Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

Einführung der Gesundheitskarte

Übergreifende Spezifikation Netzwerk

Version:	1.6.0
Revision:	\main\rel_online\rel_ors1\25
Stand:	17.07.2015
Status:	freigegeben
Klassifizierung:	öffentlich
Referenzierung:	gemSpec_Net

Dokumentinformationen

Änderungen zur Vorversion

Einarbeitung bzgl. der Errata 1.4.4 und KOM-LE.

Dokumentenhistorie

Version	Datum	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
0.5.0	20.07.12		zur Abstimmung freigegeben	PL P77
0.6.0	31.08.12		Einarbeitung von Änderungen aus dem Kommentierungsverfahren	P77
1.0.0	15.10.12		Korrekturen	gematik
1.1.0	12.11.12		Einarbeitung Kommentare aus übergreifender Konsistenzprüfung	gematik
1.2.0	13.06.13		Überarbeitung anhand interner Änderungsliste (Fehlerkorrekturen, Inkonsistenzen), Einarbeitung Kommentare LA	gematik
1.3.0	15.08.13		Einarbeitung Kommentar und gemäß Änderungsliste	gematik
1.4.0	21.02.14		Losübergreifende Synchronisation	gematik
1.5.0	17.06.14		[RFC4594bis] ersetzt durch [RFC4594], [RFC2672] gelöscht (Anforderung entfällt), Ergänzung DNSSEC-Vertrauensanker-Aktualisierung gemäß [RFC5011] und Formulierungsanpassungen gemäß P11-Änderungsliste	gematik
			Errata 1.4.4 und KOM-LE-Anpassungen eingearbeitet	gematik
1.6.0	17.07.15		freigegeben	gematik

Inhaltsverzeichnis

Dokumentinformationen **2**

Inhaltsverzeichnis **3**

1 Einordnung des Dokuments **6**

1.1 Zielsetzung **6**

1.2 Zielgruppe **6**

1.3 Geltungsbereich **6**

1.4 Abgrenzung des Dokuments **7**

1.5 Methodik **7**

2 Übergreifende Netzwerk-Festlegungen **8**

2.1 Netztopologie **8**

2.2 Netzwerkprotokolle **9**

2.2.1 OSI-Schicht 1 und 2 (Physical/Data Link) 9

2.2.2 OSI-Schicht 3 (Network) 9

2.2.2.1 IP-Version 4 ..... *9*

2.2.2.2 IP-Version 6 ..... *10*

2.2.3 OSI-Schicht 4 (Transport) 10

2.2.3.1 Transmission Control Protocol (TCP) und User Datagram Protocol (UDP) *10*

2.2.3.2 UDP/TCP-Portbereiche *11*

2.2.3.3 Transport Layer Security (TLS) *12*

2.3 IP-Adresskonzept der TI **12**

2.3.1 Adressblöcke 12

2.3.2 Prozesse zur IP-Adressvergabe 13

2.3.3 Adresskonzept IPv4 15

2.3.4 Adresskonzept IPv6 19

2.3.5 Adressen SIS-Systeme 19

2.4 IP-Routingkonzept **19**

2.5 Priorisierung auf Netzwerkebene **20**

2.5.1 Architektur 20

2.5.2 Definition und Zuordnung von Dienstklassen 20

2.5.3 Markierung 21

2.5.3.1 DSCP-Markierung Netzkonnektor *23*

2.5.3.2 DSCP-Markierung Zentrales Netz TI *23*

2.5.3.3 DSCP-Markierung Fremdnetze *24*

2.5.4 Priorisierung des markierten Datenverkehrs 25

2.5.4.1 Zentrales Netz *25*

2.5.4.2 Konnektor ... 26
2.5.4.3 VPN-Zugangsdienst ... 27

2.6 Sicherheitskomponenten im Netzwerk ... 27
2.6.1 Typen von Sicherheitskomponenten ... 27
2.6.2 Anforderungen an Sicherheitskomponenten ... 28
2.6.3 Platzierung von Sicherheitskomponenten ... 29
2.6.4 Prozesse zu Regeln für Sicherheitsgateways ... 31
2.6.5 Erlaubter Verkehr ... 32
2.6.6 Anforderungen an das Sicherheitsgateway KV-SafeNet ... 33

3 Zentrales Netz der TI ... 34

3.1 Zerlegung des Produkttyps ... 34
3.1.1 Sicherer Zentraler Zugangspunkt (SZZP) ... 35
3.1.1.1 Netzkomponente ... 35
3.1.1.2 Sicherheitsgateway ... 36
3.1.1.3 Anbindungen ... 36
3.1.2 Netzwerk ... 38
3.1.2.1 Backbone (zentrales Transportnetz Provider) ... 38

3.2 Übergreifende Festlegungen ... 39

3.3 Funktionsmerkmale ... 40
3.3.1 OSI-Schicht 1 und 2 (Physical/Data Link) ... 40
3.3.1.1 Schnittstelle CPE-Produkttyp ... 40
3.3.1.2 Hardwaremerkmale ... 41
3.3.2 OSI-Schicht 3 (Network) ... 41
3.3.2.1 Schnittstelle I_IP_Transport ... 41
3.3.3 Adressierung ... 41
3.3.3.1 Schnittstelle SZZP-Backbone (CE-PE) und SZZP intern ... 41
3.3.4 Routing ... 42
3.3.5 Abstimmung mit angeschlossenen Produkttypen ... 42

3.4 Verteilungssicht ... 43
3.4.1 Zugangsstellen ... 43

4 Namensdienst ... 45

4.1 Hostnamen ... 45

4.2 Namensräume ... 45

4.3 Domainnamen- und Hierarchie ... 46

4.4 DNS-Topologie ... 48

4.5 Dienstlokalisierung ... 50

4.6 Schnittstellen I_DNS_Name_Resolution und I_DNS_Service_Localization 51
4.6.1 Umsetzung ... 51
4.6.2 Nutzung ... 54

4.7 Anforderungen an den Produkttyp Namensdienst ... 54
4.7.1 Schnittstellen P_DNS_Name_Entry_Announcement und P_DNS_Service_Entry_Announcement ... 55
4.7.2 Schnittstelle P_DNSSEC_Key_Distribution ... 55

4.7.3 Schnittstelle P_DNS_Zone_Delegation 57
4.7.4 Sonstige Anforderungen 57

5 Zeitdienst 58

5.1 NTP-Topologie 58

5.2 Schnittstelle I_NTP_Time_Information 60
5.2.1 Umsetzung 60
5.2.2 Nutzung 61

5.3 Anforderungen an den Produkttyp Zeitdienst 62

Anhang A – Verzeichnisse 65

A1 – Abkürzungen 65

A2 – Glossar 65

A3 – Abbildungsverzeichnis 66

A4 – Tabellenverzeichnis 66

A5 – Referenzierte Dokumente 66
A5.1 – Dokumente der gematik 66
A5.2 – Weitere Dokumente 67

1 Einordnung des Dokuments

1.1 Zielsetzung

Die Spezifikation Netzwerk definiert die Rahmenbedingungen und trifft die übergreifenden Festlegungen zum Netzwerk, dem Namensdienst und dem Zeitdienst in der TI. Dabei werden die für den Online-Rollout (Stufe 1) erforderlichen Anforderungen an die Netzinfrastruktur berücksichtigt, eine Erweiterbarkeit um künftige Anwendungen jedoch beachtet.

Die übergreifende Spezifikation Netzwerk behandelt folgende inhaltlichen Schwerpunkte:

- Netztopologie und Netzumgebungen
- Vorgaben zu grundlegenden Netzwerkprotokollen
- IP-Adresskonzept - Definition von Adressbereichen
- IP-Routingkonzept
- Priorisierung auf Netzwerkebene
- Vorgaben zu Sicherheitskomponenten
- Namenskonzept - Vorgaben zu Namensräumen und DNS
- Vorgaben zum Zeitdienst

1.2 Zielgruppe

Das Dokument richtet sich an Hersteller und Anbieter von netzwerkfähigen Produkten der TI.

1.3 Geltungsbereich

Dieses Dokument enthält normative Festlegungen zur Telematikinfrastruktur des deutschen Gesundheitswesens. Der Gültigkeitszeitraum der vorliegenden Version und deren Anwendung in Zulassungsverfahren wird 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 des Dokuments

Festlegungen zu der Netzwerkkomponente VPN-Zugangsdienst erfolgen in [gemSpec_VPN_ZugD].

Die Festlegung der spezifischen Anbindungen von Komponenten an die Netzinfrastruktur der TI und die Einbindung der Netzdienste erfolgen auf der Basis dieser übergreifenden Spezifikation in den jeweiligen Spezifikationen der Produkttypen.

1.5 Methodik

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

Sie werden im Dokument wie folgt dargestellt:

⌦ **GS-A_0000 <Titel der Afo>**

Text / Beschreibung⌫

Dabei umfasst die Anforderung sämtliche innerhalb der Textmarken angeführten Inhalte.

2 Übergreifende Netzwerk-Festlegungen

2.1 Netztopologie

In diesem Kapitel wird die grundlegende Netztopologie der TI dargestellt um einen Überblick der beteiligten Systeme auf der Netzwerkebene zu geben. In den Spezifikationen der jeweiligen Produkttypen erfolgt, wo notwendig, eine detaillierte Darstellung der einzusetzenden Netztopologie.

Die Abb_NetzTopologie_Schema zeigt eine schematische Übersicht zur Netztopologie der TI auf logischer Ebene, die sich an den in der Gesamtarchitektur definierten Zonen orientiert.

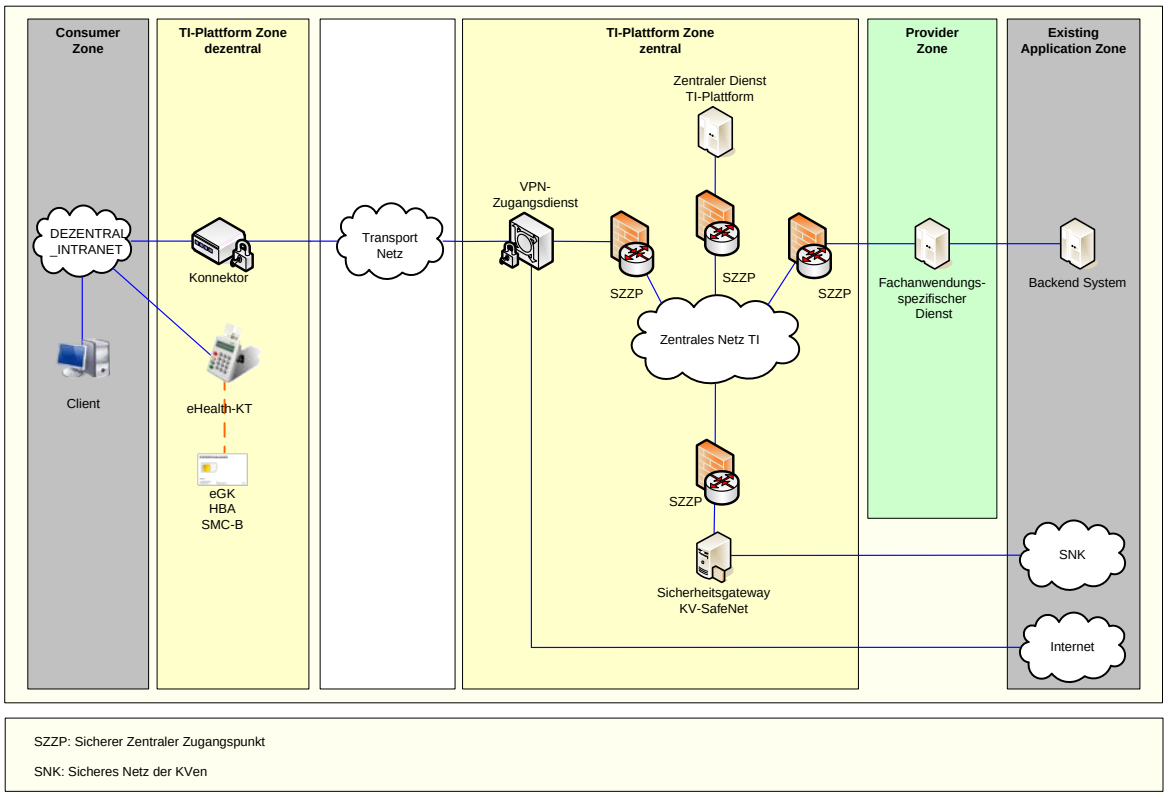


Abbildung 1: Abb_NetzTopologie_Schema, Netztopologie der TI

In Abb_NetzTopologie_Detail wird auf einer detaillierteren Netzwerkebene die mögliche Verteilung von an der TI-Plattform angebundenen Produkttypen dargestellt (ohne Secure Internet Service (SIS)).

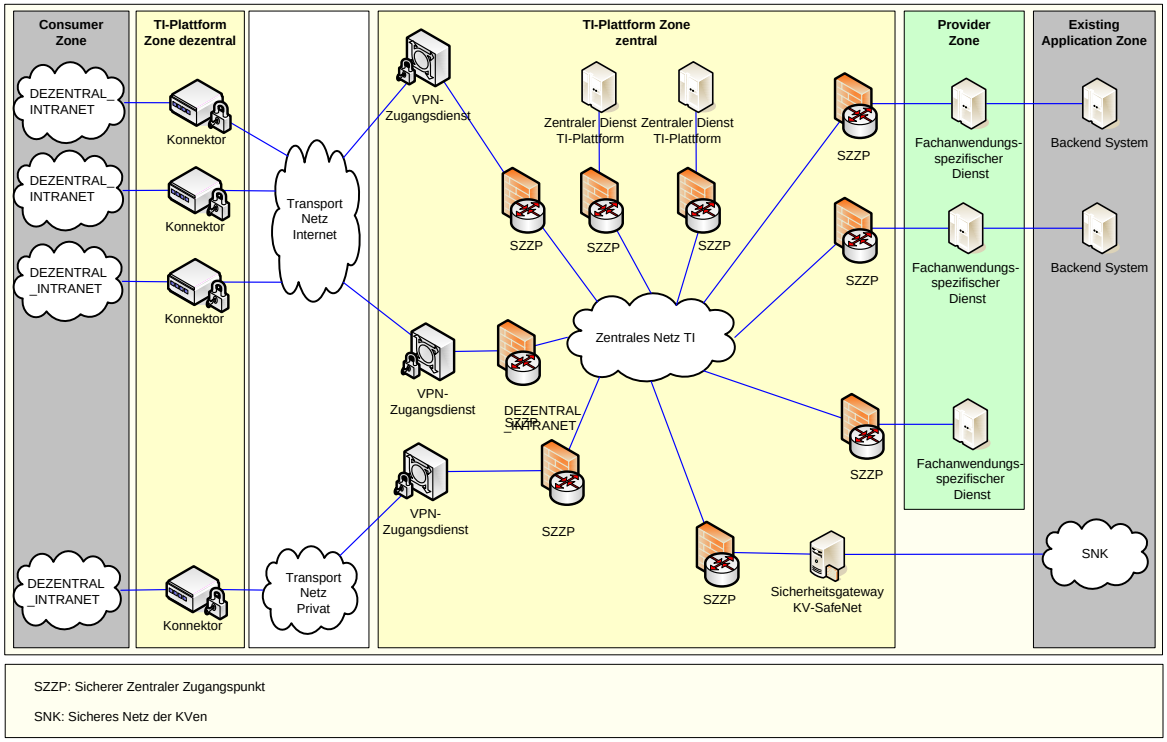


Abbildung 2: Abb_NetzTopologie_Detail, Netzwerktopologie der TI - detailliert

2.2 Netzwerkprotokolle

2.2.1 OSI-Schicht 1 und 2 (Physical/Data Link)

⌦ GS-A_4009 Übertragungstechnologie auf OSI-Schicht LAN

Alle Produkttypen der TI MÜSSEN beim Einsatz des Ethernet-Protokolls an Schnittstellen zwischen Produkttypen der TI die Einhaltung der [IEEE 802.3] sicherstellen. ⌫

2.2.2 OSI-Schicht 3 (Network)

Als produktiv eingesetztes Netzwerkprotokoll auf der OSI-Schicht 3 wird in der TI das Internetprotokoll in der Version 4 (IPv4) eingesetzt. Zur Vorbereitung einer späteren Migration wird bei definierten Produkttypen bereits die Unterstützung des Internetprotokolls in der Version 6 (IPv6) gefordert. Vorgaben zum Protokoll Encapsulation Security Payload (ESP) werden in [gemSpec_VPN_ZugD] definiert.

2.2.2.1 IP-Version 4

⌦ GS-A_4831 Standards für IPv4

Produkttypen der TI MÜSSEN mindestens die in Tab_Standards_IPv4 aufgeführten Standards unterstützen.

Tabelle 1: Tab_Standards_IPv4, Standards IPv4

Standard	Beschreibung
[RFC768]	User Datagram Protocol
[RFC791]	Internet Protocol
[RFC792]	Internet Control Message Protocol
[RFC793]	Transmission Control Protocol
[RFC826]	Ethernet Address Resolution Protocol
[RFC894]	Standard for the Transmission of IP Datagrams over Ethernet Networks
[RFC1122]	Requirements for Internet Hosts – Communication Layers

⌫

⌦ **GS-A_4832 Path MTU Discovery**

Produkttypen der TI MÜSSEN sicherstellen, dass Path MTU Discovery (PMTUD) gemäß [RFC1191] im gesamten Netzwerk funktioniert. Insbesondere MÜSSEN Router und Gateways die erforderlichen ICMP-Messages erzeugen, und Sicherheitsgateways MÜSSEN diese ICMP-Messages passieren lassen.⌫

2.2.2.2 IP-Version 6

⌦ **GS-A_4010 Standards für IPv6**

Produkttypen, die zentrale Dienste der TI-Plattform bereitstellen, MÜSSEN die in [RIPE-554] für die jeweilige Geräteklasse unter Mandatory Support aufgeführten Anforderungen erfüllen. ⌫

⌦ **GS-A_4011 Unterstützung des Dual-Stack Mode**

Zentrale Dienste der TI-Plattform MÜSSEN IPv4 und IPv6 parallel als Protokoll (Dual-Stack-Mode) unterstützen. Die TSP X.509 SOLLEN IPv4 und IPv6 parallel unterstützen.⌫

⌦ **GS-A_4012 Leistungsanforderungen an den Dual-Stack Mode**

Produkttypen, die zentrale Dienste der TI-Plattform bereitstellen, MÜSSEN IPv4 und IPv6 als Protokoll unterstützen, wobei für beide Protokolle eine vergleichbare Leistung vorhanden sein muss, d. h. weniger als 15% Unterschied zwischen den beiden Protokollen bei Input, Output, Durchsatz, Weiterleitung und Verarbeitung. ⌫

2.2.3 OSI-Schicht 4 (Transport)

2.2.3.1 Transmission Control Protocol (TCP) und User Datagram Protocol (UDP)

Für die Implementierung von TCP und UDP werden an dieser Stelle keine normativen Vorgaben erhoben. Es wird empfohlen Implementierungen von TCP/IP-Stacks zu nutzen, die aktuelle Verfahren zur Übertragung und Steuerung von Daten einsetzen.

2.2.3.2 UDP/TCP-Portbereiche

Für die Verwaltung und Dokumentation von UDP/TCP-Portbereichen ist in der TI ein übergreifender Prozess zu etablieren, der durch den Anbieter Zentrales Netz TI implementiert und vom Gesamtbetriebsverantwortlichen (GBV) freigegeben wird.

In den folgenden Anforderungen werden die Verantwortlichkeiten und weitere Vorgaben zum Prozess „Verwaltung von UDP/TCP-Portbereichen“ definiert.

⌦ GS-A_4833 Prozess „Verwaltung von UDP/TCP-Portbereichen“ –Definition/Implementierung

Der Anbieter Zentrales Netz TI MUSS den Prozess „Verwaltung von UDP/TCP-Portbereichen“ mit den folgenden Inhalten definieren und implementieren:

- Erstellung und Pflege eines Vergabeschemas für UDP/TCP-Portbereiche
- Operative Vergabe von UDP/TCP-Portbereichen
- Erstellung und Pflege von Dokumentations- und Reportingschemas
- Dokumentation und Reporting von UDP/TCP-Portbereichen

Der Anbieter Zentrales Netz TI ist der Verantwortliche für den gesamten Prozess.⌫

⌦ GS-A_4886 Prozess „Verwaltung von UDP/TCP-Portbereichen“ - Freigabe

Der GBV MUSS den vom Anbieter Zentrales Netz TI definierten Prozess „Verwaltung von UDP/TCP-Portbereichen“ freigeben.⌫

⌦ GS-A_4014 Vergabeschema für UDP/TCP-Portbereiche

Der GBV MUSS für die Zuteilung von UDP/TCP-Portbereichen ein Vergabeschema unter Berücksichtigung der Dienstklassen zur Netzwerkpriorisierung erstellen und dem Anbieter Zentrales Netz TI zur Verfügung stellen.

Der GBV MUSS das Vergabeschema für UDP/TCP-Portbereiche auf Grundlage des [RFC6335] erstellen. Der GBV MUSS für die Vergabe von UDP/TCP-Portbereichen den in [RFC6335] definierten Bereich von 49152-65535 (Dynamic/Private Ports) nutzen. Hiervon ausgenommen sind Anwendungen die in [RFC6335] definierte Bereiche der System Ports (Well-Known Ports) bzw. User Ports (Registered Ports) nutzen.⌫

⌦ GS-A_4016 Operative Vergabe von UDP/TCP-Portbereichen

Der Anbieter Zentrales Netz TI MUSS UDP/TCP-Portbereiche nach den Vorgaben des Vergabeschemas an die einzelnen Anbieter der Produkttypen der TI bedarfsgerecht zuweisen. Die Vergabe der UDP/TCP-Portbereiche erfolgt im Rahmen des Test- und Zulassungsverfahrens von Anbietern eines Produkttyps.⌫

⌦ GS-A_4013 Nutzung von UDP/TCP-Portbereichen

Produkttypen von Fachanwendungen und Zentralen Diensten der TI-Plattform MÜSSEN die zugeordneten UDP/TCP-Portbereiche für die Kommunikation in der TI nutzen.⌫

⌦ **GS-A_4753 Dokumentationsformat UDP/TCP-Portbereiche**

Der GBV MUSS in Abstimmung mit dem Anbieter Zentrales Netz TI das Dokumentationsformat für die UDP/TCP-Portbereiche festlegen und dem Anbieter von Produkttypen der TI zur Verfügung stellen.⌫

⌦ **GS-A_4017 Dokumentation UDP/TCP-Portbereiche GBV**

Der Anbieter Zentrales Netz TI MUSS die Vergabe der UDP/TCP-Portbereiche dokumentieren und diese Dokumentation dem GBV bei Änderungen und auf Anforderung zur Verfügung stellen.⌫

⌦ **GS-A_4018 Dokumentation UDP/TCP-Portbereiche Anbieter**

Die Anbieter von Produkttypen der TI MÜSSEN die Nutzung der zugeteilten UDP/TCP-Portbereiche dokumentieren und diese Dokumentation dem Anbieter Zentrales Netz TI bei Änderungen und auf Anforderung zur Verfügung stellen.⌫

2.2.3.3 Transport Layer Security (TLS)

Anforderungen zu den einzusetzenden kryptographischen Verfahren für TLS und daraus folgende resultierende Vorgaben zur TLS-Version werden in [gemSpec_Krypt] definiert.

Weitere Eigenschaften und Funktionen für das TLS-Protokoll können wo notwendig in den Spezifikationen von Produkttypen festgelegt werden.

2.3 IP-Adresskonzept der TI

In diesem Kapitel werden Festlegungen zu den in der TI zu nutzenden IP-Adressbereichen getroffen. Alle Anbieter von Produkttypen müssen das IP-Adresskonzept der TI produktiv umsetzen.

2.3.1 Adressblöcke

Die IP-Adressen in der TI werden in festen Adressblöcken an die Nutzer vergeben. Die zu nutzenden IP-Adressblöcke werden den definierten TI-Umgebungen und den dazugehörigen Netzbereichen zugeteilt.

Für jede TI-Umgebung werden zusätzlich IP-Adressblöcke als Reserve definiert.

TI-Umgebungen:

- Produktivumgebung
- Testumgebung
- Referenzumgebung

Netzbereiche:

- TI_Dezentral_SIS: Adressen für Verbindungen des Sicheren Internet Service vom Konnektor zum VPN-Zugang
- TI_Dezentral: Adressen für Verbindungen zur TI vom Konnektor zum VPN-Zugang
- TI_Zentral: Adressen für zentrale Dienste der TI
- TI_Fachdienste: Adressen für Fachdienste

Informativ wird zusätzlich der Netzbereich TI_Extern aufgeführt:

- DEZ_Transport: Anschlusspunkt einer Organisation des Gesundheitswesens an das Transportnetz, über das die Verbindung zwischen Konnektor und VPN-Zugangsdienst hergestellt wird.
- VPN_SIS: Anschlusspunkt des VPN-Zugangs zum Sicheren Internet Service (SIS)
- KVS: Öffentlicher Adressbereich des KV-SafeNets, das an die TI angekoppelt wird.
- DEZENTRAL_INTRANET: Netzwerke die über Konnektoren an die TI angeschlossen sind.
- Bestandsnetze: Bestehende Netzwerke, die (zukünftig) Anschluss an die TI erhalten sollen.
- VPN_TRANSPORT_TI: Zugangspunkt zum VPN-Konzentrator der TI (aus dem Transportnetz)
- VPN_TRANSPORT_SIS: Zugangspunkt zum VPN-Konzentrator der Sicheren Internet Services (aus dem Transportnetz)
- SIS: Systeme des Sicheren Internet Services

Über diese Netzbereiche werden hier keine Festlegungen getroffen, Adressvergabe geschieht durch die Besitzer oder Anbieter.

2.3.2 Prozesse zur IP-Adressvergabe

Für die Verwaltung und Dokumentation von IP-Adressen ist in der TI ein übergreifender Prozess zu etablieren, der durch den Anbieter Zentrales Netz TI implementiert und vom GBV freigegeben wird.

Die in der TI genutzten IP-Adressen werden von dem Anbieter Zentrales Netz TI verwaltet und im Auftrag des GBVs vergeben. Der Anbieter delegiert IP-Bereiche aus den spezifizierten Bereichen an Anbieter von TI-Produkttypen.

In den folgenden Anforderungen werden die Verantwortlichkeiten und weitere Vorgaben zum Prozess „Verwaltung von IP-Adressbereichen“ definiert.

⌦ **GS-A_4834 Prozess „Verwaltung von IP-Adressbereichen“**

Der Anbieter Zentrales Netz TI MUSS den Prozess „Verwaltung von IP-Adressbereichen“ mit den folgenden Inhalten definieren und implementieren:

- Pflege des IP-Adresskonzeptes für die TI
- Freigabe von zu nutzenden IP-Adressbereichen
- Operative Zuweisung von IP-Adressbereichen
- Erstellung und Pflege von Dokumentations- und Reportingschemas
- Dokumentation und Reporting der genutzten IP-Adressbereiche

Der Anbieter Zentrales Netz TI ist der Verantwortliche für den gesamten Prozess.⌫

⌦ **GS-A_4888 Prozess „Verwaltung von IP-Adressbereichen“ - Freigabe**

Der GBV MUSS den vom Anbieter Zentrales Netz TI definierten Prozess „Verwaltung von IP-Adressbereichen“ freigeben.⌫

⌦ **GS-A_4021 GBV Freigabe TI IP-Bereiche**

Der GBV MUSS für die Nutzung erlaubte IP-Adressbereiche und deren Vergabe in der TI freigeben.⌫

⌦ **GS-A_4022 Koordinierung Adressvergabe**

Der Anbieter Zentrales Netz TI MUSS die Adressvergabe operativ mit dem GBV und den Anbietern der Produkttypen in der TI koordinieren.⌫

⌦ **GS-A_4023 Zuweisung IP-Adressbereiche**

Der Anbieter Zentrales Netz TI MUSS im Rahmen des Test- und Zulassungsverfahrens IP-Adressbereiche an die einzelnen Anbieter der Produkttypen bedarfsgerecht zuweisen.⌫

⌦ **GS-A_4754 Zuweisung IP-Adressbereiche, Reservierung**

Der Anbieter Zentrales Netz TI SOLL den IP-Adressbereich als zusammenhängendes Subnetz (IPv4) an die einzelnen Anbieter der Produkttypen vergeben. Als Reservenetz soll er das darauf folgende, gleich große Subnetz vergeben, das jedoch nur nach Freigabe durch den Anbieter Zentrales Netz TI genutzt werden darf.⌫

⌦ **GS-A_4024 Nutzung IP-Adressbereiche**

Alle Anbieter von Diensten in der TI MÜSSEN für ihre über die TI erreichbaren Systeme die zugewiesenen IP-Bereiche nutzen. Änderungen an diesen Bereichen MÜSSEN die Anbieter einzelner TI-Dienste bei dem Anbieter Zentrales Netz TI beantragen.⌫

⌦ **GS-A_4026 Dokumentation IP-Adressbereiche**

Der Anbieter Zentrales Netz TI MUSS die Vergabe der IP-Adressbereiche dokumentieren und diese Dokumentation dem GBV bei Änderungen und auf Anforderung zur Verfügung stellen.⌫

⌦ **GS-A_4756 Reporting IP-Adressbereiche, Form**

Der Anbieter Zentrales Netz TI MUSS das Format zum Reporting der IP-Adressbereiche festgelegen.⌫

⌦ **GS-A_4027 Reporting IP-Adressbereiche**

Alle Anbieter von Diensten in der TI MÜSSEN dem Anbieter Zentrales Netz TI die Vergabe der IP-Adressbereiche dokumentieren und Änderungen an den Anbieter Zentrales Netz TI melden. Die Anbieter MÜSSEN jeweils sowohl die Änderungen als auch die Gesamtübersicht zum zugewiesenen Adressblock melden. Die Dokumentation der Nutzung von dynamisch vergebenen IP-Adressen soll nicht erfolgen.⌫

⌦ **GS-A_4028 Reserve IP-Bereiche, Freigabe**

Der GBV MUSS die in Tabelle Tab_Adrkonzept_Produktiv mit "Reserve" markierten IP-Adressbereiche im Bedarfsfall freigeben und an den Anbieter Zentrales Netz TI zur operativen Verteilung vergeben.⌫

⌦ **GS-A_4758 IPv4-Adressen SZZP zum Produkttyp**

Der Anbieter Zentrales Netz MUSS für die Adressierung der SZZPs in Richtung Produkttyp IP-Adressen aus dem zugewiesenen /26 IP-Bereich des angeschlossenen Produkttyps nutzen.⌫

⌦ **GS-A_4759 IPv4-Adressen Produkttyp zum SZZP**

Anbieter von an das Zentrale Netz der TI angeschlossenen Produkttypen MÜSSEN für die Adressierung ihrer Systeme in Richtung SZZP IP-Adressen aus dem ihnen zugewiesenen /26 IP-Bereich nutzen.⌫

2.3.3 Adresskonzept IPv4

Die folgenden Tabellen legen die zu verwendenden IPv4-Adressbereiche für die einzelnen TI-Umgebungen fest.

Die Anbieter von TI-Produkttypen erhalten in der Produktivumgebung Adressbereiche aus dem IPv4-Adressraum 100.64.0.0/10 [RFC6598]. Durch die Nutzung des in [RFC6598] definierten Adressbereiches wird ein Konflikt mit bereits genutzten privaten Adressbereichen vermieden. Die Testumgebung ist getrennt und nutzt den Adressraum 172.16.0.0/12.

⌦ **GS-A_4029 IPv4-Adresskonzept Produktivumgebung**

Der Anbieter Zentrales Netz TI MUSS den Adressbereich 100.64.0.0/10 nach dem in der Tab_Adrkonzept_Produktiv definierten Schema zur Vergabe von IPv4-Adressen an Produkttypen der TI in der Produktivumgebung verwenden.

Tabelle 2: Tab_Adrkonzept_Produktiv, Adressräume IPv4 TI Produktivumgebung

Netzbereich	Adressen	Netz	Nutzung	Verantwortlich
TI-Produktivumgebung	4M	100.64.0.0/10	TI Produktiv	Anbieter Zentrales Netz TI und GBV
TI_Dezentral_SIS	1M	100.64.0.0/12	Dezentral SIS	Anbieter Zentrales Netz TI
Konnektoren	1M	100.64.0.0/12	Konnektoren SIS	Anbieter Zugangsdienst
TI_Dezentral	1M	100.80.0.0/12	Dezentral	Anbieter Zentrales Netz TI
Konnektoren	1M	100.80.0.0/12	Konnektoren TI	Anbieter Zugangsdienst
TI_Zentral	256K	100.96.0.0/14	Zentrale Dienste	Anbieter Zentrales Netz TI
Zentrale Dienste	64K	100.96.0.0/16	Zentrale Dienste	Anbieter Zentraler Dienste
	Der Anbieter Zentrales Netz TI weist jedem zentralen Dienst ein /26 Adressblock aus dem Bereich 100.96.0.0/16 zu.			
VPN-Konzentrator	64K	100.97.0.0/16	Anschluss VPN-Konzentratoren an die TI	Anbieter Zugangsdienst
	Der Anbieter Zentrales Netz TI weist jedem VPN-Zugangsdienstprovider ein /26 Adressblock aus dem Bereich 100.97.0.0/16 zu.			
Reserveblöcke	128K	100.98.0.0/15	Reserve	Anbieter Zentrales Netz TI
TI_Fachdienste	256K	100.100.0.0/14	Fachdienste	Anbieter Zentrales Netz TI
Offene Fachdienste	64K	100.102.0.0/16	Offene Fachdienste	Anbieter Offene Fachdienste
	Der Anbieter Zentrales Netz TI weist jedem Offenen Fachdienst ein /26 Adressblock aus dem Bereich 100.102.0.0/16 zu			
Gesicherte Fachdienste	64K	100.100.0.0/16	Gesicherte Fachdienste	Anbieter Gesicherte Fachdienste
	Der Anbieter Zentrales Netz TI weist jedem Gesicherten Fachdienst ein /26 Adressblock aus dem Bereich 100.100.0.0/16 zu			
Reserveblöcke	128K	100.101.0.0/16	Reserve	Anbieter Zentrales Netz TI

© gematik – öffentlich

Netzbereich	Adressen	Netz	Nutzung	Verantwortlich
		100.103.0.0/16		
TI_Betriebsreserve	1.5M	100.104.0.0/13 100.112.0.0/12	Reserve	Anbieter Zentrales Netz TI

⌫

⌦ GS-A_4850 IPv4-Adresskonzept Testumgebung

Der Anbieter Zentrales Netz TI MUSS den Adressbereich 172.16.0.0/12 nach dem in Tab_Adrkonzept_Test definierten Schema zur Vergabe von IPv4-Adressen an Produkttypen der TI in der Testumgebung verwenden.

Tabelle 3: Tab_Adrkonzept_Test, Adressräume IPv4 TI-Testumgebung

Netzbereich	Adressen	Netz	Nutzung	Verantwortlich
TI-Testumgebung	1M	172.16.0.0/12	TI Test	Anbieter Zentrales Netz TI
TI_Test_Dezentral_SIS	256K	172.16.0.0/14	Dezentral SIS	Anbieter Zentrales Netz TI
Konnektoren	256K	172.16.0.0/14	Konnektoren SIS	Anbieter Zugangsdienst
TI_Test_Dezentral	256K	172.20.0.0/14	Dezentral	Anbieter Zentrales Netz TI
Konnektoren	256K	172.20.0.0/14	Konnektoren TI	Anbieter Zugangsdienst
TI_Test_Zentral	256K	172.24.0/14	Zentrale Dienste	Anbieter Zentrales Netz TI
Zentrale Dienste	64K	172.24.0.0/16	Zentrale Dienste	Anbieter Zentraler Dienste
	Der Anbieter Zentrales Netz TI weist jedem zentralen Dienst ein /26 Adressblock aus dem Bereich 172.24.0.0/15 zu.			
VPN-Konzentrator	64K	172.25.0.0/16	Anschluss VPN-Konzentratoren an die TI	Anbieter Zugangsdienst
	Der Anbieter Zentrales Netz TI weist jedem VPN-Zugangsdienstprovider ein /26 Adressblock aus dem Bereich 172.25.0.0/16 zu.			
Reserveblöcke	128K	172.26.0.0/15	Reserve	Anbieter Zentrales Netz TI
TI_Test_Fachdienste	256K	172.28.0.0/14	Fachdienste	Anbieter Zentrales Netz TI
Offene Fachdienste	64K	172.30.0.0/16	Offene Fachdienste	Anbieter Offene Fachdienste
	Der Anbieter Zentrales Netz TI weist jedem Offenen Fachdienst ein /26 Adress-			

© gematik – öffentlich

Netzbereich	Adressen	Netz	Nutzung	Verantwortlich
	block aus dem Bereich 172.30.0.0/16 zu			
Gesicherte Fachdienste	64K	172.28.0.0/16	Gesicherte Fachdienste	Anbieter Gesicherte Fachdienste
	Der Anbieter Zentrales Netz TI weist jedem Gesicherten Fachdienst ein /26 Adressblock aus dem Bereich 172.28.0.0/16 zu			
Reserveblöcke	128K	172.29.0.0/16 172.31.0.0/16	Reserve	Anbieter Zentrales Netz TI

⌫

⌦ **GS-A_4851 IPv4-Adresskonzept Referenzumgebung**

In der Referenzumgebung DÜRFEN die Adressbereiche aus der Produktivumgebung und Testumgebung NICHT genutzt werden. Für die Vergabe von IPv4-Adressen in der Referenzumgebung SOLL das in Tab_Adrkonzept_Test definierte Schema (nicht der IP-Adressbereich) genutzt werden.⌫

In Tabelle 4 wird informativ die Nutzung von IPv4-Adressbereichen aus Netzbereich TI_Extern dargestellt.

Tabelle 4: Adressräume IPv4 TI Extern

Netzbereich	Adressen	Netz	Nutzung	Verantwortlicher
TI Extern	Werden hier nicht festgelegt.		Extern	Extern
DEZ_Transport	Keine Vorgabe		Dezentral Internet	Anbieter Zugangsdienst
KVS	Keine Vorgabe (188.144/15)		KV-SafeNet	KV-SafeNet
Bestandsnetze	keine Vorgabe		Bestandsnetze	Bestandsnetze
DEZENTRAL_INTRANET	keine Vorgabe		LE	LE
VPN_TRANSPORT_TI	Öffentliche Adressen		Zugangsdienst	Anbieter Zugangsdienst
VPN_TRANSPORT_SIS	Öffentliche Adressen		SIS	Anbieter Zugangsdienst
SIS	Öffentliche Adressen		SIS	Anbieter Zugangsdienst

⌦ **GS-A_4760 IP-Adressbereiche Bestandsnetze**

Bestandsnetze MÜSSEN bei Anschluss an die TI für diesen Anschluss und Kommunikation mit der TI eigene, öffentliche IPv4-Adressbereiche nutzen.⌫

2.3.4 Adresskonzept IPv6

Für IPv6 wird noch kein Adresskonzept definiert, da eine produktive Nutzung von IPv6 in Phase 1 nicht vorgesehen ist. Die Anforderungen für IPv6 beziehen sich daher auf die Vorbereitung einer produktiven IPv6-Nutzung in späteren Phasen und bereiten die Migration vor.

2.3.5 Adressen SIS-Systeme

Der Anbieter des Produkttyps Zugangsdienst muss für die Systeme des Sicheren Internet Service und der dafür notwendigen eigenen Netzwerkinfrastruktur eigene öffentliche Adressbereiche verwenden (siehe Tabelle 4: Adressräume IPv4 TI Extern).

2.4 IP-Routingkonzept

Die übergreifende Netzspezifikation legt Routing-Methoden für die Anschlusspunkte der einzelnen Produkttypen an das Zentrale Netz TI fest. Routing-Methoden in den lokalen Netzwerken der einzelnen Produkttypen werden hier nicht definiert oder vorgegeben.

⌦ **GS-A_4033 Statisches Routing TI-Übergabepunkte**

Alle Anbieter von Fachdiensten und Zentralen Diensten der TI SOLLEN an den Übergabepunkten zwischen angeschlossenen Produkttypen der TI und den SZZPs des zentralen Netzwerks TI statisches Routing nutzen.⌫

⌦ **GS-A_4034 Dynamisches Routing auf den SZZPs**

Der Produkttyp Zentrales Netz TI MUSS an den Übergabepunkten des SZZP zu fachanwendungsspezifischen Diensten und zentralen Diensten dynamisches Routing ermöglichen. Es MÜSSEN als Routing-Protokolle OSPFv2 [RFC2328] und OSPFv3 [RFC5340] unterstützt werden.⌫

⌦ **GS-A_4035 Dynamisches Routing Anschluss an das Zentrale Netz TI**

Fachanwendungsspezifische Dienste und zentrale Dienste KÖNNEN am Anschluss an das zentrale Netz TI dynamisches Routing nutzen.⌫

⌦ **GS-A_4762 Dynamisches Routing Anschluss an das Zentrale Netz TI, Routing-Protokolle**

Im Fall von dynamischem Routing am Anschluss an das zentrale Netz TI MÜSSEN Anbieter von Produkttypen der TI als Routing-Protokolle OSPFv2 [RFC2328] oder OSPFv3 [RFC5340] einsetzen.⌫

⌦ **GS-A_4036 Möglichkeit des Einsatzes von Hochverfügbarkeitsprotokollen**

Fachanwendungsspezifische Dienste und zentrale Dienste KÖNNEN am Anschluss an das Zentrale Netz der TI Hochverfügbarkeitsprotokolle (z. B. VRRP, HSRP) nutzen.⌫

⌦ **GS-A_4763 Einsatz von Hochverfügbarkeitsprotokollen**

Fachanwendungsspezifische Dienste und zentrale Dienste MÜSSEN bei Nutzung von Hochverfügbarkeitsprotokollen am Anschluss an das zentrale Netz TI durch geeignete Maßnahmen (z. B. Authentisierung der Kommunikationspartner) sicherstellen, dass andere Netzwerkkomponenten nicht beeinflusst werden.⌫

2.5 Priorisierung auf Netzwerkebene

Die Priorisierung von IP-Paketen auf Netzwerkebene dient der Sicherung der Dienstgüte im Fall von Bandbreitenengpässen. Bandbreitenengpässe können durch Überbuchung von Übertragungsleitungen auftreten. Sie können kurzzeitig (transient) oder als langfristiger Mangel auftreten.

Alle Beteiligten müssen grundsätzlich sicherstellen, dass Netzwerkanschlüsse in der TI mit ausreichender Bandbreite bereitgestellt werden, da die Priorisierung lediglich bestimmten Datenverkehr bevorzugt behandelt. Die Priorisierung ermöglicht zwar eine geringfügig höhere mittlere Auslastung von Netzwerkbandbreiten, dient aber in erster Linie zur Sicherstellung kritischer Dienste im Falle einer unvorhergesehenen oder unvermeidlichen Überlast.

2.5.1 Architektur

Auf Netzwerkebene existieren etablierte Standards und Verfahren, um eine Priorisierung von Datenverkehr umzusetzen. Grundsätzlich kann die Priorisierung über zwei Verfahren implementiert werden:

- Definition einer Datenrate pro Dienst und Reservierung eines garantierten Datenpfades (Integrated Services - IntServ) über alle Netzkomponenten hinweg
- Markierung von Datenpaketen und Behandlung (Weiterleiten/Verwerfen) pro Netzwerkkomponente auf dem Transportweg (Differentiated Services – DiffServ)

Da in der TI-Plattform keine Ende-zu-Ende-Reservierung von Netzwerkressourcen möglich ist, und zudem das IntServ-Verfahren aufwändig zu implementieren und zu betreiben ist, wird eine Priorisierung auf der Basis des DiffServ-Verfahrens eingesetzt.

⌦ **GS-A_4037 Unterstützung der DiffServ-Architektur**

Die Produkttypen Konnektor, VPN-Zugangsdienst und Zentrales Netz der TI MÜSSEN die DiffServ-Architektur gemäß [RFC2474] und [RFC2475] unterstützen.⌫

2.5.2 Definition und Zuordnung von Dienstklassen

Um eine Priorisierung des Datenverkehrs vornehmen zu können, müssen die Anwendungen und Dienste klassifiziert werden. Hierzu werden in der TI die in [RFC4594] definierten Dienstklassen verwendet, die eine Zuordnung an Hand von Anforderungen der Anwendung bzw. des Dienstes ermöglichen. Die Zuordnung erfolgt gemäß [RFC4594]; die vorliegende Tabelle 5 ist ein übersetzter Auszug.

Tabelle 5: Tab_DK_AW, Zuordnung Dienstklassen zu Anwendungen (Auszug)

Dienstklasse	Beispielanwendung	Toleranz für		
		Paketverlust	Verzögerung	Jitter
Netzwerksteuerung	OSPF, BGP	Niedrig	Niedrig	Hoch
Echtzeit-Interaktiv	Remote Desktop	Niedrig	Sehr niedrig	Niedrig
Audio	VoIP, Echtzeitanwendungen	Sehr niedrig	Sehr niedrig	Sehr niedrig
Video	A/V-Konferenzen (Live, Bidirektional)	Sehr niedrig	Sehr niedrig	Sehr niedrig
Multimedia Streaming	Video und Audio Streaming auf Anforderung (nicht Live)	Niedrig - Mittel	Mittel	Hoch
Niedrige Latenz Datenübertragung	Client-Server Transaktionen	Niedrig	Niedrig - Mittel	Mittel
Hoher Durchsatz Datenübertragung	Store-and-Forward-Anwendungen, z.B. E-Mail, Filetransfer	Niedrig	Mittel - Hoch	Hoch
Best Effort	Alle Anwendungen ohne besondere Anforderungen	Unspezifiziert		
Niedrige Priorität	Anwendungen ohne Echtzeitanforderungen	Hoch	Hoch	Hoch
Signalisierung	VoIP, Protokolle für Verbindungsaufbau	Niedrig	Niedrig	Mittel
Video (Broadcast)	Video und Audio Streaming	Sehr niedrig	Mittel	Niedrig

Die Zuordnung der Dienstklassen zu den Applikationen erfolgt durch den GBV. Die initiale Zuordnung erfolgt vor Inbetriebnahme der TI. Die Zuordnung wird im Betrieb normalerweise nicht geändert. Der GBV muss die Zuordnung erweitern, sobald neue Dienste hinzukommen, die durch das vorhandene Schema nicht abgedeckt werden.

⌦ **GS-A_4039 Zuordnung Dienstklassen**

Der GBV MUSS fachanwendungsspezifischen Diensten und zentralen Diensten eine eindeutige Dienstklasse gemäß [RFC4594] zuordnen.⌫

2.5.3 Markierung

Die Markierung von IP-Paketen zur Priorisierung erfolgt in der TI ausschließlich durch das Setzen von Differentiated Services Code Point (DSCP)-Werten im IP-Header. Die Markierung erfolgt gemäß der in [RFC4594] definierten Zuordnung von Dienstklasse und Priorität zu DSCP-Werten. Tabelle 6 ist ein übersetzter Auszug.

Tabelle 6: Tab_DK_DSCP, Zuordnung Dienstklassen zu DSCP (Auszug)

Name der Dienstklasse	Beispielanwendung	DSCP-Name
Netzwerksteuerung	OSPF, BGP	CS6&CS7
Echtzeit-Interaktiv	Remote Desktop	CS5, CS5-Admit
Audio	VoIP, Echtzeitanwendungen	EF, Voice Admit
Video	A/V-Konferenzen (Live, Bidirektional)	AF41, AF42, AF43
Multimedia Streaming	Video und Audio Streaming auf Anforderung (nicht Live)	AF31, AF32, AF33
Niedrige Latenz Datenübertragung	Client-Server Transaktionen	AF21, AF22, AF23
OAM	Operations and Maintenance	CS2
Hoher Durchsatz Datenübertragung	Store-and-Forward-Anwendungen, z.B. E-Mail, Filetransfer	AF11, AF12, AF13
Best Effort	Alle Anwendungen ohne besondere Anforderungen	CS0
Niedrige Priorität	Anwendungen ohne Echtzeitanforderungen	CS1

Innerhalb der AF-Klassen wird gemäß [RFC2597] eine Unterscheidung hinsichtlich der Wahrscheinlichkeit gemacht, mit der durch Active Queue Management IP-Pakete fallen gelassen werden („Drop Precedence“). Hierbei entspricht eine niedrige Drop Precedence einer höheren Priorisierung des Datenverkehrs.

Tabelle 7: Tab_DK_AF, AF (Assured Forwarding) Drop Precedence

Dienstklasse	DSCP-Name/Klasse	Drop Precedence		
		Niedrig	Mittel	Hoch
Video	AF-Class 4	AF41	AF42	AF43
Multimedia Streaming	AF-Class 3	AF31	AF32	AF33
Niedrige Latenz Datenübertragung	AF-Class 2	AF21	AF22	AF23
Hoher Durchsatz Datenübertragung	AF-Class 1	AF11	AF12	AF13

Die DSCP-Markierungen werden so weit wie möglich am Rand des Netzwerkes vorgenommen. Nach der Markierung wird diesen Markierungen durch alle Netzelemente vertraut.

⌦ **GS-A_4765 DSCP-Transport**

Die Produkttypen Konnektor, VPN-Zugangsdienst und Zentrales Netz der TI DÜRFEN DSCP-Markierungen NICHT unaufgefordert ändern.⌫

Die folgende Grafik stellt anhand einer beispielhaften Kommunikationsbeziehung zwischen Anwendungskonnektor und Fachdienst dar, an welchen Punkten die Pakete mit den DSCP markiert werden.

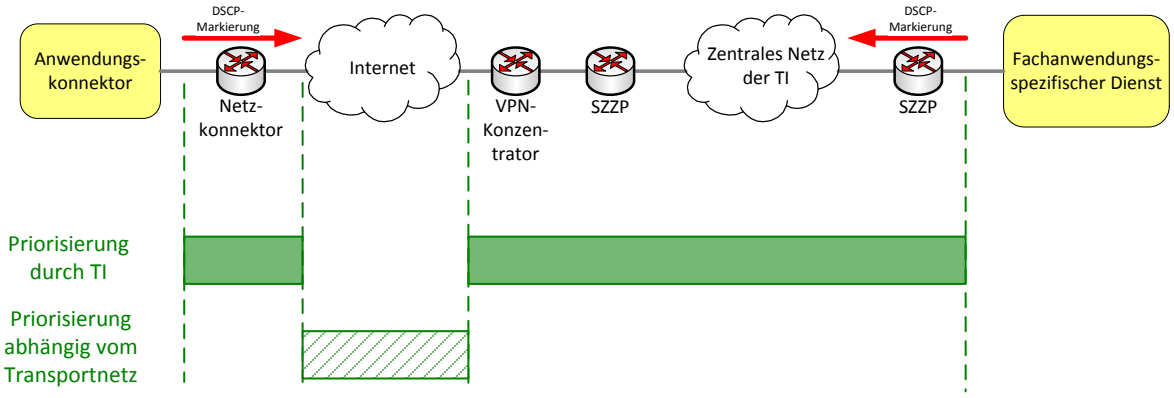


Abbildung 3: DSCP-Markierung (Beispiel)

2.5.3.1 DSCP-Markierung Netzkonnektor

GS-A_4766 DiffServ-Klassifizierung auf dem Konnektor

Der Produkttyp Konnektor MUSS die paketbasierte, zustandslose Klassifizierung unterstützen. Diese Klassifizierung MUSS gemäß zugeordneter Dienstklasse auf Grundlage einer Regel erfolgen. Der Konnektor MUSS zur Definition der Regel eine beliebige Kombination folgender Informationen aus OSI Layer 3 und 4 unterstützen: Quell- und Zieladresse, IP-Protokoll sowie Quell- und Zielport.

GS-A_4042 DSCP-Markierung durch Konnektor

Der Produkttyp Konnektor MUSS durch ihn weitergeleitete IP-Pakete aus dem dezentralen Intranet und IP-Pakete der Fachmodule gemäß Klassifizierung mit DSCP-Werten markieren.

2.5.3.2 DSCP-Markierung Zentrales Netz TI

GS-A_4044 DSCP-Kompatibilität im Zentralen Netz

Der Produkttyp Zentrales Netz MUSS den Transport von DSCP-markierten IP-Paketen unterstützen.

GS-A_4045 DSCP-Transport im Zentralen Netz

Der Produkttyp Zentrales Netz DARF die DSCP-Markierungen der transportierten IP-Pakete NICHT verändern.

GS-A_4767 DiffServ-Klassifizierung durch SZZPs des Zentralen Netzes

Der SZZP MUSS die paketbasierte, zustandslose Klassifizierung unterstützen. Diese Klassifizierung MUSS gemäß zugeordneter Dienstklasse auf Grundlage einer Regel erfolgen. Der SZZP MUSS zur Definition der Regel eine beliebige Kombination folgender Informationen aus OSI Layer 3 und 4 unterstützen: Quell- und Zieladresse, IP-Protokoll, sowie Quell- und Zielport.

GS-A_4043 DSCP-Markierung durch SZZPs des Zentralen Netzes

Der SZZP MUSS durch ihn weitergeleitete IP-Pakete aus dem Netz des Fachdienstes oder des Zentralen Dienstes in die TI gemäß Klassifizierung mit DSCP-Werten markieren.⌫

2.5.3.3 DSCP-Markierung Fremdnetze

An den Netzübergängen zu Fremdnetzen und Bestandsnetzen können folgende Maßnahmen genutzt werden:

(1) Übernahme der DSCP-Markierungen aus dem externen Netz, falls das externe Netz ebenfalls DSCP nutzt, und denselben Konventionen zur Bedeutung der DSCP folgt.

(2) Änderung der DSCP (Re-Marking) am Netzübergang, falls das externe Netz DSCP nutzt, aber diesen andere Bedeutungen zuweist. Zur Markierung wird in diesem Fall eine Regel genutzt, welche die DSCP-Werte des externen Netzes in entsprechende oder ähnliche DSCP-Werte der TI umsetzt, und umgekehrt.

(3) Markierung mit DSCP am Netzübergang in die TI, falls das externe Netz keine DSCP zur Verfügung stellt, die den DSCP der TI zugeordnet werden können. Zur Markierung wird in diesem Fall eine Liste mit Regeln genutzt, welche die gewünschten DSCP-Werte anhand einer beliebigen Kombination folgender Informationen aus OSI Layer 3 und 4 zuweist: Quell- und Zieladresse, IP-Protokoll, sowie Quell- und Zielport.

⌦ **GS-A_4047 DiffServ-Klassifizierung am Netzübergang zu Fremdnetzen**

Produkttypen mit Netzübergängen zu Fremdnetzen oder Bestandsnetzen MÜSSEN die paketbasierte, zustandslose Klassifizierung am Netzübergang unterstützen. Diese Klassifizierung MUSS gemäß zugeordneter Dienstklasse auf Grundlage einer Liste mit Regeln erfolgen. Der Netzübergang MUSS zur Definition der Regel eine beliebige Kombination folgender Informationen aus OSI Layer 3 und 4 unterstützen: Quell- und Zieladresse, IP-Protokoll sowie Quell- und Zielport.⌫

⌦ **GS-A_4768 DSCP-Markierung am Netzübergang zu Fremdnetzen**

Produkttypen mit Netzübergängen zu Fremdnetzen oder Bestandsnetzen MÜSSEN durch den Netzübergang weitergeleitete IP-Pakete aus dem Fremdnetz in die TI gemäß Klassifizierung mit DSCP-Werten markieren.⌫

⌦ **GS-A_4769 DSCP-Übersetzung am Netzübergang zu Fremdnetzen**

Produkttypen mit Netzübergängen zu Fremdnetzen oder Bestandsnetzen MÜSSEN die DSCP-Übersetzung („Re-Marking“) von IP-Paketen am Netzübergang unterstützen.

Der Netzübergang zu Fremdnetzen MUSS eine Möglichkeit zur DSCP-Übersetzung von Paketen aus dem externen Netz vorsehen. Hierzu wird am Netzübergang eine mit dem Anbieter des Fremdnetzes abzustimmende Regel hinterlegt, welche die gewünschten DSCP-Werte den IP-Paketen anhand einer Übersetzungstabelle zuordnet. Diese Funktion muss in beide Richtungen unterstützt und angewendet werden.⌫

2.5.4 Priorisierung des markierten Datenverkehrs

Zur eigentlichen Priorisierung der klassifizierten und markierten Datenpakete müssen an den einzelnen Netzkomponenten konkrete technische Maßnahmen (Queuing, Policing, Shaping) vorgesehen werden. Diese setzen die geforderten Qualitätsparameter pro definierter Dienstklasse technisch um.

Die Definition der zu den genutzten Dienstklassen gehörigen Qualitätsparameter (z. B. Bandbreite, Drop-Priority) ist durch einen übergreifenden Prozess laufend zu überwachen und weiterzuentwickeln, da sich Änderungen insbesondere durch steigende Netzlast, hinzukommende Fachdienste, hinzugewonnene Betriebserfahrung, sowie den Anschluss weiterer externer Netze und Rechenzentren an das Zentrale Netz der TI ergeben.

⌦ **GS-A_4835 Festlegung der Dienstklassen zur Priorisierung**

Der GBV MUSS die für die Priorisierung zu nutzenden Dienstklassen und deren Qualitätsparameter auf Grundlage des [RFC4594] festlegen, dokumentieren und den Anbietern und Herstellern von Produkttypen zur Verfügung stellen, welche Priorisierung einsetzen.⌫

⌦ **GS-A_4048 DiffServ-Behandlung von Datenverkehr – Produkttypen**

Die Produkttypen Zentrales Netz, VPN-Zugangsdienst und Konnektor MÜSSEN die DiffServ-Behandlung von Datenverkehr auf der Grundlage von [RFC4594] unterstützen.⌫

2.5.4.1 Zentrales Netz

⌦ **GS-A_4050 DiffServ-Behandlung innerhalb des Zentralen Netzes**

Der Produkttyp Zentrales Netz TI MUSS innerhalb des Zentralen Netzes die differenzierte Behandlung von IP-Paketen auf Grundlage der DSCP-Markierungen unterstützen.⌫

⌦ **GS-A_4051 Unterstützung von Dienstklassen im Zentralen Netz TI**

Der Produkttyp Zentrales Netz TI SOLL innerhalb des Zentralen Netzes alle vom GBV definierten Dienstklassen als Untermenge der in [RFC4594] definierten Dienstklassen in vollem Umfang unterstützen.⌫

⌦ **GS-A_4770 Minimale Unterstützung von Behandlungsaggregaten im Zentralen Netz TI**

Der Produkttyp Zentrales Netz TI MUSS innerhalb des Zentralen Netzes mindestens 4 Behandlungsaggregate einschließlich eines Echtzeit-Aggregates unterstützen, auf welche die DSCP-Werte abgebildet werden.⌫

⌦ **GS-A_4771 Aggregierung von Dienstklassen im Zentralen Netz**

Der Produkttyp Zentrales Netz TI MUSS innerhalb des Zentralen Netzes eine gegebenenfalls notwendige Aggregierung von Dienstklassen auf die in seinem Netz vorhandenen Behandlungsaggregate gemäß [RFC5127] durchführen.⌫

⌦ **GS-A_4889 Bandbreitenzuweisung am Übergang ins Zentrale Netz**

Der Produkttyp Zentrales Netz TI MUSS am Übergang zwischen dem Zugangsrouter beim Kunden (CE) und dem Zugangsrouter im Zentralen Netz (PE) die Zuweisung von Bandbreiten pro VPN ermöglichen. Diese Bandbreiten sind als Summe über den gesamten Datenverkehr eines VPNs zu verstehen.⌫

⌦ **GS-A_4890 Bandbreitenzuweisung am Übergang ins Zentrale Netz-DiffServ**

Der Produkttyp Zentrales Netz MUSS am Übergang zwischen dem Zugangsrouter beim Kunden (CE) und dem Zugangsrouter im Zentralen Netz (PE) innerhalb jeder VPN-eigenen Bandbreitenzuweisung die Behandlung von Datenverkehr gemäß DiffServ-Architektur ermöglichen. Dabei MÜSSEN mindestens 8 Behandlungsaggregate unterstützt werden, auf die die Dienstklassen der TI abgebildet werden.⌫

2.5.4.2 Konnektor

Der Netzkonnektor wird an seiner WAN-Schnittstelle in der Regel an einen stark bandbreitenlimitierten Internetzugang angeschlossen. Je nach Zugangstechnik können Uplink-Bandbreiten im Bereich einiger 10 kbit/s bis zu mehreren Gbit/s vorhanden sein.

Die Priorisierung des Datenverkehrs in das Transportnetz Internet soll direkt auf dem WAN-Router bzw. IAG des LE auf Grundlage der durch den Konnektor markierten Datenpakete erfolgen. Da nicht an jedem WAN-Router bzw. IAG eine Priorisierung möglich ist, muss im Konnektor ein Mechanismus implementiert werden, der bei Überschreitung der verfügbaren Internet-Uplink-Bandbreite den Datenverkehr priorisiert. Eine solche Priorisierung ist nur möglich, wenn unkontrollierte Warteschlangen im Internet-Uplink vermieden werden. Die Warteschlange darf sich nach Möglichkeit nur in dem Gerät ausbilden, welches eine Priorisierung des Datenverkehrs vornehmen kann. Diese Funktionalität wird vom Konnektor gefordert. Dazu wird zunächst ein Bandbreitenbeschränkung (Traffic Shaping) unterhalb der verfügbaren Internet-Uplink-Bandbreite implementiert. Auf der sich dadurch ausbildenden Warteschlange wird der Datenverkehr in geeigneter Weise behandelt.

In der Stufe 1 ist zunächst eine manuelle Konfiguration der verfügbaren Uplink-Bandbreite durch den Administrator des Konnektors vorgesehen, wobei in späteren Ausbaustufen ein Verfahren zur automatischen Ermittlung der verfügbaren Bandbreite implementiert werden soll.

⌦ **GS-A_4772 Bandbreitenbegrenzung durch Konnektor**

Der Produkttyp Konnektor MUSS die Bandbreitenbegrenzung (Traffic Shaping) der Summe des ausgehenden Datenverkehrs in Richtung des Transportnetzes Internet unterstützen. Die Bandbreitenbegrenzung muss über die Management-Schnittstelle manuell konfigurierbar sein. Die Bandbreitenbegrenzung MUSS so gestaltet sein, dass die vorgegebene gesendete Bandbreite zu keiner Zeit überschritten wird.⌫

⌦ **GS-A_4773 DiffServ-gemäße Behandlung im Konnektor**

Der Produkttyp Konnektor MUSS Datenverkehr in Richtung des Transportnetzes Internet, welcher die konfigurierte abgehende Bandbreitenbegrenzung überschreitet, gemäß DiffServ-Policy behandeln. Hierzu MUSS der Konnektor die DSCP-Werte der IP-Pakete heranziehen.⌫

⌦ **GS-A_4837 Behandlung von Dienstklassen im Konnektor**

Der Produkttyp Konnektor MUSS die differenzierte Behandlung aller vom GBV definierten Dienstklassen als Untermenge der in [RFC4594] definierten Dienstklassen in vollem Umfang unterstützen.⌫

⌦ **GS-A_4774 Klassenbasiertes Queuing im Konnektor**

Der Produkttyp Konnektor MUSS klassenbasiertes Queuing (CBQ) oder einen vergleichbaren Queuing-Algorithmus, wie zum Beispiel Hierarchical Token Bucket (HTB), unterstützen.⌫

⌦ **GS-A_4891 Klassenbasierte Zuordnung von Bandbreiten im Konnektor**

Der Produkttyp Konnektor MUSS die Zuordnung von garantierten Bandbreiten zu Dienstklassen unterstützen. Die Bandbreiten sind dabei als Mindestbandbreiten zu verstehen, die der Dienstklasse garantiert werden, aber jederzeit überschritten werden können. Diejenigen Bandbreitenanteile, welche von einer konfigurierten Dienstklasse nicht verbraucht werden, MÜSSEN anderen Dienstklassen zur Verfügung stehen.⌫

2.5.4.3 VPN-Zugangsdienst

Detaillierte Anforderungen zum Aufbau des VPN-Zugangsdienstes und zur Behandlung des Datenverkehrs werden in [gemSpec_VPN_ZugD] gestellt.

⌦ **GS-A_4840 DiffServ-Behandlung im VPN-Zugangsdienst**

Der Produkttyp VPN-Zugangsdienst MUSS die differenzierte Behandlung von IP-Paketen auf Grundlage der DSCP-Markierungen unterstützen.⌫

⌦ **GS-A_4841 Unterstützung von Dienstklassen im VPN-Zugangsdienst**

Der Produkttyp VPN-Zugangsdienst MUSS alle vom Gesamtbetriebsverantwortlichen definierten Dienstklassen als Untermenge der in [RFC4594] definierten Dienstklassen in vollem Umfang unterstützen.⌫

2.6 Sicherheitskomponenten im Netzwerk

Der Verkehr in der TI wird an Übergabepunkten zwischen Anbietern und Netzwerken mittels Sicherheitsgateways kontrolliert und auf den für die Diensterbringung erforderlichen Datenverkehr beschränkt. Der Begriff Sicherheitsgateway wird in diesem Dokument angelehnt an der Definition in [BSI SGW] verwendet, d.h. als System das aus mehreren soft- und hardwaretechnischen Sicherheitskomponenten besteht, die im folgenden Kapitel beschrieben werden.

2.6.1 Typen von Sicherheitskomponenten

Die folgenden Sicherheitskomponenten sind in dieser Spezifikation für die Kontrolle von Verkehr relevant:

Paketfilter: Paketfilter kontrollieren als Schnittstelle zwischen verschiedenen Netzen den Datenverkehr auf Transportebene (OSI-Schicht 3 und 4), damit erwünschte Datenpakete

die Paketfilter passieren und unerwünschte oder unerwartete Pakete diesen nicht passieren.

Application-Level-Gateway (ALG): ALGs, auch Proxy oder Anwendungsproxy genannt, kontrollieren den Verkehr auf Anwendungsebene (OSI-Schicht 7) zwischen Clients und Servern. Kommunikationsbeziehungen werden nur über den Proxy aufgebaut, der den Verkehr auf Anomalien, Schadprogramme oder nicht erlaubte Inhalte/Verkehre oder Protokolle kontrollieren kann.

Intrusion Detection System (IDS): IDSe untersuchen den passierenden Verkehr auf Anomalien und Angriffsversuche. Dabei können Heuristiken, Baselines oder Blacklists/Whitelists eingesetzt werden, um irregulären Verkehr und mögliche Angriffe zu erkennen. In dieser Spezifikation sind nur netzbasierte IDSe relevant, die den Verkehr an Netzübergabepunkten kontrollieren.

2.6.2 Anforderungen an Sicherheitskomponenten

⌦ **GS-A_4052 Stateful Inspection**

Die Produkttypen Zentrales Netz TI und Konnektor MÜSSEN bei der Verwendung von Paketfiltern und ALGs den passierenden Verkehr verbindungsbasiert kontrollieren (Stateful-Inspection).⌫

⌦ **GS-A_4053 Ingress und Egress Filtering**

Paketfilter und ALGs aller Anbieter und Hersteller von Produkttypen der TI MÜSSEN sowohl eingehenden als auch ausgehenden Verkehr kontrollieren (Ingress und Egress Filtering).⌫

⌦ **GS-A_4054 Paketfilter Default Deny**

Paketfilter und ALGs aller Anbieter und Hersteller von Produkttypen der TI MÜSSEN den passierenden Verkehr ausschließlich auf den spezifizierten und erlaubten begrenzen. Jeglicher nicht spezifizierter Verkehr MUSS als Standardregel verboten werden (default-deny).

Das Regelwerk MUSS die explizit erlaubte Kommunikation beinhalten.⌫

⌦ **GS-A_4057 Technische Anforderungen Sicherheitsgateways – Betriebssoftware**

Der Anbieter Zentrales Netz TI, der Anbieter Sicherheitsgateway KV-SafeNet und der Anbieter Zugangsdienst MÜSSEN auf den eingesetzten Komponenten der Sicherheitsgateways nur zum Betrieb unbedingt erforderliche Software installieren (nach [BSI-SGW#D.2 Grundlegende technische Anforderungen]), insbesondere ist die Verwendung eines Betriebssystems mit minimalem Funktionsumfang erforderlich.⌫

⌦ **GS-A_4777 Technische Anforderungen Sicherheitsgateways - Dokumentation Systemfunktion**

Der Anbieter Zentrales Netz TI, der Anbieter Sicherheitsgateway KV-SafeNet und der Anbieter Zugangsdienst MÜSSEN auf den eingesetzten Komponenten der Sicherheitsgateways die grundlegenden Systemfunktionen des minimalen Systems dokumentieren (nach [BSI-SGW#D.2 Grundlegende technische Anforderungen]).⌫

⌦ **GS-A_4778 Technische Anforderungen Sicherheitsgateways - Verbindungen nach Erstinstallation**

Der Anbieter Zentrales Netz TI, der Anbieter Sicherheitsgateway KV-SafeNet und der Anbieter Zugangsdienst MÜSSEN auf den eingesetzten Komponenten der Sicherheitsgateways nach der Erstinstallation alle Verbindungen, die nicht explizit erlaubt sind, blockieren (nach [BSI-SGW#D.2 Grundlegende technische Anforderungen]).⌫

⌦ **GS-A_4779 Technische Anforderungen Sicherheitsgateways - keine Verbindungen bei Ausfall der Komponenten**

Der Anbieter Zentrales Netz TI, der Anbieter Sicherheitsgateway KV-SafeNet und der Anbieter Zugangsdienst DÜRFEN auf den eingesetzten Komponenten der Sicherheitsgateways bei einem völligen Ausfall der Komponente NICHT IP-Pakete passieren lassen. (nach [BSI-SGW#D.2 Grundlegende technische Anforderungen]).⌫

2.6.3 Platzierung von Sicherheitskomponenten

An folgenden Stellen müssen Sicherheitsgateways in der TI-Plattform eingesetzt werden:

⌦ **GS-A_4058 Sicherheitskomponenten SZZP/Zentrales Netz TI**

Der Anbieter Zentrales Netz TI MUSS den Verkehr an den Anschlusspunkten zum zentralen Netz mit SZZPs sichern.⌫

⌦ **GS-A_4059 Sicherheitsgateway KV-SafeNet**

Der Anbieter des Sicherheitsgateway KV-SafeNet MUSS den Netzübergang zwischen SNK bzw. Bestandsnetzen und TI mit Sicherheitsgateways absichern.

Als geeignete Maßnahmen zur Unterstützung der Absicherung werden angesehen:

- Auswertung von Logfiles
- Auswertung von Netflow
- Intrusion Detection Systeme (IDS) ⌫

Der Konnektor muss den passierenden Verkehr mit einem Paketfilter sichern.

⌦ **GS-A_4061 Sicherheitskomponenten Zugangsdienst**

Der Anbieter Zugangsdienst MUSS den Verkehr zwischen VPN-Konzentratoren und Transportnetz mit einem Paketfilter sichern. ⌫

Die folgende Abbildung Abb_SichKomp_Platzierung stellt die Platzierung von Sicherheitskomponenten informativ dar. Die detaillierten Anforderungen werden in den Spezifikationen der Produkttypen definiert. Anbieter von Produkttypen der TI können zusätzliche Sicherheitsgateways zum Schutz ihrer Infrastruktur einsetzen.

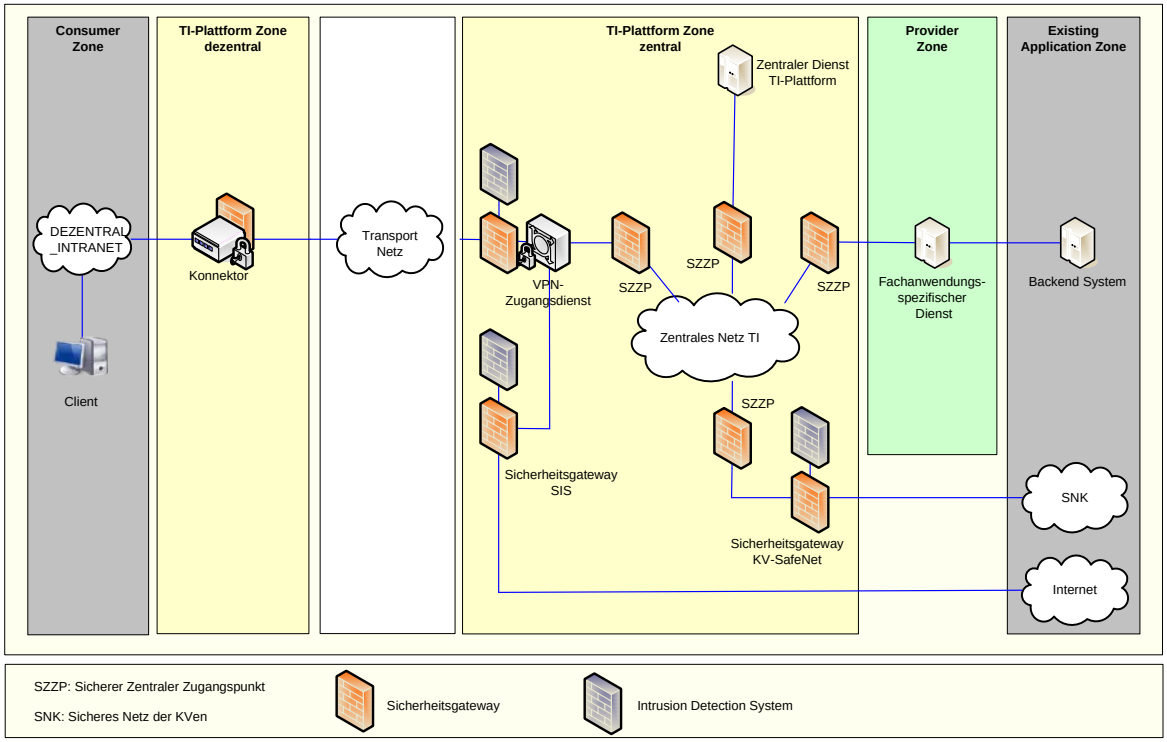


Abbildung 4: Abb_SichKomp_Platzierung, Platzierung von Sicherheitskomponenten in der TI

Implementieren Produkttypen Übergänge zu Fremdnetzen mit niedrigerem oder unbekanntem Sicherheitsniveau (z.B. bei den Produkttypen OCSP-Responder Proxy und Störungsampel), insbesondere zum Internet, müssen besondere Vorkehrungen getroffen werden, die sich an die Anforderungen des BSI für Netzübergänge anlehnen [BSI SGW#5.1, Seite 42ff].

⌦ GS-A_4062 Sicherheitskomponenten bei Netzübergängen zu Fremdnetzen

Zentrale Produkttypen MÜSSEN den Übergang zu Fremdnetzen mit niedrigerem oder unbekanntem Sicherheitsniveau, wie dem Internet mit einem vom BSI zertifizierten Sicherheitsgateway oder einem Sicherheitsgateway mit dreistufigem Aufbau, gemäß BSI-Empfehlung [BSI SGW], wie in Abbildung Abb_SichKomp_bei_Netzübergängen beschrieben, sichern. Der dreistufige Aufbau umfasst einen Paketfilter, der den Verkehr am Anschluss des Fremdnetzes kontrolliert, ein zwischengeschaltetes Application-Level-Gateway, das den passierenden Verkehr auf Applikationsschicht kontrolliert, und ein weiterer Paketfilter vor dem Netz des Produkttypen.

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

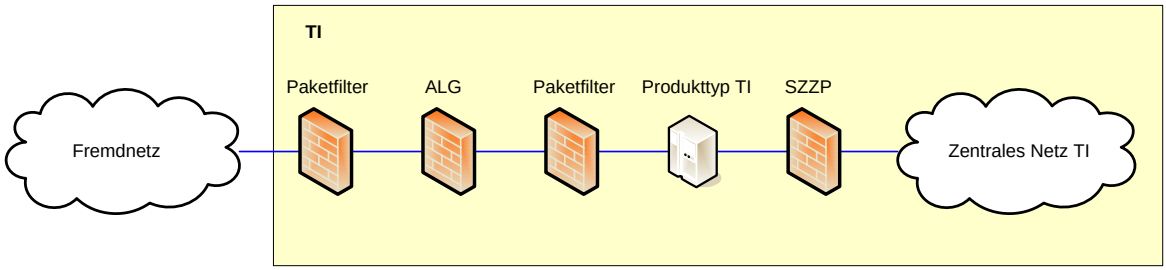


Abbildung 5: Abb_SichKomp_Netzübergänge, Sicherheitskomponenten bei Netzübergängen, generisch

⌫

2.6.4 Prozesse zu Regeln für Sicherheitsgateways

Für die Verwaltung und Dokumentation von Regeln für Sicherheitsgateway ist in der TI ein übergreifender Prozess zu etablieren, der durch den Anbieter Zentrales Netz TI implementiert und vom GBV freigegeben wird.

In den folgenden Anforderungen werden die Verantwortlichkeiten und weitere Vorgaben zum Prozess „Verwaltung von Sicherheitsgateway-Regeln“ definiert.

⌦ **GS-A_4846 Prozess „Verwaltung von Sicherheitsgateway-Regeln“**

Der Anbieter Zentrales Netz TI MUSS den Prozess „Verwaltung von Sicherheitsgateway-Regeln“ mit den folgenden Inhalten definieren und implementieren:

- Freigabe von Sicherheitsgateway-Regeln
- Erstellung und Pflege von Dokumentations- und Reportingschemas
- Dokumentation und Reporting von Sicherheitsgateway-Regeln

Der Anbieter Zentrales Netz TI ist der Verantwortliche für den gesamten Prozess. ⌫

⌦ **GS-A_4887 Prozess „Verwaltung von Sicherheitsgateway-Regeln“ – Prozess-Freigabe**

Der GBV MUSS den vom Anbieter Zentrales Netz TI definierten Prozess „Verwaltung von Sicherheitsgateway-Regeln“ freigeben.⌫

⌦ **GS-A_4063 GBV, Freigabe Sicherheitsgateway-Regeln**

Der GBV MUSS im Rahmen des Test- und Zulassungsverfahrens von neuen Diensten und bei Änderungen an bestehenden Diensten die benötigten Kommunikationsbeziehungen (Sicherheitsgateway-Regeln) freigeben und an den Anbieter Zentrales Netz TI melden.⌫

⌦ **GS-A_4064 Koordinierung Sicherheitsgateway-Regeln**

Der Anbieter Zentrales Netz TI MUSS die Anpassung von Sicherheitsgateway-Regeln operativ mit dem GBV und Anbietern von Produkttypen der TI koordinieren.⌫

© gematik – öffentlich

⌦ **GS-A_4065 Meldung neue Sicherheitsgateway-Regeln**

Der Anbieter Zentrales Netz TI MUSS die Umsetzung neuer Sicherheitsgateway-Regeln an die Anbieter von Produkttypen der TI melden.⌫

⌦ **GS-A_4066 Umsetzung Sicherheitsgateway-Regeln**

Die Anbieter der Produkttypen VPN-Zugangsdienst und Sicherheitsgateway KV-SafeNet MÜSSEN Change Requests zur Anpassung von Sicherheitsgateway-Regeln vom Anbieter Zentrales Netz TI umsetzen.⌫

⌦ **GS-A_4780 Reporting Sicherheitsgateway-Regeln, Format**

Der Anbieter Zentrales Netz TI MUSS das Schema für die Dokumentation und das Reporting von Sicherheitsgateway-Regeln festlegen.⌫

⌦ **GS-A_4067 Reporting Sicherheitsgateway-Regeln**

Die Produkttypen VPN-Zugangsdienst und Sicherheitsgateway KV-SafeNet MÜSSEN Änderungen an Sicherheitsgateway-Regeln an den Anbieter Zentrales Netz TI melden. Die Anbieter MÜSSEN diese Änderungen zusammen mit dem Gesamtsatz an Filterregeln melden. ⌫

⌦ **GS-A_4068 Dokumentation Sicherheitsgateway-Regeln**

Der Anbieter Zentrales Netz TI MUSS den Gesamtsatz an Sicherheitsgateway-Regeln dokumentieren und monatlich an den GBV melden.⌫

2.6.5 Erlaubter Verkehr

⌦ **GS-A_4069 Erlaubter Verkehr Produkttypen**

Die Produkttypen Konnektor, Zugangsdienst, Sicherheitsgateway KV-SafeNet MÜSSEN bei Einsatz von Sicherheitsgateways den Verkehr mit Sicherheitsgateways auf den Verkehr einschränken, der in der Kommunikationsmatrix in der Architektur der TI-Plattform [gemKPT_Arch_TIP#Kommunikationsmatrix] aufgeführt ist.⌫

⌦ **GS-A_4070 Netzwerksteuerungsprotokolle**

Die Produkttypen Konnektor, Zugangsdienst und Sicherheitsgateway KV-SafeNet MÜSSEN bei Einsatz von Sicherheitsgateways Protokolle zur Netzwerksteuerung erlauben (mindestens notwendiger Verkehr zur Path MTU Discovery gemäß [RFC1191]).⌫

⌦ **GS-A_4884 Erlaubte ICMP-Types**

Paketfilter und ALGs aller Anbieter von Produkttypen der TI MÜSSEN sicherstellen, dass nur die folgend aufgeführten ICMP-Types verarbeitet bzw. weitergeleitet werden:

- Type 0: Echo Reply
- Type 3: Destination Unreachable

- Type 5: Redirect
- Type 8: Echo Request
- Type 11: Time Exceeded
- Type 12: Parameter Problem

Eine weitere Einschränkung der erlaubten ICMP-Types kann auf Ebene der Spezifikationen des Produkttyps erfolgen.⌫

2.6.6 Anforderungen an das Sicherheitsgateway KV-SafeNet

Die im Folgenden geforderten Proxies dienen nicht der Kontrolle des Inhalts der Datenpakete sondern ausschließlich der Erkennung, ob es sich um zulässigen Datenverkehr handelt.

⌦ **GS-A_5055 Sicherheitsgateway KV-SafeNet, Application Layer Gateway**

Der Anbieter des Produkttyps Sicherheitsgateway KV-SafeNet MUSS 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.⌫

⌦ **GS-A_5056 Sicherheitsgateway KV-SafeNet, Bereitstellung Circuit Level Proxy**

Der Anbieter des Produkttyps Sicherheitsgateway KV-SafeNet MUSS konfigurierbare Circuit Level Proxies bereitstellen, die eine Übertragung und Prüfung von definierten Protokollen auf Basis von Protokoll und Port auf Applikationsebene ermöglichen. ⌫

⌦ **GS-A_5057 Sicherheitsgateway KV-SafeNet, Maßnahmen gegen Schadsoftware**

Der Anbieter des Produkttyps Sicherheitsgateway KV-SafeNet MUSS bei der Übertragung von Daten über unverschlüsselte Protokolle Maßnahmen zum Schutz vor Schadsoftware umsetzen.⌫

3 Zentrales Netz der TI

3.1 Zerlegung des Produkttyps

Der Produkttyp Zentrales Netz besteht aus den folgenden Komponenten:

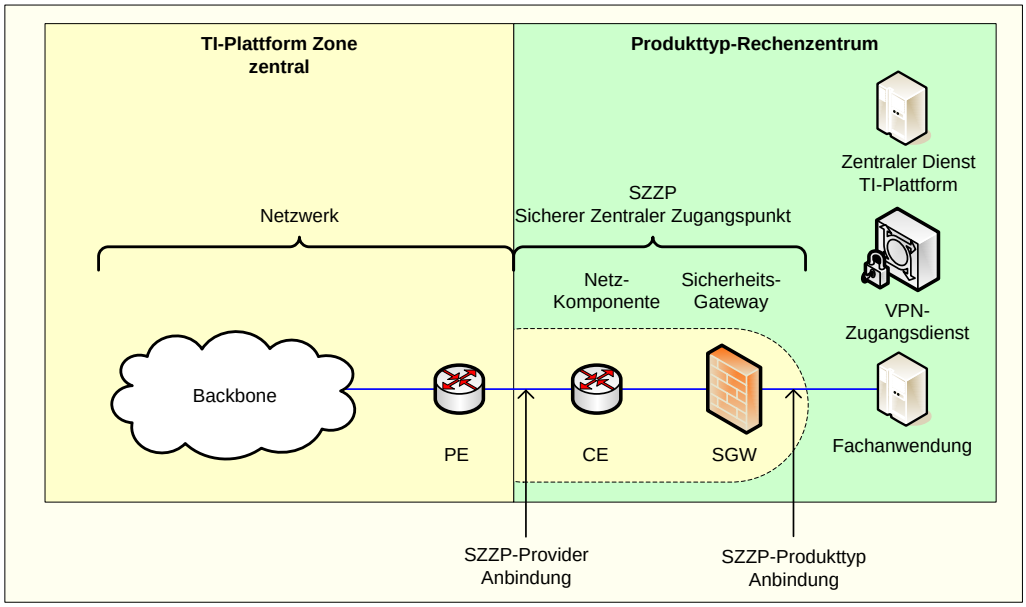
SZZPs (Sicherer Zentraler Zugangspunkt)

- Netzkomponente: Transport- und Netzwerkfunktionen (Routing, Priorisierung, Forwarding)
- Sicherheitsgateway: Sicherheitsfunktionen (Filtering)
- Anbindung SZZP-Produkttyp: Anbindung des Produkttyps an den SZZP
- Anbindung SZZP-Provider (CE-PE): Hauseinführungen vom Provider zum SZZP

Netzwerk:

- Backbone: Zentrales Transportnetz des Providers
- Routing: Erreichbarkeit der TI IP-Adressbereiche

Eine informative Darstellung der Zerlegung befindet sich in der folgenden Abbildung Abb_ZentrNetz_Zerlegung.



PE – Provider Edge router SGW - Sicherheitsgateway CE – Customer Edge router

Abbildung 6: Abb_ZentrNetz_Zerlegung, Zerlegung Zentrales Netz

3.1.1 Sicherer Zentraler Zugangspunkt (SZZP)

Die SZZPs stellen den Anschluss von Produkttypen an das Zentrale Netz TI her. Der SZZP stellt dazu in Richtung Produkttyp die Schnittstelle I_IP_Transport bereit.

SZZPs werden als CPEs (Customer Premises Equipment) in den Räumen und Einrichtungen der Produkttypen vom Anbieter Zentrales Netz betrieben.

⌦ **GS-A_4781 Logischer Aufbau SZZP**

Der Anbieter Zentrales Netz TI MUSS die für den Zugang zum Zentralen Netz notwendigen Sicheren Zentralen Zugangspunkte (SZZP) als Netzwerkgeräte implementieren, die aus logisch zwei Komponenten bestehen: a) der Netzkomponente, die die Transportfunktion übernimmt, und b) dem Sicherheitsgateway, das den Verkehr kontrolliert.⌫

⌦ **GS-A_4782 SZZPs bei angeschlossenen Produkttypen**

Der Anbieter Zentrales Netz TI MUSS die für den Zugang zum Zentralen Netz notwendigen SZZPs in den Einrichtungen der angeschlossenen Produkttypen betreiben.⌫

⌦ **GS-A_5076 SZZP für mehrere Produktinstanzen**

Das Zentrale Netz TI KANN verschiedene Produktinstanzen über einen gemeinsamen SZZP anbinden. Dabei sind folgende Bedingungen zu erfüllen:

- Die Kommunikation zwischen den angebundenen Produktinstanzen erfolgt ausschließlich über den SZZP.
- Bei der Kommunikation zwischen den angebundenen Produktinstanzen werden alle Regeln so umgesetzt und eingehalten, als wenn die Produktinstanzen über separate SZZP angebunden wären.

Ein Routing zwischen den angebundenen Produktinstanzen über das zentrale Transportnetz des Providers für das Zentrale Netz TI muss nicht erfolgen.⌫

3.1.1.1 Netzkomponente

Die Netzkomponente CE (Customer Edge) stellt die Verbindung zum zentralen Netz des Anbieters her und vermittelt dabei IP-Pakete zwischen der TI und dem angeschlossenen Produkttyp.

Die Netzkomponente hat folgende zwei logische Anschlüsse:

1. SZZP-Provider (CE-PE): Anbindung an das zentrale Transportnetz des Anbieters
2. Je nach Integration des Sicherheitsgateway:
   a) Sicherheitsgateway, falls nicht in den CE integriert, oder
   b) Anbindung SZZP-Produkttyp (Customer edge): Angebundener Produkttyp, falls Sicherheitsgateway in den CE integriert ist.

3.1.1.2 Sicherheitsgateway

SZZPs enthalten zur Kontrolle des Verkehrs Sicherheitsgateways. Es werden keine Vorgaben gemacht, ob die Sicherheitsgateways separate Systeme oder in der Netzwerkkomponente (CE) integriert sind.

SZZPs können verschiedene Arten von Sicherheitsgateways implementieren, mindestens jedoch Paketfilter.

⌦ **GS-A_4783 SZZP Sicherheitsgateways**

Das Zentrale Netz TI MUSS an den SZZPs den Verkehr mit Paketfiltern als Sicherheitsgateway kontrollieren und einschränken.⌫

3.1.1.3 Anbindungen

Anbindung SZZP-Produkttyp

Die SZZP-Produkttyp Anbindung stellt die Verbindung der angeschlossenen Produkttypen in deren Räumlichkeiten mit dem SZZP her.

Die Schnittstelle I_IP_Transport befindet sich entweder auf dem CE, falls das Sicherheitsgateway in diesen integriert ist, oder im Sicherheitsgateway, falls diese ein vom CE separates System ist.

Die Anbindung des Produkttyps kann mit einem oder zwei SZZPs in den Räumlichkeiten des angeschlossenen Produkttyps realisiert werden.

Für den Anschluss an das Zentrale Netz TI gibt es folgende Varianten:

- Variante 1: Einfache Anbindung
  - alle Datenleitungen und Komponenten eines Anschlusses sind nur einfach vorhanden
  - hierdurch ist keine Redundanz bzgl. der Anschlussvariante möglich
  - sollte ein Produkttyp seine primäre und seine sekundäre Instanz des Dienstes jeweils durch eine einfache Anbindung an das Zentrale Netz TI anschließen, muss das Umschalten im Fehlerfall zwischen diesen Instanzen von ihm selbst sichergestellt werden
- Variante 2: Einfache Anbindung mit 2 LAN-Schnittstellen
  - Sonderform von Variante 1 mit 2 physischen Schnittstellen in Richtung LAN des angeschlossenen Produkttyps
  - sonst wie Variante 1
- Variante 3: Redundante Anbindung
  - alle Datenleitungen und Komponenten eines Anschlusses sind doppelt vorhanden
  - bei Ausfall einer Komponente oder Datenleitung ist ein Umschalten auf den Ersatzweg möglich

- o für eine automatische Umschaltung ist eine Querverbindung (Cross Connect) zwischen der primären und der sekundären Instanz notwendig, die vom angeschlossenen Dienst bereitzustellen ist
- o falls die primäre und die sekundäre Instanz des Dienstes im selben Gebäude betrieben werden, ist zur Sicherstellung der Verfügbarkeit, eine getrennte Hauseinführung für die beiden Datenleitungen notwendig

- Variante 4: Redundante Anbindung mit 2 LAN-Schnittstellen
  - o Sonderform von Variante 3 mit 2 physischen Schnittstellen pro SZZP in Richtung LAN des angeschlossenen Produkttyps
  - o sonst wie Variante 3

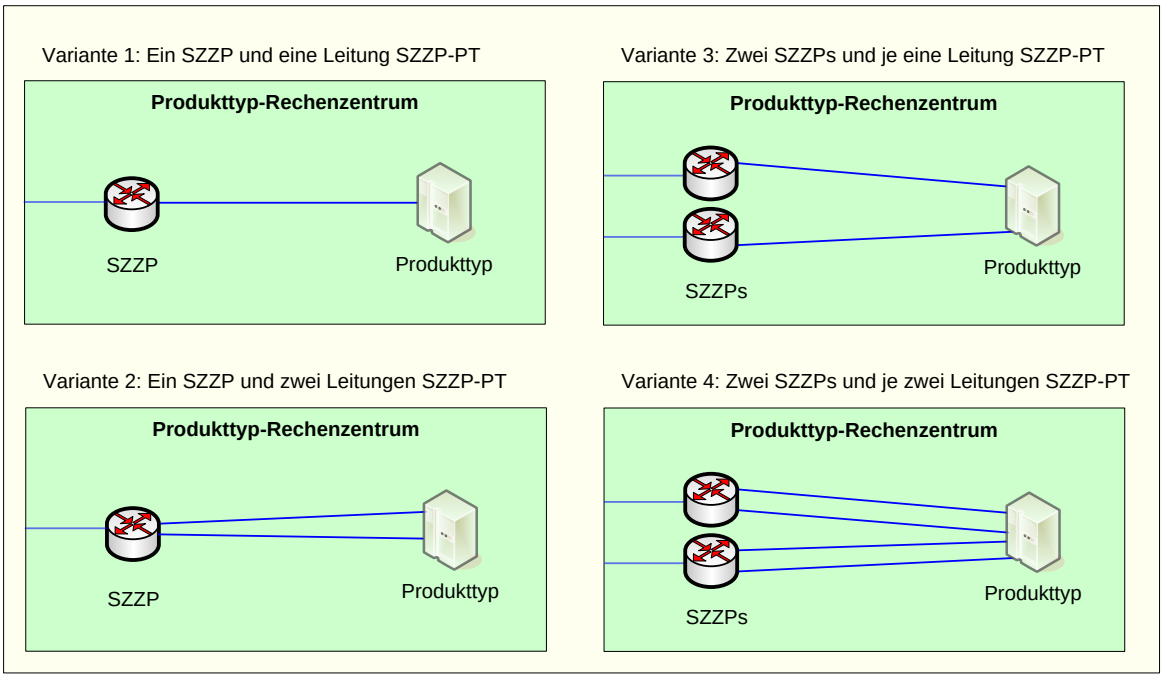


Abbildung 7: Abb_ZentrNetz_SSZP-PT, Anbindungsvarianten SZZP zum Produkttyp

⌦ GS-A_4784 Anschlussvarianten SZZP-Produkttyp

Der Anbieter Zentrales Netz MUSS für den Anschluss der Produkttypen an die SZZPs die folgenden Anschlussvarianten je Rechenzentrum unterstützen:

- einfache Anbindung über einen SZZP
- redundante Anbindung über zwei SZZP
- Jeder SZZP muss ein oder zwei physikalische Schnittstellen pro Umgebung (Produktivumgebung, Testumgebung und Referenzumgebung) in Richtung LAN des angeschlossenen Produkttyps bereitstellen.⌫

⌦ **GS-A_4785 Technische Maßnahmen bei redundanten SZZPs**

Der Anbieter Zentrales Netz MUSS bei Nutzung einer redundanten Anschlussvariante geeignete technische Maßnahmen zum redundanten Betrieb und Failover der SZZPs implementieren und nutzen.⌫

Anbindung Provider (CE-PE)

Die CE-PE Anbindung stellt die Verbindung der SZZPs (CE) in den Räumlichkeiten des angeschlossenen Produkttyps mit dem Backbone (PE) des Zentralen Netzes TI her.

⌦ **GS-A_4786 Anschlussvarianten SZZP-Provider (CE-PE)**

Das Zentrale Netz MUSS für den Anschluss der SZZPs an das Backbone an der CE-PE-Grenze die folgenden Anschlussvarianten je Rechenzentrum des angeschlossenen Produkttyps unterstützen:

- Ein Anschluss vom Provider-Transportnetz zum SZZP
- Zwei separate, redundante Anschlüsse vom Provider-Transportnetz zum SZZP, hierbei ist die Anbindung kanten- und knotendisjunkt zu realisieren⌫

⌦ **GS-A_4787 Anschlussbandbreiten SZZP-Provider (CE-PE)**

Das Zentrale Netz MUSS für den Anschluss SZZP-Provider (CE-PE) die folgenden zwei Typen von skalierbaren Bandbreiten unterstützen:

- Typ 1: 1 Mbit/s bis 100 Mbit/s
- Typ 2: 1 Mbit/s bis 1 Gbit/s

Das Zentrale Netz MUSS eine Skalierung innerhalb der Typen ohne den Austausch der CE-Hardware und Anschlussleitungen ermöglichen.⌫

3.1.2 Netzwerk

3.1.2.1 Backbone (zentrales Transportnetz Provider)

⌦ **GS-A_4788 TI zentrales Transportnetz Provider**

Der Anbieter Zentrales Netz TI MUSS das Zentrale Netz TI als skalierbares (Anzahl Anschlüsse und Bandbreite erweiterbar) privates Netz implementieren.

Das Zentrale Netz TI MUSS private, auf OSI-Schicht 3 logisch getrennte Netzwerke (IP-VPN) zwischen den einzelnen SZZPs unterstützen.

Das Zentrale Netz TI MUSS 3 IP-VPN bereitstellen.

Das Zentrale Netz TI MUSS eine Erweiterung der nutzbaren IP-VPN unterstützen.

Die Nutzbarkeit der einzelnen IP-VPN MUSS pro SZZP wählbar sein.⌫

⌦ **GS-A_4789 Ausschluss öffentlicher Transportnetze**

Der Anbieter des Produkttyps Zentrales Netzes TI MUSS sicherstellen, dass der Transport von Daten der TI zwischen den SZZP der Produkttypen über kein öffentliches Transportnetzwerk, wie z. B. dem Internet, erfolgt.⌫

⌦ **GS-A_4880 IP-VPN – Bereitstellung für TI-Umgebungen**

Der Anbieter Zentrales Netz MUSS jeweils ein IP-VPN für die Produktivumgebung, die Testumgebung und die Referenzumgebung bereitstellen.⌫

⌦ **GS-A_4881 IP-VPN– Interface zum Produkttyp**

Der Anbieter Zentrales Netz MUSS die IP-VPN für die Produktivumgebung, die Testumgebung und die Referenzumgebung am SZZP auf separaten physischen Interfaces in Richtung des angeschlossenen Produkttyps übergeben.⌫

⌦ **GS-A_4882 IP-VPN– Zugesicherte Bandbreiten**

Der Anbieter Zentrales Netz MUSS die separate Zuweisung einer vereinbarten Bandbreite (Committed Access Rate- CAR) pro bereitgestelltem IP-VPN an einem Netzwerkanschluss ermöglichen.⌫

⌦ **GS-A_4883 IP-VPN– Verhinderung von Datenaustausch**

Der Anbieter Zentrales Netz MUSS sicherstellen, dass kein Datenaustausch und keine gegenseitige Beeinflussung zwischen IP-VPN möglich sind.⌫

3.2 Übergreifende Festlegungen

Die Freigabe von erlaubten Kommunikationsbeziehungen erfolgt im Rahmen der Zulassung von Diensten in der TI. Der neu aufgenommene Dienst benennt die benötigte Kommunikation und der GBV gibt sie frei und beauftragt den Anbieter Zentrales Netz mit der Freischaltung in den SZZP.

⌦ **GS-A_4790 Zentrales Netz, nur erlaubte Kommunikation**

Das Zentrale Netz MUSS sicherstellen, dass im Zentralen Netz der TI und zwischen den angeschlossenen Produkttypen ausschließlich erlaubte IP-Kommunikation in Richtung Produkttypen und fachanwendungsspezifischer Dienste gesendet wird.

Die erlaubte Kommunikation umfasst:

- Verkehr wie spezifiziert durch die Kommunikationsmatrix in der Architektur der TI-Plattform [gemKPT_Arch_TIP#Kommunikationsmatrix]
- DNS-Anfragen an den Produkttyp Namensdienst und an Nameserver-Implementierungen in der TI, die die Zone des Produkttyps Störungsampel verwalten
- NTP-Anfragen an den Produkttyp Zeitdienst
- Übertragung von Monitoringdaten an die Störungsampel
- Verkehr zur Steuerung des Netzwerks⌫

⌦ **GS-A_4791 Zentrales Netz, neue Typen von erlaubtem Verkehr**

Das Zentrale Netz TI MUSS neuen erlaubten Datenverkehr in der TI nach Freigabe durch den GBV im Zentralen Netz ermöglichen. Nicht mehr erlaubter Verkehr darf nach Freigabe durch den GSV nicht mehr weitergeleitet werden.⌫

⌦ GS-A_4792 Onboarding zugelassene Fachdienste, Zentraler Dienste und Bestandsnetze

Der Anbieter Zentrales Netz TI MUSS durch organisatorische Maßnahmen sicherstellen, dass nur von der gematik zugelassene Fachdienste, zentrale Dienste und Bestandsnetze (inkl. KV-SafeNet) an die TI angebunden werden.⌫

3.3 Funktionsmerkmale

⌦ GS-A_4795 Produkttyp Zentrales Netz, Festlegung der Schnittstellen

Das Zentrale Netz MUSS die Schnittstellen gemäß Tabelle Tab_PT_ZentrNetz_Schnittstellen implementieren ("bereitgestellte" Schnittstellen) und nutzen ("benötigte" Schnittstellen).

Tabelle 8: Tab_PT_ZentrNetz_Schnittstellen

Schnittstelle	bereitgestellt/benötigt	obligatorisch/optional	Bemerkung
I_IP_Transport	bereitgestellt	obligatorisch	Definition in Abschnitt 3.3.2.1
I_DNS_Name_Resolution	benötigt	obligatorisch	Definition in Kapitel 4 Namensdienst
I_NTP_Time_Information	benötigt	obligatorisch	Definition in Kapitel 5 Zeitdienst
P_Monitoring_Update	benötigt	obligatorisch	Definition in [gemSpec_St_Ampel]
P_Monitoring_Read	benötigt	obligatorisch	Definition in [gemSpec_St_Ampel]

⌫

3.3.1 OSI-Schicht 1 und 2 (Physical/Data Link)

3.3.1.1 Schnittstelle CPE-Produkttyp

⌦ GS-A_4796 Anschlusstyp CPE an Produkttyp

Das Zentrale Netz MUSS die Schnittstelle der SZZPs auf der Customer Edge mit mindestens Gigabit Ethernet als 1000Base-T (IEEE 802.3ab) oder IEEE 802.3z implementieren. Das Zentrale Netz MUSS logisch getrennte Netzwerke gemäß Standard 802.1q bereitstellen.⌫

3.3.1.2 Hardwaremerkmale

⌦ **GS-A_4797 Anschlusstyp CPE an Produkttyp, Modularität**

Der Anbieter Zentrales Netz TI MUSS die Schnittstellen auf den SZZPs Richtung angeschlossenem Produkttyp der TI modular mit Small Form-factor Pluggables (SFP) nach den Spezifikationen des SFF [SFF] implementieren.

Der Anbieter Zentrales Netz MUSS sich bei der Art der Schnittstellen und Stecker auf den SZZPs Richtung angeschlossenem Produkttyp der TI nach den Vorgaben des Anbieters des angeschlossenen Produkttyps richten.⌫

3.3.2 OSI-Schicht 3 (Network)

3.3.2.1 Schnittstelle I_IP_Transport

⌦ **GS-A_4798 Schnittstelle I_IP_Transport**

Das Zentrale Netz MUSS die Schnittstelle I_IP_Transport und die Operation I_IP_Transport::send_Data umsetzen, die den Transport, Empfang und Versand von IPv4- und IPv6-Paketen gewährleistet ([gemSpec_Net#Tab_Standards_IPv4] und [gemSpec_Net#2.2.2.2]).⌫

3.3.3 Adressierung

3.3.3.1 Schnittstelle SZZP-Backbone (CE-PE) und SZZP intern

Adressierung auf der SZZP-Backbone (CE-PE), möglichen SZZP-internen Schnittstellen und Anschlüssen hinter dem PE liegen in Verantwortung des Anbieters Zentrales Netz.

⌦ **GS-A_4799 IPv4-Adressen SZZP-Backbone und SZZP intern**

Der Anbieter Zentrales Netz MUSS für die folgenden IP-Schnittstellen IP-Adressen aus seinem eigenen Bestand nutzen:

- Sicherheitsgateways und CE (falls separate Systeme)
- CE-PE
- PE-Backbone⌫

⌦ **GS-A_4800 Adresskonflikte IPv4-Adressen SZZP-Backbone und SZZP intern**

Der Anbieter Zentrales Netz TI MUSS mögliche Adresskonflikte zwischen von ihm genutzten IP-Adressen (zwischen Sicherheitsgateways und CE, CE-PE und PE-Backbone) und TI-Adressen (100.64.0.0/10 [RFC6598]) selbst lösen.⌫

3.3.4 Routing

⌦ **GS-A_4801 Erreichbarkeit TI IP-Adressbereiche**

Das Zentrale Netz MUSS gewährleisten, dass zwischen allen SZZPs alle IP-Adressblöcke der TI-Produktivumgebung (gemSpec_Net#Tab_Adrkonzept_Produktiv) erreichbar sind.⌫

⌦ **GS-A_4803 Meldung IP-Adressbereiche Bestandsnetze**

Der GBV MUSS dem Anbieter Zentrales Netz TI die Adressbereiche von Bestandsnetzen mit Anschluss an die TI bei Neuanschluss an die TI oder Änderungen melden.⌫

3.3.5 Abstimmung mit angeschlossenen Produkttypen

⌦ **GS-A_4804 Umsetzung Parameter**

Der Anbieter Zentrales Netz TI MUSS die vom Produkttyp gemeldeten Parameter nach Tab_PT_ZentrNetz_AnschlussParameter umsetzen.⌫

⌦ **GS-A_4805 Abstimmung angeschlossener Produkttyp mit dem Anbieter Zentrales Netz**

Die Anbieter aller Produkttypen der TI mit Anschluss an das Zentrale Netz TI MÜSSEN mindestens die folgenden Parameter zur Konfiguration ihres Anschlusses an das Zentrale Netz TI an den Betreiber des Zentralen Netzes melden:

Tabelle 9: Tab_PT_ZentrNetz_AnschlussParameter: Anschlussparameter

Lfd. Nr.	Parameter	Beschreibung	Mögliche Werte
1	IPv4-Bereich	Dem Produkttyp zugewiesener TI IPv4-Adressbereich, i. d. R. mit der Größe /26	IPv4-Subnet /26
2	IPv4-Adressen SZZP	IP-Adressen auf der Schnittstelle des Produkttyps zum SZZP	IPv4-Adressen
3	IPv4-Adressen Produkttyp	IP-Adressen für die Schnittstellen des/der SZZPs zum Produkttyp	IPv4-Adressen
4	Routing-Verfahren	Zwischen SZZP und Produkttyp eingesetztes Routing-Verfahren	statisch oder dynamisch
4a	Routing-Verfahren, Protokolle	Wenn dynamisches Routing-Verfahren genutzt wird: Eingesetzte Routing-Protokolle	(nur wenn Lfd. Nr. 4= „dynamisch“) OSPFv2 oder OSPFv3
5	Anzahl Hauseinführungen	Anzahl der Hauseinführungen	1 oder 2

Lfd. Nr.	Parameter	Beschreibung	Mögliche Werte
		vom Zentralen Netz zum SZZP	
5a	Anzahl der angebundenen Standorte	Anzahl der angebundenen Standorte (z.B. bei Verteilung auf mehrere RZ)	1 oder 2
6	Anschlussbandbreite	Anschlussbandbreite: Typ 1: 1 bis 100 Mbit/s Typ 2: 1 Mbit/s bis 1 Gbit/s	Typ 1 oder Typ 2
7	Anzahl SZZPs	Anzahl der SZZPs	1 oder 2
8	Hochverfügbarkeitsprotokolle	Möglicherweise vom Produkttyp eingesetzte Hochverfügbarkeitsprotokolle zwischen Netzkomponenten des Produkttyps mit Anschluss an die TI durch SZZPs	VRRP, HRSP u.a.
9	Physische Schnittstelle SZZP-Produkttyp	Art der Ethernetschnittstelle zwischen SZZPs und den Netzkomponenten des an die TI angeschlossenen Produkttyps	1 Gigabit Kupfer, 1 Gigabit Glasfaser

⌫

⌦ GS-A_4895 Meldung Anbieter Zentrales Netz an angeschlossenen Produkttyp

Der Anbieter Zentrales Netz MUSS Anbietern von Produkttypen der TI bei deren Anschluss an das Zentrale Netz TI mindestens die folgenden Informationen über die zu installierenden Komponenten des SZZP zur Verfügung stellen: Außenmaße, Gewicht, Art und Anzahl Stromzufuhr, Leistungsaufnahme, Abwärmeabfuhr oder -abtransport. ⌫

3.4 Verteilungssicht

3.4.1 Zugangsstellen

Verteilung der Backbone-Zugangsstellen

⌦ GS-A_4806 PoP Redundanter Anschluss

Der Point of Presence (PoP, Standort von PE-Routern im Backbone des Anbieters des Zentralen Netzes der TI) MUSS an das eigene zentrale Netz des Anbieters redundant angeschlossen sein.⌫

⌦ GS-A_4807 Ballungsräume PoPs Zentrales Netz

Der Anbieter Zentrales Netz MUSS in den folgenden Ballungsräumen regionale PoPs zu seinem Netzwerk betreiben:

- Berlin
- Frankfurt am Main
- Köln, Düsseldorf oder Dortmund
- Leipzig oder Dresden
- Hannover
- Hamburg
- München
- Nürnberg
- Saarbücken
- Stuttgart⌫

4 Namensdienst

Der Namensdienst bildet die Namen von Hostsystemen und netzwerkfähigen Applikationen in IP-Adressen ab und ermöglicht so die Identifizierung von Zielsystemen innerhalb der TI. Zusätzlich können durch parametrisierte Abfragen die URLs von Diensten in der TI ermittelt werden.

Die logische Struktur des DNS-Service beinhaltet einen geschlossenen, hierarchisch gegliederten Namensraum, in dem die Adressen der fachanwendungsspezifischen Dienste und der zentralen Dienste der TI-Plattform enthalten sind. Darüber hinaus müssen FQDNs aus dem Namensraum des sicheren Netzwerks der KVen sowie aus dem Namensraum des Internets (für die Adressen des Zugangsdienstes und für den Zugriff von Clientsystemen auf Dienste im Internet) aufgelöst werden.

4.1 Hostnamen

⌦ GS-A_3824 Hostnamen von Produkttypen der Fachanwendungen sowie der zentralen TI-Plattform

Anbieter von Produkttypen der Fachanwendungen sowie der zentralen TI-Plattform MÜSSEN, für die netzwerkfähigen und zur Kommunikation innerhalb der TI genutzten Außenschnittstellen, Hostnamen verwenden, die konform zu den Vorgaben in [RFC1123#2.1] sind.

Die Hostnamen müssen von den Anbietern vergeben werden. Hostnamen für Systeme in der Testumgebung der TI müssen als Namensbestandteil am Ende „-test“ enthalten. Hostnamen für Systeme in der Referenzumgebung der TI müssen als Namensbestandteil am Ende „-ref“ enthalten. Hostnamen für Systeme, die in der Testumgebung und in der Referenzumgebung der TI enthalten sind müssen als Namensbestandteil am Ende „-testref“ enthalten.

Die Hostnamen müssen so gewählt werden, dass die resultierenden FQDN eindeutig sind.⌫

4.2 Namensräume

⌦ GS-A_3828 Namensraum der TI

Der Anbieter des Produkttyps Namensdienst MUSS in der TI (Produktivumgebung) genau einen internen und geschlossenen Namensraum betreiben. In diesem Namensraum MÜSSEN die Ressource Records der, netzwerkfähigen und zur Kommunikation innerhalb der TI genutzten, Außenschnittstellen der fachanwendungsspezifischen Dienste sowie der zentralen Dienste der TI-Plattform verwaltet werden.⌫

Dieser geschlossene Namensraum wird im Folgenden Namensraum der TI genannt.

⌦ **GS-A_4071 Namensraum der TI-Testumgebung**

Der Anbieter des Produkttyps Namensdienst MUSS in der TI-Testumgebung genau einen internen und geschlossenen Namensraum bereitstellen. In diesem Namensraum MÜSSEN die Ressource Records der, netzwerkfähigen und zur Kommunikation innerhalb der TI Testumgebung genutzten, Außenschnittstellen der Testsysteme der fachanwendungsspezifischen Dienste sowie der zentralen Dienste der TI-Plattform verwaltet werden.⌫

Für die Referenzumgebung werden hinsichtlich des Namensraums keine weiteren Vorgaben getroffen.

Innerhalb der TI werden neben dem Namensraum der TI auch der Namensraum des Transportnetzes, der Namensraum des Internets sowie der Namensraum des Sicheren Netzwerks der KVen durch Clientsysteme genutzt. Diese liegen jedoch nicht in der Verantwortung der TI.

⌦ **GS-A_3829 Konnektor, Nutzung externer Namensräume**

Der Konnektor MUSS Clientsystemen der Leistungserbringer die Namens- und Adressauflösung für Namen und Adressen aus den Namensräumen Internet und Sicheres Netz der KVen über einen DNS-Forwarder ermöglichen. Um die Resource Records des VPN-Zugangsdienstes und den FQDN des CRL-Downloadpunktes auflösen zu können, MUSS der Konnektor die Nameserver (Transportnetz) abfragen.⌫

4.3 Domainnamen- und Hierarchie

⌦ **GS-A_3830 Namensdienst, Domainnamen- und Hierarchie**

Der Produkttyp Namensdienst MUSS die Festlegungen zu Domainnamen und Hierarchie umsetzen.

Abbildung 8: Domainnamen und hierarchische Struktur des Namensraums der TI

⌫

⌦ **GS-A_3926 Namensdienst, DNS-Root und Top Level Domain**

Der Anbieter des Produkttyps Namensdienst MUSS eine eigene DNS-Root und die Top Level Domain **telematik** für den Namensraum der TI bereitstellen.⌫

⌦ **GS-A_3927 Namensdienst, Second Level Domains**

Der Anbieter des Namensdienstes MUSS Second Level Domains und darunterliegende Domains für Anbieter von Diensten der TI bereitstellen.

Der Anbieter des Namensdienstes muss es ermöglichen, dass andere Anbieter von Diensten der TI eigene Second Level Domains und darunterliegende Domains betreiben.⌫

⌦ **GS-A_3928 Nameserver-Implementierungen, Second Level Domainnamen**

Produkttypen die Nameserver die Second Level Domains in der TI betreiben, MÜSSEN gewährleisten, dass sich die Namen der Second Level Domains an den Kurzformen der Produkttypnamen bzw. der Fachanwendungsnamen orientieren. Unterhalb der Second Level Domains können Anbieter der entsprechenden Dienste eigene Subdomains mit selbst gewählten Namen verwalten.⌫

⌦ **GS-A_4072 Namensdienst, DNS-Root und Top Level Domain, Domainnamen- und Hierarchie für die TI-Testumgebung**

Der Anbieter des Produkttyps Namensdienst MUSS eine eigene DNS-Root und die Top Level Domain **telematik-test** für den Namensraum der TI-Testumgebung bereitstellen.

Der Anbieter des Produkttyps Namensdienst MUSS sicherstellen, dass die übrigen Domainnamen und die Hierarchie des Namensraums der TI-Testumgebung den Domainnamen und der Hierarchie der Produktivumgebung entsprechen.⌫

Wenn Anbieter von fachanwendungsspezifischen Diensten oder von Produkttypen der zentralen TI-Plattform eigene Subzonen im Namensraum der TI betreiben, müssen grundsätzlich alle Anforderungen, die für den Produkttyp Namendienst im Rahmen der Zonenverwaltung gelten, mit erfüllt werden. Dies sind insbesondere Anforderungen an den Einsatz von DNSSEC, Anforderungen an die Verfügbarkeit und Performance sowie an das Monitoring. Ausgenommen sind Anforderungen an die Verwaltung des Trust Anchor des Namensraums der TI. Die zu erfüllenden Anforderungen werden dem Anbieter im Rahmen der Antragstellung zur Verwaltung einer eigenen Subdomain in der TI durch die gematik mitgeteilt.

4.4 DNS-Topologie

Die DNS-Topologie ergibt sich aus den Funktionalitäten, die an den verschiedenen Punkten in der TI benötigt werden.

In der TI und um Verbindungen in die TI aufzubauen werden Nameserver mit folgender Topologie und Funktionalität eingesetzt:

Tabelle 10: DNS-Topologie der TI

Produkttyp	DNS-Komponente	Funktion
Konnektor	Nameserver	DNS-Forwarder zur Namensauflösung für die Namensräume TI, Sicheren Netzwerks der KVen (SNK), Transportnetz und Internet über den SIS sowie zur Servicelokalisierung im Namensraum der TI. DNS-Domains des SNK: kv-safenet.de, kvnet4doc.de (Dienste der KV Westfalen-Lippe) DNS-Server des SNK: primär 188.144.7.140, sekundär 188.144.15.4
VPN-Zugangsdienst	Nameserver (SIS)	Nameserver zur Auflösung der FQDN im Internet. Dieser Nameserver wird vom Konnektor aus über den IPsec-Tunnel für den Sicheren Internet Service erreicht.
	Nameserver (TI)	DNS-Cache-Server für den Namensraum TI
	Nameserver (Transportnetz)	Nameserver zur Auflösung der FQDN der VPN-Konzentratoren durch den Konnektor. Diese Zone ist Teil des Namensraums Internet, wenn das Transportnetz das Internet ist.
Namensdienst	Nameserver (TI)	Nameserver für die Zonen Root, TLD und der Subdomains für alle Fachanwendungen der TI sowie für Produkttypen der Zone TI-Plattform zentral.

Produkttyp	DNS-Komponente	Funktion
		Diese Zonen sind Teil des Namensraums der TI. Von den Subdomains für alle Fachanwendungen der TI sowie für Produkttypen der Zone TI-Plattform zentral erfolgt optional eine Zone-Delegation an Anbieter von fachanwendungsspezifischen Diensten oder an Anbieter von Produkttypen.
<FA_spez_Dienst>	optionaler Nameserver (TI)	Nameserver für eine Subdomain unterhalb einer Fachanwendungsdomain oder Forwarder
<Zentraler_Dienst_TIP>	optionaler Nameserver (TI)	Nameserver für eine Subdomain unterhalb einer Produkttypdomain oder Forwarder

Die folgende Abbildung zeigt die Abfragebeziehungen zwischen den Nameservern.

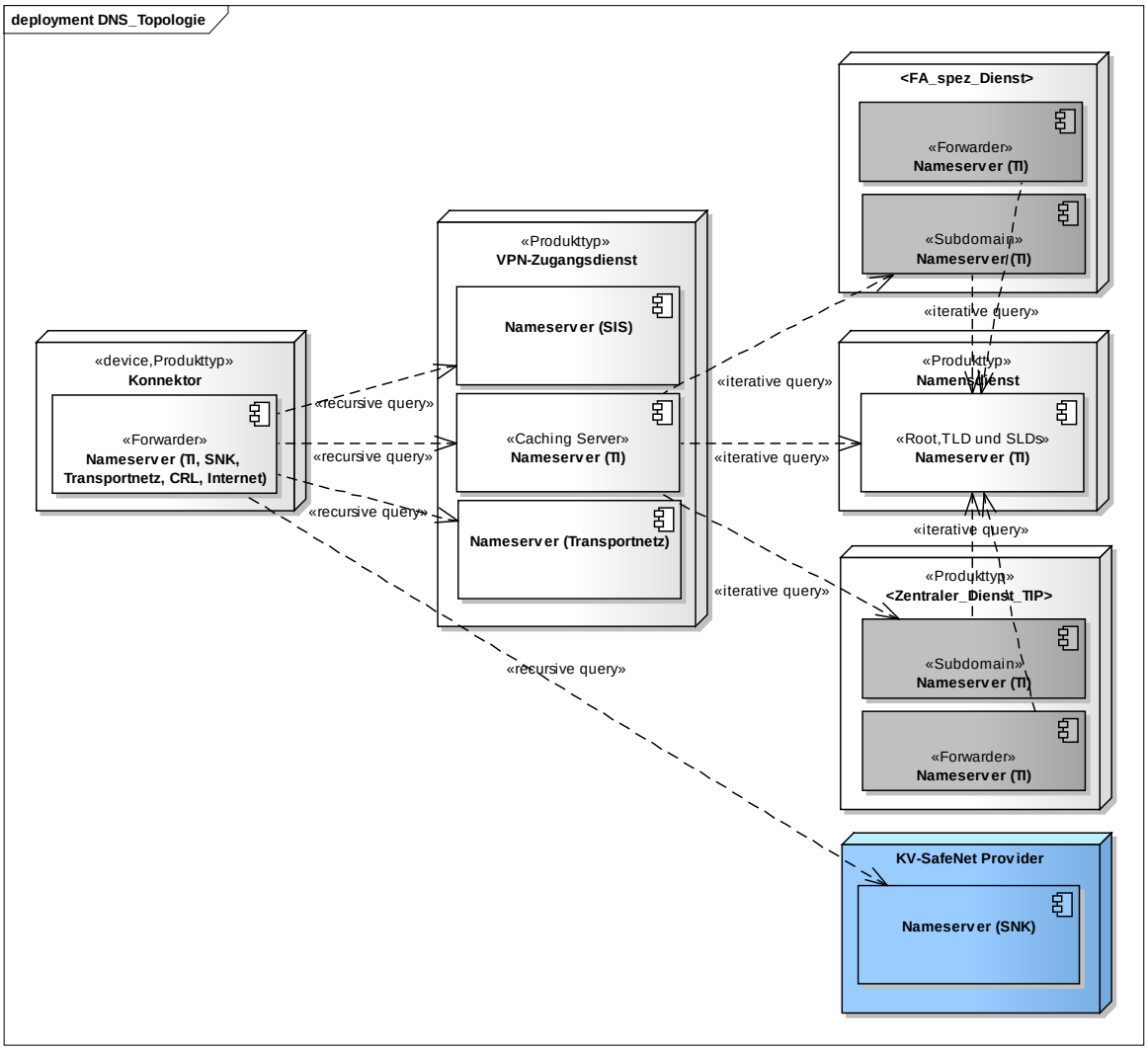


Abbildung 9: Abb_DNS_Topologie_der_TI (GS-A_3932)

Die grau dargestellten Nameserver sind optional. Der blau dargestellte Nameserver liegt außerhalb der Verantwortung der TI. Die innere Struktur der Nameserver-Implementierungen wird in den jeweiligen Produkttypspezifikationen definiert. Rekursive queries zwischen Nameservern werden nicht unterstützt.

⌦ **GS-A_4809 Nameserver-Implementierungen, Redundanz**

Die Nameserver-Implementierungen in der TI MÜSSEN, wenn sie eine Zone im Namensraum der TI verwalten oder wenn sie als Caching Nameserver implementiert sind, physisch redundant durch 2 aktive Nameserver bereitgestellt werden.⌫

⌦ **GS-A_3932 Abfrage der in der Topologie am nächsten stehenden Nameservers**

Produkttypen die innerhalb der TI DNS-Resolver implementieren, MÜSSEN zur Auflösung von FQDNs im Namensraum der TI die in der DNS-Topologie der TI gemäß Abbildung Abb_DNS_Topologie_der_TI am nächsten stehenden Nameserver abfragen.

Für Stub-Resolver der Clientsysteme in den Organisationen des Gesundheitswesens ist dies der Konnektor.

Für Resolver der fachanwendungsspezifischen Dienste sind dies die Nameserver (TI) des Namensdienstes oder, wenn Zone Delegation für die Second Level Domain oder in der Hierarchie darunterliegende Domains genutzt wird, die Nameserver (TI), die die delegierte Zone verwalten.

Für Resolver der zentralen Dienste der TI-Plattform sind dies die Nameserver des Namensdienstes.

Zur Auflösung von FQDN in IP-Adressen verwendet der Stub-Resolver des Konnektors den Nameserver (Forwarder) des Konnektors. Dies gilt für die Namensräume TI, Transportnetz und SNK.

Der Nameserver des Konnektors muss für den Namensraum der TI die Caching Nameserver (TI) des für ihn zuständigen VPN-Zugangsdienstes abfragen. Für den Namensraum des Sicheren Netzwerks der KVen (SNK) muss der Nameserver die Nameserver (SNK) des SNK abfragen. Für den Namensraum des Internet sollen die vom VPN-Zugangsdienst bereitgestellten Nameserver (SIS) für den Namensraum des Internet abgefragt werden.

Die Caching Nameserver (TI) des VPN-Zugangsdienstes müssen die Nameserver (TI) des Namensdienstes und Nameserver (TI), die delegierte Zonen im Namensraum der TI verwalten, abfragen.

In den Resolver-Konfigurationen müssen mindestens 2 zuständige Nameserver eingetragen werden. Ausgenommen davon ist der Stub-Resolver des Konnektors.⌫

4.5 Dienstlokalisierung

Um auf die zentralen Dienste KSR und TSL-Dienst zugreifen zu können, wird die Lokalisierung über DNS Service Discovery unterstützt.

⌦ **GS-A_5024 KSR, Bereitstellung von DNS SRV Resource Records**

Der Anbieter des KSR MUSS DNS SRV Resource Records gemäß Tabelle Tab_KSR_SRV-RR im Namensraum TI verwalten. Wenn die Domain „ksr.telematik“ nicht durch den Anbieter des KSR verwaltet wird, erfolgt der Betrieb dieser Zone beim Anbieter des Namensdienstes und die SRV Resource Records müssen an den Anbieter des Namensdienstes zur Eintragung in die Nameserverkonfiguration übergeben werden.

Tabelle 11: Tab_KSR_SRV-RR

Resource Record Bezeichner	Beschreibung
_ksrkonfig._tcp.ksr.telematik	SRV Resource Record zur Ermittlung der URL des KSR Downloadpunktes für Konfigurationsdaten in der TI
_ksrfirmware._tcp.ksr.telematik	SRV Resource Record zur Ermittlung der URL des KSR Downloadpunktes für Konnektor-Updates in der TI

⌫

4.6 Schnittstellen I_DNS_Name_Resolution und I_DNS_Service_Localization

Beide Schnittstellen werden durch die Standard-DNS-Funktionalität technisch umgesetzt und daher zusammen in einem Abschnitt betrachtet.

4.6.1 Umsetzung

Neben den grundlegenden Funktionen zur Namensauflösung wird für Nameserver im Namensraum der TI die Unterstützung von DNSSEC und von DNS-SD gefordert.

⌦ **GS-A_3834 DNS-Protokoll, Nameserver-Implementierungen**

Produkttypen die Nameserver implementieren, MÜSSEN [RFC1034], [RFC1035] für das DNS-Protokoll und [RFC3596] für IPv6-Anpassungen unterstützen.

Zusätzlich müssen diese Nameserver-Implementierungen die folgenden Aktualisierungen und Ergänzungen zu den oben genannten RFCs unterstützen: [RFC1123] Abschnitt 6.1, [RFC1982], [RFC1995], [RFC1996], [RFC2181], [RFC2308], [RFC2671], [RFC2782], [RFC2930], [RFC2931], [RFC3225].

Die Nameserver-Implementierungen müssen neben UDP auch TCP unterstützen.⌫

⌦ **GS-A_5199 DNSSEC im Namensraum Internet, Vertrauensanker**

Produkte, die DNSSEC im Namensraum Internet nutzen und den Trust Anchor der IANA zur Validierung von DNS-Antworten verwenden, MÜSSEN den DNSSEC-Vertrauensanker gemäß [RFC5011] aktualisieren.⌫

⌦ **GS-A_3842 DNS, Verwendung von iterativen queries zwischen Nameservern**

Anbieter von Produkttypen die Nameserver implementieren, MÜSSEN zur Abfrage anderer Nameserver iterative queries verwenden. Recursive queries dürfen nicht verwendet werden.

Der Konnektor ist von dieser Regelung ausgenommen.⌫

⌦ **GS-A_4849 Produkttyp Konnektor, recursive queries**

Der Nameserver des Konnektors MUSS zur Auflösung von FQDNs die entsprechenden Nameserver mit recursive queries anfragen.⌫

⌦ **GS-A_3930 Nameserver-Implementierungen, TTL**

Produkttypen die Nameserver implementieren, MÜSSEN initial für jeden Resource Record eine Time To Live (TTL) von 86400 einstellen, wenn es keine anderslautenden Festlegungen zur TTL für den jeweiligen Resource Record gibt. Die TTL-Werte können im Rahmen des Change-Management geändert werden.⌫

⌦ **GS-A_3835 DNS-Protokoll, Unterstützung von DNS-SD**

Produkttypen die autoritative Nameserver implementieren, MÜSSEN DNS Service Discovery (DNS-SD) gemäß dem [RFC6763] unterstützen.⌫

⌦ **GS-A_4810 DNS-SD, Format von TXT Resource Records**

Anbieter von Diensten in der TI, die ihren Dienst über DNS-SD durch den Konnektor lokalisieren lassen MÜSSEN die Vorgaben an das Format von TXT Resource Records umsetzen.

Der Schlüssel „txtvers“ muss mit einem Wert angegeben sein.

Wenn der Dienst über eine URL lokalisiert werden soll, so muss der Schlüssel „path“ mit dem Wert des URL-Pfads angegeben sein. Der URL-Pfad muss mit einem „/“ beginnen. Ein leerer URL-Pfad muss als „/“ angegeben werden.

Weitere Schlüssel=Wert-Strings können angegeben werden.⌫

⌦ **GS-A_4811 Produkttyp Konnektor, DNS-SD, Interpretation von TXT Resource Records**

Der Konnektor MUSS TXT Resource Records den Vorgaben entsprechend interpretieren.

Der Schlüssel „txtvers“ ist mit einem Wert angegeben.

Wenn der Dienst über eine URL lokalisiert wird, so ist der Schlüssel „path“ mit dem Wert des URL-Pfads angegeben. Der URL-Pfad beginnt mit einem „/“. Ein leerer URL-Pfad ist als „/“ angegeben.

Weitere Schlüssel=Wert-Strings können nach Vorgabe des zu lokalisierenden Dienstes angegeben sein.⌫

⌦ **GS-A_3931 DNSSEC-Protokoll, Nameserver-Implementierungen**

Produkttypen die Nameserver implementieren, MÜSSEN [RFC4033], [RFC4034] und [RFC4035] für DNSSEC unterstützen.

Zusätzlich müssen diese Nameserver-Implementierungen Aktualisierungen und Ergänzungen zu den oben genannten RFCs unterstützen. Dies sind Abschnitt 6.1 in [RFC1123], [RFC1982], [RFC1995], [RFC1996], [RFC2181], [RFC2308], [RFC2671], [RFC2782], [RFC2930], [RFC2931], [RFC3225], [RFC5155].⌫

⌦ GS-A_5132 Namensdienst, DNSSEC Trust Anchor TI PU basierend auf der TLD

Der Anbieter des Namensdienstes MUSS den DNSSEC Trust Anchor der TI für die Produktionsumgebung basierend auf der Top Level Domain der Produktionsumgebung der TI "telematik." erstellen.⌫

⌦ GS-A_5133 Namensdienst, DNSSEC Trust Anchor TU/RU basierend auf der TLD

Der Anbieter des Namensdienstes MUSS den DNSSEC Trust Anchor der TI für die Test- und Referenzumgebung basierend auf der Top Level Domain der Test- und Referenzumgebung "telematik-test." erstellen.⌫

⌦ GS-A_3839 DNSSEC, Zonen mittels DNSSEC sichern

Anbieter von Produkttypen die Zonen im Namensraum der TI bereitstellen, MÜSSEN diese Zonen mittels DNSSEC sichern. Die Sicherung MUSS auf Basis des Trust Anchors des Anbieters des Produkttyps Namensdienst erfolgen.

DNSSEC Zone Signing Keys (ZSK) im Namensraum der TI müssen nach Ablauf von 120 Tagen ersetzt werden. Key Signing Keys (KSK) im Namensraum der TI müssen nach 12 Monaten ausgetauscht werden. Hinsichtlich der zur Generierung der asymmetrischen ZSK und KSK Schlüsselpaare in der TI zu verwendenden Algorithmen und Schlüssellängen gelten die Festlegungen aus [gemSpec_Krypt].

Die Empfehlungen aus [RFC4641] müssen beachtet werden.⌫

⌦ GS-A_4879 DNSSEC, Zonen im Namensraum Internet mittels DNSSEC sichern

Anbieter von Produkttypen die Zonen im Namensraum Internet bereitstellen, MÜSSEN diese Zonen mittels DNSSEC sichern. Die Sicherung MUSS auf Basis des Trust Anchors für das Internet (bereitgestellt durch die IANA) erfolgen.

DNSSEC Zone Signing Keys (ZSK) im Namensraum Internet müssen nach Ablauf von 120 Tagen ersetzt werden. Key Signing Keys (KSK) im Namensraum Internet müssen nach 12 Monaten ausgetauscht werden. Hinsichtlich der, zur Generierung der asymmetrischen ZSK und KSK Schlüsselpaare, zu verwendenden Algorithmen und Schlüssellängen gelten die Festlegungen aus [gemSpec_Krypt].

Die Empfehlungen aus [RFC4641] müssen beachtet werden.⌫

⌦ **GS-A_3841 Nameserver-Implementierungen, Einsatz von TSIG**

Anbieter von Produkttypen die Zonen im Namensraum der TI bereitstellen, MÜSSEN Zonentransfers mit Transaction Signature (TSIG) gemäß [RFC2845] und [RFC4635] absichern.

Je Nameserver-Paar muss ein eigener symmetrischer Schlüssel (1:1 Beziehung) verwendet werden. Hinsichtlich des zu verwendenden Algorithmus und der Schlüssellänge gelten die Festlegungen aus [gemSpec_Krypt].⌫

⌦ **GS-A_5089 Nameserver-Implementierungen, private Schlüssel sicher speichern**

Produkte die Nameserver implementieren, MÜSSEN private Schlüssel sicher speichern und ihr Auslesen verhindern.⌫

4.6.2 Nutzung

⌦ **GS-A_3832 DNS-Protokoll, Resolver-Implementierungen**

Produkttypen die DNS-Resolver implementieren, MÜSSEN [RFC1034], [RFC1035] für das DNS-Protokoll und [RFC3596] für IPv6-Anpassungen unterstützen.

Zusätzlich müssen diese Resolver-Implementierungen die folgenden Aktualisierungen und Ergänzungen zu den oben genannten RFCs unterstützen: [RFC1123] Abschnitt 6.1, [RFC2181], [RFC2308], [RFC2671], [RFC2845], [RFC5452] und [RFC3225].

Der Konnektor ist von dieser Anforderung ausgenommen.⌫

⌦ **GS-A_3833 DNSSEC-Protokoll, Resolver-Implementierungen**

Produkttypen von Fachanwendungsspezifischen Diensten und Zentraler Dienste der TI-Plattform sowie der Konnektor MÜSSEN DNS-Resolver implementieren die [RFC4033], [RFC4034] und [RFC4035] für DNSSEC unterstützen.⌫

⌦ **GS-A_3840 DNS-Resolver, Nutzung von DNSSEC**

Produkttypen von Fachanwendungsspezifischen Diensten und Zentraler Dienste der TI-Plattform sowie der Produkttyp Konnektor MÜSSEN DNS-Resolver implementieren die „security-aware“ gemäß [RFC4035] sind. Dies beinhaltet insbesondere die Validierung der DNS-Response. ⌫

4.7 Anforderungen an den Produkttyp Namensdienst

⌦ **GS-A_4812 Produkttyp Namensdienst, Festlegung der Schnittstellen**

Der Produkttyp Namensdienst MUSS die Schnittstellen gemäß Tabelle Tab_PT_Namensdienst_Schnittstellen implementieren („bereitgestellte“ Schnittstellen) und nutzen („benötigte“ Schnittstellen).

Tabelle 12: Tab_PT_Namensdienst_Schnittstellen

Schnittstelle	bereitgestellt / benötigt	obligatorisch / optional	Bemerkung
I_DNS_Name_Resolution	bereitgestellt	obligatorisch	Definition in Abschnitt 4.6
I_DNS_Service_Localization	bereitgestellt	obligatorisch	Definition in Abschnitt 4.6
P_DNS_Name_Entry_Announcement	bereitgestellt	obligatorisch	Definition in Abschnitt 4.7.1
P_DNS_Service_Entry_Announcement	bereitgestellt	obligatorisch	Definition in Abschnitt 4.7.1
P_DNS_Zone_Delegation	bereitgestellt	obligatorisch	Definition in Abschnitt 4.7.3
P_DNSSEC_Key_Distribution	bereitgestellt	obligatorisch	Definition in Abschnitt 4.7.2
I_NTP_Time_Information	benötigt	obligatorisch	Definition in Abschnitt 5.1
I_IP_Transport	benötigt	obligatorisch	Definition in Abschnitt 3.3.2.1
I_Monitoring_Update	benötigt	obligatorisch	Definition durch den Anbieter der Störungsampel
I_Monitoring_Read	benötigt	obligatorisch	Definition durch den Anbieter der Störungsampel

⌫

4.7.1 Schnittstellen P_DNS_Name_Entry_Announcement und P_DNS_Service_Entry_Announcement

⌦ **GS-A_4814 Prozess zur Verwaltung von DNS Resource Records**

Der Anbieter des Namensdienstes MUSS einen Prozess implementieren, der es Anbietern von fachanwendungsspezifischen Diensten und Anbietern von zentralen Diensten der TI-Plattform ermöglicht, DNS Resource Records innerhalb des Namensraums der TI bekannt zu machen.

Der Prozess muss dokumentiert sein und dem GBV zur Freigabe vorgelegt werden.

Zusätzlich muss der Anbieter des Namensdienstes alle Anbietern von Diensten in der TI informieren, wie sie diesen Prozess nutzen können.⌫

4.7.2 Schnittstelle P_DNSSEC_Key_Distribution

⌦ **GS-A_4815 Prozess zur DNSSEC Schlüsselverteilung**

Der Anbieter des Namensdienstes MUSS einen Prozess implementieren, der es ermöglicht den Hash des DNSSEC Trust Anchor für den Namensraum TI an Resolver und Nameserver der fachanwendungsspezifischen Dienste und der zentralen Dienste der TI-Plattform sowie an Nameserver der Konnektoren und Hersteller von Konnektoren zu verteilen.

Die Empfehlungen aus [RFC4641] Kapitel 4 müssen beachtet werden.

Der Prozess muss dokumentiert sein und dem GBV zur Freigabe vorgelegt werden.

Nach diesem Prozess muss initial der Hash des DNSSEC Trust Anchor für den Namensraum TI an den GBV, an Anbieter von Resolver und Nameserver der fachanwendungsspezifischen Dienste und der zentralen Dienste der TI-Plattform sowie an Hersteller von Konnektoren verteilt werden. Das Format für die Verteilung des

DNSSEC Trust Anchor muss dem IANA XML-Format zur Verteilung des Internet DNSSEC Trust Anchor entsprechen. Die Aktualisierung des DNSSEC Trust Anchor für den Namensraum TI muss gemäß [RFC5011] automatisch erfolgen.

Zusätzlich muss der Trust Anchor bei Aktualisierungen dem GBV zur Verfügung gestellt werden. Die Aktualisierung des Trust Anchor für den Namensraum TI muss über einen genehmigungspflichtigen Change gemäß [gemRL_Betr_TI] erfolgen.⌫

⌦ GS-A_4885 Namensdienst, Gültigkeitszeitraum des DNSSEC Trust Anchor TI

Der Anbieter des Namensdienstes MUSS den DNSSEC Trust Anchor der TI nach 5 Jahren oder nach Kompromittierung aktualisieren. Der bisherige DNSSEC Trust Anchor muss für eine Übergangszeit von 6 Monaten gültig bleiben.⌫

⌦ GS-A_4816 Produkttyp Konnektor, Einbringung des DNSSEC Trust Anchor für den Namensraum TI

Hersteller von Konnektoren MÜSSEN initial bei der Herstellung den Hash des aktuellen DNSSEC Trust Anchor für den Namensraum TI im DNS Forwarder des Konnektors eintragen. Updates der Software des Konnektors müssen den Hash des aktuellen DNSSEC Trust Anchor für den Namensraum TI beinhalten.

Die Aktualisierung des DNSSEC Trust Anchor für den Namensraum TI muss im Konnektor gemäß [RFC5011] automatisch erfolgen.⌫

⌦ GS-A_4817 Produkttypen der Fachanwendungen sowie der zentralen TI-Plattform, Einbringung des DNSSEC Trust Anchor für den Namensraum TI

Anbieter von Produkttypen der Fachanwendungen sowie der zentralen TI-Plattform MÜSSEN initial bei der Inbetriebnahme den Hash des aktuellen DNSSEC Trust Anchor für den Namensraum TI in der Konfiguration ihrer Resolver- und Nameserver-Implementierungen eintragen und sicher speichern.

Die Aktualisierung des DNSSEC Trust Anchor für den Namensraum TI muss gemäß [RFC5011] automatisch erfolgen können.⌫

⌦ GS-A_4847 Produkttyp VPN-Zugangsdienst, DNSSEC im Namensraum Transportnetz

Anbieter von VPN-Zugangsdiensten MÜSSEN den Namensraum Transportnetz per DNSSEC sichern. ⌫

⌦ GS-A_5037 VPN-Zugangsdienst, Prozess zur Verteilung des DNSSEC Trust Anchor im Namensraum Transportnetz

Der Anbieter VPN-Zugangsdienstes MUSS bei Verwendung eines vom Internet verschiedenen Transportnetzes einen Prozess implementieren, der es ermöglicht den Hash des DNSSEC Trust Anchor für den Namensraum Transportnetz an Betreiber von Konnektoren zu verteilen.⌫

⌦ GS-A_4848 Produkttyp Konnektor, DNSSEC im Namensraum Transportnetz

Der Konnektor MUSS ermöglichen, dass der aktuelle DNSSEC Trust Anchor für den Namensraum Transportnetz im DNS Forwarder des Konnektors eingetragen werden kann. Wenn der DNSSEC Trust Anchor für den Namensraum Transport-

netz eingetragen ist, dann MÜSSEN die Antworten vom Nameserver Transportnetz durch den Konnektor validiert werden.

Die Aktualisierung des DNSSEC Trust Anchor für den Namensraum Transportnetz muss im Konnektor gemäß [RFC5011] automatisch erfolgen.⌧

4.7.3 Schnittstelle P_DNS_Zone_Delegation

⌦ **GS-A_4818 Prozess zur Verwaltung von Subdomains**

Der Anbieter des Namensdienstes MUSS einen Prozess implementieren, der es Anbietern von fachanwendungsspezifischen Diensten und Anbietern von zentralen Diensten der TI-Plattform ermöglicht, eigene DNS-Subdomains innerhalb des Namensraums der TI zu betreiben.

Der Prozess muss dokumentiert sein und dem GBV zur Freigabe vorgelegt werden.

Zusätzlich muss der Anbieter des Namensdienstes alle Anbietern von Diensten in der TI informieren, wie sie diesen Prozess nutzen können.⌧

4.7.4 Sonstige Anforderungen

⌦ **GS-A_3838 DNSSEC, Trust Anchor**

Der Anbieter des Produkttyps Namensdienst MUSS den Trust Anchor für den Namensraum der TI erzeugen und verwalten.⌧

⌦ **GS-A_4813 Produkttyp Namensdienst, nur erlaubte Kommunikation**

Der Produkttyp Namensdienst MUSS sicherstellen, dass vom Namensdienst aus, über das Zentrale Netz der TI, nur erlaubte IP-Kommunikation in Richtung Produkttypen der TI-Plattform und fachanwendungsspezifischer Dienste gesendet wird.

Zur erlaubten Kommunikation des Namensdienstes zählen:

- DNS-Nachrichten an Fachanwendungsspezifische Dienste und an Zentrale Dienste der TI-Plattform
- NTP-Nachrichten an den Produkttyp Zeitdienst
- Übertragung von Monitoringdaten an die Störungsampel⌧

⌦ **GS-A_4808 Nameserver-Implementierungen, nichtautorisierte Zonentransfers**

Die Möglichkeit, Zonentransfers durchzuführen, ohne dass dies in der Topologie durch den Anbieter vorgesehen ist, MUSS auf allen Nameserver-Implementierungen im Namensraum der TI ausgeschlossen sein.⌧

5 Zeitdienst

Der Zeitdienst in der TI basiert auf dem Network Time Protocol (NTP) und ermöglicht es, eine einheitliche Zeit innerhalb der TI zu nutzen.

Dabei synchronisiert sich der Produkttyp Zeitdienst mit der gesetzlichen Zeitinformation. Diese wird über mehrere Stufen in der gesamten TI verteilt und zur Abfrage bereitgestellt.

5.1 NTP-Topologie

Die NTP-Topologie ergibt sich aus der Netztopologie und dem daraus abgeleiteten minimalen Synchronisierungsabstand. Die gewählte Topologie berücksichtigt die Lastverteilung der Konnektoren auf die VPN-Zugangsdienste.

Die folgende Abbildung zeigt die Beziehungen zwischen den NTP-Servern. Die grau dargestellten NTP-Server sind optional. Die blau dargestellte Zeitquelle liegt außerhalb der Verantwortung der TI. Es erfolgt keine Synchronisation zwischen Stratum-2-NTP-Servern. Die innere Struktur (Anzahl der NTP-Server-Instanzen) der NTP-Server-Implementierungen wird in den jeweiligen Produkttypspezifikationen definiert.

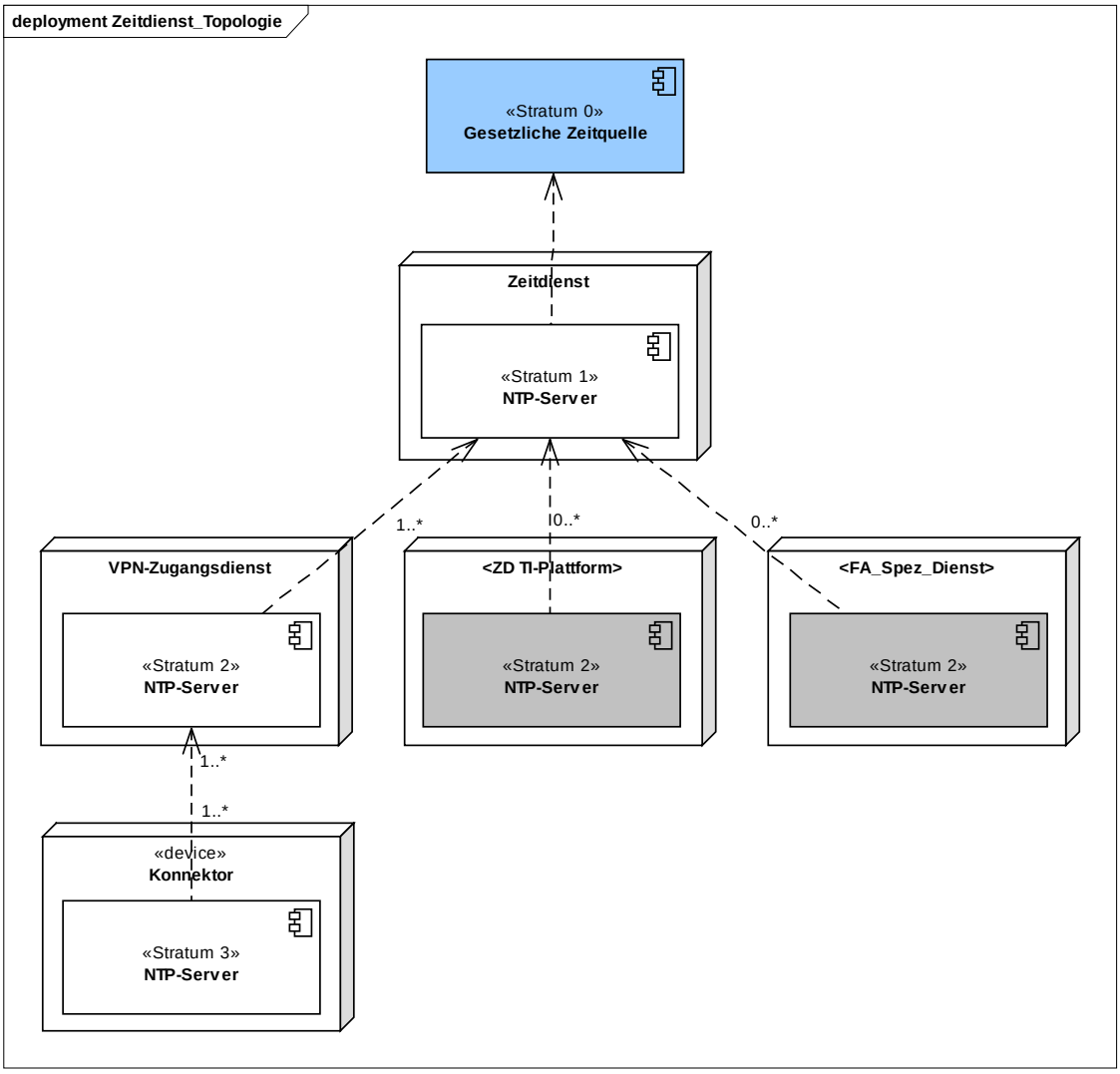


Abbildung 10: NTP-Topologie der TI

⌦ GS-A_3940 Produkttyp Zeitdienst, Stratum 1

Der Produkttyp Zeitdienst MUSS Stratum-1-NTP-Server implementieren. Stratum-1-NTP-Server MÜSSEN sich mit der gesetzlichen Zeitquelle synchronisieren.⌫

⌦ GS-A_3941 Produkttyp VPN-Zugangsdienst, Stratum 2

Der Produkttyp VPN-Zugangsdienst MUSS Stratum-2-NTP-Server bereitstellen, die sich mit allen Stratum-1-NTP-Servern des Produkttyps Zeitdienst synchronisieren MÜSSEN.⌫

⌦ GS-A_3942 Produkttyp Konnektor, Stratum 3

Der Produkttyp Konnektor MUSS einen Stratum-3-NTP-Server implementieren, der sich bei bestehender Verbindung mit Stratum-2-NTP-Servern des Produkttyps VPN-Zugangsdienst synchronisieren MUSS.⌫

5.2 Schnittstelle I_NTP_Time_Information

5.2.1 Umsetzung

⌦ **GS-A_3933 NTP-Server-Implementierungen, Protokoll NTPv4**

Produkttypen die innerhalb der TI NTP-Server implementieren, MÜSSEN das NTP-Protokoll Version 4 gemäß [RFC5905] unterstützen.⌫

⌦ **GS-A_3935 NTP-Server-Implementierungen, Kiss-o´-Death**

Produkttypen die innerhalb der TI NTP-Server implementieren, MÜSSEN zur Abwehr von nicht böswilligen NTP-basierten Denial-of-Service bzw. Distributed-Denial-of-Service Angriffen das Kiss-o´-Death-Verfahren einsetzen.⌫

⌦ **GS-A_3936 NTP-Server-Implementierungen, IBURST**

Produkttypen die innerhalb der TI NTP-Server implementieren, DÜRFEN IBURST NICHT einsetzen.⌫

⌦ **GS-A_3938 NTP-Server-Implementierungen, Association Mode und Polling Intervall**

Produkttypen die innerhalb der TI NTP-Server implementieren, MÜSSEN gemäß [RFC5905] den Association Mode Client für NTP-Anfragen bei NTP-Servern mit niedrigerem Stratum Wert und den Association Mode Server für Antworten auf NTP-Anfragen verwenden. Das Polling-Intervall MUSS nach dem clock discipline algorithm dynamisch eingestellt werden.⌫

⌦ **GS-A_3945 NTP-Server-Implementierungen, SNTP**

Produkttypen die innerhalb der TI NTP-Server implementieren, DÜRFEN zur Abfrage anderer NTP-Server NICHT SNTP einsetzen.⌫

⌦ **GS-A_4074 NTP-Server-Implementierungen, Maximale Abweichung der Zeitinformation von Stratum-1- und -2-NTP-Servern**

Produkttypen die Stratum-1- und -2-NTP-Server in der TI implementieren MÜSSEN gewährleisten, dass die durch sie verteilte Zeitinformation nicht mehr als 330ms von der Zeitinformation der darüberliegenden Stratum Ebene abweicht.⌫

Da der Konnektor nicht immer online ist oder ggf. auch nie online ist (Offline-Szenario), gelten hier andere Anforderungen an die Genauigkeit des NTP-Servers.

⌦ **GS-A_4075 Produkttyp Konnektor, Maximale Abweichung der Zeitinformation des NTP-Servers**

Der Hersteller des Konnektors SOLL für die durch ihn implementierten NTP-Server gewährleisten, dass die durch sie verteilte Zeitinformation nicht mehr als 330ms von der Zeitinformation der darüberliegenden Stratum Ebene abweicht.⌫

5.2.2 Nutzung

⌦ **GS-A_3934 NTP-Client-Implementierungen, Protokoll NTPv4**

Produkttypen die innerhalb der TI NTP-Clients implementieren, MÜSSEN das NTP-Protokoll Version 4 gemäß [RFC5905] unterstützen.⌫

Um auf der Clientseite Falseticker gemäß [RFC5905] erkennen zu können, müssen alle Stratum-1-NTP-Server abgefragt werden.

⌦ **GS-A_4819 Schnittstelle I_NTP_Time_Information, Nutzung durch fachanwendungsspezifische Dienste**

Fachanwendungsspezifische Dienste SOLLEN sich mit den Stratum-1-NTP-Servern des Produkttyps Zeitdienst synchronisieren. Dies beinhaltet grundsätzlich alle an der Diensterbringung des fachanwendungsspezifischen Dienstes beteiligten Komponenten.

Wenn sich Fachanwendungsspezifische Dienste mit den Stratum-1-NTP-Servern des Produkttyps Zeitdienst synchronisieren, so müssen immer alle Stratum-1-NTP-Server abgefragt werden.

Fachanwendungsspezifische Dienste können einen oder mehrere Stratum-2-NTP-Server betreiben, die sich mit allen Stratum-1-NTP-Servern synchronisieren. Die an der Diensterbringung beteiligten Komponenten synchronisieren sich dann mit den eigenen Stratum-2-NTP-Servern.⌫

⌦ **GS-A_4820 Schnittstelle I_NTP_Time_Information, Nutzung durch Zentrale Dienste der TI-Plattform**

Produkttypen, die zentrale Dienste der TI-Plattform bereitstellen, SOLLEN sich mit allen Stratum-1-NTP-Servern des Produkttyps Zeitdienst synchronisieren. Dies beinhaltet alle an der Diensterbringung des Produkttypen beteiligten Komponenten.

Folgende Ausnahmen gelten:

- Der Produkttyp Zentrales Netz der TI ist von dieser Regelung befreit und muss sich nicht mit den Stratum-1-NTP-Servern des Produkttyps Zeitdienst synchronisieren.
- Der Produkttyp gematik Root-CA ist von dieser Regelung befreit und muss sich nicht mit den Stratum-1-NTP-Servern des Produkttyps Zeitdienst synchronisieren.
- Anbieter von PKI-Dienstleistungen in der TI sollen sich mit Stratum-1-NTP-Servern des Produkttyps Zeitdienst synchronisieren. Sie können sich von dieser Regelung befreien, wenn bereits eine Zeitsynchronisation mit der gesetzlichen Zeit erfolgt.
- Produkttypen, die zentrale Dienste der TI-Plattform bereitstellen, können einen oder mehrere Stratum-2-NTP-Server betreiben, die sich mit allen Stratum-1-NTP-Servern synchronisieren. Die an der Diensterbringung beteiligten Komponenten synchronisieren sich dann mit den eigenen Stratum-2-NTP-Servern.⌫

⌦ GS-A_4821 Schnittstelle I_NTP_Time_Information, Ersatzverfahren für Zentrale Dienste der TI-Plattform

Produkttypen, die zentrale Dienste der TI-Plattform bereitstellen, MÜSSEN, wenn sie sich nicht mit den Stratum-1-NTP-Servern des Produkttyps Zeitdienst synchronisieren, ein Ersatzverfahren einsetzen, dass eine maximale Abweichung von einer Sekunde gegenüber der gesetzlichen Zeit gewährleistet.⌫

⌦ GS-A_3937 NTP-Client-Implementierungen, Association Mode und Polling Intervall

Produkttypen die innerhalb der TI NTP-Clients implementieren, MÜSSEN gemäß [RFC5905] den Association Mode Client verwenden und das Polling-Intervall nach dem clock discipline algorithm dynamisch einstellen.⌫

⌦ GS-A_3939 Produkttypen der TI-Plattform, Zeitsynchronisierung nach Neustart

Produkttypen der TI-Plattform, die mittels NTP synchronisiert werden, MÜSSEN nach jedem Neustart initial ihre Systemzeit in einem einzigen Stellvorgang nach der Zeit der zugeordneten NTP-Server stellen. Danach MUSS die Synchronisation mit den zugeordneten NTP-Servern gemäß NTP-Protokoll erfolgen.⌫

⌦ GS-A_3946 NTP-Client-Implementierungen, SNTP

Produkttypen die innerhalb der TI NTP-Clients implementieren, KÖNNEN zur Abfrage von NTP-Servern SNTP einsetzen.⌫

5.3 Anforderungen an den Produkttyp Zeitdienst

⌦ GS-A_4822 Produkttyp Zeitdienst, Festlegung der Schnittstellen

Der Produkttyp Zeitdienst MUSS die Schnittstellen gemäß Tabelle Tab_PT_Zeitdienst_Schnittstellen implementieren („bereitgestellte“ Schnittstellen) und nutzen („benötigte“ Schnittstellen).

Tabelle 13: Tab_PT_Zeitdienst_Schnittstellen

Schnittstelle	bereitgestellt / benötigt	obligatorisch / optional	Bemerkung
I_NTP_Time_Information	bereitgestellt	obligatorisch	Definition in Abschnitt 5.1
DCF77	benötigt	obligatorisch	Zeitzeichensender DCF77 der PTB
I_IP_Transport	benötigt	obligatorisch	Definition in Kapitel 3 Zentrales Netz der TI
I_DNS_Name_Resolution	benötigt	obligatorisch	Definition in Kapitel 4 Namensdienst
I_Monitoring_Update	benötigt	obligatorisch	Definition durch den Anbieter der Störungsampel
I_Monitoring_Read	benötigt	obligatorisch	Definition durch den Anbieter der Störungsampel
P_DNS_Name_Entry_Announcement	benötigt	obligatorisch	Definition in Kapitel 4 Namensdienst
Schnittstelle zur GLONASS Zeitquelle	benötigt	optional	NTP Server mit GLONASS Zeitquelle.
Schnittstelle zur GPS	benötigt	optional	NTP Server mit GPS Zeitquelle.

Schnittstelle	bereitgestellt / benötigt	obligatorisch / optional	Bemerkung
Zeitquelle			
NTP Schnittstelle zu ptbtime1.ptb.de, ptbtime2.ptb.de, ptbtime3.ptb.de	benötigt	optional	NTP Zeitserver der Physikalisch Technischen Bundesanstalt ptbtime1.ptb.de, ptbtime2.ptb.de und ptbtime3.ptb.de.

Die Client-Funktionalität von mindestens einer der drei optionalen Schnittstellen muss implementiert werden.⌫

Die Synchronisation mit der gesetzlichen Zeit erfolgt über den Zeitsignalsender DCF77 der Physikalisch-Technischen Bundesanstalt (PTB). Die dazugehörige Schnittstelle wird nicht durch die TI bereitgestellt und daher nicht in diesem Dokument beschrieben.

Die Stratum-1-NTP-Server synchronisieren sich mittels jeweils eines Standard-DCF77-Empfängers als gesetzliche Zeitquelle.

⌦ GS-A_4823 Produkttyp Zeitdienst, Synchronisierung der Stratum-1-NTP-Server mit DCF77

Alle Stratum-1-NTP-Server des Produkttyps Zeitdienst MÜSSEN sich im ungestörten Betrieb mit der gesetzlichen Zeit der Bundesrepublik Deutschland über den Zeitsignalsender DCF77 synchronisieren.

Bei Ausfall oder Störung des DCF77-Senders MUSS eine Zeitquelle gemäß Tabelle Tab_PT_Zeitdienst_vertrauenswürdige_Zeitquellen zur Synchronisierung genutzt werden. ⌫

Tabelle 14: Tab_PT_Zeitdienst_vertrauenswürdige_Zeitquellen

Vertrauenswürdige Zeitquelle	Bemerkung
ptbtime1.ptb.de, ptbtime2.ptb.de, ptbtime3.ptb.de	NTP-Zeitserver der Physikalisch Technischen Bundesanstalt
NTP-Server mit GLONASS-Zeitquelle	
NTP-Server mit GPS-Zeitquelle	
eine Kombination der oben genannten Quellen	

⌦ GS-A_4824 Produkttyp Zeitdienst, Anzahl der Stratum-1-NTP-Server

Der Produkttyp Zeitdienst MUSS vier aktive Stratum-1-NTP-Server bereitstellen, die mit der gesetzlichen Zeitquelle synchronisiert sind.⌫

⌦ GS-A_4825 Produkttyp Zeitdienst, nur erlaubte Kommunikation

Der Produkttyp Zeitdienst MUSS sicherstellen, dass vom Zeitdienst aus, über das Zentrales Netz der TI, ausschließlich erlaubte IP-Kommunikation in Richtung Produkttypen der TI-Plattform und fachanwendungsspezifischer Dienste gesendet wird.

Zur erlaubten Kommunikation des Zeitdienstes zählen:

- NTP-Nachrichten an Fachanwendungsspezifische Dienste und an Zentrale Dienste der TI-Plattform gemäß [RFC5905]

- DNS-Anfragen an den Produkttyp Namensdienst und an Nameserver-Implementierungen in der TI, die die Zone des Produkttyps Störungsampel verwalten.
- Übertragung von Monitoringdaten an die Störungsampel⌫

⌦ **GS-A_4826 Produkttyp Zeitdienst, Monitoring der Stratum-1-NTP-Server**

Der Anbieter des Zeitdienstes MUSS die Stratum-1-NTP-Server hinsichtlich der bereitgestellten Zeitinformation überwachen.

Die Überwachung muss alle 5 Minuten erfolgen. Die von den Stratum-1-NTP-Servern bereitgestellten Zeitinformationen dürfen nicht mehr als 100ms voneinander abweichen. Wenn die Zeitinformationen 3 Mal hintereinander mehr als 100ms voneinander abweichen, gilt dies als Prio-3-Störung gemäß [gemRL_Betr_TI].⌫

⌦ **GS-A_4827 Produkttyp Zeitdienst, Vergleich mit Referenzzeitquelle**

Der Anbieter des Zeitdienstes MUSS die von den Stratum-1-NTP-Servern bereitgestellten Zeitinformationen mit einer vertrauenswürdigen Referenzzeitquelle gemäß Tabelle Tab_PT_Zeitdienst_vertrauenswürdige_Zeitquellen vergleichen.

Die Überwachung muss alle 5 Minuten erfolgen. Wenn die Zeitinformation eines oder mehrerer Stratum-1-Server der TI mehr als 500ms von der vertrauenswürdigen Referenzzeitquelle abweichen, gilt dies als Störung. Tritt die Störung 3 Mal hintereinander auf, so muss sie als Prio-3-Störung gemäß [gemRL_Betr_TI] behandelt werden. Ab einer Abweichung von 1000ms ist die Störung als Prio-2-Störung gemäß [gemRL_Betr_TI] zu behandeln.⌫

Anhang A – Verzeichnisse

A1 – Abkürzungen

Kürzel	Erläuterung
AF	Assured Forwarding
AF-Klasse	Assured Forwarding Klasse
BE	Best Effort
CE	Customer Edge
CPE	Customer Premises Equipment
CS	Class Selector
DNS	Domain Name System
DNSSEC	Domain Name System Security Extensions
DSCP	Differentiated Services Code Point
EF	Expedited Forwarding
GBV	Gesamtbetriebsverantwortlicher
GPS	Global Positioning System
IP	Internet Protocol (bezeichnet IPv4 und IPv6)
NTP	Network Time Protocol
PE	Provider Edge
PoP	Point-of-Presence
SFP	Small Form-factor Pluggable
SGW	Sicherheitsgateway
SIS	Sicherer Internet Service
SNTP	Simple Network Time Protocol
SZZP	Sicherer Zentraler Zugangspunkt
TI	Telematikinfrastruktur

A2 – Glossar

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

© gematik – öffentlich

A3 – Abbildungsverzeichnis

Abbildung 1: Abb_NetzTopologie_Schema, Netztopologie der TI 8
Abbildung 2: Abb_NetzTopologie_Detail, Netzwerktopologie der TI - detailliert 9
Abbildung 3: DSCP-Markierung (Beispiel) 23
Abbildung 4: Abb_SichKomp_Platzierung, Platzierung von Sicherheitskomponenten in der TI 30
Abbildung 5: Abb_SichKomp_Netzübergänge, Sicherheitskomponenten bei Netzübergängen, generisch 31
Abbildung 6: Abb_ZentrNetz_Zerlegung, Zerlegung Zentrales Netz 34
Abbildung 7: Abb_ZentrNetz_SSZP-PT, Anbindungsvarianten SZZP zum Produkttyp....37
Abbildung 8: Domainnamen und hierarchische Struktur des Namensraums der TI 47
Abbildung 9: Abb_DNS_Topologie_der_TI (GS-A_3932) 49
Abbildung 10: NTP-Topologie der TI 59

A4 – Tabellenverzeichnis

Abbildung 1: Abb_NetzTopologie_Schema, Netztopologie der TI 8
Abbildung 2: Abb_NetzTopologie_Detail, Netzwerktopologie der TI - detailliert 9
Abbildung 3: DSCP-Markierung (Beispiel) 23
Abbildung 4: Abb_SichKomp_Platzierung, Platzierung von Sicherheitskomponenten in der TI 30
Abbildung 5: Abb_SichKomp_Netzübergänge, Sicherheitskomponenten bei Netzübergängen, generisch 31
Abbildung 6: Abb_ZentrNetz_Zerlegung, Zerlegung Zentrales Netz 34
Abbildung 7: Abb_ZentrNetz_SSZP-PT, Anbindungsvarianten SZZP zum Produkttyp....37
Abbildung 8: Domainnamen und hierarchische Struktur des Namensraums der TI 47
Abbildung 9: Abb_DNS_Topologie_der_TI (GS-A_3932) 49
Abbildung 10: NTP-Topologie der TI 59

A5 – Referenzierte Dokumente

A5.1 – Dokumente der gematik

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

diesem Dokument passende jeweils gültige Versionsnummer sind in der aktuellsten, von der gematik veröffentlichten Dokumentenlandkarte enthalten, in der die vorliegende Version aufgeführt wird.

[Quelle]	Herausgeber: Titel
[gemGlossar]	gematik: Glossar der Telematikinfrastruktur
[gemKPT_Arch_TIP]	gematik: Konzept Architektur der TI-Plattform
[gemRL_Betr_TI]	gematik: Übergreifende Richtlinien zum Betrieb der TI
[gemSpec_Krypt]	gematik: Übergreifende Spezifikation – Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur
[gemSpec_St_Ampel]	gematik: Spezifikation Störungsampel
[gemSpec_VPN_ZugD]	gematik: Spezifikation VPN-Zugangsdienst

A5.2 – Weitere Dokumente

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[BSI SGW]	Bundesamt für Sicherheit in der Informationstechnik (o.J.): Konzeption von Sicherheitsgateways, Version 1.0
[RFC6763]	IETF RFC6763 (Februar 2013) DNS-Based Service Discovery http://tools.ietf.org/html/rfc6763
[IEEE 802.3]	IEEE 802.3™-2008 – IEEE Standard for Information technology-Specific requirements - Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications http://standards.ieee.org/about/get/802/802.3.html
[RFC1034]	RFC 1034 (November 1987): Domain Names – Concepts and Facilities http://tools.ietf.org/html/rfc1034
[RFC1035]	RFC 1035 (November 1987): Domain Names – Implementation and Specification http://tools.ietf.org/html/rfc1035
[RFC1122]	RFC 1122 (Oktober 1989): Requirements for Internet Hosts -- Communication Layers http://tools.ietf.org/html/rfc1122
[RFC1123]	IETF (1989): Requirements for Internet Hosts – Application and Support http://datatracker.ietf.org/doc/rfc1123/
[RFC1191]	RFC 1191 (November 1990): Path MTU Discovery http://tools.ietf.org/html/rfc1191
[RFC1982]	IETF (1996): Serial Number Arithmetic http://datatracker.ietf.org/doc/rfc1982/
[RFC1995]	IETF (1996): Incremental Zone Transfer in DNS http://datatracker.ietf.org/doc/rfc1995/

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[RFC1996]	IETF (1996): A Mechanism for Prompt Notification of Zone Changes (DNS NOTIFY) http://datatracker.ietf.org/doc/rfc1996/
[RFC2119]	RFC 2119 (März 1997): Key words for use in RFCs to Indicate Requirement Levels S. Bradner, http://tools.ietf.org/html/rfc2119
[RFC2181]	IETF (1997): Clarifications to the DNS Specification http://datatracker.ietf.org/doc/rfc2181/
[RFC2308]	IETF (1998): Negative Caching of DNS Queries (DNS NCACHE) http://datatracker.ietf.org/doc/rfc2308/
[RFC2328]	RFC 2328 (April 1998): OSPF Version 2 http://tools.ietf.org/html/rfc2328
[RFC2474]	RFC 2474 (Dezember 1998): Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers http://tools.ietf.org/html/rfc2474
[RFC2475]	RFC 2475 (Dezember 1998): An Architecture for Differentiated Services http://tools.ietf.org/html/rfc2475
[RFC2597]	IETF (1999): Assured Forwarding PHB Group http://datatracker.ietf.org/doc/rfc2597/
[RFC2671]	IETF (1999): Extension Mechanisms for DNS (EDNS0) http://datatracker.ietf.org/doc/rfc2671/
[RFC2672]	IETF (1999): Non-Terminal DNS Name Redirection
[RFC2782]	IETF (2000): A DNS RR for specifying the location of services (DNS SRV) http://datatracker.ietf.org/doc/rfc2782/
[RFC2845]	IETF (2000): Secret Key Transaction Authentication for DNS (TSIG) http://datatracker.ietf.org/doc/rfc2845/
[RFC2930]	IETF (2000): Secret Key Establishment for DNS (TKEY RR) http://datatracker.ietf.org/doc/rfc2930/
[RFC2931]	IETF (2000): DNS Request and Transaction Signatures (SIG(0)s) http://datatracker.ietf.org/doc/rfc2931/
[RFC3168]	RFC 3168 (September 2001): The Addition of Explicit Congestion Notification (ECN) to IP
[RFC3225]	IETF (2001): Indicating Resolver Support of DNSSEC http://datatracker.ietf.org/doc/rfc3225/
[RFC3596]	RFC3596 (Oktober 2003): DNS Extensions to Support IP Version 6 http://datatracker.ietf.org/doc/rfc3596/
[RFC4033]	RFC 4033 (Mai 2005): DNS Security Introduction and Requirements http://tools.ietf.org/html/rfc4033

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[RFC4034]	RFC 4034 (März 2005): Resource Records for the DNS Security Extensions http://tools.ietf.org/html/rfc4034
[RFC4035]	RFC 4035 (März 2005): Protocol Modifications for the DNS Security Extensions http://tools.ietf.org/html/rfc4035
[RFC4594]	RFC 4594: Configuration Guidelines for DiffServ Service Classes http://datatracker.ietf.org/doc/rfc4594/
[RFC4635]	IETF (2006): HMAC SHA TSIG Algorithm Identifiers http://datatracker.ietf.org/doc/rfc4635/
[RFC4641]	RFC4641 (September 2006): DNSSEC Operational Practices http://datatracker.ietf.org/doc/rfc4641/
[RFC5011]	RFC5011 (September 2007): Automated Updates of DNS Security (DNSSEC) Trust Anchors http://datatracker.ietf.org/doc/rfc5011/
[RFC5127]	IETF (2008): Aggregation of DiffServ Service Classes http://datatracker.ietf.org/doc/rfc5127/
[RFC5155]	IETF (2008): DNS Security (DNSSEC) Hashed Authenticated Denial of Existence http://datatracker.ietf.org/doc/rfc5155/
[RFC5340]	IETF (2008): OSPF for IPv6 http://datatracker.ietf.org/doc/rfc5340/
[RFC5452]	IETF (2009): Measures for Making DNS More Resilient against Forged Answers http://datatracker.ietf.org/doc/rfc5452/
[RFC5905]	IETF (2010): Network Time Protocol Version 4: Protocol and Algorithms Specification http://datatracker.ietf.org/doc/rfc5905/
[RFC6335]	IETF (2011): Internet Assigned Numbers Authority (IANA) Procedures for the Management of the Service Name and Transport Protocol Port Number Registry http://datatracker.ietf.org/doc/rfc6335/
[RFC6598]	IETF (2012): IANA-Reserved IPv4 Prefix for Shared Address Space http://datatracker.ietf.org/doc/rfc6598/
[RFC768]	RFC768 (28.08.1980): User Datagram Protocol http://tools.ietf.org/html/rfc768
[RFC791]	RFC 791 (September 1981): INTERNET PROTOCOL DARPA INTERNET PROGRAM PROTOCOL SPEZIFICATION http://tools.ietf.org/html/rfc791
[RFC792]	RFC 792 (September 1981): Internet Control Message Protocol http://tools.ietf.org/html/rfc792
[RFC793]	RFC 793 (September 1981): Transmission Control Protocol http://tools.ietf.org/html/rfc793

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[RFC826]	RFC 826 (November 1982): An Ethernet Address Resolution Protocol http://tools.ietf.org/html/rfc826
[RFC894]	RFC 894 (April 1984): A Standard for the Transmission of IP Datagrams over Ethernet Networks http://tools.ietf.org/html/rfc894
[RIPE-554]	RIPE (2012): Requirements for IPv6 in ICT Equipment
[SFF]	Small Form Factor Committee (SFF): Index of Specifications ftp://ftp.seagate.com/sff/8000_PRJ.HTM