Elektronische Gesundheitskarte und Telematikinfrastruktur

Spezifikation
VPN-Zugangsdienst

Version:	1.~~1~~820.0
Revision:	~~443220~~457470
Stand:	04.~~03~~05.2022
Status:	freigegeben
Klassifizierung:	öffentlich
Referenzierung:	gemSpec_VPN_ZugD

Dokumentinformationen

Änderungen zur Vorversion

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

Dokumentenhistorie

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
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 Netztopologie 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
1.8.0	06.02.17		Einarbeitung lt. Änderungsliste	gematik
1.9.0	20.04.17		Einarbeitung lt. Änderungsliste	gematik
1.10.0	18.12.17		Überarbeitung Online-Produktivbetrieb (Stufe 2.1)	gematik
1.11.0	14.05.18		Einarbeitung lt. Änderungsliste 15.2, 15.4 und 15.5	gematik

1.12.0			Einarbeitung lt. Änderungsliste 15.9	gematik
1.13.0	15.05.19		Einarbeitung lt. Änderungsliste 18.1	gematik
1.14.0	02.10.19		Einarbeitung lt. Änderungsliste 20.1	gematik
1.15.0	02.03.20		Einarbeitung lt. Änderungsliste 21.1	gematik
1.16.0	09.12.20		Einarbeitung lt. Änderungsliste 22.5	gematik
1.17.0	30.06.21		Einarbeitung Featurespezifikation gemF_Laufzeitverlängerung_gSMC-K und Konn_Maintenance_21.3	gematik
1.18.0	04.03.22		Einarbeitung Hotfix CI_Maintenance_22.1: Erweiterung des Registrierungsdienstes zur Unterstützung von Mehrfachregistrierungen des VPN-Zugangsdienstes sowie die Übermittlung der Betriebsstättenart durch die VPN-Zugangsdienst-Anbieter	gematik
1.19.0	29.04.22		Einarbeitung CI_Maintenance_22.2: Streichung Textanteile für die gSMC-K Laufzeitverlängerung und Ergänzung der Registrierungsserver Fehlermeldung,	gematik
1.20.0	04.05.22		Einarbeitung CI_Maintenance_22.3: Optimierung des Aufrufs der Operation „sendData" für die Verwendung von beliebigen freigeschalteten SMC-B (Tab_ZD_sendData).	gematik

Inhaltsverzeichnis

1 Einordnung des Dokumentes

1.1 Zielsetzung

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

1.2 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.

1.3 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.

1.4 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.

1.5 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:

<AFO-ID> - <Titel der Afo>
Text / Beschreibung
[<=**]**

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

2 Systemüberblick

2.1 Funktion

Der VPN-Zugangsdienst ermöglicht den berechtigten Teilnehmern den Zugang zur Telematikinfrastruktur (TI) und zum Secure Internet Service (SIS). Für berechtigte Teilnehmer ist die Nutzung des SIS optional. Als Transportinfrastruktur zwischen dem Netz des berechtigten Teilnehmers 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 berechtigten Teilnehmer 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.

2.2 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.

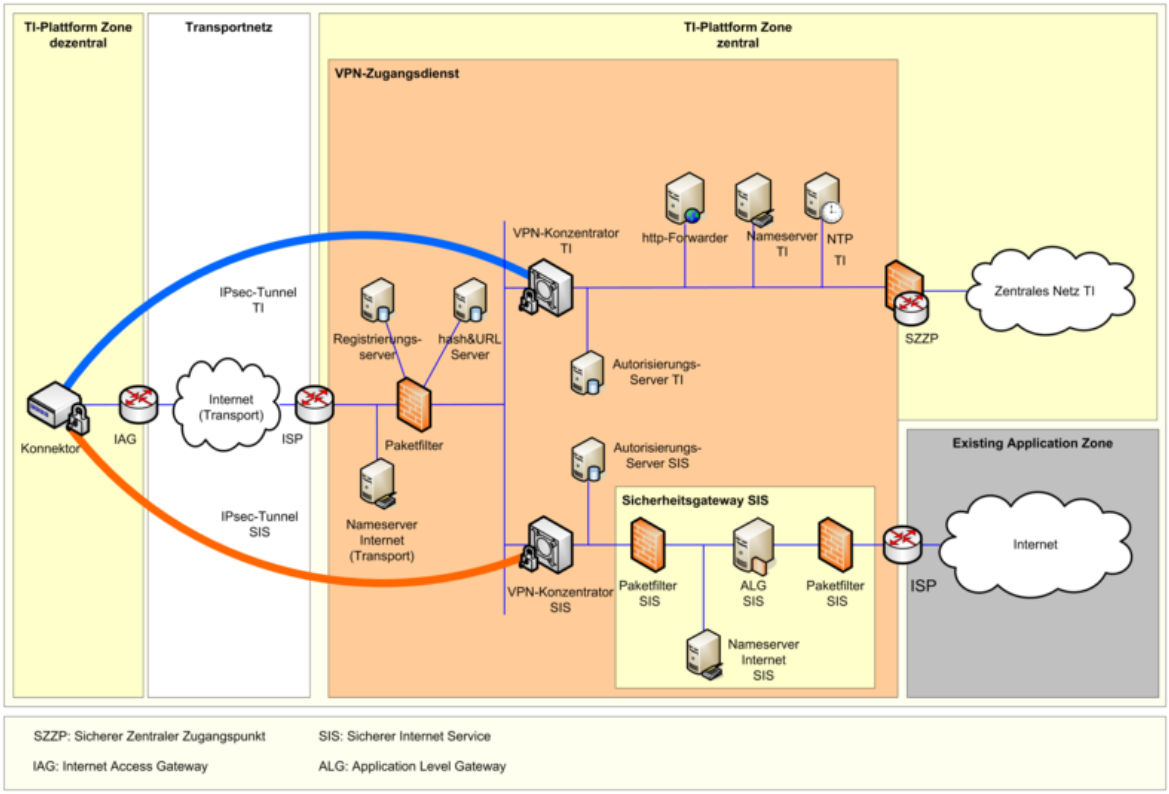

Abbildung 1: Netztopologie VPN-Zugangsdienst (logisch)

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.

3 Zerlegung des Produkttyps

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

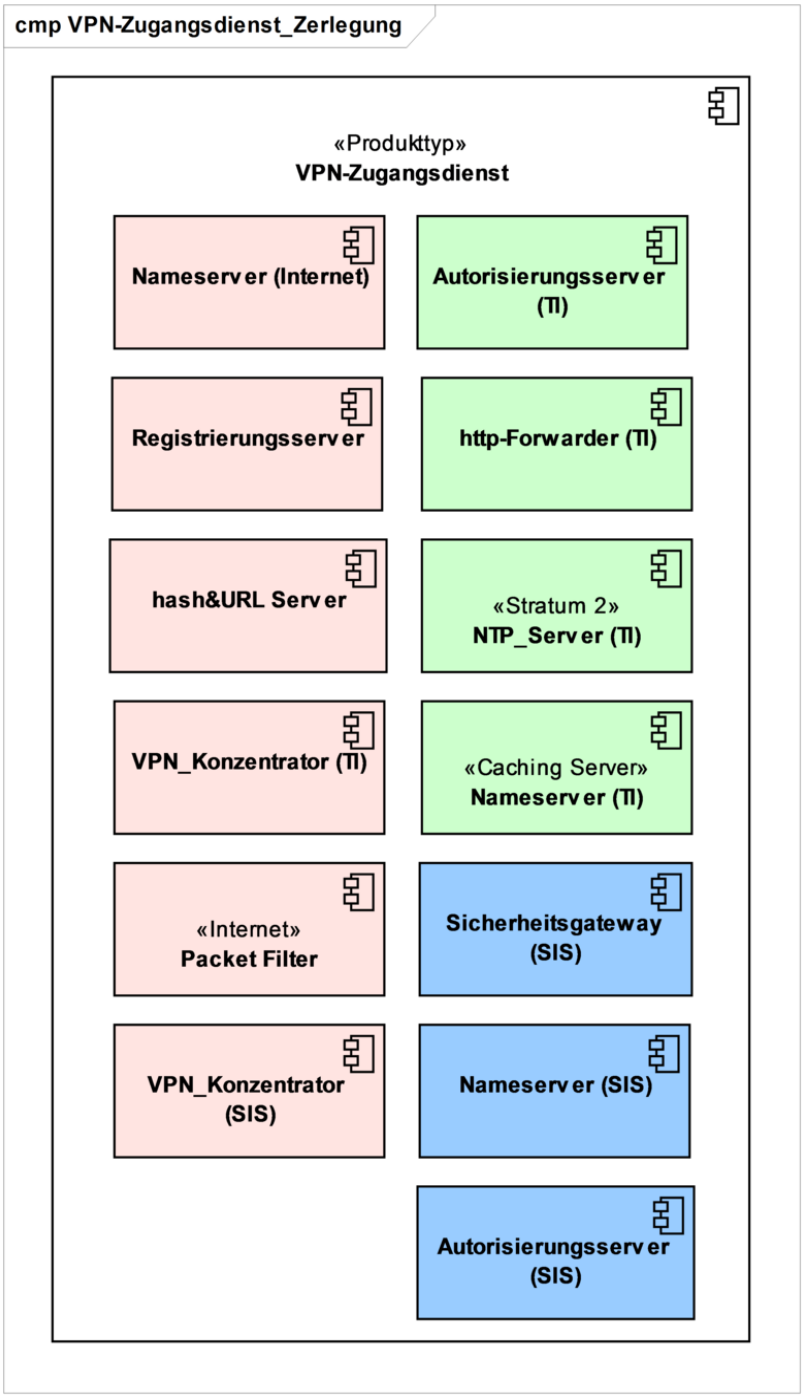

Abbildung 2: Zerlegung des VPN-Zugangsdienstes

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.

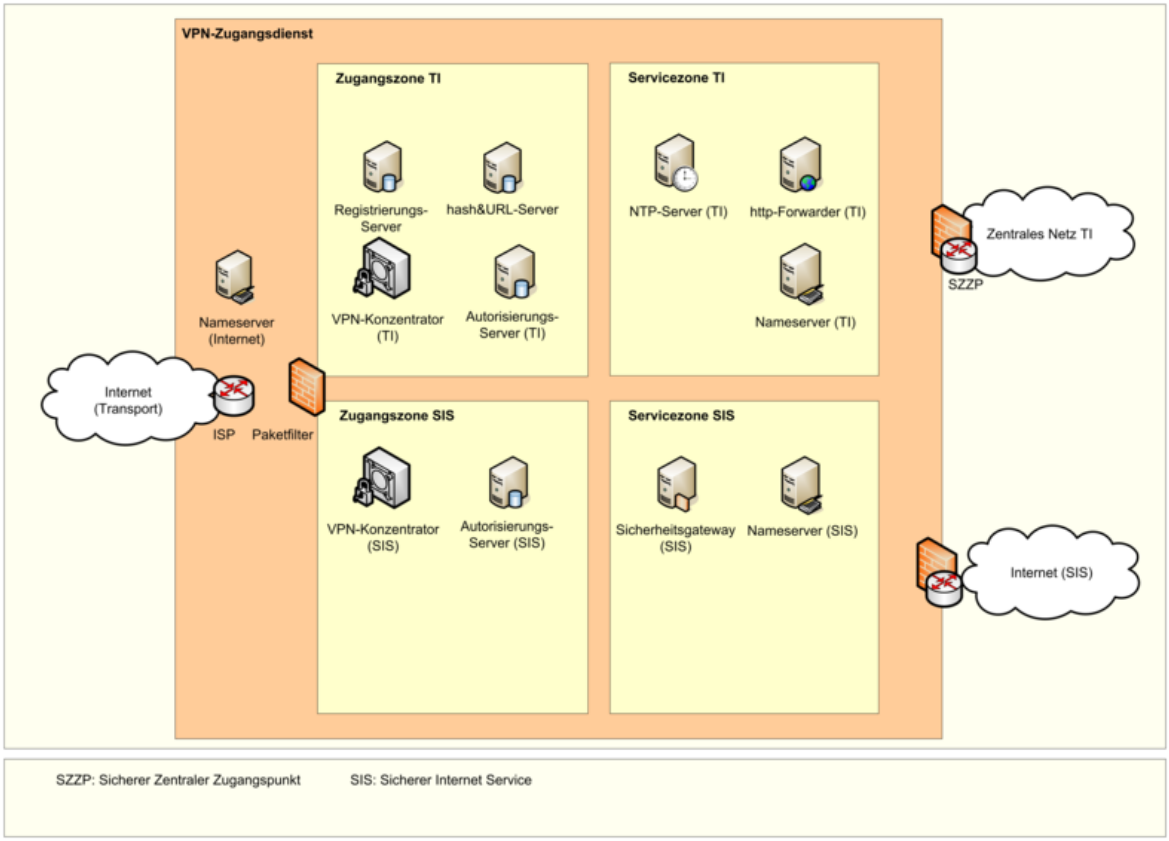

Abbildung 3: Übersicht VPN-Zugangsdienst (Zonen)

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.

3.1 VPN-Konzentratoren

3.1.1 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.

3.1.2 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.
[<=]

3.1.3 Standorte des VPN-Zugangsdienstes

Bei der Auswahl der Standorte soll die Nähe zu einer Vielzahl von berechtigten Teilnehmern 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 berechtigten Teilnehmer 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.

3.1.4 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.
[<=]

3.1.5 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]).

3.1.6 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.

3.1.7 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.
[<=]

3.1.8 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.
[<=]

3.1.9 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.
[<=]

3.1.10 Adressierung

3.1.10.1 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.
[<=]

3.1.10.2 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.

3.1.10.3 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.
[<=]

3.1.11 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

[<=]

3.1.12 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 berechtigten Teilnehmern 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.
[<=]

3.2 Nameserver Internet

3.2.1 Funktion

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

3.2.2 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**.**

3.2.3 Redundanz

Die hierfür geltenden Anforderungen zur Verfügbarkeit werden in [gemSpec_Perf#4.2] definiert.

3.2.4 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"`

[<=]

3.2.5 Adressierung

TIP1-A_4305 - VPN-Zugangsdienst, IPv4-Adressierung Nameserver Internet
Der Anbieter des VPN-Zugangsdienstes MUSS jedem der drei Nameserver Internet genau eine öffentliche IPv4-Adresse zuweisen.**[<=]**

3.3 Nameserver TI

3.3.1 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).
[<=]

3.3.2 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.
[<=]

3.3.3 Redundanz

Die hierfür geltenden Anforderungen zur Verfügbarkeit werden in [gemSpec_Perf#4.2] definiert.

3.3.4 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

[<=]

3.3.5 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.
[<=]

3.4 Nameserver SIS

3.4.1 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).
[<=]

3.4.2 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.
[<=]

3.4.3 Redundanz

Die hierfür geltenden Anforderungen zur Verfügbarkeit werden in [gemSpec_Perf#4.2] definiert.

3.4.4 Konfiguration

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

3.4.5 Adressierung

TIP1-A_4311 - VPN-Zugangsdienst, Adressierung Nameserver SIS
Der Anbieter des VPN-Zugangsdienstes MUSS jedem Nameserver SIS eine öffentliche IP-Adresse zuweisen.
[<=]

3.5 Registrierungsserver

3.5.1 Funktion

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

Der Registrierungsvorgang ist im Kapitel 5.3 dieses Dokuments funktional beschrieben.

3.5.2 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.
[<=]

3.5.3 Redundanz

Die hierfür geltenden Anforderungen zur Verfügbarkeit werden in [gemSpec_Perf#4.2] definiert.

3.5.4 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 konfigurieren, dass an der Schnittstelle zum Internet ausschließlich https-Anfragen akzeptiert werden.

[<=]

3.5.5 Adressierung

TIP1-A_4314 - VPN-Zugangsdienst, IPv4-Adressierung Registrierungsserver
Der Anbieter des VPN-Zugangsdienstes MUSS jedem Registrierungsserver mindestens eine öffentliche IPv4-Adresse zuweisen.

[<=]

3.6 Autorisierungsserver

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

3.6.1 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.
[<=]

3.6.2 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.
[<=]

3.6.3 Redundanz

Die hierfür geltenden Anforderungen zur Verfügbarkeit werden in [gemSpec_Perf#4.2] definiert.

3.6.4 Konfiguration

Der Autorisierungsserver nimmt Autorisierungsanfragen der VPN-Konzentratoren entgegen.

3.6.5 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.
[<=]

3.7 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.

3.7.1 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.
[<=]

3.7.2 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.
[<=]

3.7.3 Redundanz

Die hierfür geltenden Anforderungen zur Verfügbarkeit werden in [gemSpec_Perf#4.2] definiert.

3.7.4 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.
[<=]

3.7.5 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.
[<=]

3.8 http-Forwarder

3.8.1 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.

3.8.2 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.
[<=]

3.8.3 Redundanz

Die hierfür geltenden Anforderungen zur Verfügbarkeit werden in [gemSpec_Perf#4.2] definiert.

3.8.4 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.
[<=]

3.8.5 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.
[<=]

3.9 NTP-Server TI

3.9.1 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.
[<=]

3.9.2 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.
[<=]

3.9.3 Redundanz

Die hierfür geltenden Anforderungen zur Verfügbarkeit werden in [gemSpec_Perf#4.2] definiert.

3.9.4 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.

3.9.5 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.
[<=]

3.10 Secure Internet Service

3.10.1 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.

3.10.2 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.
[<=]

3.10.3 Redundanz

Die hierfür geltenden Anforderungen zur Verfügbarkeit werden in [gemSpec_Perf#4.2] definiert.

3.10.4 Konfiguration

TIP1-A_4480 - VPN-Zugangsdienst,
Der VPN-Zugangsdienst MUSS ermöglichen, dass die Sicherheitsleistungen des SIS anpassbar sind.
[<=]

A_13542 - VPN-Zugangsdienst, SIS ohne Proxy-Konfiguration
Der Anbieter des VPN-Zugangsdienstes MUSS ermöglichen, dass über SIS auch Systeme, die keine Proxy-Konfiguration zulassen, das Internet erreichen können.
[<=]

3.10.5 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.
[<=]

3.10.6 Informationen Funktionsmerkmale

A_18748 - Informationensbereitstellung Sicherheitsleistungen SIS
Der VPN-Zugangsdienstanbieter MUSS den Vertragspartnern, Leistungserbringern und Dienstleistern vor Ort Informationen zu den Sicherheitsleistungen des sicheren Internet Service (SIS) sowie deren Grenzen (z.B. Umgang mit verschlüsseltem Datenverkehr, freigeschaltete Ports, Leistung des Virenschutzes) transparent und verständlich bereitstellen.
[<=]

Mit diesen Informationen sollen die Vertragspartner in die Lage versetzt werden, die erforderlichen Sicherheitsmaßnahmen in der Leistungserbringerumgebung abstimmen zu können.

4 Übergreifende Festlegungen

4.1 Sicherheit

4.1.1 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.
[<=]

4.1.2 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_4340-01 - 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)
- ICMPv6 Destination Unreachable (Type 1, all Codes)
- ICMPv6 Packet to Big (Type 2)
- ICMPv6 Time Exceeded (Type 3, all Codes)
- ICMPv6 Parameter Problems (Type 4, all Codes)
- ICMPv6 Echo Request (Type 128)/Echo Response (Type 129)
- 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)

[<=]

4.1.3 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.

4.1.4 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)

[<=]

4.1.5 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.
[<=]

4.1.6 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.

[<=]

A_18733-01 - Prüfung zugelassener Produkte bei Verbindung zur TI
Der Anbieter VPN-Zugangsdienst MUSS über ein Service Request beim Anbieter Zentrale Plattformdienste auf Weisung der gematik prüfen, ob sich nicht-zugelassene Produkte (Konnektor, eHealth-Kartenterminal) zur TI verbinden.**[<=]**

Dafür wird dem jeweiligen VPN-Zugangsdienst vom Anbieter Zentrale Plattformdienste über ein Service Request eine Liste zur Verfügung gestellt, welche die Geräte und ihre IP-Adressen enthält, die nicht mehr zugelassen bzw. genehmigt sind.

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

A_18736 - Informationsinhalt an Leistungserbringer
Der Anbieter VPN-Zugangsdienst MUSS die über seinen Dienst angebundenen Leistungserbringer gemäß A_18734 schriftlich darauf hinweisen, die betroffene Hardware entsprechend der Zulassungsbeschränkung der gematik, zu aktualisieren oder auszutauschen.**[<=]**

Entsprechend der Bewertung der nicht-zugelassenen Produkte durch die gematik kann - nach Ablauf einer von der gematik gesetzten, angemessenen Frist - im Rahmen der betrieblichen Prozesse gemäß [gemKPT_Betr], [gemRL_Betr_TI] und [gemSpec_DS_Anbieter] durch einen technischen Mechanismus die (zeitweise) Sperrung / Deaktivierung der ContractID des Leistungserbringers im VPN-Zugangsdienst erfolgen.

A_18737 - ~~Sperrung von Zugägngen zur TI~~Sperrung von Zugängen zur TI
Der Anbieter VPN-Zugangsdienst MUSS nach Weisung der gematik Zugänge zur TI sperren.**[<=]**

A_18738 - Information an Leistungserbringer über Monitoring nach nicht-zugelassenen Komponenten
Der Anbieter VPN-Zugangsdienst MUSS Leistungserbringer, die er über seinen Dienst an die TI anbindet, vor dem ersten Abruf der Informationen über nicht-zugelassene Komponenten beim Anbieter Zentrale Plattformdienste, in verständlicher Form darüber informieren,

- dass der Anbieter VPN-Zugangsdienst vom Anbieter Zentrale Plattformdienste Informationen erhält, über die der Anbieter VPN-Zugangsdienst erkennt, ob die vom Leistungserbringer eingesetzten Konnektoren und Kartenterminals mit einer nicht-zugelassenen Software betrieben werden und

- zu welchem Zweck diese Informationen durch den Anbieter des VPN-Zugangsdienstes genutzt werden, insbesondere welche Prozesse vom Anbieter VPN-Zugangsdienst ausgeführt werden, falls nicht-zugelassene Komponenten oder Kartenterminals beim Leistungserbringer entdeckt werden.

[<=]

Es wird erwartet, dass die betroffenen Leistungserbringer oder ihre DVOs auf Grundlage der Mitteilung des VPN-Zugangsdienstes die jeweilige Firmware bzw. Geräte rechtzeitig aktualisieren bzw. aktualisieren lassen oder austauschen bzw. austauschen lassen.

4.2 Protokollanforderungen

4.2.1 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.
[<=]

Die nachfolgende Anforderung richtet sich an den VPN-Zugangsdienst und an die Konnektoren der Produkttypversionen 1 bis 3.

TIP1-A_4351 - VPN-Zugangsdienst und Konnektor (PTV 1 bis 3), 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.
[<=]

Die nächste Anforderung richtet sich an den VPN-Zugangsdienst und an die Konnektoren ab Produkttypversion 4.

A_17118 - VPN-Zugangsdienst und Konnektor (PTV 4 und höher), Verwendung erweiterter Sequenznummern
Der Konnektor und der VPN-Konzentrator des VPN-Zugangsdienstes MÜSSEN zum Schutz vor Replay-Attacken die Nutzung von Extended Sequence Numbers (ESN) aushandeln und verwenden.
[<=]

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.
[<=]

4.2.2 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 berechtigten Teilnehmer 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.
[<=]

4.2.3 Verschlüsselung

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

4.2.4 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.**[<=]**

A_13506 - VPN-Zugangsdienst, Liveness Check VPN-Konzentrator
Der VPN-Konzentrator MUSS in einem regelmäßigen Zeitintervall durch Liveness Check gemäß [RFC 7296] seine IPsec-Verbindungen überprüfen.**[<=]**

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.
[<=]

4.2.5 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.

A_17169 - VPN-Zugangsdienst, Fragmentierung der IKEv2-Nachrichten
Der VPN-Zugangsdienst, der IPv6 an den Netzwerkschnittstellen zum Transportnetz einsetzt, MUSS die Fragmentierung von IKEv2-Nachrichten gemäß [RFC7383] unterstützen.
[<=]

4.3 Netzanforderungen

4.3.1 Routing

4.3.1.1 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.
[<=]

4.3.1.2 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

4.3.2 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.
[<=]

4.3.2.1 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.
[<=]

4.3.2.2 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 berechtigten Teilnehmer 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 berechtigten Teilnehmers geführt, die miteinander nicht kommunizieren, und auf unterschiedlichen VPN-Konzentratoren terminiert.
- Es wäre eine Pflege der Bandbreiteneinstellungen pro berechtigtem Teilnehmer durch den VPN-Zugangsdienst erforderlich.

Es werden daher keine Anforderungen in diesem Bereich gestellt.

4.3.2.3 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.
[<=]

4.3.2.4 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.
[<=]

4.3.2.5 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.
[<=]

4.4 Einsatz von IPv6

Der VPN-Zugangsdienst muss für den Einsatz von IPv6 (Dual-Stack-Mode) die nachfolgenden Anforderungen umsetzen.

4.4.1 Nameserver Internet

A_17171 - VPN-Zugangsdienst, IPv6-Adressierung der Nameserver Internet
Der VPN Zugangsdienst MUSS jedem rekursiven Nameserver Internet eine öffentliche IPv6-Adresse zuweisen (Dual-Stack-Mode). Die IPv6-Adressen der Nameserver werden vom Anbieter des VPN-Zugangsdienstes zur Verfügung gestellt.
[<=]

A_17173 - VPN-Zugangsdienst, IPv6 Resource Records im Nameserver Internet
Der VPN Zugangsdienst MUSS in den autoritativen Nameservern Internet die weiteren Resource Records gemäß Tabelle Tab_ZD_Nameserver_Int_RR_IPv6 verwalten.

Tabelle 3: Tab_ZD_Nameserver_Int_RR_IPv6

Resource Record Bezeichner	Beschreibung
REGISTRIERUNGSSERVER_FQDN	AAAA Resource Records zur Namensauflösung des FQDN des Registrierungsservers in IPv6-Adressen
VPN_KONZENTRATOR_TI_FQDN	AAAA Resource Records zur Namensauflösung von FQDN der VPN-Konzentratoren TI in IPv6-Adressen
VPN_KONZENTRATOR_SIS_FQDN	AAAA Resource Records zur Namensauflösung von FQDN der VPN-Konzentratoren SIS in IPv6-Adressen

[<=]

4.4.2 Registrierungsserver

A_17180 - VPN-Zugangsdienst, IPv6-Adressierung Registrierungsserver
Der VPN-Zugangsdienst MUSS jedem Registrierungsserver eine öffentliche IPv6-Adresse zuweisen (Dual-Stack-Mode). Die öffentlichen IPv6-Adressen der Registrierungsserver werden vom Anbieter des VPN-Zugangsdienstes zur Verfügung gestellt.
[<=]

4.4.3 VPN-Konzentratoren TI und SIS

A_17181 - VPN-Zugangsdienst, IPv6-Adressierung der Internetschnittstellen der VPN-Konzentratoren
Der VPN-Zugangsdienst MUSS jedem VPN-Konzentrator TI und SIS eine IPv6-Adresse zuweisen (Dual-Stack-Mode). Diese Adresse wird auf der physischen Schnittstelle zum Internet konfiguriert. Die öffentlichen IPv6-Adressen der VPN-Konzentratoren TI und SIS

werden vom Anbieter des VPN-Zugangsdienstes zur Verfügung gestellt.
[<=]

5 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 4: 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.

5.1 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 5: 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

[<=]

5.1.1 Operation connect

5.1.1.1 Umsetzung

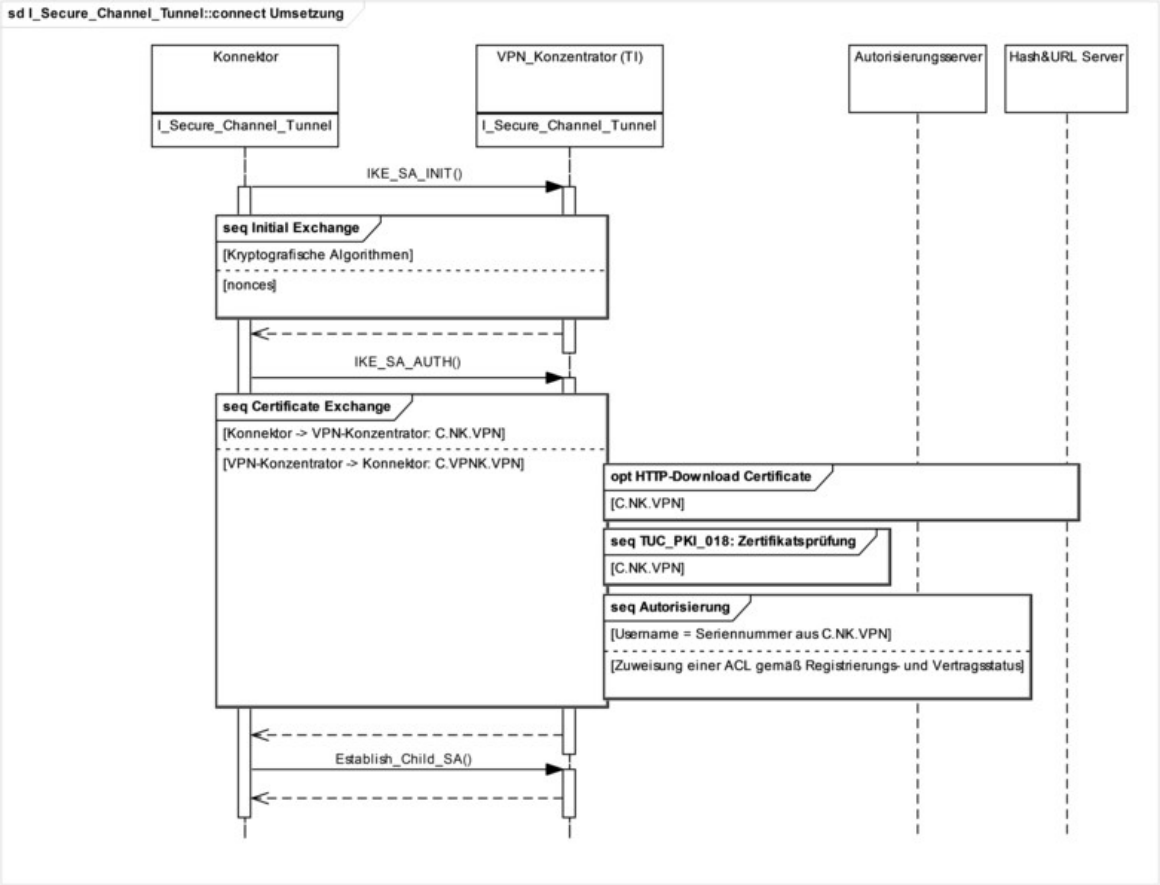

Abbildung 4: Ablauf der Operation I_Secure_Channel_Tunnel::connect im VPN-Zugangsdienst

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.

[<=]

5.1.1.2 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 6: 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] 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 der Verbindungsaufbau abgebrochen und es wird die nächste IP-Adresse aus der Liste der VPN-Konzentratoren angesprochen. • 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 TI verbunden.	
Fehlerfälle	Zur Behandlung auftretender Fehlerfälle werden Fehlermeldungen gemäß [RFC 7296] verwendet.	

[<=]

5.1.1.3 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.
[<=]

5.1.1.4 Adressierung

Es muss sichergestellt sein, dass keine Profilbildung in der TI durch Identifikation anhand der IP-Adresse des berechtigten Teilnehmers 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.
[<=]

5.1.2 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.
[<=]

5.1.3 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.

5.2 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 7: 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

[<=]

5.2.1 Operation connect

5.2.1.1 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.

[<=]

5.2.1.2 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 8: 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-Nameserver DNS_SERVERS_INT mit den DNS_SERVERS_SIS überschrieben. Wenn die Verbindung zum VPN-Konzentrator SIS abgebaut wurde, müssen die Ziel-Nameserver 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] 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 der Verbindungsaufbau abgebrochen und es wird die nächste IP-Adresse aus der Liste der VPN-Konzentratoren angesprochen. • 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.	

[<=]

5.2.2 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.
[<=]

5.3 Schnittstelle I_Registration_Service

Im Rahmen der ~~Laufzeitverlängerung der gSMC-K der Konnektoren~~ ECC-Migration können sich Konnektoren über die vorhandene Schnittstelle I_Registration_Service ~~automatisiert~~ mit einem ~~erneuerten~~ECC basierten Zertifikat C.NK.VPN gemäß [gemSpec_Kon#TUC_KON_411] erneut registrieren.

TIP1-A_5118-01 - 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 9: 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.

	sendData	Diese Operation ermöglicht es Daten (z.B. Betriebsdaten) an den Registrierungsdienst zu senden

[<=]

Der Registrierungsserver muss die kryptographischen Anforderungen aus [gemSpec_Krypt] erfüllen. Abweichend dazu gilt für den Registrierungsserver die folgende Anforderung.

A_14646 - VPN-Zugangsdienst, kryptographischen Vorgaben für den Registrierungsserver
Der VPN-Zugangsdienst DARF bei der Signaturprüfung der SOAP-Requests der Operationen registerKonnektor und deregisterKonnektor NICHT XAdES-spezifische Signatureigenschaften voraussetzen.**[<=]**

A_17288 - VPN-Zugangsdienst, Unterstützung der kryptographischen Vorgaben
Der VPN-Zugangsdienst MUSS die kryptografischen Vorgaben für ECC-basierte und RSA-basierte Signaturverfahren gemäß [gemSpec_Krypt] unterstützen.
[<=]

5.3.1 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 10: 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 berechtigten Teilnehmers 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 C.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 berechtigten Teilnehmer 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.

A_14623 - VPN-Zugangsdienst, Zeichensatz der ContractID
Der VPN-Zugangsdienst MUSS die ContractID ausschließlich aus folgender Teilmenge des ASCII-Zeichensatzes bilden:

- ABCDEFGHIJKLMNOPQRSTUVWXYZ
- abcdefghijklmnopqrstuvwxyz
- 0123456789
- %()=!?+-*/#_@:.

[<=]

TIP1-A_5074 - VPN-Zugangsdienst, Einhaltung des Datenschutzes bei Protokollierung
Der Anbieter des VPN-Zugangsdienstes MUSS unter Berücksichtigung des Art. 25 Abs. 2 DSGVO 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.
[<=]

A_22543 - VPN-Zugangsdienst, Anzahl der Zertifikate pro ContractID im Registrierungsserver
Der VPN-Zugangsdienst MUSS die Registrierung von mindestens zwei Zertifikaten eines Konnektors pro ContractID unterstützen.**[<=]**

5.3.1.1 Umsetzung

An die Umsetzung der Schnittstelle werden keine zusätzlichen Anforderungen gestellt.

5.3.1.2 Nutzung

An die Nutzung der Schnittstelle werden keine zusätzlichen Anforderungen gestellt.

5.3.2 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 11: 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 berechtigten Teilnehmer 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	

[<=]

5.3.2.1 Umsetzung

An die Umsetzung der Schnittstelle werden keine zusätzlichen Anforderungen gestellt.

5.3.2.2 Nutzung

An die Nutzung der Schnittstelle werden keine zusätzlichen Anforderungen gestellt.

5.3.3 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 12: 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 berechtigten Teilnehmer mitteilen möchte.
Zustand nach erfolgreichem Ablauf	Keine Änderung	
Zustand nach fehlerhaftem Ablauf	Keine Änderung	
Nichtfunktionale Eigenschaften	Keine	

[<=]

5.3.3.1 Umsetzung

An die Umsetzung der Schnittstelle werden keine zusätzlichen Anforderungen gestellt.

5.3.3.2 Nutzung

An die Nutzung der Schnittstelle werden keine zusätzlichen Anforderungen gestellt.

5.3.4 Operation sendData

A_21159-01~~A_21159~~ - VPN-Zugangsdienst, Operation sendData
Der VPN-Zugangsdienst MUSS an der Schnittstelle I_Registration_Service die Operation sendData gemäß Tabelle Tab_ZD_sendData anbieten**.**

Tabelle 13: Tab_ZD_sendData

Name	sendData	
Beschreibung	Diese Operation ermöglicht es Daten (z.B. Betriebsdaten) an den Registrierungsdienst zu senden	
Vorbedingungen	• Die URL des Registrierungsdienstes ist bekannt. • Der FQDN des Registrierungsservers TI wurde in IP-Adressen aufgelöst.	
Aufrufparameter	Name	Beschreibung
	SOAP-Request „sendDataRequest"	Dies ist ein SOAP-Request „sendDataRequest" gemäß ProvisioningService.xsd. Dabei gilt:

		• Das Element vpnk:Type enthält den Typ der Daten. • Das Element vpnk:Base64Date enthält die base64-kodierten Daten.
Standardablauf	Aktion	Beschreibung
	Operation sendData des Registrierungsdienstes aufrufen	Der Client ruft den Dienst regService(sendDataPort) des VPN-Zugangsdienstes, mit der SOAP-Operation sendData(sendDataRequest) 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 ~~der zur Registrierung verwendeten~~einer beliebigen 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 dekodierten Base64Data entsprechen dem MimeType. • Bei MimeType text/xml wird eine Schemaprüfung durchgeführt. Sind die gesendeten Daten vom Type OperatingDataConnector, so erfolgt die Schemaprüfung gegen das Schema conn/OperatingData.xsd. Wenn die Prüfung erfolgreich war, wird im Standardablauf fortgefahren. Anderenfalls wird eine Fehlermeldung generiert (siehe Abschnitt Fehler).
	OperatingDataConnector auffüllen	Sind die gesendeten Daten vom Type OperatingDataConnector, so sind die OperatingSiteExtension gemäß Schema

		conn/OperatingData.xsd auszufüllen und die Daten abzuspeichern.
	SOAP-Response „sendDataResponse" erzeugen	Der Registrierungsserver des VPN-Zugangsdienstes erzeugt eine SOAP-Response „sendDataResponse" gemäß ProvisioningService.xsd.
	SOAP-Response „sendData" an den Client senden	Der Registrierungsserver des VPN-Zugangsdienstes sendet die SOAP-Response (sendDataResponse) an den Konnektor gemäß ProvisioningService.wsdl.
Rückgabe	Name	Beschreibung
	SOAP-Response „sendDataResponse"	Dies ist eine SOAP-Response „sendDataResponse" gemäß ProvisioningService.xsd. Dabei gilt für einen erfolgreichen sendData Request: • Das Element vpnk:Timestamp enthält den aktuellen Erstellungszeitstempel der SOAP-Response.
Zustand nach erfolgreichem Ablauf	Keine Änderung	
Zustand nach fehlerhaftem Ablauf	Keine Änderung	
Nichtfunktionale Eigenschaften	Keine	

[<=]

A_21611 - Information des Konnektorbetreibers auf Grund von Betriebsdaten
Der VPN-Zugangsdienst MUSS den Betreiber eines angeschlossenen Konnektors innerhalb von einer Woche informieren, wenn die vom Konnektor übermittelten Betriebsdaten ergeben, dass:

- die Produkttypversion des Konnektors nicht mehr zugelassen ist
- für seinen Konnektor eine neue Firmewareversion auf dem KSR vorliegt, die vom Konnektor nicht automatisch installiert wird
- an den Konnektor Kartenterminals angeschlossen sind, die nicht mehr zugelassen sind

[<=]

A_21161 - Bereitstellung öffentlicher IP-Adressen
Der VPN-Zugangsdienst bzw. der VPN-Zugangsdienst Anbieter MUSS im Rahmen des Security Monitorings entsprechend gemSpec_DS_Anbieter#A_20720 täglich die öffentlichen IP-Adressen seiner Kunden übermitteln. Die öffentlichen IP-Adressen sind separat zu den Betriebsdaten und ohne Verbindung zu anderen personenbezogenen und/oder personenbeziehbaren Daten zu übermitteln.**[<=]**

A_21339-01 - Löschung von Betriebsdaten
Der VPN-Zugangsdienst MUSS die empfangenen Betriebsdaten nach spätestens 6 Wochen löschen. Zusammengefasste Auswertungen sind von der Löschpflicht nicht betroffen. Betriebsdaten, die für die Pflichten des Zugangsdienstes nach A_21611 nicht notwendig sind, MÜSSEN unverzüglich nach Übertragung an die gematik gelöscht werden.
[<=]

A_21612 - Betriebsdaten: Zweckbindung und Weiterleitung
Der VPN-Zugangsdienst DARF die Betriebsdaten NICHT für andere Zwecke verwenden, als in gemKPT_Betriebsdaten_Kon definiert. Der VPN-Zugangsdienst DARF die Betriebsdaten NICHT an jemanden anderen weitegeben, als die gematik.**[<=]**

A_21160-01 - Bereitstellung von Betriebsdaten
Der VPN-Zugangsdienst MUSS die vom Konnektor erhaltenen Betriebsdaten, reduziert um die ContractID und den UpdateMode und ergänzt um die Betriebsstättenart, an die Betriebsdatenerfassung gemäß gemSpec_SST_LD_BD an die Schnittstelle I_OpsData_Update übermitteln.
[<=]

A_22510 - VPN-Zugangsdienst: Bereitstellung der Betriebsstättenart
Der VPN-Zugangsdienst Anbieter MUSS die Betriebsstättenart und Contract-ID seiner Kunden an den Betreiber VPN-Zugangsdienst übermitteln.
Änderungen MÜSSEN quartalsweise an den Betreiber VPN-Zugangsdienst übermittelt werden.**[<=]**

5.3.5 Registrierungsserver Fehlermeldungen

TIP1-A_4491-03~~TIP1-A_4491-02~~ - VPN-Zugangsdienst, Registrierungsserver Fehlermeldungen
Der Registrierungsserver des VPN-Zugangsdienstes und der Konnektor MÜSSEN für die Operationen registerKonnektor, deregisterKonnektor ~~und~~ , registerStatus und sendData die Fehlermeldungen gemäß Tabelle Tab_Registrierungsserver_Fehlermeldungen implementieren.

Tabelle 14: 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	Technical	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	Technical	Error	Eintragung der Registrierung im Autorisierungsserver fehlgeschlagen	siehe Text
7081	Technical	Error	Deregistrierung im Autorisierungsserver fehlgeschlagen	siehe Text
7091	Technical	Error	Dokument nicht schemakonform	siehe Text

Weitere Elemente der Fehlermeldung müssen wie folgt angegeben werden:
CompType = VPN-Zugangsdienst**[<=]**

5.4 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-Zugangsdienstes 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.

5.5 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.

5.6 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.

5.7 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.

5.8 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.
[<=]

5.9 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 berechtigten Teilnehmern 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 berechtigtem Teilnehmer 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 berechtigten Teilnehmer übergeben.

Tabelle 15: 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 berechtigten Teilnehmer ermöglicht.

[<=]

6 Anhang A – Verzeichnisse

6.1 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
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

6.2 Glossar

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

6.3 Abbildungsverzeichnis

6.4 Tabellenverzeichnis

6.5 Referenzierte Dokumente

6.5.1 Dokumente der gematik

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

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

6.5.2 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~~https://tools.ietf.org/html/rfc7296
[W3C XML-DSig]	W3C (10.06.2008): XML Signature Syntax and Processing (Second Edition)
[RFC7383]	RFC 7383 (November 2014): Internet Key Exchange Protocol Version 2 (IKEv2) Message Fragmentation https://tools.ietf.org/html/rfc7383