.

**⌫**

**⌦ TIP1-A\_4485 Routing VPN-Zugangsdienst Bestandsnetze**

Der VPN-Zugangsdienst MUSS IP-Pakete, die vom Konnektor über den IPsec-Tun­nel des VPN-Konzentrators TI zu Diensten in den Be­standsnetzen gesendet werden, zu den entsprechenden Bestandsnetzen mit Anschluss an die TI weiterleiten.

Zur jeweiligen Kommunikationsbeziehung zugehörige IP-Pakete der Gegenrichtung müssen zum Konnektor weitergeleitet werden.

**⌫**

**⌦ TIP1-A\_6748 Traffic Selectoren VPN-Zugangsdienst TI**

Der VPN-Zugangsdienst MUSS den VPN-Konzentratoren TI den Traffic Selector 0.0.0.0/0 für das lokale und das remote Subnet zuweisen.

**⌫**

**⌦ TIP1-A\_4486 Routing VPN-Zugangsdienst TI, lokale Dienste**

Der VPN-Zugangsdienst MUSS die lokalen TI-Dienste des VPN-Zugangsdienstes (Nameserver TI, NTP-Server, http-Forwarder) für Konnektoren über den IPsec-Tunnel des VPN-Konzentrators TI erreichbar machen.

**⌫**

**⌦ TIP1-A\_4487 Routing VPN-Zugangsdienst SIS**

Der VPN-Zugangsdienst MUSS IP-Pakete, die vom Konnektor über den IPsec-Tunnel des VPN-Konzentrators SIS in Richtung Internet gesendet werden, zum Sicherheitsgateway SIS weiterleiten. Die für die Nutzung des SIS benötigten lokalen Dienste des VPN-Zugangsdienstes (Nameserver SIS) MÜSSEN für die Konnektoren erreichbar sein.

Zur jeweiligen Kommunikationsbeziehung zugehörige IP-Pakete der Gegenrichtung müssen zum Konnektor weitergeleitet werden.

**⌫**

#### Konnektor

Im Konnektor sind folgende Routing-Informationen definiert:

* spezifische Route Richtung Dienste der TI über den IPsec-Tunnel TI
* spezifische Route Richtung Bestandsnetze über den IPsec-Tunnel TI
* spezifische Route Richtung VPN-Konzentratoren TI und SIS über das WAN-Interface zum Transportnetz Internet
* spezifische Route Richtung Nameserver Internet (Transport) über das WAN-Interface zum Transportnetz Internet
* spezifische Route Richtung CRL-Server über das WAN-Interface zum Transportnetz Internet
* Default-Route Richtung Internet über den IPsec-Tunnel zum SIS

### Behandlung gemäß DiffServ-Architektur

Der VPN-Zugangsdienst dient in erster Linie als Durchgang zwischen jeweils zwei exter­nen Netzen (Internet und TI bzw. Internet und Internet über SIS).

Es wird erwartet, dass Da­ten­ver­kehr, der innerhalb eines Standortes des VPN-Zugangsdienstes transportiert wird, niemals einen Eng­pass erfährt, da die Bandbreiten, mit denen die durchlaufenen Geräte untereinander ver­bun­den wer­den, höher sind, als die Bandbreiten, mit denen der VPN-Zugangsdienst an exter­ne Netze an­ge­schlossen ist. Dieser Zustand entspricht einer Überbuchung. Eine DiffServ-gemäße Be­handlung ist innerhalb des VPN-Zugangsdienstes daher verzichtbar.

**⌦ TIP1-A\_4488 Bandbreiten innerhalb des VPN-Zugangsdienstes**

Der Anbieter des VPN-Zugangsdienstes MUSS sicherstellen, dass in seinem Netzwerk keine Bandbreitenengpässe entstehen können.

**⌫**

#### VPN-Konzentratoren zum Transportnetz Internet

An der Schnittstelle zwischen VPN-Zugangsdienst und Transportnetz wird eine DiffServ-Behand­lung vorgenommen, wobei die DSCP-Markierungen der getunnelten Pakete beachtet wer­den. Dies geschieht in beiden Richtungen. Soweit der Internetzugang durch einen exter­nen Backbone-Anbieter bereitgestellt wird, muss dieser die geforderte Policy seiner­seits auf dem Provider Edge (PE) Router und gegebenenfalls dem Customer Edge (CE) Router implementieren.

**⌦ TIP1-A\_4364 VPN-Zugangsdienst, DiffServ-Behandlung zwischen VPN-Kon­zen­trator und Transportnetz Internet**

Der Anbieter des VPN-Zugangsdienstes MUSS an der Schnittstelle des VPN-Zugangs­dienstes zum Transportnetz Internet in beiden Richtungen die DiffServ-gemäße Behandlung von Datenverkehr unterstützen.

Die Erkennung und/oder Verarbeitung der DiffServ-Flags darf die Werte nicht verändern.

**⌫**

#### VPN-Konzentratoren zu Konnektoren

Es ist wünschenswert, den Datenverkehr über den Tunnel zwischen VPN-Konzentrator und Konnektor gemäß DiffServ-Architektur zu behandeln. Dies ist trotz der Tatsache, dass das unterliegende Transportnetz zumeist keine DiffServ-Markierungen auswertet, im Prin­zip möglich, indem für jeden Tunnel von VPN-Konzentrator zum Konnektor ein Traffic-Shaping konfiguriert wird, welches auf eine Bandbreite knapp unterhalb der ver­füg­baren Downstream-Bandbreite des Internetanschlusses beim LE eingestellt wird. Auf der entstehenden Warteschlange wird dann die DiffServ-Behandlung durchgeführt.

Diese Prinziplösung ist jedoch aus folgenden Gründen schwer umsetzbar:

* Es werden zwei voneinander unabhängige Tunnel über den Internetanschluss des LE geführt, die miteinander nicht kom­mu­ni­zieren, und auf unterschiedlichen VPN-Konzentratoren terminiert.
* Es wäre eine Pflege der Bandbreiteneinstellungen pro LE durch den VPN-Zu­gangs­dienst erforderlich.

Es werden daher keine Anforderungen in diesem Bereich gestellt.

#### VPN-Zugangsdienst zur TI

**⌦ TIP1-A\_4367 VPN-Zugangsdienst, DiffServ-Behandlung zwischen VPN-Zu­gangs­dienst und Zentralem Netz**

Der Anbieter des VPN-Zugangsdienstes MUSS an der Schnittstelle zum Zentralen Netz die DiffServ-gemäße Behandlung von Datenverkehr unterstützen.

Die Erkennung und/oder Verarbeitung der DiffServ-Flags darf die Werte nicht verändern.

**⌫**

#### Alternatives Zugangsnetz

**⌦ TIP1-A\_4489 DiffServ-Behandlung im alternativen Zugangsnetz**

Sofern der Anbieter des VPN-Zugangsdienstes einen alternativen Zugang anbietet, der nicht das Internet als Transportnetz nutzt, MUSS er auf diesem Transportnetz durchgehend die DiffServ-gemäße Behandlung von Datenverkehr unterstützen.

Die Erkennung und/oder Verarbeitung der DiffServ-Flags darf die Werte nicht verändern.

**⌫**

#### SIS zum Internet

**⌦ TIP1-A\_4490 DiffServ-Markierung durch SIS**

Der Secure Internet Service (SIS) des VPN-Zugangsdienstes MUSS an der Schnittstelle Sicherheitsgateway zum Internet die DiffServ-gemäße Markierung von Datenverkehr unterstützen.

**⌫**

**⌦ TIP1-A\_4368 VPN-Zugangsdienst, DiffServ-Behandlung SIS zum Internet**

Der Secure Internet Service (SIS) des VPN-Zugangsdienstes MUSS an der Schnittstelle Sicherheitsgateway zum Internet die DiffServ-gemäße Behandlung von Datenverkehr unterstützen.

Das ALG muss ermöglichen, dass die Regeln zur Kontrolle des Datenverkehrs um eine DSCP-Markierung der ausgehenden IP-Pakete erweitert werden können.

**⌫**

# Funktionsmerkmale

**⌦ TIP1-A\_4369 VPN-Zugangsdienst, Festlegung der Schnittstellen**

Der Produkttyp VPN-Zugangsdienst MUSS die Schnittstellen gemäß Tabelle Tab\_PT\_VPN-Zugangsdienst\_Schnittstellen implementieren („bereitgestellte“ Schnitt­stellen) und nutzen („benötigte“ Schnittstellen).

Tabelle 3: Tab\_PT\_VPN-Zugangsdienst\_Schnittstellen

| Schnittstelle | bereitgestellt/benötigt | obligatorisch/optional | Bemerkung |
| --- | --- | --- | --- |
| I\_Secure\_Channel\_Tunnel | bereitgestellt | obligatorisch |  |
| I\_Secure\_Internet\_Tunnel | bereitgestellt | obligatorisch |  |
| I\_DNS\_Name\_Resolution (Namensraum TI) | bereitgestellt | obligatorisch |  |
| I\_DNS\_Name\_Resolution (Namensraum Internet) | bereitgestellt | obligatorisch | zur Auflösung von FQDN der VPN-Konzentratoren und des Download-Punktes der CRL |
| I\_DNS\_Name\_Resolution (Namensraum Internet) | bereitgestellt | obligatorisch | zur Auflösung von FQDN von Diensten im Internet (über den SIS) |
| I\_NTP\_Time\_Information | bereitgestellt | obligatorisch |  |
| I\_Registration\_Service | bereitgestellt | obligatorisch |  |
| P\_DNSSEC\_Key\_Distribution | bereitgestellt | obligatorisch |  |
| I\_NTP\_Time\_Information | benötigt | obligatorisch | Definition in [gemSpec\_Net] |
| I\_IP\_Transport | benötigt | obligatorisch | Definition in [gemSpec\_Net] |
| I\_Monitoring\_Update | benötigt | obligatorisch | Definition durch den Anbieter der Störungsampel |
| I\_Monitoring\_Read | benötigt | obligatorisch | Definition durch den Anbieter der Störungsampel |
| I\_OCSP\_Status\_Information | benötigt | obligatorisch | Definition in [gemSpec\_PKI] |

**⌫**

Für den Aufbau und die Nutzung der VPN-Anbindung zwischen Konnektor und VPN-Konzentrator sowie für die Nutzung weiterer Dienste müssen dem Konnektor Kon­figurations­daten zur Verfügung gestellt werden.

Diese werden über die folgenden Methoden in den Konnektor eingebracht:

* Manuelle Eingabe durch den Administrator (Nameserver im Internet des VPN-Zugangsdienstes)
* Dynamische Servicelokalisierung über DNS mittels DNS-SRV und DNS-TXT Ressource Records
* Automatisierter Download von Firmware-Updates und Bestandsnetz-Konfigurationsdaten vom KSR über definierte Downloadpunkte

Damit der Konnektor sich mit den VPN-Konzentratoren TI und SIS verbinden kann müssen im Konnektor die Nameserver Internet und die Domain, die die SRV-Records der VPN-Konzentratoren enthält, bekannt sein.

## Schnittstelle I\_Secure\_Channel\_Tunnel

**⌦ TIP1-A\_4370 VPN-Zugangsdienst, Schnittstelle I\_Secure\_Channel\_Tunnel**

Der VPN-Zugangsdienst MUSS für Konnektoren die Schnittstelle I\_Se­cure\_Chan­nel\_Tunnel gemäß Tabelle Tab\_ZD\_Schnitt­stelle\_I\_Secure\_Chan­nel\_Tun­nel an­bieten.

Tabelle 4: Tab\_ZD\_Schnittstelle\_I\_Secure\_Channel\_Tunnel

|  |  |  |
| --- | --- | --- |
| Name | I\_Secure\_Channel\_Tunnel | |
| Version | wird im Produktsteckbrief des VPN-Zugangsdienstes definiert | |
| Operationen | Name | Kurzbeschreibung |
| connect | Herstellung einer IPsec-gesicherten Verbindung |
| disconnect | Abbau der Verbindung |
| send\_secure\_IP\_Packet | Senden und Empfangen von Daten in die TI über den IPsec-Tunnel |

**⌫**

### Operation connect

#### Umsetzung



Abbildung 4: Ablauf der Operation I\_Secure\_Channel\_Tunnel::connect im VPN-Zugangsdienst

**⌦ TIP1-A\_4371 VPN-Zugangsdienst, Identität zur Authentisierung des VPN-Konzentrators TI beim Konnektor**

Der VPN-Konzentrator MUSS zur Identifizierung beim Konnektor für den Zugang zur TI die Identität ID.VPNK.VPN benutzen.

**⌫**

**⌦ TIP1-A\_4372 VPN-Zugangsdienst, Ablauf des IPsec-Verbindungsaufbaus zur TI**

Der VPN-Zugangsdienst MUSS beim vom Konnektor initiierten Verbindungsaufbau in die TI gemäß [RFC 7296] vorgehen und dabei folgende Ablaufschritte implementieren.

* Der VPN-Konzentrator TI empfängt vom Konnektor das Zertifikat C.NK.VPN. Wird vom Konnektor das hash&URL-Verfahren für die Übermittlung der Referenz seines Zertifikates C.NK.VPN genutzt, muss dieses Zertifikat vom hash&URL-Server des VPN-Zugangsdienstes per HTTP-Download bezogen werden.
* Das Zertifikat C.NK.VPN wird gemäß [gemSpec\_PKI#TUC\_PKI\_018] mit Prüfmodus OCSP geprüft.
  + Wenn das Zertifikat C.NK.VPN nicht gültig ist, wird der Verbindungs­aufbau mit einer Fehlermeldung gemäß [RFC 7296] abgebrochen.
* Der VPN-Konzentrator authentisiert sich beim Konnektor mit seinem Zertifikat C.VPNK.VPN.
* Der VPN-Konzentrator erzeugt aus Aussteller und Seriennummer des Zertifikats einen Benutzernamen und sendet ihn an den Autorisierungsserver.
* Über den Autorisierungsserver wird geprüft, ob bereits ein Benutzerkonto für den Benutzernamen besteht. Der VPN-Konzentrator TI muss dem Konnektor auf der Grundlage seines Registrierungsstatus eine IP-basierte Zugangskontrollliste (ACL) zuweisen.
  + Wenn kein Benutzerkonto besteht MUSS der VPN-Verbindungsaufbau abgebrochen werden.
  + Wenn ein Benutzerkonto besteht, wird der Zugang zum Zentralen Netz der TI freigeschaltet.
* Der VPN-Konzentrator weist dem Konnektor eine Adresse aus dem Adressraum TI\_Dezentral zu. Die Adresse wird als innere Adresse des IPsec-Tunnels verwendet.

**⌫**

#### Nutzung

**⌦ TIP1-A\_4373 Konnektor, TUC\_VPN-ZD\_0001 “IPsec-Tunnel TI aufbauen”**

Der Konnektor MUSS den technischen Use Case TUC\_VPN-ZD\_0001 “IPsec-Tunnel TI aufbauen” gemäß Tabelle Tab\_ZD\_TUC\_IPsec\_Tunnel\_TI\_aufbauen umsetzen.

Tabelle 5: Tab\_ZD\_TUC\_IPsec\_Tunnel\_TI\_aufbauen

|  |  |  |
| --- | --- | --- |
| Name | TUC\_VPN-ZD\_0001 “IPsec-Tunnel TI aufbauen” | |
| Beschreibung | Dieser TUC stellt eine IPsec-gesicherte Verbindung zwischen dem Kon­nek­tor und einem VPN-Konzentrator TI des VPN-Zugangsdienstes her. | |
| Vorbedingungen | * Eine gültige TSL ist im Konnektor geladen. * Eine gültige CRL ist im Konnektor geladen. * Es besteht eine IP-Netzwerkverbindung vom Konnektor zum Internet * Der gültige Internet DNS Root Trust Anchor der IANA ist in der DNS-Forwarder Konfiguration des Konnektors enthalten. * Der DNS-Resolver des Konnektors kann auf die vom Anbieter des VPN-Zugangsdienstes bereitgestellten Nameserver im Internet (Bezeichner DNS\_SERVERS\_INT) zugreifen. | |
| Eingangsdaten | * CRL (die im Konnektor verfügbare CRL) * TUNNEL\_MTU (optional, Maximum Transfer Unit für den IPsec Tunnel) * TOP\_LEVEL\_DOMAIN\_TI (Top-Level-Domain der TI) * DNS\_DOMAIN\_VPN\_ZUGD\_INT (DNS-Domainname für die Service Discovery der VPN-Konzentratoren) * DNS\_SERVERS\_INT (DNS Server im Internet) * HASH\_AND\_URL | |
| Komponenten | Konnektor, VPN-Zugangsdienst | |
| Ausgangsdaten | * VPN\_TUNNEL\_TI\_INNER\_IP (innere IP-Adresse des IPsec-Tunnels TI) * DNS\_SERVERS\_TI (Nameserver TI des VPN-Zugangsdienstes) * DOMAIN \_SRVZONE\_TI * VPN\_KONZENTRATOR\_TI\_IP\_ADDRESS (IP-Adresse des VPN-Konzentrators TI im Transportnetz zu dem der IPsec-Tunnel VPN aufgebaut wird) | |
| Standardablauf | Aktion | Beschreibung |
|  | FQDN und IP-Adressen der VPN-Konzen­tratoren TI ermitteln | Durch eine DNS-Anfrage zur Auflösung eines SRV-RR mit dem Bezeichner "\_isakmp.\_udp.ti-extern.<DNS\_DOMAIN\_VPN\_ZUGD\_INT>“ erhält der Konnektor eine Liste von priorisierten und gewichteten FQDN der VPN-Konzentratoren TI.  Alle FQDN mit der höchsten Priorität (kleinere Zahlen entsprechen einer höheren Priorität) werden ihrem Gewicht entsprechend nach einem Zufallsverfahren neu sortiert. Dahinter folgen die ebenfalls zufällig sortierten FQDN der nächst niedrigeren Priorität. Dieser Vorgang wird wiederholt, bis alle FQDN in der neuen Liste enthalten sind. Der erste FQDN aus der Liste wird daraufhin in eine IP-Adresse aufgelöst (TUC-interner Bezeichner VPN\_KONZENTRATOR\_TI\_FQDN). Es wird eine Firewall-Regel erzeugt, die einen IPsec-Verbindungsaufbau zu dieser IP-Adresse ermöglicht. Sollte sich im Folgenden herausstellen, dass es nicht möglich ist mit diesem VPN-Konzentrator eine Verbindung aufzubauen, wird der nächste FQDN aus der Liste verwendet. Dieses Verfahren wird wiederholt, bis der Verbindungsaufbau erfolgreich war oder alle Adressen erfolglos probiert wurden. |
|  | Nameserver TI und Domainnamen der Service-Zone des VPN-Zugangs­dienstes ermitteln | Durch eine DNS-Anfrage zur Auflösung eines TXT-RR mit dem Bezeichner VPN\_KONZENTRATOR\_TI\_FQDN an den DNS-Forwarder erhält der Konnektor die IP-Adressen der Nameserver TI (DNS\_SERVERS\_TI) sowie die Domainnamen der Service Zone TI (DOMAIN\_SRVZONE\_TI) des VPN-Zugangsdienstes.  Die key/value Paare der TXT-Records haben folgende Struktur (die spitzen Klammern dienen der Abgrenzung eines Wertes):  "txtvers=1"  "NameserverTI=<IP-Adresse1>,<IP-Adresse2>[,<weitere IP-Adressen>]"  "DomainSrvTI=<Domainname der Servicezone TI des VPN-Zugangsdienstes>"  Beispiel für einen Zonendateieintrag:  vpnk1.ham.ti-vpn-zugd.anbieter.de. 3600 IN TXT "txtvers=1"  "NameserverTI=100.97.20.13,100.97.20.14"  "DomainSrvTI=ti-sz.ham.anbieter.vpn-zugd.telematik" |
|  | DNS-Forwarder für Namensraum TI konfigurieren | Die IP-Adressen aus DNS\_SERVERS\_TI werden in der Nameserver Konfiguration des DNS-Forwarders als Zieladressen für den Forward-Eintrag des Namensraumes TI eingetragen |
|  | Verbindung aufbauen | * Der Verbindungsaufbau erfolgt gemäß oder [RFC7296] mit der ersten IP-Adresse aus der erzeugten IP-Adressliste der VPN-Konzentratoren. * Es muss das Encapsulating Security Payload Protocol (ESP) mit Verschlüsselung (siehe [RFC4303#3.2.1]) und Integritätsschutz (siehe [RFC4303#3.2.2]) verwendet werden. Die zu nutzenden kryptographischen Algorithmen sind in [gemSpec\_Krypt#3.3.1] beschrieben. Der Aufbau der Security Association (SA) erfolgt nach dem Internet Key Exchange Protocol Version 2 gemäß [RFC 7296] oder [RFC7427.] * Der Konnektor empfängt vom VPN-Konzentrator das Zertifikat C.VPNK.VPN. Falls HASH\_AND\_URL = Enabled muss das Hash & URL Verfahren gemäß [RFC7296] zum Austausch der Zertifikate zwischen Konnektor und VPN-Konzentrator verwendet werden. * Das Zertifikat C.VPNK.VPN wird gemäß [gemSpec\_PKI#TUC\_PKI\_018] mit Prüfmodus CRL geprüft. Wenn das Zertifikat C.VPNK.VPN nicht gültig oder das Zertifikat gesperrt ist, wird der Verbindungsaufbau mit einer Fehlermeldung gemäß [RFC7296] abgebrochen und es wird die nächste IP-Adresse aus der Liste der VPN-Konzentratoren angesprochen. * Der Konnektor authentisiert sich beim VPN-Konzentrator mit seinem Zertifikat C.NK.VPN * Die Autorisierungsprüfung erfolgt durch den VPN-Zugangsdienst. Bei einem negativen Prüfergebnis wird an den Konnektor die Fehlermeldung "AUTHENTICATION\_FAILED" gemäß [ [RFC7296] gesendet. Der IPsec-Tunnelaufbau ist damit beendet. * Bei erfolgreicher gegenseitiger Authentifizierung und Autorisierung durch den VPN-Zugangsdienst wird die Verbindung gemäß [RFC7296] weiter aufgebaut. Das IKE-Protokoll weist dem Konzentrator die innere IP-Adresse des IPsec-Tunnels aus dem Adressraum TI\_Dezentral zu. Bei jedem Verbindungsaufbau wird eine andere IP-Adresse verwendet. * Die MTU wird automatisch mittels Path MT+R765U Discovery ermittelt und entsprechend eingestellt. Wenn der optionale Parameter TUNNEL\_MTU angegeben ist, wird die MTU auf maximal diesen Wert eingestellt. |
| Varianten/Alterna­tiven | Keine |  |
| Zustand nach erfolgreichem Ablauf | Der Konnektor ist mit dem VPN-Konzentrator TI verbunden. | |
| Fehlerfälle | Zur Behandlung auftretender Fehlerfälle werden Fehlermeldungen gemäß [RFC 7296] verwendet. | |

**⌫**

#### Verbindungsaufbau

Der Konnektor besteht aus einem Netzwerkanteil und einem Anwendungsanteil. Die VPN-Verbindung zur TI und zum SIS wird durch den Netzwerkanteil aufgebaut.

**⌦ TIP1-A\_4374 VPN-Zugangsdienst, Verbindungsaufbau**

Der Konnektor MUSS die IKEv2-Verbindung aufbauen, d.h. der Konnektor ist der Initiator.

**⌫**

**⌦ TIP1-A\_4375 VPN-Zugangsdienst, Verhalten bei Verbindungsabbau**

Der Konnektor MUSS, sobald ein Verbindungsabbau erkannt wird, den IPsec-Tunnel mittels IKEv2 unverzüglich neu herstellen.

**⌫**

**⌦ TIP1-A\_4376 VPN-Zugangsdienst, Auswahl des VPN-Konzentrators aufgrund von SRV-Records**

Der Konnektor MUSS im Rahmen des Verbindungsaufbaus zur TI oder zum SIS die SRV-Records des VPN-Zugangsdienstes heranziehen. Bei der Auswahl des zu kontaktierenden VPN-Konzentrators MUSS er sowohl die Priorität als auch die Gewichtung der SRV-Records gemäß [RFC2782#S.3ff.] berücksichtigen. Die DNS TTL MUSS beachtet werden.

**⌫**

**⌦ TIP1-A\_4377 VPN-Zugangsdienst, Namensauflösung**

Der Konnektor MUSS die Address-Records des VPN-Zugangsdienstes bei jedem Verbindungsaufbau durch eine DNS-Anfrage auflösen. Die DNS TTL MUSS beachtet werden.

**⌫**

#### Adressierung

Es muss sichergestellt sein, dass keine Profilbildung in der TI durch Identifikation anhand der IP-Adresse des LE stattfinden kann.

**⌦ TIP1-A\_4492 VPN-Zugangsdienst, Zuweisung der Adressen, Verhinderung der Profilbildung**

Der Anbieter des VPN-Zugangsdienstes DARF die IP-Adressen aus dem Adress­raum TI\_Dezentral NICHT bestimmten Kunden fest zuweisen. Beim Neuaufbau eines Tunnels MUSS dem Konnektor jeweils eine beliebige Adresse aus dem Adress-Pool des VPN-Konzentrators zugewiesen werden.

**⌫**

**⌦ TIP1-A\_4387 VPN-Zugangsdienst, Adressblöcke für VPN-Konzentratoren**

Der Anbieter des VPN-Zugangsdienstes MUSS für den Betrieb des Dienstes einen Adressblock in der erforderlichen Größe vom Anbieter des Zentralen Netzes der TI anfordern.

**⌫**

### Operation disconnect

**⌦ TIP1-A\_4389 VPN-Zugangsdienst, I\_Secure\_Channel\_Tunnel::disconnect**

Der VPN-Zugangsdienst MUSS für Konnektoren an der Schnittstelle I\_Secure\_Channel\_Tunnel die Operation disconnect zum kontrollierten Trennen der IPsec-Verbindung gemäß [RFC 7296#1.4.1. Deleting an SA with INFORMATIONAL Exchanges] anbieten.

**⌫**

### Operation send\_secure\_IP\_Packet

Nachdem vom Konnektor der IPsec-gesicherte Tunnel zum VPN-Konzentrator TI erfolg­reich aufgebaut wurde, kann der Konnektor über diesen Tunnel IP-Pakete an fachanwen­dungsspezifische Dienste und zentrale Dienste der TI-Plattform senden und zur jeweili­gen Kommunikationsbeziehung zugehörige IP-Pakete empfangen. Zusätzlich können Clientsysteme über den Konnektor und diesen Tunnel IP-Pakete zu Diensten in den Bestandsnetzen senden und zur jeweiligen Kommunikationsbeziehung zugehörige IP-Pakete empfangen.

Die Funktion wird hier nicht weiter beschrieben, da sie implizit durch die geforderten Kom­ponenten des VPN-Zugangsdienstes und deren Kommunikationsbeziehungen mit anderen Produkttypen der TI implementiert ist.

## Schnittstelle I\_Secure\_Internet\_Tunnel

**⌦ TIP1-A\_4394 VPN-Zugangsdienst, Schnittstelle I\_Secure\_Internet\_Tunnel**

Der VPN-Zugangsdienst MUSS für Konnektoren die Schnittstelle I\_Secure\_Inter­net\_Tun­nel gemäß Tabelle Tab\_ZD\_Schnitt­stelle\_I\_Secure\_Internet\_Tunnel an­bieten.

Tabelle 6: Tab\_ZD\_Schnittstelle\_I\_Secure\_Internet\_Tunnel

|  |  |  |
| --- | --- | --- |
| Name | I\_Secure\_Internet\_Tunnel | |
| Version | wird im Produktsteckbrief des VPN-Zugangsdienstes definiert | |
| Operationen | Name | Kurzbeschreibung |
| connect | Herstellung einer IPsec-gesicherten Verbindung |
| disconnect | Abbau der Verbindung |
| send\_secure\_IP\_Packet | Senden und Empfangen von Daten in das Internet über den IPsec-Tunnel |

**⌫**

### Operation connect

#### Umsetzung

Die Operation I\_Secure\_Internet\_Tunnel::connect verläuft analog zur Operation I\_Secure\_Channel\_Tunnel::connect mit dem Unterschied, dass die Verbindung zum VPN-Konzentrator SIS aufgebaut wird (siehe 5.1.1.1).

**⌦ TIP1-A\_4395 VPN-Zugangsdienst, Identität zur Authentisierung des VPN-Konzentrators SIS beim Konnektor**

Der VPN-Konzentrator MUSS zur Identifizierung beim Konnektor für den Zugang die Identität ID.VPNK.VPN-SIS benutzen.

**⌫**

**⌦ TIP1-A\_4396 VPN-Zugangsdienst, Ablauf des IPsec-Verbindungsaufbaus Richtung Internet**

Der VPN-Zugangsdienst MUSS beim vom Konnektor initiierten Verbindungsaufbau Richtung SIS gemäß [RFC7296] vorgehen und dabei folgende Ablaufschritte implementieren.

* Der VPN-Konzentrator SIS empfängt vom Konnektor das Zertifikat C.NK.VPN. Wird vom Konnektor das hash&URL-Verfahren für die Übermittlung der Referenz seines Zertifikates C.NK.VPN genutzt, muss dieses Zertifikat vom hash&URL-Server des VPN-Zugangsdienstes per HTTP-Download bezogen werden.
* Das Zertifikat C.NK.VPN wird gemäß gemSpec\_PKI#TUC\_PKI\_018 mit Offline-Modus = ja geprüft.
  + Wenn das Zertifikat C.NK.VPN nicht gültig ist, wird der Verbindungs­aufbau mit einer Fehlermeldung gemäß [RFC 7296] abgebrochen.
* Der VPN-Konzentrator authentisiert sich beim Konnektor mit seinem Zertifikat C.VPNK.VPN-SIS.
* Der VPN-Konzentrator erzeugt aus Aussteller und Seriennummer des Zertifikats einen Benutzernamen und sendet ihn an den Autorisierungsserver.
* Über den Autorisierungsserver wird geprüft, ob bereits ein Benutzerkonto für den Benutzernamen besteht. Der VPN-Konzentrator SIS muss dem Konnektor auf der Grundlage seines Registrierungsstatus eine IP-basierte Zugangskontrollliste (ACL) zuweisen.
  + Wenn kein Benutzerkonto besteht, wird der Verbindungsaufbau mit einer Fehlermeldung gemäß [RFC 7296] abgebrochen.
  + Wenn ein Benutzerkonto besteht, wird der Zugang im Internet über den SIS freigeschaltet.
* Der VPN-Konzentrator weist dem Konnektor eine Adresse aus dem Adressraum TI\_Dezentral zu. Die Adresse wird als innere Adresse des IPsec-Tunnels verwendet.

**⌫**

#### Nutzung

**⌦ TIP1-A\_4397 Konnektor, TUC\_VPN-ZD\_0002 “IPsec Tunnel SIS aufbauen”**

Der Konnektor MUSS den technischen Use Case TUC\_VPN-ZD\_0002 “IPsec-Tunnel SIS aufbauen” gemäß Tabelle Tab\_ZD\_TUC\_IPsec\_Tunnel\_SIS\_aufbauen umsetzen.

Tabelle 7: Tab\_ZD\_TUC\_IPsec\_Tunnel\_SIS\_aufbauen

|  |  |  |
| --- | --- | --- |
| Name | TUC\_VPN-ZD\_0002 “IPsec-Tunnel SIS aufbauen” | |
| Beschreibung | Dieser TUC stellt eine IPsec-gesicherte Verbindung zwischen dem Konnek­tor und dem VPN-Konzentrator SIS des VPN-Zugangsdienstes her. | |
| Vorbedingungen | * Eine gültige TSL ist im Konnektor geladen. * Eine gültige CRL ist im Konnektor geladen. * Es besteht eine IP-Netzwerkverbindung vom Konnektor zum Internet * Der gültige Internet DNS Root Trust Anchor der IANA ist in der DNS-Forwarder Konfiguration des Konnektors enthalten. * Der Konnektor ist beim Anbieter des VPN-Zugangsdienstes registriert und zur Verbindung mit dem Sicheren Internet Service berechtigt. * Der DNS-Resolver des Konnektors kann auf die vom Anbieter des VPN-Zugangsdienstes bereitgestellten Nameserver im Internet (Bezeichner DNS\_SERVERS\_INT) zugreifen. | |
| Eingangsdaten | * CRL (die im Konnektor verfügbare CRL) * TUNNEL\_MTU (optional, Maximum Transfer Unit für den IPsec Tunnel) * DNS\_DOMAIN\_VPN\_ZUGD\_INT (DNS-Domainname für die Service Discovery der VPN-Konzentratoren) * DNS\_SERVERS\_INT (DNS Server im Internet) * HASH\_AND\_URL | |
| Komponenten | Konnektor, VPN-Zugangsdienst | |
| Ausgangsdaten | * VPN\_TUNNEL\_SIS\_INNER\_IP (innere IP-Adresse des IPsec-Tunnels SIS) * DNS\_SERVERS\_SIS (Nameserver SIS des VPN-Zugangsdienstes) * VPN\_KONZENTRATOR\_SIS\_IP\_ADDRESS (IP-Adresse des VPN-Konzentrators SIS im Transportnetz zu dem der IPsec-Tunnel VPN\_SIS aufgebaut wird) | |
| Standardablauf | Aktion | Beschreibung |
|  | FQDN und IP-Adressen der VPN-Konzentratoren SIS ermitteln | Durch eine DNS-Anfrage zur Auflösung eines SRV-RR mit dem Bezeichner "\_isakmp.\_udp.sis-extern.<DNS\_DOMAIN\_VPN\_ZUGD\_INT>“ erhält der Konnektor eine Liste von priorisierten und gewichteten FQDN der VPN-Konzentratoren SIS.  Alle FQDN mit der höchsten Priorität (kleinere Zahlen entsprechen einer höheren Priorität) werden ihrem Gewicht entsprechend nach einem Zufallsverfahren neu sortiert. Dahinter folgen die ebenfalls zufällig sortierten FQDN der nächst niedrigeren Priorität. Dieser Vorgang wird wiederholt, bis alle FQDN in der neuen Liste enthalten sind. Der erste FQDN aus der Liste wird daraufhin in eine IP-Adresse aufgelöst (TUC-interner Bezeichner VPN\_KONZENTRATOR\_SIS\_FQDN). Es wird eine Firewall-Regel erzeugt, die einen IPsec-Verbindungsaufbau zu dieser IP-Adresse ermöglicht. Sollte sich im Folgenden herausstellen, dass es nicht möglich ist mit diesem VPN-Konzentrator eine Verbindung aufzubauen, wird der nächste FQDN aus der Liste verwendet. Dieses Verfahren wird wiederholt, bis der Verbindungsaufbau erfolgreich war oder alle Adressen erfolglos probiert wurden. |
|  | Nameserver SIS und Domainnamen der Service-Zone des VPN-Zugangsdienstes ermitteln | Durch eine DNS-Anfrage zur Auflösung eines TXT-RR mit dem Bezeichner VPN\_KONZENTRATOR\_SIS\_FQDN an den DNS-Forwarder erhält der Konnektor die IP-Adressen der Nameserver SIS (DNS\_SERVERS\_SIS) sowie die Domainnamen der Service Zone SIS (DOMAIN\_SRVZONE\_SIS) des VPN-Zugangsdienstes.  Die key/value Paare der TXT-Records haben folgende Struktur (die spitzen Klammern dienen der Abgrenzung eines Wertes):  "txtvers=1"  "NameserverSIS=<IP-Adresse1>,<IP-Adresse2>[,<weitere IP-Adressen>]"  "DomainSrvSIS=<Domainname der Servicezone SIS des VPN-Zugangsdienstes>"  Beispiel für einen Zonendateieintrag:  vpnk1.ham.sis-vpn-zugd.anbieter.de. 3600 IN TXT "txtvers=1"  "NameserverSIS=100.97.21.13,100.97.21.14"  "DomainSrvSIS=sis-sz.ham.anbieter.vpn-zugd.telematik" |
|  | DNS-Forwarder für Namensraum SIS konfigurieren | Die IP-Adressen aus DNS\_SERVERS\_SIS werden in der Nameserver Konfiguration des DNS-Forwarders als Zieladressen für den Forward-Eintrag des Namensraumes Internet eingetragen. Dabei werden die bestehenden Ziel-Nameservern DNS\_SERVERS\_INT mit den DNS\_SERVERS\_SIS überschrieben. Wenn die Verbindung zum VPN-Konzentrator SIS abgebaut wurde, müssen die Ziel-Nameservern wieder DNS\_SERVERS\_INT sein. |
|  | Verbindung aufbauen | * Der Verbindungsaufbau erfolgt gemäß [RFC7296] mit der ersten IP-Adresse aus der erzeugten IP-Adressliste der VPN-Konzentratoren. * Es muss das Encapsulating Security Payload Protocol (ESP) mit Verschlüsselung (siehe [RFC4303#3.2.1]) und Integritätsschutz (siehe [RFC4303#3.2.2]) verwendet werden. Die zu nutzenden kryptographischen Algorithmen sind in [gemSpec\_Krypt#3.3.1] beschrieben. Der Aufbau der Security Association (SA) erfolgt nach dem Internet Key Exchange Protocol Version 2 gemäß 7296 oder [RFC7427]. * Der Konnektor empfängt vom VPN-Konzentrator das Zertifikat C.VPNK.VPN-SIS. Falls HASH\_AND\_URL = Enabled muss das Hash & URL Verfahren gemäß [RFC7296] zum Austausch der Zertifikate zwischen Konnektor und VPN-Konzentrator verwendet werden. * Das Zertifikat C.VPNK.VPN-SIS wird gemäß [gemSpec\_PKI#TUC\_PKI\_018] mit Prüfmodus CRL geprüft. Wenn das Zertifikat C.VPNK.VPN-SIS nicht gültig oder das Zertifikat gesperrt ist, wird der Verbindungsaufbau mit einer Fehlermeldung gemäß [RFC 7296] abgebrochen und es wird die nächste IP-Adresse aus der Liste der VPN-Konzentratoren angesprochen. * Der Konnektor authentisiert sich beim VPN-Konzentrator mit seinem Zertifikat C.NK.VPN * Die Autorisierungsprüfung erfolgt durch den VPN-Zugangsdienst. Bei einem negativen Prüfergebnis wird an den Konnektor die Fehlermeldung "AUTHENTICATION\_FAILED" gemäß [RFC7296] gesendet. Der IPsec-Tunnelaufbau ist damit beendet. * Bei erfolgreicher gegenseitiger Authentifizierung und Autorisierung durch den VPN-Zugangsdienst wird die Verbindung gemäß [RFC7296] weiter aufgebaut. Das IKE-Protokoll weist dem Konzentrator die innere IP-Adresse des IPsec-Tunnels aus dem Adressraum TI\_Dezentral zu. Bei jedem Verbindungsaufbau wird eine andere IP-Adresse verwendet. * Die MTU wird automatisch mittels Path MTU Discovery ermittelt und entsprechend eingestellt. Wenn der optionale Parameter TUNNEL\_MTU angegeben ist, wird die MTU auf maximal diesen Wert eingestellt. |
| Varianten/Alterna­tiven | Keine |  |
| Zustand nach erfolgreichem Ablauf | Der Konnektor ist mit dem VPN-Konzentrator SIS verbunden. | |
| Fehlerfälle | Zur Behandlung auftretender Fehlerfälle werden Fehlermeldungen gemäß [RFC7296] verwendet. | |

**⌫**

### Operation disconnect

**⌦ TIP1-A\_4398 VPN-Zugangsdienst, I\_Secure\_Internet\_Tunnel::disconnect**

Der VPN-Zugangsdienst MUSS an der Schnittstelle I\_Secure\_Internet\_Tunnel die Operation disconnect zum kontrollierten Trennen der IPsec-Verbindung gemäß [RFC7296] anbieten.

**⌫**

## Schnittstelle I\_Registration\_Service

**⌦ TIP1-A\_5118 VPN-Zugangsdienst, Schnittstelle I\_Registration\_Service**

Der VPN-Zugangsdienst MUSS für Konnektoren die Schnittstelle I\_Re­gis­tration\_Service gemäß Tabelle Tab\_ZD\_Schnittstelle\_I\_Re­gistration\_Service an­bieten.

Tabelle 8: Tab\_ZD\_Schnittstelle\_I\_Registration\_Service

|  |  |  |
| --- | --- | --- |
| Name | I\_Registration\_Service | |
| Version | wird im Produktsteckbrief des VPN-Zugangsdienstes definiert | |
| Operationen | Name | Kurzbeschreibung |
| registerKonnektor | Registrierung des Konnektors |
| deregisterKonnektor | Deregistrierung des Konnektors |
| registerStatus | Registrierungs- und Vertragsstatus des Konnektors beim VPN-Zugangsdienst abfragen. |

**⌫**

### Operation registerKonnektor

**⌦ TIP1-A\_4390 VPN-Zugangsdienst und Konnektor, Operation registerKon­nektor**

Der VPN-Zugangsdienst MUSS für Konnektoren an der Schnittstelle I\_Re­gis­tra­tion\_Service die Operation registerKonnektor gemäß Tabelle Tab\_ZD\_re­gisterKon­nektor anbieten**.**

Tabelle 9: Tab\_ZD\_registerKonnektor

|  |  |  |
| --- | --- | --- |
| Name | registerKonnektor | |
| Beschreibung | Diese Operation registriert den Konnektor beim Anbieter des VPN-Zugangs-dienstes. Dabei wird eine eindeutige Beziehung zwischen Konnektor, Organisation des Gesundheitswesens und Vertrag des Leistungserbringers mit dem Anbieter des VPN-Zugangsdienstes hergestellt und zur Registrierung genutzt. Zusätzlich kann durch diese Operation auch eine Reregistrierung mit einer neuen oder alternativen SMC-B erfolgen. | |
| Vorbeding­ungen | * Die URL des Registrierungsdienstes ist im Konnektor bekannt. * Der FQDN des Registrierungsservers TI wurde in IP-Adressen aufgelöst. | |
| Aufrufparameter | Name | Beschreibung |
| SOAP-Request „registerKonnek­torRequest“ | Dies ist ein SOAP-Request „registerKonnektorRequest“ gemäß ProvisioningService.xsd. Dabei gilt:   * Das Element vpnk:Timestamp enthält den aktuellen Erstellungszeitstempel des SOAP-Requests. * Das Element vpnk:X509Certificate enthält die base64-Kodierung des ASN.1 DER-kodierten Zertifikats C.NK.VPN. * Das Element vpnk:ContractID enthält die vom VPN-Zugangsdienst erwartete ID zur Zuordnung zum Vertrag. * Das Element ds:Signature enthält die mit PRK.HCI.OSIG erstellte Signatur (mittels SMC-B) gemäß [W3C XML-DSig] über den gesamten SOAP-Request (<ds:Reference URI=““>). * Das Element ds:KeyInfo wird gemäß [W3C XML-DSig] mit Daten gefüllt. * Die base64-Kodierung des ASN.1 DER-kodierten Zertifikats C.HCI.OSIG (SMC-B-OSIG-Zertifikat) ist innerhalb des Elements ds:KeyInfo und innerhalb des Elements ds:X509Data im Element ds:X509Certificate enthalten. |
| Standardablauf | Aktion | Beschreibung |
| Operation registerKon­nektor des Registrierungs­dienstes aufrufen | Der Konnektor ruft den Dienst regService(regPort) des VPN-Zugangsdienstes, mit der SOAP-Operation registerKonnektor(registerKonnektorRequest) gemäß ProvisioningService.wsdl 1.1, auf. Dabei wird SOAP über HTTPS verwendet.  Die TLS-Verbindung erfordert eine beidseitige Authentifizierung.   * Der Konnektor prüft das Zertifikat .ZD.TLS-S gemäß [gemSpec\_PKI#TUC\_PKI\_018] mit Offline-Modus = ja und, ob die Rollen-OID "oid\_vpnz\_ti" mit der im Zertifikat enthaltenen Rollen-OID identisch ist. * Das Zertifikat C.HCI.AUT der zur Registrierung verwendeten SMC-B wird gemäß [gemSpec\_PKI#TUC\_PKI\_018] mit Prüfmodus OCSP durch den Registrierungsserver geprüft. |
| Daten im SOAP-Request prüfen | Der Registrierungsserver des VPN-Zugangsdienstes prüft die empfangenen Daten:   * Die Signatur des SOAP-Requests wird geprüft. Das zugehörige SMC-B-Zertifikat C.HCI.OSIG wird gemäß [gemSpec\_PKI#TUC\_PKI\_018] geprüft. * Das SMC-K-Zertifikat C.NK.VPN wird gemäß [gemSpec\_PKI#TUC\_PKI\_018]geprüft. * Die vpnk:ContractID aus dem Request wird mit den aus dem Vertrag zugeordneten Wert verglichen. * Der Timestamp im Request wird mit der aktuellen Zeit im Registrierungsserver verglichen. Die Abweichung darf nicht mehr als 300 Sekunden betragen. * Wenn alle Prüfungen erfolgreich waren, wird im Standardablauf fortgefahren. Anderenfalls wird eine Fehlermeldung generiert (siehe Abschnitt Fehler). |
| Registrierungsin­formationen im Autorisierungs­server eintragen | Durch den vorangegangenen Ablaufschritt ist geprüft, dass der Konnektor mit der Identität ID.NK.VPN in der Organisation des Gesundheitswesens mit der Identität ID.HCI.OSIG eingesetzt wird und dass der Vertrag mit dem Anbieter des VPN-Zugangsdienstes geschlossen wurde.  Für die Prüfung des Autorisierungsstatus beim IPsec-Verbindungsaufbau und die zyklische Prüfung der genutzten Zertifikate müssen das C.HCI.OSIG (SM-B-OSIG-Zertifikat) und das C.NK.VPN (gSMC-K-Zertifikat) im Autorisierungsserver gespeichert werden. Weiterhin muss eine Zuordnung zu den gemäß Vertrag vereinbarten Zugriffsrechten im Autorisierungsserver des VPN-Zugangsdienstes hinterlegt werden. |
| Zertifikat des Konnektors im hash&URL-Server zum Download bereitstellen | Das Zertifikat C.NK.VPN wird im hash&URL-Server gemäß [RFC7296] zum Download bereitgestellt. |
| SOAP-Response „registerKonnek­torResponse“ erzeugen | Es wird eine SOAP-Response „registerKonnektorResponse“ gemäß ProvisioningService.xsd 1.1 erzeugt (siehe Abschnitt Rückgabe). |
| SOAP-Response „registerKonnektorResponse“ an den Konnektor senden | Die SOAP-Response „registerKonnektorResponse“ wird an den Konnektor gemäß ProvisioningService.wsdl gesendet. |
|  |  |
| Rückgabe | Name | Beschreibung |
| SOAP-Response „registerKonnek­torResponse“ | Dies ist eine SOAP-Response „registerKonnektorResponse“ gemäß ProvisioningService.xsd. Dabei gilt für eine erfolgreiche Registrierung:   * Das Element vpnk:Timestamp enthält den aktuellen Erstellungszeitstempel der SOAP-Response. * Das Element vpnk:RegistrationStatus enthält den Status des Registrierungsvorgangs („Registriert“). * Das Element vpnk:ContractStatus enthält den Vertragsstatus („Zugriff auf TI erlaubt“ oder „Zugriff auf TI und SIS erlaubt“). * Das Element vpnk:AdditionalInformation enthält textuelle Informationen, die der Anbieter des VPN-Zugangsdienstes dem LE mitteilen möchte. |
| Zustand nach erfolgreichem Ablauf | Der Konnektor ist beim Anbieter des VPN-Zugangsdienstes registriert und kann (über die IPsec-gesicherte Verbindung zum VPN-Konzentrator TI) Verbindungen zu Diensten in der TI und (wenn vertraglich vereinbart) über den VPN-Konzentrator SIS Verbindungen zu Diensten im Internet aufbauen. Über diese Verbindungen können die Fachanwendungsspezifischen Dienste und die Zentralen Dienste der TI-Plattform sowie der Secure Internet Service der TI-Plattform genutzt werden. | |
| Zustand nach fehlerhaftem Ablauf | Der Konnektor ist nicht registriert und kann keine IPsec-gesicherte Verbindung zum VPN-Konzentrator TI aufbauen. | |
| Nichtfunktionale Eigenschaften | Keine | |

**⌫**

Es werden keine Vorgaben bzgl. Art und Weise der Zuordnung des Vertrages zum Kon­nektor und der Organisation des Gesundheitswesens getroffen. Insbesondere wird nicht vorgegeben wie die ContractID für diesen Zweck eingesetzt wird.

**⌦ TIP1-A\_4495 VPN-Zugangsdienst, Nutzung der ContractID**

Der Anbieter des VPN-Zugangsdienstes MUSS in seinem Registrierungsprozess vor­sehen, dass eine ContractID zur Registrierung und Deregistrierung des Konnektors verwendet wird.

Die ContractID muss für die Dauer des Vertrages konstant sein.

Der sichere Umgang mit der ContractID MUSS im Sicherheitskonzept nachge­wiesen werden.

**⌫**

Um eine Missbrauchserkennung zu unterstützen, wird empfohlen, die Daten aus dem SOAP-Request „registerKonnektorRequest“ für die Dauer der Vertragslaufzeit persistent zu speichern.

**⌦ TIP1-A\_5074 VPN-Zugangsdienst, Einhaltung des Datenschutzes bei Proto­kollierung**

Der Anbieter des VPN-Zugangsdienstes MUSS sicherstellen, dass die Daten aus dem SOAP-Request „registerKonnektorRequest“ nur für den Zweck der Re­gistrierung von Konnektoren und der Missbrauchserkennung für die Dauer der Vertragslaufzeit verwendet werden.

Diese Daten unterliegen der besonderen Zweckbestimmung gemäß § 31 BDSG und dienen nur zur Sicherstellung eines ordnungsgemäßen Betriebes des VPN-Zugangsdienstes.

**⌫**

#### Umsetzung

An die Umsetzung der Schnittstelle werden keine zusätzlichen Anforderungen gestellt.

#### Nutzung

An die Nutzung der Schnittstelle werden keine zusätzlichen Anforderungen gestellt.

### Operation deregisterKonnektor

**⌦ TIP1-A\_4391 VPN-Zugangsdienst und Konnektor, Operation deregisterKon­nektor**

Der VPN-Zugangsdienst MUSS für Konnektoren an der Schnittstelle I\_Re­gis­tra­tion\_Service die Operation deregisterKonnektor gemäß Tabelle Tab\_ZD\_dere­gister­Kon­nektor anbieten**.**

Tabelle 10: Tab\_ZD\_deregisterKonnektor

|  |  |  |
| --- | --- | --- |
| Name | deregisterKonnektor | |
| Beschreibung | Diese Operation löscht die Registrierung des Konnektors beim Anbieter des VPN-Zugangsdienstes. Nachdem diese Operation ausgeführt wurde, kann der Konnektor keinen IPsec-Tunnel TI mehr aufbauen und die Dienste der TI sind nicht mehr erreichbar. Der Konnektor kann über das Internet weiterhin den Registrierungsserver erreichen. | |
| Vorbedingungen | * Die URL des Registrierungsdienstes ist im Konnektor bekannt. * Der FQDN des Registrierungsservers TI wurde in IP-Adressen aufge­löst. | |
| Aufrufparameter | Name | Beschreibung |
| SOAP-Request „deregisterKonnektorRequest“ | Dies ist ein SOAP-Request „deregisterKonnektorRequest“ gemäß ProvisioningService.xsd. Dabei gilt:   * Das Element vpnk:Timestamp enthält den aktuellen Erstellungszeitstempel des SOAP-Requests. * Das Element vpnk:X509Certificate enthält die base64-Kodierung des ASN.1 DER-kodierten SMC-K-Zertifikats. * Das Element vpnk:ContractID enthält die vom VPN-Zugangsdienst erwartete ID zur Zuordnung zum Vertrag. * Das Element ds:Signature enthält die mit PRK.HCI.OSIG erstellte Signatur (mittels SMC-B) gemäß [W3C XML-Dsig] über den gesamten SOAP-Request (<ds:Reference URI=““>). * Das Element ds:KeyInfo wird gemäß [W3C XML-Dsig] mit Daten gefüllt. * Die base64-Kodierung des ASN.1 DER-kodierten Zertifikats C.HCI.OSIG (SMC-B-OSIG-Zertifikat) ist innerhalb des Elements ds:KeyInfo und innerhalb des Elements ds:X509Data im Element ds:X509Certificate enthalten. |
| Standardablauf | Aktion | Beschreibung |
| Operation deregisterKon­nektor des Registrierungs­dienstes aufrufen | Der Konnektor ruft den Dienst regService(deregPort) des VPN-Zugangsdienstes, mit der SOAP-Operation deregisterKonnektor(deregisterKonnektorRequest) gemäß ProvisioningService.wsdl , auf. Dabei wird SOAP über HTTPS verwendet.  Die TLS-Verbindung erfordert eine beidseitige Authentifizierung.   * Der Konnektor prüft das Zertifikat .ZD.TLS-S gemäß [gemSpec\_PKI#TUC\_PKI\_018] mit Offline-Modus = ja und, ob die Rollen-OID "oid\_vpnz\_ti" mit der im Zertifikat enthaltenen Rollen-OID identisch ist. * Das Zertifikat C.HCI.AUT einer beliebigen SMC-B, mit der die Deregistrierung durchgeführt werden soll, wird gemäß [gemSpec\_PKI#TUC\_PKI\_018] mit Prüfmodus OCSP durch den Registrierungsserver geprüft. |
| Daten im SOAP-Request prüfen | Der Registrierungsserver des VPN-Zugangsdienstes prüft die empfangenen Daten:   * Die Signatur des SOAP-Requests wird geprüft. Das zugehörige SMC-B-Zertifikat C.HCI.OSIG wird gemäß [gemSpec\_PKI#TUC\_PKI\_018] geprüft. * Das SMC-K-Zertifikat C.NK.VPN wird gemäß [gemSpec\_PKI#TUC\_PKI\_018] geprüft. * Die vpnk:ContractID aus dem Request wird mit den aus dem Vertrag zugeordneten Wert verglichen. * Der Timestamp im Request wird mit der aktuellen Zeit im Registrierungsserver verglichen. Die Abweichung darf nicht mehr als 300 Sekunden betragen. * Wenn alle Prüfungen erfolgreich waren, wird im Standardablauf fortgefahren. Anderenfalls wird eine Fehlermeldung generiert (siehe Abschnitt Fehler). |
| Registrierungsin­formationen im Autorisierungs­server löschen | Durch den vorangegangenen Ablaufschritt ist geprüft, dass der Konnektor mit der Identität ID.NK.VPN in der Organisation des Gesundheitswesens mit der Identität ID.HCI.OSIG einge­setzt wird und dass der Vertrag mit dem Anbieter des VPN-Zugangsdienstes geschlossen wurde. Die Registrierungsinformationen des Konnektors müssen aus dem Autorisierungsserver des VPN-Zugangs­dienstes gelöscht werden. |
| Zertifikat des Konnektors im hash&URL-Server löschen | Das Zertifikat C.NK.VPN wird im hash&URL-Server gelöscht. |
| SOAP-Response „deregisterKon­nektorResponse“ erzeugen | Der Registrierungsserver des VPN-Zugangsdienstes erzeugt eine SOAP-Response „deregisterKonnektorResponse“ gemäß ProvisioningService.xsd erzeugt (siehe Abschnitt Rückgabe). |
| SOAP-Response „deregisterKon­nektorResponse“ an den Kon­nektor senden | Der Registrierungsserver des VPN-Zugangsdienstes sendet die SOAP-Response(deregisterKonnektorResponse) an den Konnektor gemäß ProvisioningService.wsdl. |
| Rückgabe | Name | Beschreibung |
| SOAP-Response „deregisterKon­nektorResponse“ | Dies ist eine SOAP-Response „deregisterKonnektorResponse“ gemäß ProvisioningService.xsd. Dabei gilt für eine erfolgreiche Deregistrierung:   * Das Element vpnk:Timestamp enthält den aktuellen Erstellungs­zeitstempel der SOAP-Response. * Das Element vpnk:RegistrationStatus enthält den Status des Deregistrierungsvorgangs („Nicht registriert“). * Das Element vpnk:ContractStatus enthält den Vertragsstatus („Zugriff auf TI erlaubt“, „Zugriff auf TI und SIS erlaubt“ oder „Kein Zugriff auf TI und SIS“). * Das Element vpnk:AdditionalInformation enthält textuelle Informationen, die der Anbieter des VPN-Zugangsdienstes dem LE mitteilen möchte. |
| Zustand nach erfolgreichem Ablauf | Der Konnektor ist beim Anbieter des VPN-Zugangsdienstes deregistriert und es kann keine IPsec-gesicherte Verbindung zum VPN-Konzentrator TI aufgebaut werden. | |
| Zustand nach fehlerhaftem Ablauf | Der Konnektor bleibt beim Anbieter des VPN-Zugangsdienstes registriert und kann (über die IPsec-gesicherte Verbindung zum VPN-Konzentrator TI) Verbindungen zu Diensten in der TI und (wenn vertraglich vereinbart) über den VPN-Konzentrator SIS Verbindungen zu Diensten im Internet aufbauen. | |
| Nichtfunktionale Eigenschaften | Keine | |

**⌫**

#### Umsetzung

An die Umsetzung der Schnittstelle werden keine zusätzlichen Anforderungen gestellt.

#### Nutzung

An die Nutzung der Schnittstelle werden keine zusätzlichen Anforderungen gestellt.

### Operation registerStatus

**⌦ TIP1-A\_4392 VPN-Zugangsdienst und Konnektor, Operation registerStatus**

Der VPN-Zugangsdienst MUSS für Konnektoren an der Schnittstelle I\_Re­gis­tration\_Service die Operation registerStatus gemäß Tabelle Tab\_ZD\_registerSta­tus anbieten**.**

Tabelle 11: Tab\_ZD\_registerStatus

|  |  |  |
| --- | --- | --- |
| Name | registerStatus | |
| Beschreibung | Diese Operation ermöglicht den Registrierungsstatus und den Vertragsstatus bzgl. eines Konnektors abzufragen. | |
| Vorbedingungen | * Die URL des Registrierungsdienstes ist im Konnektor bekannt. * Der FQDN des Registrierungsservers TI wurde in IP-Adressen aufge­löst. | |
| Aufrufparameter | Name | Beschreibung |
| SOAP-Request „registerStatus­Request“ | Dies ist ein SOAP-Request „registerStatusRequest“ gemäß ProvisioningService.xsd. Dabei gilt:   * Das Element vpnk:Timestamp enthält den aktuellen Erstellungszeitstempel des SOAP-Requests. * Das Element vpnk:X509Certificate enthält die base64-Kodierung des ASN.1 DER-kodierten SMC-K-Zertifikats. |
| Standardablauf | Aktion | Beschreibung |
| Operation registerStatus des Registrierungs­dienstes aufrufen | Der Konnektor ruft den Dienst regService(regStatusPort) des VPN-Zugangsdienstes, mit der SOAP-Operation registerStatus(registerStatusRequest) gemäß ProvisioningService.wsdl, auf. Dabei wird SOAP über HTTPS verwendet.  Die TLS-Verbindung erfordert eine beidseitige Authentifizierung.  Die TLS-Verbindung erfordert eine beidseitige Authentifizierung.   * Der Konnektor prüft das Zertifikat .ZD.TLS-S gemäß [gemSpec\_PKI#TUC\_PKI\_018] mit Offline-Modus = ja und, ob die Rollen-OID "oid\_vpnz\_ti" mit der im Zertifikat enthaltenen Rollen-OID identisch ist. * Das Zertifikat C.HCI.AUT der zur Registrierung verwendeten SMC-B wird gemäß [gemSpec\_PKI#TUC\_PKI\_018] mit Prüfmodus OCSP durch den Registrierungsserver geprüft. |
| Daten im SOAP-Request prüfen | Der Registrierungsserver des VPN-Zugangsdienstes prüft die empfangenen Daten:   * Der Timestamp im Request wird mit der aktuellen Zeit im Registrierungsserver verglichen. Die Ab­weichung darf nicht mehr als 300 Sekunden be­tra­gen.   Wenn die Prüfung erfolgreich war, wird im Standardablauf fortgefahren. Anderenfalls wird eine Fehlermeldung generiert (siehe Abschnitt Fehler). |
| SOAP-Response „registerStatus­Response“ erzeugen | Der Registrierungsserver des VPN-Zugangsdienstes erzeugt eine SOAP-Response „registerStatusResponse“ gemäß ProvisioningService.xsd (siehe Abschnitt Rückgabe). |
| SOAP-Response „registerStatus“ an den Konnektor senden | Der Registrierungsserver des VPN-Zugangsdienstes sendet die SOAP-Response(registerStatusResponse) an den Konnektor gemäß ProvisioningService.wsdl. |
| Rückgabe | Name | Beschreibung |
| SOAP-Response „registerStatusResponse“ | Dies ist eine SOAP-Response „registerStatusResponse“ gemäß ProvisioningService.xsd. Dabei gilt für eine erfolgreiche registerStatus Abfrage:   * Das Element vpnk:Timestamp enthält den aktuellen Erstellungszeitstempel der SOAP-Response. * Das Element vpnk:RegistrationTimestamp enthält den Erstellungszeitstempel der Registrierung. * Das Element vpnk:RegistrationStatus enthält den Status des der Registrierung („Registriert“ oder „Nicht registriert“). * Das Element vpnk:ContractStatus enthält den Vertragsstatus („Zugriff auf TI erlaubt“, „Zugriff auf TI und SIS erlaubt“ oder „Kein Zugriff auf TI und SIS“). * Das Element vpnk:AdditionalInformation enthält textuelle Informationen, die der Anbieter des VPN-Zugangsdienstes dem LE mitteilen möchte. |
| Zustand nach erfolgreichem Ablauf | Keine Änderung | |
| Zustand nach fehlerhaftem Ablauf | Keine Änderung | |
| Nichtfunktionale Eigenschaften | Keine | |

**⌫**

#### Umsetzung

An die Umsetzung der Schnittstelle werden keine zusätzlichen Anforderungen gestellt.

#### Nutzung

An die Nutzung der Schnittstelle werden keine zusätzlichen Anforderungen gestellt.

### Registrierungsserver Fehlermeldungen

**⌦ TIP1-A\_4491 VPN-Zugangsdienst, Registrierungsserver Fehlermeldungen**

Der Registrierungsserver des VPN-Zugangsdienstes und der Konnektor MÜSSEN für die Operationen registerKonnektor, deregisterKonnektor und registerStatus die Fehlermeldungen gemäß Tabelle Tab\_Registrierungsserver\_Fehlermeldungen im­ple­mentieren.

Tabelle 12: Tab\_Registrierungsserver\_Fehlermeldungen

| Code | ErrorType | Severity | ErrorText | Auslösende Bedingung |
| --- | --- | --- | --- | --- |
| 7011 | Security | Error | Prüfung der SMC-B-Signatur der SMC-B-Identität des Ausstellers <Aussteller> mit der Seriennummer <Seriennummer> nicht erfolgreich | siehe Text |
| 7021 | Security | Error | Prüfung des SMC-K-Zertifikats des Ausstellers <Aussteller> mit der Seriennummer <Seriennummer> nicht erfolgreich | siehe Text |
| 7031 | Security | Error | Prüfung des SMC-B-Zertifikats des Ausstellers <Aussteller> mit der Seriennummer <Seriennummer> nicht erfolgreich | siehe Text |
| 7041 | Business | Error | Prüfung der ContractID nicht erfolgreich | siehe Text |
| 7061 | Technical | Error | Der Timestamp im Request weicht mehr als 300 Sekunden von der aktuellen Zeit im Registrierungsserver ab | siehe Text |
| 7071 | Business | Error | Eintragung der Registrierung im Autorisierungsserver fehlgeschlagen | siehe Text |
| 7081 | Business | Error | Deregistrierung im Autorisierungsserver fehlgeschlagen | siehe Text |

Weitere Elemente der Fehlermeldung müssen wie folgt angegeben werden:

CompType = VPN-Zugangsdienst

**⌫**

## Schnittstelle I\_DNS\_Name\_Resolution (Namensraum TI)

**⌦ TIP1-A\_4497 VPN-Zugangsdienst, sichere Speicherung des Key Signing Keys des TI Trust Anchors**

Die Nameserver im Namensraum TI des VPN-Zugangdienstes MÜSSEN den Hash des Key Signing Key des TI Trust Anchors in aktueller Version enthalten und sicher speichern. Der Key Signing Key darf dabei nur durch autorisierte Akteure eingebracht werden.

**⌫**

Weitere Vorgaben zur Schnittstelle I\_DNS\_Name\_Resolution und zu den zu nutzenden Stan­dards sind in [gemSpec\_Net#5] beschrieben.

## Schnittstelle I\_DNS\_Name\_Resolution (Namensraum Internet)

Die Vorgaben zur Schnittstelle I\_DNS\_Name\_Resolution und zu den zu nutzenden Stan­dards sind in [gemSpec\_Net#5] beschrieben.

## Schnittstelle I\_DNS\_Name\_Resolution (Namensraum SIS)

Die Vorgaben zur Schnittstelle I\_DNS\_Name\_Resolution und zu den zu nutzenden Stan­dards sind in [gemSpec\_Net#5] beschrieben.

## Schnittstelle I\_NTP\_Time\_Information

Die Vorgaben zur Schnittstelle I\_NTP\_Time\_Information und zu den zu nutzenden Stan­dards sind in [gemSpec\_Net#5] beschrieben.

## Prozess Änderung der Sicherheitsleistungen des SIS

**⌦ TIP1-A\_4399 VPN-Zugangsdienst, Prozess Änderung der Sicherheits­leis­tungen des SIS**

Der Anbieter des VPN-Zugangsdienstes MUSS einen Prozess implementieren, der die Änderung von Sicherheitsleistungen des Secure Internet Service durch den GBV ermöglicht.

Der Anbieter des VPN-Zugangsdienstes ist der Eigentümer des Prozesses.

**⌫**

## Prozess zum Abschluss, Ändern und Auflösen des Vertragsverhältnisses

**⌦ TIP1-A\_4498 VPN-Zugangsdienst, Prozess Abschluss, Ändern und Auflösen des Vertragsverhältnisses sowie Deregistrierung von Konnektoren**

Der Anbieter des VPN-Zugangsdienstes MUSS einen Prozess implementieren, der es Leistungserbringern ermöglicht, mit dem Anbieter des VPN-Zugangsdienstes einen Vertrag abzuschließen, zu ändern oder aufzulösen um Zugang zur TI inklusive Bestandsnetze sowie Zugang zum sicheren Internet­anschluss zu erhalten.

Zusätzlich MUSS dieser Prozess ermöglichen, dass Konnektoren deregistriert werden können.

Der Anbieter des VPN-Zugangsdienstes ist der Owner des Prozesses.

Vertragsdaten MÜSSEN bei Vertragsende nach Ablauf der gesetzlichen Aufbe­wahrungsfristen gelöscht werden.

**⌫**

Damit der Konnektor sich mit den VPN-Konzentratoren TI und SIS verbinden kann, müssen im Konnektor die Nameserver Internet und die Domain, die die SRV-Records der VPN-Konzentratoren enthält, bekannt sein.

Zur Registrierung des Konnektors beim Anbieter des VPN-Zugangsdienstes ist es erforderlich, dass der Konnektor dem richtigen Vertrag zwischen LE und dem Anbieter des VPN-Zugangsdienstes zugeordnet werden kann. Zu diesem Zweck wird ein Vertrags-Kennzeichen (CONTRACT\_ID\_VPN\_ZUGD) eingeführt.

**⌦ TIP1-A\_5105 VPN-Zugangsdienst, Konfigurationsdaten zur Übergabe bei Vertragsabschluss**

Der Anbieter des VPN-Zugangsdienstes MUSS die Daten gemäß Tab\_ZD\_Kon­figurationsdaten\_bei\_Vertragsabschluss im Rahmen des Vertragsabschlusses an den jeweiligen LE übergeben.

Tabelle 13: Tab\_ZD\_Konfigurationsdaten\_bei\_Vertragsabschluss

| **Variable** | **Beschreibung** |
| --- | --- |
| DNS\_SERVERS\_INT | Internet Nameserver des VPN-Zugangsdienstes |
| DNS\_DOMAIN\_VPN\_ZUGD\_INT | Internet Domain des VPN-Zugangsdienstes |
| CONTRACT\_ID\_VPN\_ZUGD | Dieser String enthält die vom VPN-Zugangsdienst erwartete ID, die eine Zuordnung zum Vertrag mit dem LE ermöglicht. |

**⌫**

# 

# Anhang A – Verzeichnisse

## A1 – Abkürzungen

| Kürzel | Erläuterung |
| --- | --- |
| AAA | Authentifizierung, Autorisierung und Accounting (Triple-A-System) |
| ACL | Access Control List |
| ASN.1 | Abstract Syntax Notation One |
| base64 | Verfahren zur Kodierung von 8-Bit-Binärdaten in 7-Bit-ASCII-Zeichen |
| C.HCI.OSIG | SMC-B OSIG Zertifikat |
| C.NK.VPN | SMC-K Zertifikat |
| C.VPNK.VPN | VPN-Konzentrator TI-Zertifikat |
| C.VPNK.VPN-SIS | VPN-Konzentrator SIS-Zertifikat |
| CE | Customer Edge |
| CRL | Certificate Revocation List |
| DER | ASN.1 Distinguished Encoding Rules |
| DIAMETER | Client-Server-Protokoll zur Authentifizierung, Autorisierung und zum Accounting (Triple-A-System) von Benutzern bei Einwahlverbindungen in ein Computernetzwerk |
| DiffServ | Differentiated Services |
| DMZ | Demilitarized Zone |
| DNS | Domain Name System |
| DNSSEC | Domain Name System Security Extensions |
| DSCP | Differentiated Services Code Point |
| DSL | Digital Subscriber Line |
| ESP | Encapsulating Security Payload |
| FQDN | Full Qualified Domain Name |
| http | hypertext transport protocol |
| IAG | Internet Access Gateway |
| ICMP | Internet Control Message Protocol |
| ID | Identifier |
| ID.HCI.OSIG | SMC-B OSIG Identität |
| ID.NK.VPN | SMC-K Identität (Zertifikat und Privater Schlüssel) |
| ID.VPNK.VPN | VPN-Konzentrator TI Identität (Zertifikat und Privater Schlüssel) |
| ID.VPNK.VPN-SIS | VPN-Konzentrator SIS Identität (Zertifikat und Privater Schlüssel) |
| ID.ZD.TLS-S | Registrierungsserver Identität (Zertifikat und Privater Schlüssel) |
| IKEv2 | Internet Key Exchange Version 2 |
| IP | Internet Protocol (bezeichnet IPv4 und IPv6) |
| IPComp | IP Payload Compression Protocol |
| IPsec | Internet Protocol Security |
| LDAP | Lightweight Directory Access Protocol |
| LE | Leistungserbringer |
| ms | Millisekunden |
| MTU | Maximum Transmission Unit |
| NAT | Network Address Translation |
| NAT-T | NAT-Traversal |
| NTP | Network Time Protocol |
| OCSP | Online Certificate Status Protocol |
| PAP | Paketfilter−Application Layer Gateway–Paketfilter |
| PE | Provider Edge |
| PMTUD | Path MTU Discovery |
| PRK.HCI.OSIG | Privater Schlüssel des OSIG Zertifikats der SMC-B |
| RADIUS | Remote Authentication Dial-In User Service  (siehe DIAMETER) |
| SA | Security Association |
| SIS | Secure Internet Service |
| SMC | Secure Module Card |
| SOAP | Simple Object Access Protocol |
| SQL | Structured Query Language |
| SRV-Record | DNS Service Resource Record |
| SZZP | Sicherer Zentraler Zugangspunkt |
| TCP | Transmission Control Protocol |
| TI | Telematikinfrastruktur |
| TTL | Time to live |
| UDP | User Datagram Protocol |
| UML | Unified Markup Language |
| URL | Uniform Resource Locator |
| VPN | Virtual Private Network |
| WAN | Wide Area Network |
| XML | Extensible Markup Language |
| ISAKMP | Internet Security Association and Key Management Protocol |
| A-Record | DNS A Resource Record |
| Bestandsnetz | sicheres Netz der KVen |

## A2 – Glossar

Das Glossar wird als eigenständiges Dokument, vgl. [gemGlossar] zur Verfügung gestellt.

## A3 – Abbildungsverzeichnis

[Abbildung 1: Netztopologie VPN-Zugangsdienst (logisch) 10](#_Toc501452986)

[Abbildung 2: Zerlegung des VPN-Zugangsdienstes 11](#_Toc501452987)

[Abbildung 3: Übersicht VPN-Zugangsdienst (Zonen) 12](#_Toc501452988)

[Abbildung 4: Ablauf der Operation I\_Secure\_Channel\_Tunnel::connect im VPN-Zugangsdienst 44](#_Toc501452989)

## A4 – Tabellenverzeichnis

[Tabelle 1: Tab\_ZD\_Nameserver\_Int\_RR 20](#_Toc501452990)

[Tabelle 2: Tab\_ZD\_Nameserver\_TI\_RR 22](#_Toc501452991)

[Tabelle 3: Tab\_PT\_VPN-Zugangsdienst\_Schnittstellen 42](#_Toc501452992)

[Tabelle 4: Tab\_ZD\_Schnittstelle\_I\_Secure\_Channel\_Tunnel 43](#_Toc501452993)

[Tabelle 5: Tab\_ZD\_TUC\_IPsec\_Tunnel\_TI\_aufbauen 45](#_Toc501452994)

[Tabelle 6: Tab\_ZD\_Schnittstelle\_I\_Secure\_Internet\_Tunnel 49](#_Toc501452995)

[Tabelle 7: Tab\_ZD\_TUC\_IPsec\_Tunnel\_SIS\_aufbauen 51](#_Toc501452996)

[Tabelle 8: Tab\_ZD\_Schnittstelle\_I\_Registration\_Service 54](#_Toc501452997)

[Tabelle 9: Tab\_ZD\_registerKonnektor 54](#_Toc501452998)

[Tabelle 10: Tab\_ZD\_deregisterKonnektor 58](#_Toc501452999)

[Tabelle 11: Tab\_ZD\_registerStatus 60](#_Toc501453000)

[Tabelle 12: Tab\_Registrierungsserver\_Fehlermeldungen 62](#_Toc501453001)

[Tabelle 13: Tab\_ZD\_Konfigurationsdaten\_bei\_Vertragsabschluss 64](#_Toc501453002)

## A5 – Referenzierte Dokumente

### A5.1 – 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 passende jeweils gültige Versionsnummer sind in der aktuellsten, von der gematik veröffentlichten Dokumentenlandkarte enthalten, in der die vorliegende Ver­sion aufgeführt wird.

|  |  |
| --- | --- |
| [Quelle] | Herausgeber: Titel |
| [gemGlossar] | gematik: Glossar der Telematikinfrastruktur |
| [gemSpec\_Krypt] | gematik: Übergreifende Spezifikation – Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur |
| [gemSpec\_Net] | gematik: Übergreifende Spezifikation – Spezifikation Netzwerk |
| [gemSpec\_PKI] | gematik: Übergreifende Spezifikation – Spezifikation PKI |
| [gemSpec\_Perf] | gematik: Übergreifende Spezifikation – Performance und Mengengerüst TI-Plattform |

### A5.2 – Weitere Dokumente

| [Quelle] | Herausgeber (Erscheinungsdatum): Titel |
| --- | --- |
| [BSI-SiGw] | Bundesamt für Sicherheit in der Informationstechnik (o.J.): Konzeption von Sicherheitsgateways, Version 1.0 |
| [RFC2119] | RFC 2119 (März 1997):  Key words for use in RFCs to Indicate Requirement Levels S. Bradner,  <http://tools.ietf.org/html/rfc2119> |
| [RFC2782] | RFC 2782 (Februar 2000): A DNS RR for specifying the location of services (DNS SRV) <http://www.ietf.org/html/rfc2782> |
| [RFC3173] | IETF (2001): IP Payload Compression Protocol (IPComp) |
| [RFC4301] | RFC 4301 (Dezember 2005):  Security Architecture for the Internet Protocol <http://tools.ietf.org/html/rfc4301> |
| [RFC4303] | RFC 4303 (Dezember 2005):  IP Encapsulating Security Payload (ESP); <http://tools.ietf.org/html/rfc4303> |
| [RFC7296] | RFC 7296 ( October 2014):  Internet Key Exchange Protocol Version 2 (IKEv2);  https://tools.ietf.org/html/rfc7296 |
| [W3C XML-DSig] | W3C (10.06.2008): XML Signature Syntax and Processing (Second Edition) |