

Beim vorliegenden Dokument handelt es sich um einen Entwurf der gematik in Vorbereitung auf zukünftige normative Festlegungen als Grundlage entsprechender Zulassungs- und Bestätigungsverfahren. Die gematik veröffentlicht diesen Entwurf mit dem Ziel, dass sich Interessierte bereits frühzeitig einen Überblick über die mögliche Weiterentwicklung der Telematikinfrastruktur verschaffen können. Die gematik übernimmt keine Gewähr für die Aktualität, Richtigkeit und Vollständigkeit dieses Entwurfes und behält sich das Recht vor, ohne vorherige Ankündigung Änderungen oder Ergänzungen vorzunehmen oder von den Regelungen insgesamt bzw. teilweise Abstand zu nehmen.

## Elektronische Gesundheitskarte und Telematikinfrastruktur

# Spezifikation VPN-Zugangsdienst

Version: 1.1516.0 CC  
Revision: 199243306132  
Stand: 02.0309.12.2020  
Status: zur Abstimmung freigegeben  
Klassifizierung: öffentlich\_Entwurf  
Referenzierung: gemSpec\_VPN\_ZugD

23

## Dokumentinformationen

### Änderungen zur Vorversion

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

27

### 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
1.15.16.0	<del>02.03.20</del> 09.12.20		<del>freigegeben</del> Einarbeitung lt. Änderungsliste 22.5	gematik

## Inhaltsverzeichnis

<b>1 Einordnung des Dokumentes</b>	<b>11</b>
1.1 Zielsetzung	11
1.2 Zielgruppe	11
1.3 Geltungsbereich	11
1.4 Abgrenzung	11
1.5 Methodik	12
<b>2 Systemüberblick</b>	<b>13</b>
2.1 Funktion	13
2.2 Netzaufbau	13
<b>3 Zerlegung des Produkttyps</b>	<b>15</b>
<b>3.1 VPN-Konzentratoren</b>	<b>16</b>
3.1.1 Funktion	16
3.1.2 Topologie	17
3.1.3 Standorte des VPN-Zugangsdienstes	17
3.1.4 Anbindung an das Transportnetz Internet	18
3.1.5 Anbindung an die TI	18
3.1.6 Anbindung an den SIS	19
3.1.7 Service-Zone des Standortes TI	19
3.1.8 Redundanz	19
3.1.9 Konfiguration	20
3.1.10 Adressierung	21
3.1.10.1 VPN-Konzentratoren zum Transportnetz Internet	21
3.1.10.2 VPN-Konzentratoren TI zum Zentralen Netz	21
3.1.10.3 VPN-Konzentratoren SIS zum Internet	21
3.1.11 DNS	21
3.1.12 Performance	22
<b>3.2 Nameserver Internet</b>	<b>23</b>
3.2.1 Funktion	23
3.2.2 Verteilung	23
3.2.3 Redundanz	24
3.2.4 Konfiguration	24
3.2.5 Adressierung	26
<b>3.3 Nameserver TI</b>	<b>26</b>
3.3.1 Funktion	26
3.3.2 Verteilung	26
3.3.3 Redundanz	26
3.3.4 Konfiguration	26
3.3.5 Adressierung	27
<b>3.4 Nameserver SIS</b>	<b>27</b>
3.4.1 Funktion	27
3.4.2 Verteilung	27
3.4.3 Redundanz	27

73	3.4.4 Konfiguration .....	27
74	3.4.5 Adressierung .....	28
75	<b>3.5 Registrierungsserver .....</b>	<b>28</b>
76	3.5.1 Funktion .....	28
77	3.5.2 Verteilung .....	28
78	3.5.3 Redundanz .....	28
79	3.5.4 Konfiguration .....	28
80	3.5.5 Adressierung .....	28
81	<b>3.6 Autorisierungsserver .....</b>	<b>29</b>
82	3.6.1 Funktion .....	29
83	3.6.2 Verteilung .....	30
84	3.6.3 Redundanz .....	30
85	3.6.4 Konfiguration .....	30
86	3.6.5 Adressierung .....	30
87	<b>3.7 hash&amp;URL-Server .....</b>	<b>30</b>
88	3.7.1 Funktion .....	30
89	3.7.2 Verteilung .....	31
90	3.7.3 Redundanz .....	31
91	3.7.4 Konfiguration .....	31
92	3.7.5 Adressierung .....	31
93	<b>3.8 http-Forwarder .....</b>	<b>31</b>
94	3.8.1 Funktion .....	31
95	3.8.2 Verteilung .....	32
96	3.8.3 Redundanz .....	32
97	3.8.4 Konfiguration .....	32
98	3.8.5 Adressierung .....	32
99	<b>3.9 NTP-Server TI .....</b>	<b>32</b>
100	3.9.1 Funktion .....	32
101	3.9.2 Verteilung .....	33
102	3.9.3 Redundanz .....	33
103	3.9.4 Konfiguration .....	33
104	3.9.5 Adressierung .....	34
105	<b>3.10 Secure Internet Service .....</b>	<b>34</b>
106	3.10.1 Funktion .....	34
107	3.10.2 Verteilung .....	34
108	3.10.3 Redundanz .....	34
109	3.10.4 Konfiguration .....	34
110	3.10.5 Adressierung .....	34
111	3.10.6 Informationen Funktionsmerkmale .....	35
112	<b>4 Übergreifende Festlegungen .....</b>	<b>36</b>
113	<b>4.1 Sicherheit .....</b>	<b>36</b>
114	4.1.1 Kommunikation zwischen Service-Zonen und Zugangszonen .....	36
115	4.1.2 Übergang der VPN-Konzentratoren zum Transportnetz Internet .....	36
116	4.1.3 Übergang der VPN-Konzentratoren zur TI .....	38
117	4.1.4 Sicherheitsleistung des Secure Internet Service .....	38
118	4.1.5 Kommunikation zwischen Konnektoren .....	39
119	4.1.6 Durchsetzung der Zugangsberechtigung .....	39
120	<b>4.2 Protokollanforderungen .....</b>	<b>41</b>
121	4.2.1 IPsec .....	41

122	4.2.2 IKEv2.....	42
123	4.2.3 Verschlüsselung.....	42
124	4.2.4 Verbindungszustand.....	42
125	4.2.5 Fragmentierung von IKE-Paketen.....	43
126	<b>4.3 Netzanforderungen.....</b>	<b>43</b>
127	4.3.1 Routing.....	43
128	4.3.1.1 VPN-Zugangsdienst.....	43
129	4.3.1.2 Konnektor.....	44
130	4.3.2 Behandlung gemäß DiffServ-Architektur.....	44
131	4.3.2.1 VPN-Konzentratoren zum Transportnetz Internet.....	44
132	4.3.2.2 VPN-Konzentratoren zu Konnektoren.....	45
133	4.3.2.3 VPN-Zugangsdienst zur TI.....	45
134	4.3.2.4 Alternatives Zugangsnetz.....	45
135	4.3.2.5 SIS zum Internet.....	45
136	<b>4.4 Einsatz von IPv6.....</b>	<b>46</b>
137	4.4.1 Nameserver Internet.....	46
138	4.4.2 Registrierungsserver.....	46
139	4.4.3 VPN-Konzentratoren TI und SIS.....	46
140	<b>5 Funktionsmerkmale.....</b>	<b>48</b>
141	<b>5.1 Schnittstelle I_Secure_Channel_Tunnel.....</b>	<b>49</b>
142	5.1.1 Operation connect.....	50
143	5.1.1.1 Umsetzung.....	50
144	5.1.1.2 Nutzung.....	51
145	5.1.1.3 Verbindungsaufbau.....	55
146	5.1.1.4 Adressierung.....	55
147	5.1.2 Operation disconnect.....	55
148	5.1.3 Operation send_secure_IP_Packet.....	56
149	<b>5.2 Schnittstelle I_Secure_Internet_Tunnel.....</b>	<b>56</b>
150	5.2.1 Operation connect.....	56
151	5.2.1.1 Umsetzung.....	56
152	5.2.1.2 Nutzung.....	57
153	5.2.2 Operation disconnect.....	61
154	<b>5.3 Schnittstelle I_Registration_Service.....</b>	<b>61</b>
155	5.3.1 Operation registerKonnektor.....	62
156	5.3.1.1 Umsetzung.....	66
157	5.3.1.2 Nutzung.....	67
158	5.3.2 Operation deregisterKonnektor.....	67
159	5.3.2.1 Umsetzung.....	70
160	5.3.2.2 Nutzung.....	70
161	5.3.3 Operation registerStatus.....	70
162	5.3.3.1 Umsetzung.....	73
163	5.3.3.2 Nutzung.....	73
164	5.3.4 Registrierungsserver Fehlermeldungen.....	75
165	<b>5.4 Schnittstelle I_DNS_Name_Resolution (Namensraum TI).....</b>	<b>76</b>
166	<b>5.5 Schnittstelle I_DNS_Name_Resolution (Namensraum Internet).....</b>	<b>77</b>
167	<b>5.6 Schnittstelle I_DNS_Name_Resolution (Namensraum SIS).....</b>	<b>77</b>
168	<b>5.7 Schnittstelle I_NTP_Time_Information.....</b>	<b>77</b>
169	<b>5.8 Prozess Änderung der Sicherheitsleistungen des SIS.....</b>	<b>77</b>

170	<del>5.9 Prozess zum Abschluss, Ändern und Auflösen des Vertragsverhältnisses</del>	<del>77</del>
171	<b>6 Anhang A Verzeichnisse</b>	<b>79</b>
172	6.1 Abkürzungen	79
173	6.2 Glossar	83
174	6.3 Abbildungsverzeichnis	83
175	6.4 Tabellenverzeichnis	83
176	6.5 Referenzierte Dokumente	84
177	6.5.1 Dokumente der gematik	84
178	6.5.2 Weitere Dokumente	85
179	<b>1 Einordnung des Dokumentes</b>	<b>11</b>
180	1.1 Zielsetzung	11
181	1.2 Zielgruppe	11
182	1.3 Geltungsbereich	11
183	1.4 Abgrenzung	11
184	1.5 Methodik	12
185	<b>2 Systemüberblick</b>	<b>13</b>
186	2.1 Funktion	13
187	2.2 Netzaufbau	13
188	<b>3 Zerlegung des Produkttyps</b>	<b>15</b>
189	3.1 VPN-Konzentratoren	16
190	3.1.1 Funktion	16
191	3.1.2 Topologie	17
192	3.1.3 Standorte des VPN-Zugangsdienstes	17
193	3.1.4 Anbindung an das Transportnetz Internet	18
194	3.1.5 Anbindung an die TI	18
195	3.1.6 Anbindung an den SIS	19
196	3.1.7 Service-Zone des Standortes TI	19
197	3.1.8 Redundanz	19
198	3.1.9 Konfiguration	20
199	3.1.10 Adressierung	21
200	3.1.10.1 VPN-Konzentratoren zum Transportnetz Internet	21
201	3.1.10.2 VPN-Konzentratoren TI zum Zentralen Netz	21
202	3.1.10.3 VPN-Konzentratoren SIS zum Internet	21
203	3.1.11 DNS	21
204	3.1.12 Performance	22
205	3.2 Nameserver Internet	23
206	3.2.1 Funktion	23
207	3.2.2 Verteilung	23
208	3.2.3 Redundanz	24
209	3.2.4 Konfiguration	24
210	3.2.5 Adressierung	26
211	3.3 Nameserver TI	26

212	3.3.1 Funktion .....	26
213	3.3.2 Verteilung .....	26
214	3.3.3 Redundanz .....	26
215	3.3.4 Konfiguration .....	26
216	3.3.5 Adressierung .....	27
217	<b>3.4 Nameserver SIS .....</b>	<b>27</b>
218	3.4.1 Funktion .....	27
219	3.4.2 Verteilung .....	27
220	3.4.3 Redundanz .....	27
221	3.4.4 Konfiguration .....	27
222	3.4.5 Adressierung .....	28
223	<b>3.5 Registrierungsserver .....</b>	<b>28</b>
224	3.5.1 Funktion .....	28
225	3.5.2 Verteilung .....	28
226	3.5.3 Redundanz .....	28
227	3.5.4 Konfiguration .....	28
228	3.5.5 Adressierung .....	28
229	<b>3.6 Autorisierungsserver .....</b>	<b>29</b>
230	3.6.1 Funktion .....	29
231	3.6.2 Verteilung .....	30
232	3.6.3 Redundanz .....	30
233	3.6.4 Konfiguration .....	30
234	3.6.5 Adressierung .....	30
235	<b>3.7 hash&amp;URL-Server .....</b>	<b>30</b>
236	3.7.1 Funktion .....	30
237	3.7.2 Verteilung .....	31
238	3.7.3 Redundanz .....	31
239	3.7.4 Konfiguration .....	31
240	3.7.5 Adressierung .....	31
241	<b>3.8 http-Forwarder .....</b>	<b>31</b>
242	3.8.1 Funktion .....	31
243	3.8.2 Verteilung .....	32
244	3.8.3 Redundanz .....	32
245	3.8.4 Konfiguration .....	32
246	3.8.5 Adressierung .....	32
247	<b>3.9 NTP-Server TI .....</b>	<b>32</b>
248	3.9.1 Funktion .....	32
249	3.9.2 Verteilung .....	33
250	3.9.3 Redundanz .....	33
251	3.9.4 Konfiguration .....	33
252	3.9.5 Adressierung .....	34
253	<b>3.10 Secure Internet Service .....</b>	<b>34</b>
254	3.10.1 Funktion .....	34
255	3.10.2 Verteilung .....	34
256	3.10.3 Redundanz .....	34
257	3.10.4 Konfiguration .....	34
258	3.10.5 Adressierung .....	34
259	3.10.6 Informationen Funktionsmerkmale .....	35
260	<b>4 Übergreifende Festlegungen .....</b>	<b>36</b>



261	<b>4.1 Sicherheit .....</b>	<b>36</b>
262	4.1.1 Kommunikation zwischen Service-Zonen und Zugangszonen .....	36
263	4.1.2 Übergang der VPN-Konzentratoren zum Transportnetz Internet .....	36
264	4.1.3 Übergang der VPN-Konzentratoren zur TI .....	38
265	4.1.4 Sicherheitsleistung des Secure Internet Service .....	38
266	4.1.5 Kommunikation zwischen Konnektoren .....	39
267	4.1.6 Durchsetzung der Zugangsberechtigung .....	39
268	<b>4.2 Protokollanforderungen .....</b>	<b>41</b>
269	4.2.1 IPsec .....	41
270	4.2.2 IKEv2 .....	42
271	4.2.3 Verschlüsselung .....	42
272	4.2.4 Verbindungszustand .....	42
273	4.2.5 Fragmentierung von IKE-Paketen .....	43
274	<b>4.3 Netzanforderungen .....</b>	<b>43</b>
275	4.3.1 Routing .....	43
276	4.3.1.1 VPN-Zugangsdienst .....	43
277	4.3.1.2 Konnektor .....	44
278	4.3.2 Behandlung gemäß DiffServ-Architektur .....	44
279	4.3.2.1 VPN-Konzentratoren zum Transportnetz Internet .....	44
280	4.3.2.2 VPN-Konzentratoren zu Konnektoren .....	45
281	4.3.2.3 VPN-Zugangsdienst zur TI .....	45
282	4.3.2.4 Alternatives Zugangsnetz .....	45
283	4.3.2.5 SIS zum Internet .....	45
284	<b>4.4 Einsatz von IPv6 .....</b>	<b>46</b>
285	4.4.1 Nameserver Internet .....	46
286	4.4.2 Registrierungsserver .....	46
287	4.4.3 VPN-Konzentratoren TI und SIS .....	46
288	<b>5 Funktionsmerkmale .....</b>	<b>48</b>
289	<b>5.1 Schnittstelle I_Secure_Channel_Tunnel .....</b>	<b>49</b>
290	5.1.1 Operation connect .....	50
291	5.1.1.1 Umsetzung .....	50
292	5.1.1.2 Nutzung .....	51
293	5.1.1.3 Verbindungsaufbau .....	55
294	5.1.1.4 Adressierung .....	55
295	5.1.2 Operation disconnect .....	55
296	5.1.3 Operation send_secure_IP_Packet .....	56
297	<b>5.2 Schnittstelle I_Secure_Internet_Tunnel .....</b>	<b>56</b>
298	5.2.1 Operation connect .....	56
299	5.2.1.1 Umsetzung .....	56
300	5.2.1.2 Nutzung .....	57
301	5.2.2 Operation disconnect .....	61
302	<b>5.3 Schnittstelle I_Registration_Service .....</b>	<b>61</b>
303	5.3.1 Operation registerKonnektor .....	62
304	5.3.1.1 Umsetzung .....	66
305	5.3.1.2 Nutzung .....	67
306	5.3.2 Operation deregisterKonnektor .....	67
307	5.3.2.1 Umsetzung .....	70
308	5.3.2.2 Nutzung .....	70
309	5.3.3 Operation registerStatus .....	70
310	5.3.3.1 Umsetzung .....	73

§11	5.3.3.2 Nutzung.....	73
§12	5.3.4 Operation sendData.....	73
§13	5.3.5 Registrierungsserver Fehlermeldungen.....	75
§14	<b>5.4 Schnittstelle I_DNS_Name_Resolution (Namensraum TI).....</b>	<b>76</b>
§15	<b>5.5 Schnittstelle I_DNS_Name_Resolution (Namensraum Internet).....</b>	<b>77</b>
§16	<b>5.6 Schnittstelle I_DNS_Name_Resolution (Namensraum SIS).....</b>	<b>77</b>
§17	<b>5.7 Schnittstelle I_NTP_Time_Information .....</b>	<b>77</b>
§18	<b>5.8 Prozess Änderung der Sicherheitsleistungen des SIS.....</b>	<b>77</b>
§19	<b>5.9 Prozess zum Abschluss, Ändern und Auflösen des Vertragsverhältnisses.....</b>	<b>77</b>
§20	<b>6 Anhang A – Verzeichnisse.....</b>	<b>79</b>
§21	<b>6.1 Abkürzungen .....</b>	<b>79</b>
§22	<b>6.2 Glossar .....</b>	<b>83</b>
§23	<b>6.3 Abbildungsverzeichnis.....</b>	<b>83</b>
§24	<b>6.4 Tabellenverzeichnis.....</b>	<b>83</b>
§25	<b>6.5 Referenzierte Dokumente.....</b>	<b>84</b>
§26	6.5.1 Dokumente der gematik.....	84
§27	6.5.2 Weitere Dokumente.....	85

---

## 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.

361 **1.5 Methodik**

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

366 Sie werden im Dokument wie folgt dargestellt:

367 **<AFO-ID> - <Titel der Afo>**

368 Text / Beschreibung

369 [**<=**]

370

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

ENTWURF

373

---

## 2 Systemüberblick

---

### 2.1 Funktion

Der VPN-Zugangsdienst ermöglicht den berechtigten Teilnehmern den Zugang zur Telematikinfrastruktur (TI) und zum Secure Internet Service (SIS). Für berechnigte 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.

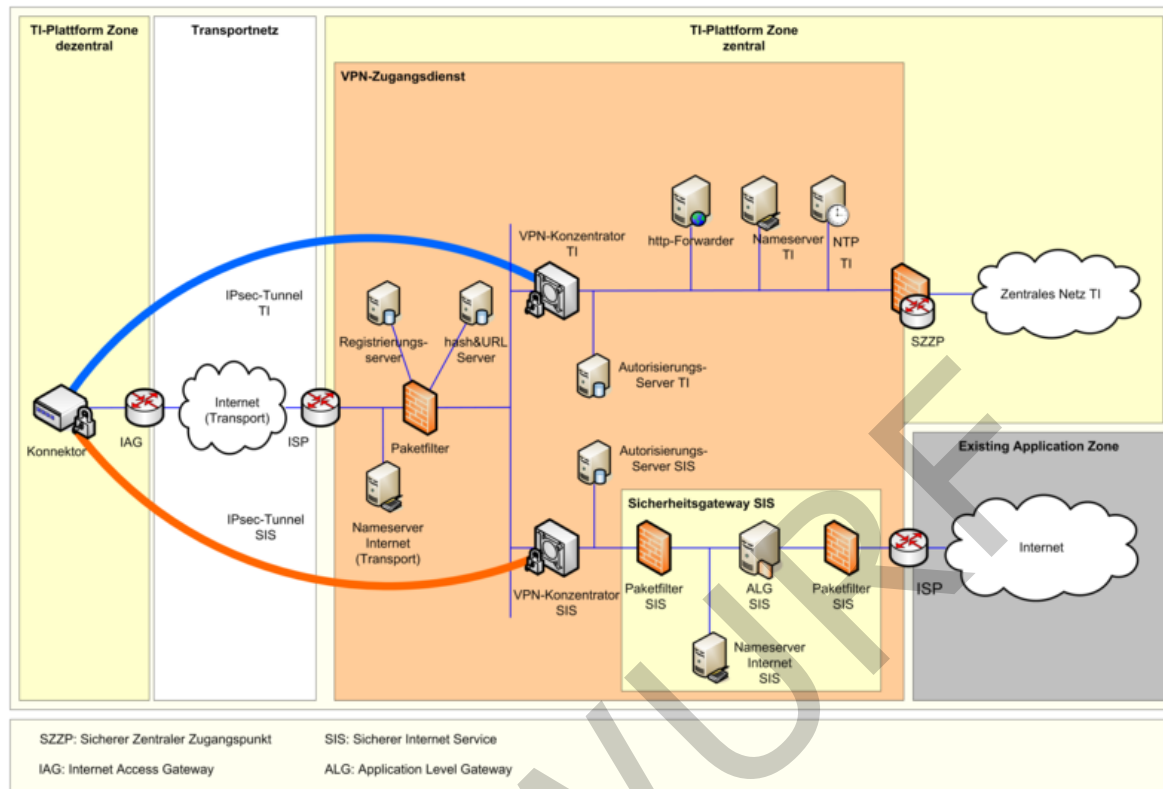
### 2.2 Netzaufbau

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.

399



**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.

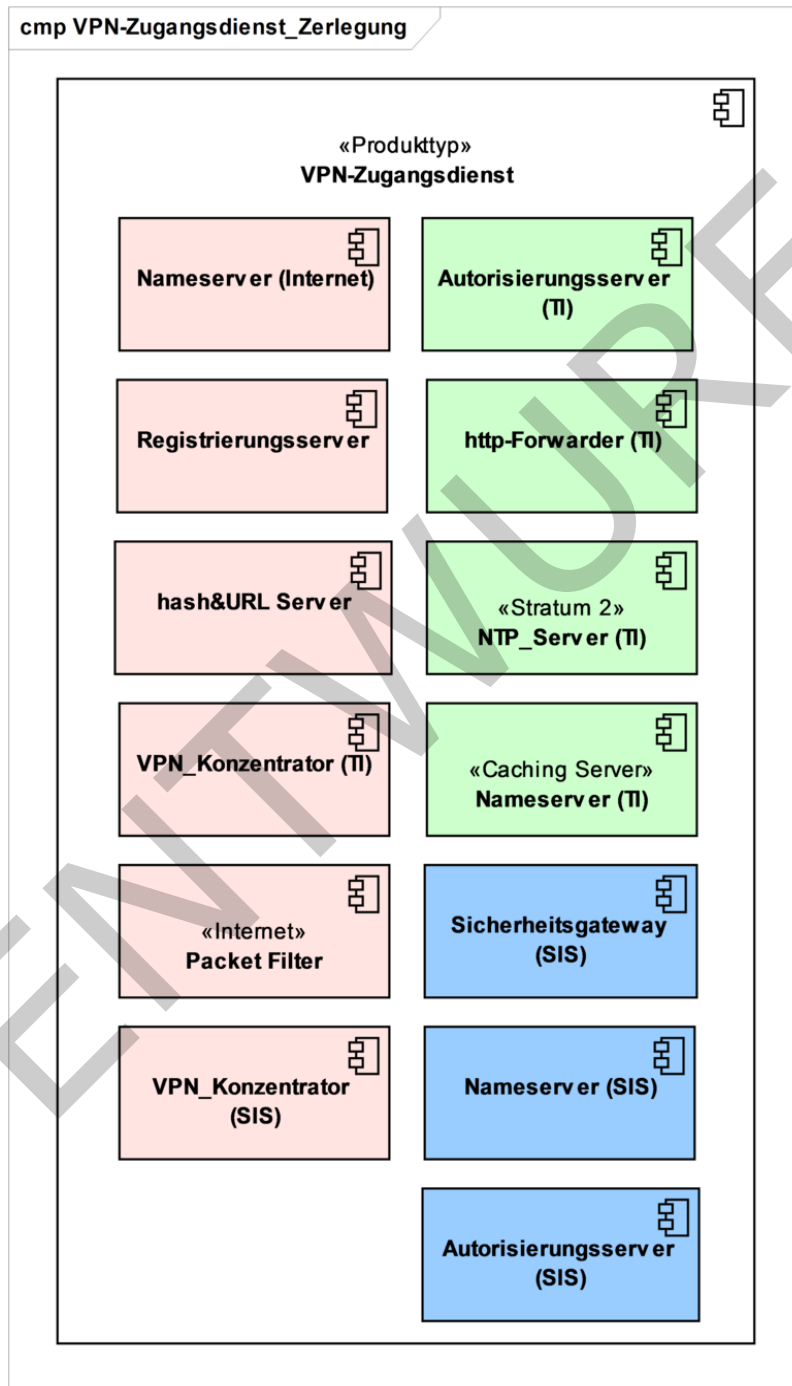
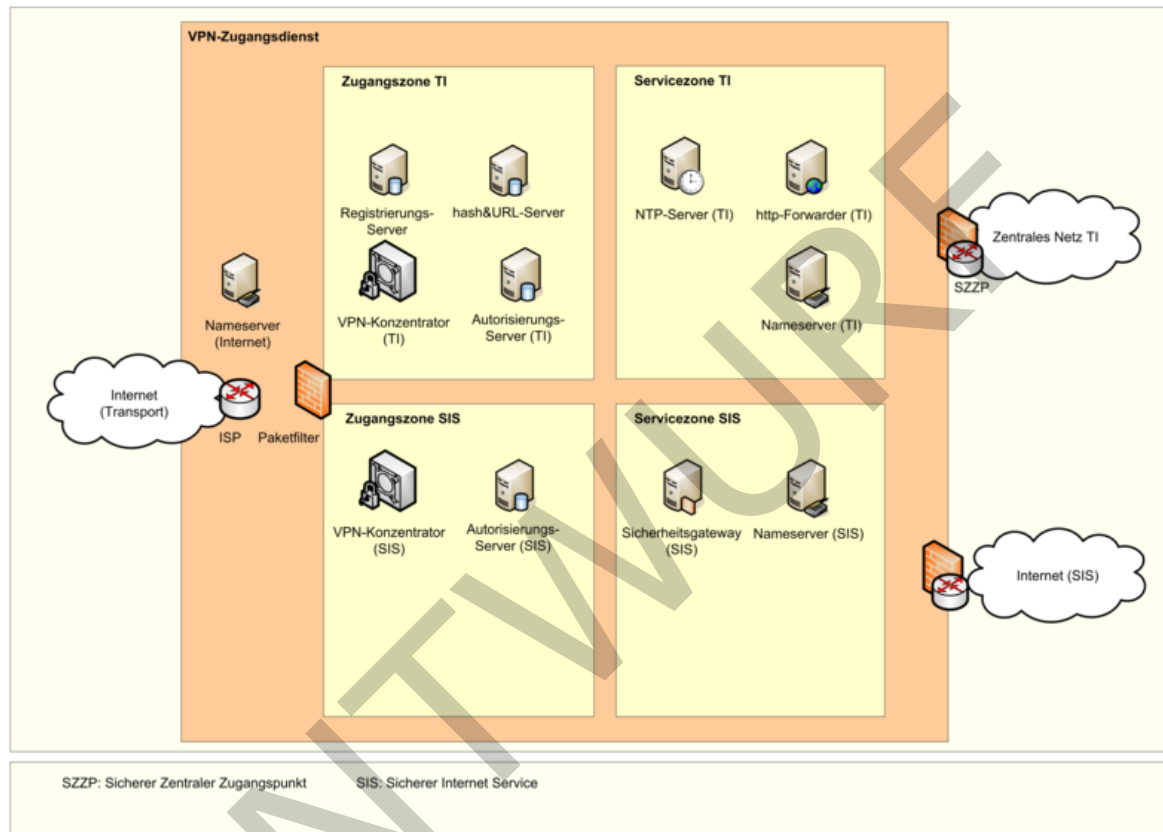


Abbildung 2: Zerlegung des VPN-Zugangsdienstes

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 Registrierungs-Server 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



440 gewählten Implementation werden diese Funktionseinheiten im Folgenden als VPN-  
441 Konzentratoren bezeichnet.

### 442 3.1.2 Topologie

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

#### 446 **TIP1-A\_4277 - VPN-Zugangsdienst, Physische Trennung der VPN-** 447 **Konzentratoren**

448 Der Anbieter des VPN-Zugangsdienstes MUSS zwischen den VPN-Konzentratoren, welche  
449 für den Zugang zur TI verwendet werden, und den VPN-Konzentratoren für den Zugang  
450 zum SIS eine physische Trennung der Hardware gewährleisten.  
451 [ <= ]

### 452 3.1.3 Standorte des VPN-Zugangsdienstes

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

#### 456 **TIP1-A\_4278 - VPN-Zugangsdienst, Geografische Verteilung der VPN-** 457 **Konzentratoren**

458 Der Anbieter des VPN-Zugangsdienstes MUSS die Standorte seiner VPN-Konzentratoren  
459 geografisch in seinem Einzugsgebiet verteilen, so dass die durchschnittliche Distanz und  
460 Laufzeit von den Netzen der berechtigten Teilnehmer zu den VPN-Konzentratoren  
461 optimiert wird.  
462 [ <= ]

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

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

468 Der Anbieter des VPN-Zugangsdienstes MUSS VPN-Konzentratoren an mindestens zwei  
469 geografisch getrennten Standorten betreiben.  
470 [ <= ]

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

472 Der Anbieter des VPN-Zugangsdienstes KANN für den Nachweis der  
473 standortübergreifenden Redundanzfunktionen in der Referenz- und der Testumgebung  
474 die VPN-Konzentratoren an einer Lokation betreiben.  
475 [ <= ]

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

- 478 • Frankfurt
- 479 • Hamburg
- 480 • München
- 481 • Berlin
- 482 • Köln, Düsseldorf, Bonn

- 483 • Ruhrgebiet (Dortmund, Essen)

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

- 486 • Stuttgart
- 487 • Nürnberg
- 488 • Saarbrücken
- 489 • Leipzig/Dresden
- 490 • Hannover
- 491 • Bremen

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

## 494 3.1.4 Anbindung an das Transportnetz Internet

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

496 Der Anbieter des VPN-Zugangsdienstes DARF NICHT zwischen der internetseitigen  
497 Schnittstelle der VPN-Konzentratoren und dem Internet NAT-Verfahren einsetzen.  
498 [ $\leq$ ]

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

500 Der Anbieter des VPN-Zugangsdienstes MUSS jeden VPN-Konzentrator mit einem  
501 eindeutigen FQDN versehen.  
502 [ $\leq$ ]

### 503 **TIP1-A\_4284 - VPN-Zugangsdienst, Redundanter Internetzugang**

504 Der Anbieter des VPN-Zugangsdienstes MUSS die VPN-Konzentratoren über einen  
505 redundanten Zugang an das Internet anbinden. Hierzu sind mindestens zwei vollständig  
506 unabhängige Leitungsführungen zwischen dem Standort und dem IP-Backbone sowie  
507 unabhängige Zugangsroutern erforderlich.  
508 [ $\leq$ ]

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

510 Der Anbieter des VPN-Zugangsdienstes MUSS sicherstellen, dass die Umschaltzeit vom  
511 Ausfall einer Verbindung zwischen VPN-Konzentrator und Internet-Router oder beim  
512 Ausfall eines Internet-Routers bis zur Wiederherstellung des Internetzugangs unter einer  
513 Sekunde liegt.  
514 [ $\leq$ ]

## 515 3.1.5 Anbindung an die TI

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

517 Der Anbieter des VPN-Zugangsdienstes MUSS die Standorte des VPN-Zugangsdienstes  
518 redundant an das Zentrale Netz der TI anbinden.  
519 [ $\leq$ ]

520 Der SZSP 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 Konzentratoren 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 Konzentratoren 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 Autorisierungsanfragen 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.

[&lt;=]

**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.

[&lt;=]

**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.

[&lt;=]

**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.

[&lt;=]

**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.

[&lt;=]

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



	<p>Wertes):</p> <p>"txtvers=1"</p> <p>"NameserverTI=&lt;IP-Adresse1&gt;,&lt;IP-Adresse2&gt;[,&lt;weitere IP-Adressen&gt;]"</p> <p>"DomainSrvTI=&lt;Domainname der Servicezone TI des VPN-Zugangsdienstes&gt;"</p> <p>Beispiel für einen Zonendateieintrag:</p> <pre>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"</pre>
VPN_KONZENTRATOR_SIS_FQDN	<p>A Resource Records zur Namensauflösung von FQDN der VPN-Konzentratoren SIS in IP-Adressen</p>
VPN_KONZENTRATOR_SIS_FQDN	<p>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.</p> <p>Die key/value Paare der TXT-Records haben folgende Struktur (die spitzen Klammern dienen der Abgrenzung eines Wertes):</p> <p>"txtvers=1"</p> <p>"NameserverSIS=&lt;IP-Adresse1&gt;,&lt;IP-Adresse2&gt;[,&lt;weitere IP-Adressen&gt;]"</p> <p>"DomainSrvSIS=&lt;Domainname der Servicezone SIS des VPN-Zugangsdienstes&gt;"</p> <p>Beispiel für einen Zonendateieintrag:</p> <pre>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"</pre>

[&lt;=]

### 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

792 [ $\leq$ ]

### 793 3.3.5 Adressierung

#### 794 TIP1-A\_4308 - VPN-Zugangsdienst, Adressierung des Nameservers TI

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

797 [ $\leq$ ]

### 798 3.4 Nameserver SIS

#### 799 3.4.1 Funktion

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

#### 802 TIP1-A\_4309 - VPN-Zugangsdienst, Nameserver im Namensraum SIS

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

807 [ $\leq$ ]

#### 808 3.4.2 Verteilung

#### 809 TIP1-A\_4310 - VPN-Zugangsdienst, Bereitstellung Nameserver SIS

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

813 [ $\leq$ ]

#### 814 3.4.3 Redundanz

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

#### 817 3.4.4 Konfiguration

818 Der Nameserver SIS erlaubt rekursive Anfragen. Er löst diese Anfragen über das  
819 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-Zugangsdiensteanbieters 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.

[<=]

899 **3.6.2 Verteilung**900 **TIP1-A\_4319 - VPN-Zugangsdienst, Verteilung des Autorisierungsservers**

901 Der Anbieter des VPN-Zugangsdienstes MUSS die Autorisierungsserver in Kolokation mit  
902 jedem Standort des VPN-Zugangsdienstes aufstellen. Sie MÜSSEN sich jeweils  
903 netzwerktechnisch in der Zugangszone TI bzw. Zugangszone SIS des Standortes  
904 befinden.  
905 [ $\leq$ ]

906 **3.6.3 Redundanz**

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

909 **3.6.4 Konfiguration**

910 Der Autorisierungsserver nimmt Autorisierungsanfragen der VPN-Konzentratoren  
911 entgegen.

912 **3.6.5 Adressierung**913 **TIP1-A\_4321 - VPN-Zugangsdienst, IP-Adresse des Autorisierungsservers**

914 Der Anbieter des VPN-Zugangsdienstes MUSS dem Autorisierungsserver eine IP-Adresse  
915 aus dem Adressbereich der jeweiligen Zugangszone TI bzw. Zugangszone SIS des  
916 Standortes zuweisen.  
917 [ $\leq$ ]

918 **3.7 hash&URL-Server**

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

922 **3.7.1 Funktion**923 **TIP1-A\_5709 - VPN-Zugangsdienst, bereitgestellte Zertifikate**

924 Der Anbieter des VPN-Zugangsdienstes MUSS die Zertifikate

- 925 • der VPN-Konzentratoren TI C.VPNK.VPN
- 926 • der VPN-Konzentratoren SIS C.VPNK.VPN-SIS
- 927 • der registrierten Konnektoren C.NK.VPN

928 im hash&URL-Server bereitstellen.

929 Der Anbieter des VPN-Zugangsdienstes muss sicherstellen, dass die bereitgestellten  
930 Zertifikate gültig sind. Ungültige Zertifikate müssen gelöscht werden.  
931 [ $\leq$ ]

### 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 weitergeleiteten 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)



- 1006 • VPN-Konzentrator (TI)
- 1007 • http-Forwarder
- 1008 • Autorisierungsserver

1009 [ $\leq$ ]

## 1010 **TIP1-A\_4478 - VPN-Zugangsdienst, Synchronisierung der Komponenten mit**

## 1011 **Ersatzverfahren**

1012 Der VPN-Zugangsdienst MUSS folgende Komponenten mit einem Ersatzverfahren  
 1013 synchronisieren, das sicherstellt, dass die maximale Abweichung von der gesetzlichen  
 1014 Zeit nicht größer als eine Sekunde ist:

- 1015 • VPN-Konzentrator (SIS)
- 1016 • Sicherheitgateway (SIS)
- 1017 • Autorisierungsserver (SIS)
- 1018 • Nameserver (SIS)
- 1019 • Packet Filter (SIS)
- 1020 • Packet Filter (TI)

1021 Die Stratum-1- und 2-NTP-Server für die TI dürfen dazu nicht verwendet werden.

1022 [ $\leq$ ]

## 1023 **3.9.2 Verteilung**

### 1024 **TIP1-A\_4328 - VPN-Zugangsdienst, Anzahl der Stratum-2-NTP-Server**

1025 Der Anbieter des VPN-Zugangsdienstes MUSS pro Standort mindestens zwei aktive  
 1026 Stratum-2-NTP-Server bereitstellen, die mit den Stratum-1-NTP-Servern des Zeitdienstes  
 1027 synchronisiert sind. Sie MÜSSEN sich netzwerktechnisch in der Service-Zone TI des  
 1028 Standortes befinden.

1029 [ $\leq$ ]

### 1030 **TIP1-A\_4479 - VPN-Zugangsdienst, maximale Zeitabweichung der Stratum-2-**

### 1031 **NTP-Server**

1032 Der Anbieter des VPN-Zugangsdienstes MUSS gewährleisten, dass die Zeitabweichung  
 1033 zwischen den Stratum-2-NTP-Servern eines Standortes nicht mehr als 330ms beträgt.

1034 [ $\leq$ ]

## 1035 **3.9.3 Redundanz**

1036 Die hierfür geltenden Anforderungen zur Verfügbarkeit werden in [gemSpec\_Perf#4.2]  
 1037 definiert.

## 1038 **3.9.4 Konfiguration**

### 1039 **TIP1-A\_4330 - VPN-Zugangsdienst, Synchronisierung der Konnektoren**

1040 Der Anbieter des VPN-Zugangsdienstes MUSS gewährleisten, dass sich die über die VPN-  
 1041 Konzentratoren TI verbundenen Konnektoren mit den Stratum-2-NTP-Servern des  
 1042 Standortes synchronisieren können.

1043 [ $\leq$ ]

1044 Die NTP-Server nehmen NTP-Anfragen aller an der Dienstleistung beteiligten  
 1045 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.  
[<=]

1082 **TIP1-A\_4335 - VPN-Zugangsdienst, Bereitstellung der öffentlichen Adressen**  
1083 Der Anbieter des VPN-Zugangsdienstes MUSS die öffentlichen IP-Adressen für die  
1084 Service-Zone SIS bereitstellen.  
1085 [ $\leq$ ]

### 1086 **3.10.6 Informationen Funktionsmerkmale**

1087 **A\_18748 - Informationsbereitstellung Sicherheitsleistungen SIS**  
1088 Der VPN-Zugangsdienstanbieter MUSS den Vertragspartnern, Leistungserbringern und  
1089 Dienstleistern vor Ort Informationen zu den Sicherheitsleistungen des sicheren Internet  
1090 Service (SIS) sowie deren Grenzen (z.B. Umgang mit verschlüsseltem Datenverkehr,  
1091 freigeschaltete Ports, Leistung des Virenschutzes) transparent und verständlich  
1092 bereitstellen.  
1093 [ $\leq$ ]  
1094 Mit diesen Informationen sollen die Vertragspartner in die Lage versetzt werden, die  
1095 erforderlichen Sicherheitsmaßnahmen in der Leistungserbringerumgebung abstimmen zu  
1096 können.

1097

## 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 Netzwerkcommunication 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 angebotenen 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 angebotenen 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 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



- 1313 • zu welchem Zweck diese Informationen durch den Anbieter des VPN-
- 1314 Zugangsdienstes genutzt werden, insbesondere welche Prozesse vom Anbieter
- 1315 VPN-Zugangsdienst ausgeführt werden, falls nicht-zugelassene Komponenten oder
- 1316 Kartenterminals beim Leistungserbringer entdeckt werden.

1317 [ $\leq$ ]

1318 Es wird erwartet, dass die betroffenen Leistungserbringer oder ihre DVOs auf Grundlage  
 1319 der Mitteilung des VPN-Zugangsdienstes die jeweilige Firmware bzw. Geräte rechtzeitig  
 1320 aktualisieren bzw. aktualisieren lassen oder austauschen bzw. austauschen lassen.

## 1321 4.2 Protokollanforderungen

### 1322 4.2.1 IPsec

1323 Die Verbindung zwischen dem Konnektor und dem VPN-Konzentrator des VPN-  
 1324 Zugangsdienstes wird im Ipsec-Tunnel-Mode hergestellt. Es kommt das ESP-Protokoll  
 1325 gemäß [RFC4303] zum Einsatz.

#### 1326 **TIP1-A\_4349 - VPN-Zugangsdienst und Konnektor, IPsec-Protokoll**

1327 Konnektor und VPN-Konzentrator des VPN-Zugangsdienstes MÜSSEN die „Security  
 1328 Architecture for the Internet Protocol“ gemäß [RFC4301] unterstützen.

1329 [ $\leq$ ]

#### 1330 **TIP1-A\_4350 - VPN-Zugangsdienst und Konnektor, ESP**

1331 Konnektor und VPN-Konzentrator des VPN-Zugangsdienstes MÜSSEN das ESP-Protokoll  
 1332 (Encapsulating Security Payload) gemäß [RFC4303] unterstützen.

1333 [ $\leq$ ]

1334 Die nachfolgende Anforderung richtet sich an den VPN-Zugangsdienst und an die  
 1335 Konnektoren der Produkttypversionen 1 bis 3.

#### 1336 **TIP1-A\_4351 - VPN-Zugangsdienst und Konnektor (PTV 1 bis 3), Auswertung** 1337 **der Sequenznummern**

1338 Der Konnektor und der VPN-Konzentrator des VPN-Zugangsdienstes MÜSSEN  
 1339 ermöglichen, dass die Auswertung der Sequenznummern zur Unterstützung der  
 1340 Fehlersuche empfängerseitig abschaltbar ist.

1341 [ $\leq$ ]

1342 Die nächste Anforderung richtet sich an den VPN-Zugangsdienst und an die Konnektoren  
 1343 ab Produkttypversion 4.

#### 1344 **A\_17118 - VPN-Zugangsdienst und Konnektor (PTV 4 und höher), Verwendung** 1345 **erweiterter Sequenznummern**

1346 Der Konnektor und der VPN-Konzentrator des VPN-Zugangsdienstes MÜSSEN zum Schutz  
 1347 vor Replay-Attacken die Nutzung von Extended Sequence Numbers (ESN) aushandeln  
 1348 und verwenden.

1349 [ $\leq$ ]

#### 1350 **TIP1-A\_4352 - VPN-Zugangsdienst und Konnektor, Fenster für die Auswertung** 1351 **der Sequenznummern**

1352 Der Konnektor und der VPN-Konzentrator des VPN-Zugangsdienstes MÜSSEN  
 1353 ermöglichen, dass das Fenster für die Auswertung der Sequenznummern im Rahmen des  
 1354 Anti Replay Service empfängerseitig konfigurierbar ist.

1355 [ $\leq$ ]

## 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.

[<=]

## 1400 4.2.5 Fragmentierung von IKE-Paketen

1401 Bei der Aushandlung der IKE-SA werden die Zertifikate zwischen Konnektor und VPN-  
1402 Konzentrador über UDP übertragen. Aufgrund der genutzten Zertifikatsprofile und  
1403 Schlüssellängen können die ISAKMP-Pakete größer als die MTU des Transportnetzes  
1404 werden, so dass diese fragmentiert werden müssen. Hierbei kann es potentiell zu  
1405 Problemen mit auf der Übertragungsstrecke liegenden Netzwerkkomponenten kommen,  
1406 die fragmentierte UDP-Pakete nicht weiterleiten.

### 1407 **A\_17169 - VPN-Zugangsdienst, Fragmentierung der IKEv2-Nachrichten**

1408 Der VPN-Zugangsdienst, der IPv6 an den Netzwerkschnittstellen zum Transportnetz  
1409 einsetzt, MUSS die Fragmentierung von IKEv2-Nachrichten gemäß [RFC7383]  
1410 unterstützen.  
1411 [ $\leq$ ]

## 1412 4.3 Netzanforderungen

### 1413 4.3.1 Routing

#### 1414 4.3.1.1 VPN-Zugangsdienst

##### 1415 **TIP1-A\_4484 - Routing VPN-Zugangsdienst TI**

1416 Der VPN-Zugangsdienst MUSS IP-Pakete, die vom Konnektor über den IPsec-Tunnel des  
1417 VPN-Konzentrators TI zu fachanwendungsspezifischen Diensten, zentralen Diensten der  
1418 TI-Plattform gesendet werden, zu den entsprechenden Diensten der TI weiterleiten.  
1419 Zur jeweiligen Kommunikationsbeziehung zugehörige IP-Pakete der Gegenrichtung  
1420 müssen zum Konnektor weitergeleitet werden.  
1421 [ $\leq$ ]

##### 1422 **TIP1-A\_4485 - Routing VPN-Zugangsdienst Bestandsnetze**

1423 Der VPN-Zugangsdienst MUSS IP-Pakete, die vom Konnektor über den IPsec-Tunnel des  
1424 VPN-Konzentrators TI zu Diensten in den Bestandsnetzen gesendet werden, zu den  
1425 entsprechenden Bestandsnetzen mit Anschluss an die TI weiterleiten.  
1426 Zur jeweiligen Kommunikationsbeziehung zugehörige IP-Pakete der Gegenrichtung  
1427 müssen zum Konnektor weitergeleitet werden.  
1428 [ $\leq$ ]

##### 1429 **TIP1-A\_6748 - Traffic Selectoren VPN-Zugangsdienst TI**

1430 Der VPN-Zugangsdienst MUSS den VPN-Konzentratoren TI den Traffic Selector 0.0.0.0/0  
1431 für das lokale und das remote Subnet zuweisen.  
1432 [ $\leq$ ]

##### 1433 **TIP1-A\_4486 - Routing VPN-Zugangsdienst TI, lokale Dienste**

1434 Der VPN-Zugangsdienst MUSS die lokalen TI-Dienste des VPN-Zugangsdienstes  
1435 (Nameserver TI, NTP-Server, http-Forwarder) für Konnektoren über den IPsec-Tunnel  
1436 des VPN-Konzentrators TI erreichbar machen.  
1437 [ $\leq$ ]

##### 1438 **TIP1-A\_4487 - Routing VPN-Zugangsdienst SIS**

1439 Der VPN-Zugangsdienst MUSS IP-Pakete, die vom Konnektor über den IPsec-Tunnel des  
1440 VPN-Konzentrators SIS in Richtung Internet gesendet werden, zum Sicherheitsgateway  
1441 SIS weiterleiten. Die für die Nutzung des SIS benötigten lokalen Dienste des VPN-  
1442 Zugangsdienstes (Nameserver SIS) MÜSSEN für die Konnektoren erreichbar sein.  
1443 Zur jeweiligen Kommunikationsbeziehung zugehörige IP-Pakete der Gegenrichtung

1444 müssen zum Konnektor weitergeleitet werden.  
1445 [=]

#### 1446 **4.3.1.2 Konnektor**

1447 Im Konnektor sind folgende Routing-Informationen definiert:

- 1448 • spezifische Route Richtung Dienste der TI über den IPsec-Tunnel TI
- 1449 • spezifische Route Richtung Bestandsnetze über den IPsec-Tunnel TI
- 1450 • spezifische Route Richtung VPN-Konzentratoren TI und SIS über das WAN-Interface zum Transportnetz Internet
- 1451
- 1452 • spezifische Route Richtung Nameserver Internet (Transport) über das WAN-Interface zum Transportnetz Internet
- 1453
- 1454 • spezifische Route Richtung CRL-Server über das WAN-Interface zum Transportnetz Internet
- 1455
- 1456 • Default-Route Richtung Internet über den IPsec-Tunnel zum SIS

#### 1457 **4.3.2 Behandlung gemäß DiffServ-Architektur**

1458 Der VPN-Zugangsdienst dient in erster Linie als Durchgang zwischen jeweils zwei  
1459 externen Netzen (Internet und TI bzw. Internet und Internet über SIS).

1460 Es wird erwartet, dass Datenverkehr, der innerhalb eines Standortes des VPN-  
1461 Zugangsdienstes transportiert wird, niemals einen Engpass erfährt, da die Bandbreiten,  
1462 mit denen die durchlaufenen Geräte untereinander verbunden werden, höher sind, als die  
1463 Bandbreiten, mit denen der VPN-Zugangsdienst an externe Netze angeschlossen ist.  
1464 Dieser Zustand entspricht einer Überbuchung. Eine DiffServ-gemäße Behandlung ist  
1465 innerhalb des VPN-Zugangsdienstes daher verzichtbar.

##### 1466 **TIP1-A\_4488 - Bandbreiten innerhalb des VPN-Zugangsdienstes**

1467 Der Anbieter des VPN-Zugangsdienstes MUSS sicherstellen, dass in seinem Netzwerk  
1468 keine Bandbreitenengpässe entstehen können.  
1469 [=]

#### 1470 **4.3.2.1 VPN-Konzentratoren zum Transportnetz Internet**

1471 An der Schnittstelle zwischen VPN-Zugangsdienst und Transportnetz wird eine DiffServ-  
1472 Behandlung vorgenommen, wobei die DSCP-Markierungen der getunnelten Pakete  
1473 beachtet werden. Dies geschieht in beiden Richtungen. Soweit der Internetzugang durch  
1474 einen externen Backbone-Anbieter bereitgestellt wird, muss dieser die geforderte Policy  
1475 seinerseits auf dem Provider Edge (PE) Router und gegebenenfalls dem Customer Edge  
1476 (CE) Router implementieren.

##### 1477 **TIP1-A\_4364 - VPN-Zugangsdienst, DiffServ-Behandlung zwischen VPN-Konzentrator und Transportnetz Internet**

1478 Der Anbieter des VPN-Zugangsdienstes MUSS an der Schnittstelle des VPN-  
1479 Zugangsdienstes zum Transportnetz Internet in beiden Richtungen die DiffServ-gemäße  
1480 Behandlung von Datenverkehr unterstützen.  
1481 Die Erkennung und/oder Verarbeitung der DiffServ-Flags darf die Werte nicht verändern.  
1482 [=]  
1483

#### 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.

[<=]

## 1527 4.4 Einsatz von IPv6

1528 Der VPN-Zugangsdienst muss für den Einsatz von IPv6 (Dual-Stack-Mode) die  
1529 nachfolgenden Anforderungen umsetzen.

### 1530 4.4.1 Nameserver Internet

#### 1531 **A\_17171 - VPN-Zugangsdienst, IPv6-Adressierung der Nameserver Internet**

1532 Der VPN Zugangsdienst MUSS jedem rekursiven Nameserver Internet eine öffentliche  
1533 IPv6-Adresse zuweisen (Dual-Stack-Mode). Die IPv6-Adressen der Nameserver werden  
1534 vom Anbieter des VPN-Zugangsdienstes zur Verfügung gestellt.

1535 [ $\leq$ ]

#### 1536 **A\_17173 - VPN-Zugangsdienst, IPv6 Resource Records im Nameserver Internet**

1537 Der VPN Zugangsdienst MUSS in den autoritativen Nameservern Internet die weiteren  
1538 Resource Records gemäß Tabelle Tab\_ZD\_Nameserver\_Int\_RR\_IPv6 verwalten.

1539

1540 **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

1541 [ $\leq$ ]

### 1542 4.4.2 Registrierungsserver

#### 1543 **A\_17180 - VPN-Zugangsdienst, IPv6-Adressierung Registrierungsserver**

1544 Der VPN-Zugangsdienst MUSS jedem Registrierungsserver eine öffentliche IPv6-Adresse  
1545 zuweisen (Dual-Stack-Mode). Die öffentlichen IPv6-Adressen der Registrierungsserver  
1546 werden vom Anbieter des VPN-Zugangsdienstes zur Verfügung gestellt.

1547 [ $\leq$ ]

### 1548 4.4.3 VPN-Konzentratoren TI und SIS

#### 1549 **A\_17181 - VPN-Zugangsdienst, IPv6-Adressierung der Internetschnittstellen 1550 der VPN-Konzentratoren**

1551 Der VPN-Zugangsdienst MUSS jedem VPN-Konzentrator TI und SIS eine IPv6-Adresse  
1552 zuweisen (Dual-Stack-Mode). Diese Adresse wird auf der physischen Schnittstelle zum  
1553 Internet konfiguriert. Die öffentlichen IPv6-Adressen der VPN-Konzentratoren TI und SIS

1554 werden vom Anbieter des VPN-Zugangsdienstes zur Verfügung gestellt.  
1555 [ $\leq$ ]

ENTWURF



1556

## 5 Funktionsmerkmale

1557

### TIP1-A\_4369 - VPN-Zugangsdienst, Festlegung der Schnittstellen

1558

Der Produkttyp VPN-Zugangsdienst MUSS die Schnittstellen gemäß Tabelle Tab\_PT\_VPN-

1559

Zugangsdienst\_Schnittstellen implementieren („bereitgestellte“ Schnittstellen) und

1560

nutzen („benötigte“ Schnittstellen).

1561

1562

**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- Konzentrato ren 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_Distributi on	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



			Störungssampe l
I_Monitoring_Read	benötigt	obligatorisch	Definition durch den Anbieter der Störungssampe l
I_OCSP_Status_Informatio n	benötigt	obligatorisch	Definition in [gemSpec_PKI ]

[&lt;=]

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

[&lt;=]

## 5.1.1 Operation connect

### 5.1.1.1 Umsetzung

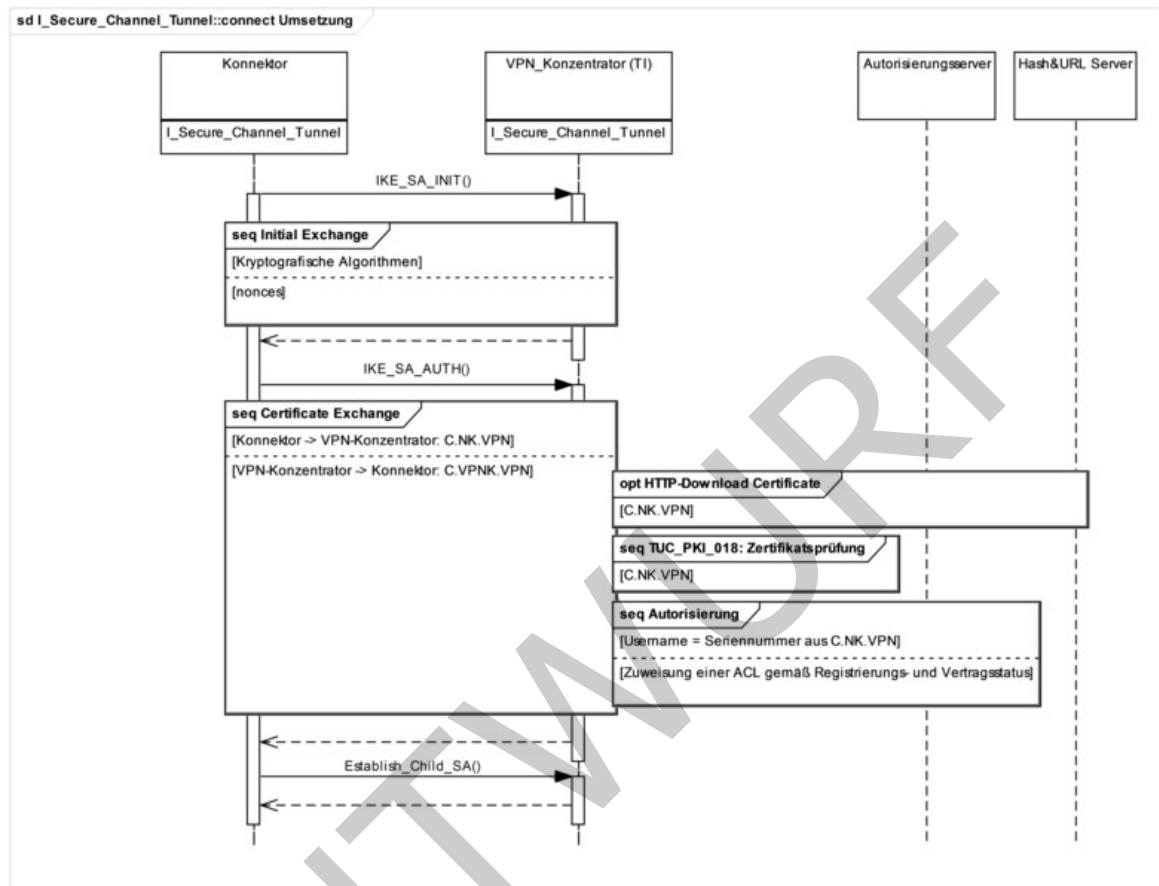


Abbildung 4: Ablauf der Operation I\_Secure\_Channel\_Tunnel::connect im VPN-Zugangsdienst

#### 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.

- 1607 • Das Zertifikat C.NK.VPN wird gemäß [gemSpec\_PKI#TUC\_PKI\_018] mit
- 1608 Prüfmodus OCSP geprüft.
- 1609 • Wenn das Zertifikat C.NK.VPN nicht gültig ist, wird der Verbindungsaufbau mit
- 1610 einer Fehlermeldung gemäß [RFC 7296] abgebrochen.
- 1611 • Der VPN-Konzentrator authentisiert sich beim Konnektor mit seinem Zertifikat
- 1612 C.VPNK.VPN.
- 1613 • Der VPN-Konzentrator erzeugt aus Aussteller und Seriennummer des Zertifikats
- 1614 einen Benutzernamen und sendet ihn an den Autorisierungsserver.
- 1615 • Über den Autorisierungsserver wird geprüft, ob bereits ein Benutzerkonto für den
- 1616 Benutzernamen besteht. Der VPN-Konzentrator TI muss dem Konnektor auf der
- 1617 Grundlage seines Registrierungsstatus eine IP-basierte Zugangskontrollliste (ACL)
- 1618 zuweisen.
- 1619 • Wenn kein Benutzerkonto besteht MUSS der VPN-Verbindungsaufbau
- 1620 abgebrochen werden.
- 1621 • Wenn ein Benutzerkonto besteht, wird der Zugang zum Zentralen Netz der TI
- 1622 freigeschaltet.
- 1623 • Der VPN-Konzentrator weist dem Konnektor eine Adresse aus dem Adressraum
- 1624 TI\_Dezentral zu. Die Adresse wird als innere Adresse des IPsec-Tunnels
- 1625 verwendet.

1626 [ $\leq$ ]

#### 1627 5.1.1.2 Nutzung

##### 1628 TIP1-A\_4373 - Konnektor, TUC\_VPN-ZD\_0001 "IPsec-Tunnel TI aufbauen"

1629 Der Konnektor MUSS den technischen Use Case TUC\_VPN-ZD\_0001 "IPsec-Tunnel TI

1630 aufbauen" gemäß Tabelle Tab\_ZD\_TUC\_IPsec\_Tunnel\_TI\_aufbauen umsetzen.

1631

1632 **Tabelle 6: Tab\_ZD\_TUC\_IPsec\_Tunnel\_TI\_aufbauen**

<b>Name</b>	TUC_VPN-ZD_0001 "IPsec-Tunnel TI aufbauen"
<b>Beschreibung</b>	Dieser TUC stellt eine IPsec-gesicherte Verbindung zwischen dem Konnektor und einem VPN-Konzentrator TI des VPN-Zugangsdienstes her.
<b>Vorbedingungen</b>	<ul style="list-style-type: none"> <li>• Eine gültige TSL ist im Konnektor geladen.</li> <li>• Eine gültige CRL ist im Konnektor geladen.</li> <li>• Es besteht eine IP-Netzwerkverbindung vom Konnektor zum Internet</li> <li>• Der gültige Internet DNS Root Trust Anchor der IANA ist in der DNS-Forwarder Konfiguration des Konnektors enthalten.</li> <li>• Der DNS-Resolver des Konnektors kann auf die vom Anbieter des VPN-Zugangsdienstes bereitgestellten Nameserver im Internet (Bezeichner DNS_SERVERS_INT) zugreifen.</li> </ul>
<b>Eingangsdaten</b>	<ul style="list-style-type: none"> <li>• CRL (die im Konnektor verfügbare CRL)</li> </ul>

	<ul style="list-style-type: none"> <li>TUNNEL_MTU (optional, Maximum Transfer Unit für den IPsec Tunnel)</li> <li>TOP_LEVEL_DOMAIN_TI (Top-Level-Domain der TI)</li> <li>DNS_DOMAIN_VPN_ZUGD_INT (DNS-Domainname für die Service Discovery der VPN-Konzentratoren)</li> <li>DNS_SERVERS_INT (DNS Server im Internet)</li> <li>HASH_AND_URL</li> </ul>	
<b>Komponenten</b>	Konnektor, VPN-Zugangsdienst	
<b>Ausgangsdaten</b>	<ul style="list-style-type: none"> <li>VPN_TUNNEL_TI_INNER_IP (innere IP-Adresse des IPsec-Tunnels TI)</li> <li>DNS_SERVERS_TI (Nameserver TI des VPN-Zugangsdienstes)</li> <li>DOMAIN_SRVZONE_TI</li> <li>VPN_KONZENTRATOR_TI_IP_ADDRESS (IP-Adresse des VPN-Konzentrators TI im Transportnetz zu dem der IPsec-Tunnel VPN aufgebaut wird)</li> </ul>	
<b>Standardablauf</b>	Aktion	Beschreibung
	FQDN und IP-Adressen der VPN-Konzentratoren TI ermitteln	<p>Durch eine DNS-Anfrage zur Auflösung eines SRV-RR mit dem Bezeichner "_isakmp._udp.ti-extern.&lt;DNS_DOMAIN_VPN_ZUGD_INT&gt;" erhält der Konnektor eine Liste von priorisierten und gewichteten FQDN der VPN-Konzentratoren TI.</p> <p>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.</p> <p>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.</p>

	Nameserver TI und Domainnamen der Service-Zone des VPN-Zugangsdienstes ermitteln	<p>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.</p> <p>Die key/value Paare der TXT-Records haben folgende Struktur (die spitzen Klammern dienen der Abgrenzung eines Wertes):</p> <p>"txtvers=1"</p> <p>"NameserverTI=&lt;IP-Adresse1&gt;,&lt;IP-Adresse2&gt;[,&lt;weitere IP-Adressen&gt;]"</p> <p>"DomainSrvTI=&lt;Domainname der Servicezone TI des VPN-Zugangsdienstes&gt;"</p> <p>Beispiel für einen Zoneneintrag:</p> <pre>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"</pre>
	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	<ul style="list-style-type: none"> <li>Der Verbindungsaufbau erfolgt gemäß oder [RFC7296] mit der ersten IP-Adresse aus der erzeugten IP-Adressliste der VPN-Konzentratoren.</li> <li>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.]</li> <li>Der Konnektor empfängt vom VPN-Konzentrator das Zertifikat C.VPNK.VPN. Falls HASH_AND_URL</li> </ul>

		<p>= Enabled muss das Hash &amp; URL Verfahren gemäß [RFC7296] zum Austausch der Zertifikate zwischen Konnektor und VPN-Konzentrator verwendet werden.</p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• Der Konnektor authentisiert sich beim VPN-Konzentrator mit seinem Zertifikat C.NK.VPN</li> <li>• 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.</li> <li>• Bei erfolgreicher gegenseitiger Authentifizierung und Autorisierung durch den VPN-Zugangsdienst wird die Verbindung gemäß [RFC7296] weiter aufgebaut. Das IKE-Protokoll weist dem Konzentratoren die innere IP-Adresse des IPsec-Tunnels aus dem Adressraum TI_Dezentral zu. Bei jedem Verbindungsaufbau wird eine andere IP-Adresse verwendet.</li> <li>• 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.</li> </ul>
<b>Varianten/Alternativen</b>	Keine	
<b>Zustand nach erfolgreichem Ablauf</b>	Der Konnektor ist mit dem VPN-Konzentrator TI verbunden.	
<b>Fehlerfälle</b>	Zur Behandlung auftretender Fehlerfälle werden Fehlermeldungen gemäß [RFC 7296] verwendet.	

1633 [ $\leq$ ]

### 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**

<b>Name</b>	TUC_VPN-ZD_0002 "IPsec-Tunnel SIS aufbauen"
<b>Beschreibung</b>	Dieser TUC stellt eine IPsec-gesicherte Verbindung zwischen dem Konnektor und dem VPN-Konzentrator SIS des VPN-Zugangsdienstes her.
<b>Vorbedingungen</b>	<ul style="list-style-type: none"> <li>• Eine gültige TSL ist im Konnektor geladen.</li> <li>• Eine gültige CRL ist im Konnektor geladen.</li> <li>• Es besteht eine IP-Netzwerkverbindung vom Konnektor zum Internet</li> </ul>

	<ul style="list-style-type: none"> <li>• Der gültige Internet DNS Root Trust Anchor der IANA ist in der DNS-Forwarder Konfiguration des Konnektors enthalten.</li> <li>• Der Konnektor ist beim Anbieter des VPN-Zugangsdienstes registriert und zur Verbindung mit dem Sicheren Internet Service berechtigt.</li> <li>• Der DNS-Resolver des Konnektors kann auf die vom Anbieter des VPN-Zugangsdienstes bereitgestellten Nameserver im Internet (Bezeichner DNS_SERVERS_INT) zugreifen.</li> </ul>	
<b>Eingangsdaten</b>	<ul style="list-style-type: none"> <li>• CRL (die im Konnektor verfügbare CRL)</li> <li>• TUNNEL_MTU (optional, Maximum Transfer Unit für den IPsec Tunnel)</li> <li>• DNS_DOMAIN_VPN_ZUGD_INT (DNS-Domainname für die Service Discovery der VPN-Konzentratoren)</li> <li>• DNS_SERVERS_INT (DNS Server im Internet)</li> <li>• HASH_AND_URL</li> </ul>	
<b>Komponenten</b>	Konnektor, VPN-Zugangsdienst	
<b>Ausgangsdaten</b>	<ul style="list-style-type: none"> <li>• VPN_TUNNEL_SIS_INNER_IP (innere IP-Adresse des IPsec-Tunnels SIS)</li> <li>• DNS_SERVERS_SIS (Nameserver SIS des VPN-Zugangsdienstes)</li> <li>• VPN_KONZENTRATOR_SIS_IP_ADDRESS (IP-Adresse des VPN-Konzentrators SIS im Transportnetz zu dem der IPsec-Tunnel VPN_SIS aufgebaut wird)</li> </ul>	
<b>Standardablauf</b>	Aktion	Beschreibung
	FQDN und IP-Adressen der VPN-Konzentratoren SIS ermitteln	<p>Durch eine DNS-Anfrage zur Auflösung eines SRV-RR mit dem Bezeichner "_isakmp._udp.sis-extern.&lt;DNS_DOMAIN_VPN_ZUGD_INT&gt;" erhält der Konnektor eine Liste von priorisierten und gewichteten FQDN der VPN-Konzentratoren SIS.</p> <p>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.</p> <p>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</p>

		<p>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.</p>
	<p>Nameserver SIS und Domainnamen der Service-Zone des VPN-Zugangsdienst es ermitteln</p>	<p>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.</p> <p>Die key/value Paare der TXT-Records haben folgende Struktur (die spitzen Klammern dienen der Abgrenzung eines Wertes):</p> <p>"txtvers=1"</p> <p>"NameserverSIS=&lt;IP-Adresse1&gt;,&lt;IP-Adresse2&gt;[,&lt;weitere IP-Adressen&gt;]"</p> <p>"DomainSrvSIS=&lt;Domainname der Servicezone SIS des VPN-Zugangsdienstes&gt;"</p> <p>Beispiel für einen Zoneneintrag:</p> <pre>vpnkl.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"</pre>
	<p>DNS-Forwarder für Namensraum SIS konfigurieren</p>	<p>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.</p> <p>Dabei werden die bestehenden Ziel-Nameserver DNS_SERVERS_INT mit den DNS_SERVERS_SIS überschrieben.</p> <p>Wenn die Verbindung zum VPN-Konzentrator SIS abgebaut wurde, müssen die Ziel-Nameserver wieder DNS_SERVERS_INT sein.</p>
	<p>Verbindung aufbauen</p>	<ul style="list-style-type: none"> <li>• Der Verbindungsaufbau erfolgt gemäß [RFC7296] mit der ersten IP-Adresse aus der erzeugten IP-Adressliste der VPN-Konzentratoren.</li> <li>• Es muss das Encapsulating Security Payload Protocol (ESP) mit</li> </ul>

		<p>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].</p> <ul style="list-style-type: none"> <li>• Der Konnektor empfängt vom VPN-Konzentrator das Zertifikat C.VPNK.VPN-SIS. Falls HASH_AND_URL = Enabled muss das Hash &amp; URL Verfahren gemäß [RFC7296] zum Austausch der Zertifikate zwischen Konnektor und VPN-Konzentrator verwendet werden.</li> <li>• 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.</li> <li>• Der Konnektor authentisiert sich beim VPN-Konzentrator mit seinem Zertifikat C.NK.VPN</li> <li>• 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.</li> <li>• 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.</li> </ul>
--	--	---

		<ul style="list-style-type: none"> <li>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.</li> </ul>
<b>Varianten/Alternativen</b>	Keine	
<b>Zustand nach erfolgreichem Ablauf</b>	Der Konnektor ist mit dem VPN-Konzentrator SIS verbunden.	
<b>Fehlerfälle</b>	Zur Behandlung auftretender Fehlerfälle werden Fehlermeldungen gemäß [RFC7296] verwendet.	

[&lt;=]

## 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.

[&lt;=]

### TIP1-A\_4398-01 - 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.

[&lt;=]

## 5.3 Schnittstelle I\_Registration\_Service

### TIP1-A\_5118-01TIP1-A\_5118 - VPN-Zugangsdienst, Schnittstelle I\_Registration\_Service

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

**Tabelle 9: Tab\_ZD\_Schnittstelle\_I\_Registration\_Service**

<b>Name</b>	I_Registration_Service	
<b>Version</b>	wird im Produktsteckbrief des VPN-Zugangsdienstes definiert	
<b>Operationen</b>	<b>Name</b>	<b>Kurzbeschreibung</b>
	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-Zugangsdienstes. 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	<ul style="list-style-type: none"> <li>Die URL des Registrierungsdienstes ist im Konnektor bekannt.</li> <li>Der FQDN des Registrierungsservers TI wurde in IP-Adressen aufgelöst.</li> </ul>	
Aufrufparameter	Name	Beschreibung
	SOAP-Request „registerKonnektorRequest“	<p>Dies ist ein SOAP-Request „registerKonnektorRequest“ gemäß ProvisioningService.xsd. Dabei gilt:</p> <ul style="list-style-type: none"> <li>Das Element vpnk:Timestamp enthält den aktuellen</li> </ul>

		<p>Erstellungszeitstempel des SOAP-Requests.</p> <ul style="list-style-type: none"> <li>Das Element <code>vpnk:X509Certificate</code> enthält die base64-Kodierung des ASN.1 DER-kodierten Zertifikats <code>C.NK.VPN</code>.</li> <li>Das Element <code>vpnk:ContractID</code> enthält die vom VPN-Zugangsdienst erwartete ID zur Zuordnung zum Vertrag.</li> <li>Das Element <code>ds:Signature</code> enthält die mit <code>PRK.HCI.OSIG</code> erstellte Signatur (mittels <code>SMC-B</code>) gemäß [W3C XML-DSig] über den gesamten SOAP-Request (<code>&lt;ds:Reference URI=""&gt;</code>).</li> <li>Das Element <code>ds:KeyInfo</code> wird gemäß [W3C XML-DSig] mit Daten gefüllt.</li> <li>Die base64-Kodierung des ASN.1 DER-kodierten Zertifikats <code>C.HCI.OSIG</code> (<code>SMC-B-OSIG-Zertifikat</code>) ist innerhalb des Elements <code>ds:KeyInfo</code> und innerhalb des Elements <code>ds:X509Data</code> im Element <code>ds:X509Certificate</code> enthalten.</li> </ul>
<b>Standardablauf</b>	<b>Aktion</b>	<b>Beschreibung</b>
	Operation <code>registerKonnektor</code> des Registrierungsdienstes aufrufen	<p>Der Konnektor ruft den Dienst <code>regService(regPort)</code> des VPN-Zugangsdienstes, mit der SOAP-Operation <code>registerKonnektor(registerKonnektorRequest)</code> gemäß <code>ProvisioningService.wsdl 1.1</code>, auf.</p> <p>Dabei wird SOAP über HTTPS verwendet.</p> <p>Die TLS-Verbindung erfordert eine beidseitige Authentifizierung.</p> <ul style="list-style-type: none"> <li>Der Konnektor prüft das Zertifikat <code>C.ZD.TLS-S</code> gemäß [gemSpec_PKI#TUC_PKI_018] mit <code>Offline-Modus = ja</code> und, ob die Rollen-OID "<code>oid_vpnz_ti</code>" mit der im Zertifikat enthaltenen Rollen-OID identisch ist.</li> <li>Das Zertifikat <code>C.HCI.AUT</code> der zur Registrierung verwendeten <code>SMC-</code></li> </ul>



		B wird gemäß [gemSpec_PKI#TUC_PKI_018] mit Prüfmodus OCSP durch den Registrierungsserver geprüft.
	Daten im SOAP-Request prüfen	<p>Der Registrierungsserver des VPN-Zugangsdienstes prüft die empfangenen Daten:</p> <ul style="list-style-type: none"> <li>Die Signatur des SOAP-Requests wird geprüft. Das zugehörige SMC-B-Zertifikat C.HCI.OSIG wird gemäß [gemSpec_PKI#TUC_PKI_018] geprüft.</li> <li>Das SMC-K-Zertifikat C.NK.VPN wird gemäß [gemSpec_PKI#TUC_PKI_018] geprüft.</li> <li>Die vpnk:ContractID aus dem Request wird mit den aus dem Vertrag zugeordneten Wert verglichen.</li> <li>Der Timestamp im Request wird mit der aktuellen Zeit im Registrierungsserver verglichen. Die Abweichung darf nicht mehr als 300 Sekunden betragen.</li> <li>Wenn alle Prüfungen erfolgreich waren, wird im Standardablauf fortgefahren. Anderenfalls wird eine Fehlermeldung generiert (siehe Abschnitt Fehler).</li> </ul>
	Registrierungsinformation en 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.
<b>Rückgabe</b>	<b>Name</b>	<b>Beschreibung</b>
	SOAP-Response „registerKonnektorResponse“	<p>Dies ist eine SOAP-Response „registerKonnektorResponse“ gemäß ProvisioningService.xsd. Dabei gilt für eine erfolgreiche Registrierung:</p> <ul style="list-style-type: none"> <li>• Das Element vpnk:Timestamp enthält den aktuellen Erstellungszeitstempel der SOAP-Response.</li> <li>• Das Element vpnk:RegistrationStatus enthält den Status des Registrierungsvorgangs („Registriert“).</li> <li>• Das Element vpnk:ContractStatus enthält den Vertragsstatus („Zugriff auf TI erlaubt“ oder „Zugriff auf TI und SIS erlaubt“).</li> <li>• Das Element vpnk:AdditionalInformation enthält textuelle Informationen, die der Anbieter des VPN-Zugangsdienstes dem berechtigten Teilnehmer mitteilen möchte.</li> </ul>
<b>Zustand nach erfolgreichem Ablauf</b>	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.
<b>Zustand nach fehlerhaftem Ablauf</b>	Der Konnektor ist nicht registriert und kann keine IPsec-gesicherte Verbindung zum VPN-Konzentrator TI aufbauen.
<b>Nichtfunktionale Eigenschaften</b>	Keine

[&lt;=]

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.

[&lt;=]

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
- %()=!?+~\*/#\_@:.

[&lt;=]

**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.

[&lt;=]

**5.3.1.1 Umsetzung**

An die Umsetzung der Schnittstelle werden keine zusätzlichen Anforderungen gestellt.

1818 **5.3.1.2 Nutzung**

1819 An die Nutzung der Schnittstelle werden keine zusätzlichen Anforderungen gestellt.

1820 **5.3.2 Operation deregisterKonnektor**1821 **TIP1-A\_4391 - VPN-Zugangsdienst und Konnektor, Operation**  
1822 **deregisterKonnektor**

1823 Der VPN-Zugangsdienst MUSS für Konnektoren an der Schnittstelle  
1824 I\_Registration\_Service die Operation deregisterKonnektor gemäß Tabelle  
1825 Tab\_ZD\_deregisterKonnektor anbieten.

1826

1827 **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	<ul style="list-style-type: none"> <li>Die URL des Registrierungsdienstes ist im Konnektor bekannt.</li> <li>Der FQDN des Registrierungservers TI wurde in IP-Adressen aufgelöst.</li> </ul>	
Aufrufparameter	Name	Beschreibung
	SOAP-Request „deregisterKonnektorRequest“	<p>Dies ist ein SOAP-Request „deregisterKonnektorRequest“ gemäß ProvisioningService.xsd. Dabei gilt:</p> <ul style="list-style-type: none"> <li>Das Element vpnk:Timestamp enthält den aktuellen Erstellungszeitstempel des SOAP-Requests.</li> <li>Das Element vpnk:X509Certificate enthält die base64-Kodierung des ASN.1 DER-kodierten SMC-K-Zertifikats.</li> <li>Das Element vpnk:ContractID enthält die vom VPN-Zugangsdienst erwartete ID zur Zuordnung zum Vertrag.</li> <li>Das Element ds:Signature enthält die mit PRK.HCI.OSIG erstellte Signatur (mittels SMC-B) gemäß [W3C XML-Dsig] über den gesamten SOAP-Request (&lt;ds:Reference URI=""&gt;).</li> </ul>

		<ul style="list-style-type: none"> <li>Das Element ds:KeyInfo wird gemäß [W3C XML-Dsig] mit Daten gefüllt.</li> <li>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.</li> </ul>
<b>Standardablauf</b>	<b>Aktion</b>	<b>Beschreibung</b>
	Operation deregisterKonnektor des Registrierungsdienstes aufrufen	<p>Der Konnektor ruft den Dienst regService(deregPort) des VPN-Zugangsdienstes, mit der SOAP-Operation deregisterKonnektor(deregisterKonnektorRequest) gemäß ProvisioningService.wsdl, auf.</p> <p>Dabei wird SOAP über HTTPS verwendet. Die TLS-Verbindung erfordert eine beidseitige Authentifizierung.</p> <ul style="list-style-type: none"> <li>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.</li> <li>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.</li> </ul>
	Daten im SOAP-Request prüfen	<p>Der Registrierungsserver des VPN-Zugangsdienstes prüft die empfangenen Daten:</p> <ul style="list-style-type: none"> <li>Die Signatur des SOAP-Requests wird geprüft. Das zugehörige SMC-B-Zertifikat C.HCI.OSIG wird gemäß [gemSpec_PKI#TUC_PKI_018] geprüft.</li> <li>Das SMC-K-Zertifikat C.NK.VPN wird gemäß [gemSpec_PKI#TUC_PKI_018] geprüft.</li> </ul>

		<ul style="list-style-type: none"> <li>Die vpnk:ContractID aus dem Request wird mit den aus dem Vertrag zugeordneten Wert verglichen.</li> <li>Der Timestamp im Request wird mit der aktuellen Zeit im Registrierungsserver verglichen. Die Abweichung darf nicht mehr als 300 Sekunden betragen.</li> <li>Wenn alle Prüfungen erfolgreich waren, wird im Standardablauf fortgefahren. Anderenfalls wird eine Fehlermeldung generiert (siehe Abschnitt Fehler).</li> </ul>
	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.
<b>Rückgabe</b>	Name	Beschreibung
	SOAP-Response „deregisterKonnektorResponse“	<p>Dies ist eine SOAP-Response „deregisterKonnektorResponse“ gemäß ProvisioningService.xsd. Dabei gilt für eine erfolgreiche Deregistrierung:</p> <ul style="list-style-type: none"> <li>Das Element vpnk:Timestamp enthält den aktuellen</li> </ul>

		<p>Erstellungszeitstempel der SOAP-Response.</p> <ul style="list-style-type: none"> <li>Das Element vpnk:RegistrationStatus enthält den Status des Deregistrierungsvorgangs („Nicht registriert“).</li> <li>Das Element vpnk:ContractStatus enthält den Vertragsstatus („Zugriff auf TI erlaubt“, „Zugriff auf TI und SIS erlaubt“ oder „Kein Zugriff auf TI und SIS“).</li> <li>Das Element vpnk:AdditionalInformation enthält textuelle Informationen, die der Anbieter des VPN-Zugangsdienstes dem berechtigten Teilnehmer mitteilen möchte.</li> </ul>
<b>Zustand nach erfolgreichem Ablauf</b>	Der Konnektor ist beim Anbieter des VPN-Zugangsdienstes deregistriert und es kann keine IPsec-gesicherte Verbindung zum VPN-Konzentrator TI aufgebaut werden.	
<b>Zustand nach fehlerhaftem Ablauf</b>	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.	
<b>Nichtfunktionale Eigenschaften</b>	Keine	

1828 [ $\leq$ ]

### 1829 5.3.2.1 Umsetzung

1830 An die Umsetzung der Schnittstelle werden keine zusätzlichen Anforderungen gestellt.

### 1831 5.3.2.2 Nutzung

1832 An die Nutzung der Schnittstelle werden keine zusätzlichen Anforderungen gestellt.

## 1833 5.3.3 Operation registerStatus

### 1834 TIP1-A\_4392 - VPN-Zugangsdienst und Konnektor, Operation registerStatus

1835 Der VPN-Zugangsdienst MUSS für Konnektoren an der Schnittstelle  
1836 I\_Registration\_Service die Operation registerStatus gemäß Tabelle  
1837 Tab\_ZD\_registerStatus anbieten.

1838

1839 **Tabelle 12: Tab\_ZD\_registerStatus**

<b>Name</b>	registerStatus	
<b>Beschreibung</b>	Diese Operation ermöglicht den Registrierungsstatus und den Vertragsstatus bzgl. eines Konnektors abzufragen.	
<b>Vorbedingungen</b>	<ul style="list-style-type: none"> <li>Die URL des Registrierungsdienstes ist im Konnektor bekannt.</li> <li>Der FQDN des Registrierungsservers TI wurde in IP-Adressen aufgelöst.</li> </ul>	
<b>Aufrufparameter</b>	<b>Name</b>	<b>Beschreibung</b>
	SOAP-Request „registerStatusRequest“	<p>Dies ist ein SOAP-Request „registerStatusRequest“ gemäß ProvisioningService.xsd. Dabei gilt:</p> <ul style="list-style-type: none"> <li>Das Element vpnk:Timestamp enthält den aktuellen Erstellungszeitstempel des SOAP-Requests.</li> <li>Das Element vpnk:X509Certificate enthält die base64-Kodierung des ASN.1 DER-kodierten SMC-K-Zertifikats.</li> </ul>
<b>Standardablauf</b>	<b>Aktion</b>	<b>Beschreibung</b>
	Operation registerStatus des Registrierungsdienstes aufrufen	<p>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.</p> <ul style="list-style-type: none"> <li>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.</li> <li>Das Zertifikat C.HCI.AUT der zur Registrierung verwendeten SMC-B wird gemäß [gemSpec_PKI#TUC_PKI_018]</li> </ul>

		mit Prüfmodus OCSP durch den Registrierungsserver geprüft.
	Daten im SOAP-Request prüfen	<p>Der Registrierungsserver des VPN-Zugangsdienstes prüft die empfangenen Daten:</p> <ul style="list-style-type: none"> <li>Der Timestamp im Request wird mit der aktuellen Zeit im Registrierungsserver verglichen. Die Abweichung darf nicht mehr als 300 Sekunden betragen.</li> </ul> <p>Wenn die Prüfung erfolgreich war, wird im Standardablauf fortgefahren. Anderenfalls wird eine Fehlermeldung generiert (siehe Abschnitt Fehler).</p>
	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.
<b>Rückgabe</b>	<b>Name</b>	<b>Beschreibung</b>
	SOAP-Response „registerStatusResponse“	<p>Dies ist eine SOAP-Response „registerStatusResponse“ gemäß ProvisioningService.xsd. Dabei gilt für eine erfolgreiche registerStatus Abfrage:</p> <ul style="list-style-type: none"> <li>Das Element vpnk:Timestamp enthält den aktuellen Erstellungszeitstempel der SOAP-Response.</li> <li>Das Element vpnk:RegistrationTimestamp enthält den Erstellungszeitstempel der Registrierung.</li> <li>Das Element vpnk:RegistrationStatus enthält den Status des der Registrierung („Registriert“ oder „Nicht registriert“).</li> <li>Das Element vpnk:ContractStatus enthält den Vertragsstatus („Zugriff auf</li> </ul>



		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.
<b>Zustand nach erfolgreichem Ablauf</b>	Keine Änderung	
<b>Zustand nach fehlerhaftem Ablauf</b>	Keine Änderung	
<b>Nichtfunktionale Eigenschaften</b>	Keine	

1840 [ $\leq$ ]1841 **5.3.3.1 Umsetzung**

1842 An die Umsetzung der Schnittstelle werden keine zusätzlichen Anforderungen gestellt.

1843 **5.3.3.2 Nutzung**

1844 An die Nutzung der Schnittstelle werden keine zusätzlichen Anforderungen gestellt.

1845 **5.3.4 Operation sendData**1846 **A\_21159 - VPN-Zugangsdienst, Operation sendData**
 1847 Der VPN-Zugangsdienst MUSS an der Schnittstelle I\_Registration\_Service die Operation  
 1848 sendData gemäß Tabelle Tab\_ZD\_sendData anbieten.

 1849  
 1850 Tabelle 13: Tab\_ZD\_sendData

<b>Name</b>	sendData	
<b>Beschreibung</b>	Diese Operation ermöglicht es Daten (z.B. Betriebsdaten) an den Registrierungsdienst zu senden	
<b>Vorbedingungen</b>	<ul style="list-style-type: none"> <li>Die URL des Registrierungsdienstes ist bekannt.</li> <li>Der FQDN des Registrierungsservers TI wurde in IP-Adressen aufgelöst.</li> </ul>	
<b>Aufrufparameter</b>	<b>Name</b>	<b>Beschreibung</b>
	SOAP-Request „sendDataRequest“	Dies ist ein SOAP-Request „sendDataRequest“ gemäß ProvisioningService.xsd. Dabei gilt:

		<ul style="list-style-type: none"> <li>Das Element vpnk:Type enthält den Typ der Daten.</li> <li>Das Element vpnk:Base64Date enthält die base64-kodierten Daten.</li> </ul>
Standardablauf	Aktion	Beschreibung
	Operation sendData des Registrierungsdienstes aufrufen	<p>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.</p> <p>Die TLS-Verbindung erfordert eine beidseitige Authentifizierung.</p> <ul style="list-style-type: none"> <li>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.</li> <li>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.</li> </ul>
	Daten im SOAP-Request prüfen	<p>Der Registrierungsserver des VPN-Zugangsdienstes prüft die empfangenen Daten:</p> <ul style="list-style-type: none"> <li>Die dekodierten Base64Data entsprechen dem MimeType.</li> <li>Bei MimeType text/xml wird eine Schemaprüfung durchgeführt.</li> </ul> <p>Sind die gesendeten Daten vom Type OperatingDataConnector, so erfolgt die Schemaprüfung gegen das Schema conn/OperatingData.xsd.</p> <p>Wenn die Prüfung erfolgreich war, wird im Standardablauf fortgefahren. Anderenfalls wird eine Fehlermeldung generiert (siehe Abschnitt Fehler).</p>
	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.
<b>Rückgabe</b>	Name	Beschreibung
	SOAP-Response „sendDataResponse“	Dies ist eine SOAP-Response „sendDataResponse“ gemäß ProvisioningService.xsd. Dabei gilt für einen erfolgreichen sendData Request: <ul style="list-style-type: none"> <li>Das Element vpnk:Timestamp enthält den aktuellen Erstellungszeitstempel der SOAP-Response.</li> </ul>
<b>Zustand nach erfolgreichem Ablauf</b>	Keine Änderung	
<b>Zustand nach fehlerhaftem Ablauf</b>	Keine Änderung	
<b>Nichtfunktionale Eigenschaften</b>	Keine	

[&lt;=]

**A\_21160 - Bereitstellung von Betriebsdaten**

Der VPN-Zugangsdienst MUSS die vom Konnektor erhaltenen Betriebsdaten, reduziert um die ContractID und ergänzt um die Betriebsstättenart, an die Betriebsdatenerfassung gemäß gemSpec\_SST\_LD\_BD an die Schnittstelle I\_OpsData\_Update übermitteln.[<=]

**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.[<=]

**5.3.45.3.5 Registrierungsserver Fehlermeldungen****TIP1-A\_4491-02TIP1-A\_4491-01 - VPN-Zugangsdienst, Registrierungsserver Fehlermeldungen**

Der Registrierungsserver des VPN-Zugangsdienstes und der Konnektor MÜSSEN für die Operationen registerKonnektor, deregisterKonnektor und registerStatus die

1867 Fehlermeldungen gemäß Tabelle Tab\_Registrierungsserver\_Fehlermeldungen  
 1868 implementieren.  
 1869

1870 **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

1871 Weitere Elemente der Fehlermeldung müssen wie folgt angegeben werden:  
 1872 CompType = VPN-Zugangsdienst  
 1873 [ $\leq$ ]

## 1874 5.4 Schnittstelle I\_DNS\_Name\_Resolution (Namensraum TI)

### 1875 TIP1-A\_4497 - VPN-Zugangsdienst, sichere Speicherung des Key Signing Keys 1876 des TI Trust Anchors

1877 Die Nameserver im Namensraum TI des VPN-Zugangsdienstes MÜSSEN den Hash des  
 1878 Key Signing Key des TI Trust Anchors in aktueller Version enthalten und sicher speichern.  
 1879 Der Key Signing Key darf dabei nur durch autorisierte Akteure eingebracht werden.  
 1880 [ $\leq$ ]

1881 Weitere Vorgaben zur Schnittstelle I\_DNS\_Name\_Resolution und zu den zu nutzenden  
 1882 Standards sind in [gemSpec\_Net#5] beschrieben.

## 1883 **5.5 Schnittstelle I\_DNS\_Name\_Resolution (Namensraum Internet)**

1884 Die Vorgaben zur Schnittstelle I\_DNS\_Name\_Resolution und zu den zu nutzenden  
1885 Standards sind in [gemSpec\_Net#5] beschrieben.

## 1886 **5.6 Schnittstelle I\_DNS\_Name\_Resolution (Namensraum SIS)**

1887 Die Vorgaben zur Schnittstelle I\_DNS\_Name\_Resolution und zu den zu nutzenden  
1888 Standards sind in [gemSpec\_Net#5] beschrieben.

## 1889 **5.7 Schnittstelle I\_NTP\_Time\_Information**

1890 Die Vorgaben zur Schnittstelle I\_NTP\_Time\_Information und zu den zu nutzenden  
1891 Standards sind in [gemSpec\_Net#5] beschrieben.

1892

## 1893 **5.8 Prozess Änderung der Sicherheitsleistungen des SIS**

### 1894 **TIP1-A\_4399 - VPN-Zugangsdienst, Prozess Änderung der Sicherheitsleistungen** 1895 **des SIS**

1896 Der Anbieter des VPN-Zugangsdienstes MUSS einen Prozess implementieren, der die  
1897 Änderung von Sicherheitsleistungen des Secure Internet Service durch den GBV  
1898 ermöglicht.

1899 Der Anbieter des VPN-Zugangsdienstes ist der Eigentümer des Prozesses.

1900 [ $\leq$ ]

## 1901 **5.9 Prozess zum Abschluss, Ändern und Auflösen des** 1902 **Vertragsverhältnisses**

### 1903 **TIP1-A\_4498 - VPN-Zugangsdienst, Prozess Abschluss, Ändern und Auflösen** 1904 **des Vertragsverhältnisses sowie Deregistrierung von Konnektoren**

1905 Der Anbieter des VPN-Zugangsdienstes MUSS einen Prozess implementieren, der es  
1906 berechtigten Teilnehmern ermöglicht, mit dem Anbieter des VPN-Zugangsdienstes einen  
1907 Vertrag abzuschließen, zu ändern oder aufzulösen um Zugang zur TI inklusive  
1908 Bestandsnetze sowie Zugang zum sicheren Internetanschluss zu erhalten.

1909 Zusätzlich MUSS dieser Prozess ermöglichen, dass Konnektoren deregistriert werden  
1910 können.

1911 Der Anbieter des VPN-Zugangsdienstes ist der Owner des Prozesses.

1912 Vertragsdaten MÜSSEN bei Vertragsende nach Ablauf der gesetzlichen

1913 Aufbewahrungsfristen gelöscht werden.

1914 [ $\leq$ ]

1915 Damit der Konnektor sich mit den VPN-Konzentratoren TI und SIS verbinden kann,  
1916 müssen im Konnektor die Nameserver Internet und die Domain, die die SRV-Records der  
1917 VPN-Konzentratoren enthält, bekannt sein.

1918 Zur Registrierung des Konnektors beim Anbieter des VPN-Zugangsdienstes ist es  
1919 erforderlich, dass der Konnektor dem richtigen Vertrag zwischen berechtigtem  
1920 Teilnehmer und dem Anbieter des VPN-Zugangsdienstes zugeordnet werden kann. Zu  
1921 diesem Zweck wird ein Vertrags-Kennzeichen (CONTRACT\_ID\_VPN\_ZUGD) eingeführt.

1922 **TIP1-A\_5105 - VPN-Zugangsdienst, Konfigurationsdaten zur Übergabe bei**  
1923 **Vertragsabschluss**

1924 Der Anbieter des VPN-Zugangsdienstes MUSS die Daten gemäß  
1925 Tab\_ZD\_Konfigurationsdaten\_bei\_Vertragsabschluss im Rahmen des Vertragsabschlusses  
1926 an den jeweiligen berechtigten Teilnehmer übergeben.  
1927

1928 **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.

1929 [**<=**]

1930

## 6 Anhang A – Verzeichnisse

1931

### 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

## 1932 6.2 Glossar

1933 Das Glossar wird als eigenständiges Dokument (vgl. [gemGlossar]) zur Verfügung  
1934 gestellt.

## 1935 6.3 Abbildungsverzeichnis

1936	Abbildung 1: Netztopologie VPN-Zugangsdienst (logisch) .....	14
1937	Abbildung 2: Zerlegung des VPN-Zugangsdienstes .....	15
1938	Abbildung 3: Übersicht VPN-Zugangsdienst (Zonen) .....	16
1939	Abbildung 4: Ablauf der Operation I_Secure_Channel_Tunnel::connect im VPN-	
1940	Zugangsdienst .....	50
1941	Abbildung 1: Netztopologie VPN-Zugangsdienst (logisch) .....	14
1942	Abbildung 2: Zerlegung des VPN-Zugangsdienstes .....	15
1943	Abbildung 3: Übersicht VPN-Zugangsdienst (Zonen) .....	16
1944	Abbildung 4: Ablauf der Operation I_Secure_Channel_Tunnel::connect im VPN-	
1945	Zugangsdienst .....	50
1946		

## 1947 6.4 Tabellenverzeichnis

1948	Tabelle 1: Tab_ZD_Nameserver_Int_RR .....	24
1949	Tabelle 2: Tab_ZD_Nameserver_TI_RR .....	26
1950	Tabelle 3: Tab_ZD_Nameserver_Int_RR_IPv6 .....	46
1951	Tabelle 4: Tab_PT_VPN_Zugangsdienst_Schnittstellen .....	48
1952	Tabelle 5: Tab_ZD_Schnittstelle_I_Secure_Channel_Tunnel .....	49
1953	Tabelle 6: Tab_ZD_TUC_IPsec_Tunnel_TI_aufbauen .....	51
1954	Tabelle 7: Tab_ZD_Schnittstelle_I_Secure_Internet_Tunnel .....	56
1955	Tabelle 8: Tab_ZD_TUC_IPsec_Tunnel_SIS_aufbauen .....	57
1956	Tabelle 9: Tab_ZD_Schnittstelle_I_Registration_Service .....	61
1957	Tabelle 10: Tab_ZD_registerKonnektor .....	62
1958	Tabelle 11: Tab_ZD_deregisterKonnektor .....	67
1959	Tabelle 12: Tab_ZD_registerStatus .....	71
1960	Tabelle 13: Tab_Registrierungsserver_Fehlermeldungen .....	76
1961	Tabelle 14: Tab_ZD_Konfigurationsdaten_bei_Vetragsabschluss .....	78
1962	Tabelle 1: Tab_ZD_Nameserver_Int_RR .....	24
1963	Tabelle 2: Tab_ZD_Nameserver_TI_RR .....	26
1964	Tabelle 3: Tab_ZD_Nameserver_Int_RR_IPv6 .....	46

1965	Tabelle 4: Tab_PT_VPN-Zugangsdienst_Schnittstellen .....	48
1966	Tabelle 5: Tab_ZD_Schnittstelle_I_Secure_Channel_Tunnel .....	49
1967	Tabelle 6: Tab_ZD_TUC_IPsec_Tunnel_TI_aufbauen .....	51
1968	Tabelle 7: Tab_ZD_Schnittstelle_I_Secure_Internet_Tunnel .....	56
1969	Tabelle 8: Tab_ZD_TUC_IPsec_Tunnel_SIS_aufbauen .....	57
1970	Tabelle 9: Tab_ZD_Schnittstelle_I_Registration_Service .....	61
1971	Tabelle 10: Tab_ZD_registerKonnektor.....	62
1972	Tabelle 11: Tab_ZD_deregisterKonnektor .....	67
1973	Tabelle 12: Tab_ZD_registerStatus .....	71
1974	Der VPN-Zugangsdienst MUSS an der Schnittstelle I_Registration_Service die Operation	
1975	sendData gemäß Tabelle Tab_ZD_sendData anbieten. Tabelle 13:	
1976	Tab_ZD_sendData.....	73
1977	Tabelle 14: Tab_Registrierungsserver_Fehlermeldungen .....	76
1978	Tabelle 15: Tab_ZD_Konfigurationsdaten_bei_Vetragsabschluss .....	78
1979		

## 1980 6.5 Referenzierte Dokumente

### 1981 6.5.1 Dokumente der gematik

1982 Die nachfolgende Tabelle enthält die Bezeichnung der in dem vorliegenden Dokument  
 1983 referenzierten Dokumente der gematik zur Telematikinfrastruktur. Der mit der  
 1984 vorliegenden Version korrelierende Entwicklungsstand dieser Konzepte und  
 1985 Spezifikationen wird pro Release in einer Dokumentenlandkarte definiert; Version und  
 1986 Stand der referenzierten Dokumente sind daher in der nachfolgenden Tabelle nicht  
 1987 aufgeführt. Deren zu diesem Dokument jeweils gültige Versionsnummern sind in der  
 1988 aktuellen, von der gematik veröffentlichten Dokumentenlandkarte enthalten, in der die  
 1989 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
----------------	--

1990

## 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, <a href="http://tools.ietf.org/html/rfc2119">http://tools.ietf.org/html/rfc2119</a>
[RFC2782]	RFC 2782 (Februar 2000): A DNS RR for specifying the location of services (DNS SRV) <a href="http://www.ietf.org/html/rfc2782">http://www.ietf.org/html/rfc2782</a>
[RFC3173]	IETF (2001): IP Payload Compression Protocol (IPComp)
[RFC4301]	RFC 4301 (Dezember 2005): Security Architecture for the Internet Protocol <a href="http://tools.ietf.org/html/rfc4301">http://tools.ietf.org/html/rfc4301</a>
[RFC4303]	RFC 4303 (Dezember 2005): IP Encapsulating Security Payload (ESP); <a href="http://tools.ietf.org/html/rfc4303">http://tools.ietf.org/html/rfc4303</a>
[RFC7296]	RFC 7296 (Oktober 2014): Internet Key Exchange Protocol Version 2 (IKEv2); <a href="https://tools.ietf.org/html/rfc7296">https://tools.ietf.org/html/rfc7296</a>
[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 <a href="https://tools.ietf.org/html/rfc7383">https://tools.ietf.org/html/rfc7383</a>

1991

1992