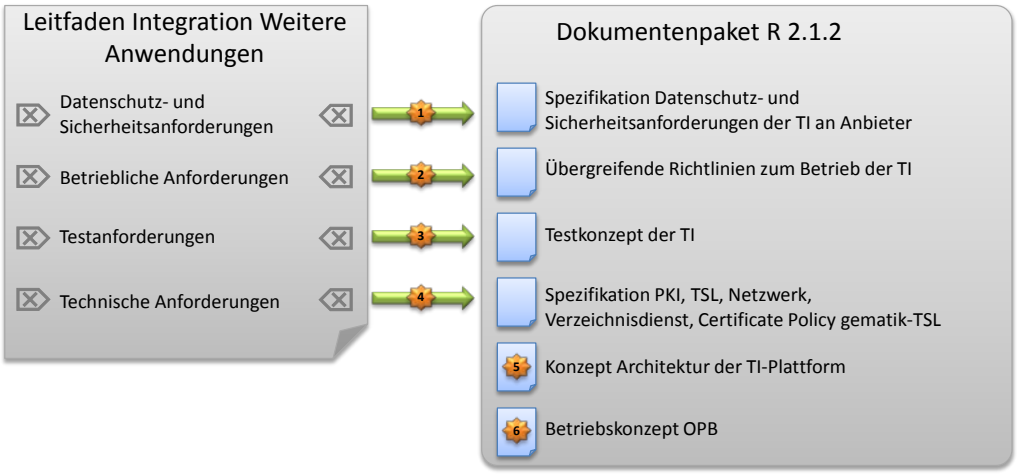
Beim vorliegenden Dokument handelt es sich um einen Entwurf der gematik in Vorbereitung auf zukünftige normative Festlegungen als Grundlage entsprechender Zulassungs- und Bestätigungsverfahren. Die gematik veröffentlicht diesen Entwurf mit dem Ziel, dass sich Interessierte bereits frühzeitig einen Überblick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

Änderungsbedarf

Bisher wurden die Anforderungen an weitere Anwendungen und deren Anbieter im Leitfaden Integration weiterer Anwendungen in die TI veröffentlicht.

Mit dieser Änderung sollen weitere Anwendungen insgesamt in das Dokumentenpaket eingearbeitet werden. Dies erfolgt durch die Einführung der betrieblichen Rolle der Anbieter weiterer Anwendungen, das Erweitern von Umsetzungsanforderungen der TI-Plattform um weitere Anwendungen und das Überführen der Anforderungen aus dem Leitfaden Integration weiterer Anwendungen in die TI in die Spezifikationen des Dokumentenpakets. Informelle Texte des Integrationsleitfadens, werden in den geplanten Anbieterleitfaden für weitere Anwendungen übertragen, sofern sie nicht in die einzelnen Spezifikationen übernommen wurden.

Im Überblick ergeben sich Änderungen wie in Abbildung 1 dargestellt.



1. Anforderungen werden Bestandteil des neuen Zieldokuments; Freigabe des Zieldokuments erfolgt im Rahmen der Freigabe der Neustrukturierung der Datenschutz- und Sicherheitsanforderungen; Auswirkung auf die Anwendungssteckbriefe für weitere Anwendungen: geänderte Anforderungen gemäß modularer Zuordnung.
2. Anforderungen waren und sind Bestandteil des Zieldokuments, bis auf eine Anforderung im Leitfaden, die durch eine Bestandsanforderung aus der Übergreifende Richtlinien zum Betrieb der TI ersetzt wird. Die Richtlinien Betrieb ändern sich daher nicht. Auswirkung auf die Anwendungssteckbriefe für weitere Anwendungen: Anforderung WA-A_2019 wird durch GS-A_3886 ersetzt (mit entsprechender Quelle).
3. Anforderungen werden Bestandteil des Zieldokuments. Auswirkung auf die Anwendungssteckbriefe für weitere Anwendungen: Quelle ändert sich.
4. Die Bestandsanforderungen der Zieldokumente werden im Adressat um die Anwendungskategorien der weiteren Anwendungen erweitert, unter Beachtung bei der Formulierung, dass weitere Anwendungen keine Produkttypen der TI sind. Auswirkung auf die Anwendungssteckbriefe für weitere Anwendungen: Änderung der Anforderungsnummern und der Quellen.
5. Erweiterung diverser Anforderungen um weitere Anwendungen; Auswirkung auf die Anwendungssteckbriefe für weitere Anwendungen: keine.
6. Einführung der Rolle Anbieter einer weiteren Anwendung; Auswirkung auf die Anwendungssteckbriefe für weitere Anwendungen: keine.

Abbildung 1: Überblick der Änderungen aufgrund Einführung weiterer Anwendungen

Die Auswirkungen auf die betroffenen Dokumente sind im Einzelnen wie folgt:

Änderungsbedarf in gemKPT_Arch_TIP

Ergänzung der konzeptionellen Sicht der TI-Plattform auf diese weitere Anwendungen und Darstellung der Positionierung entsprechender Netze und Dienste im Verhältnis zur TIP (z.B. in welcher Zone sie verortet sind). Die relevanten Umsetzungsanforderungen im Dokument wurden um weitere Anwendungen erweitert.

Zudem wurden im Konzept der TI-Plattform die generischen Aspekte sicherer Übermittlungsverfahren in den Änderungen mitberücksichtigt.

Das Dokument wird in Gänze - inklusive dieser Änderungen - vorgelegt.

Änderungsbedarf in gemKPT_Betr

Im Betriebskonzept wird die Rolle des Anbieters einer weiteren Anwendung als TI-ITSM-Teilnehmer eingeführt.

Das Dokument wird in Gänze - inklusive dieser Änderungen - vorgelegt.

Änderungsbedarf in gemKPT_Test

Im Testkonzept wird das neue Kapitel 7 eingeführt, das alle Informationen aus dem Integrationsleitfaden zu Testanforderungen enthält.

Konkret werden die Anforderungen WA-A_2121, WA-A_2122, WA-A_2123, WA-A_2124 aus dem Integrationsleitfaden im Testkonzept aufgenommen.

Das Dokument wird in Gänze - inklusive dieser Änderungen - vorgelegt.

Änderungsbedarf in gemSpec_Net

In diesem Dokument werden die Anforderungen GS-A_4831, GS-A_4009, GS-A_4024, GS-A_4027, GS-A_4759, GS-A_4805, GS-A_4013, GS-A_4018, GS-A_3934, GS-A_3937, GS-A_3932 und GS-A_4760 angepasst und die Anforderungen, GS-A_5583, GS-A_5584, GS-A_5585, GS-A_5586 ergänzt.

⌦ **GS-A_4831 Standards für IPv4**

Produkttypen der TI und andere Anwendungen des Gesundheitswesens mit Anschluss an die 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_4009 Übertragungstechnologie auf OSI-Schicht LAN**

Alle Produkttypen der TI und andere Anwendungen des Gesundheitswesens mit Anschluss an die TI MÜSSEN beim Einsatz des Ethernet-Protokolls an Schnittstellen zwischen Produkttypen der TI die Einhaltung der [IEEE 802.3] sicherstellen. ⌫

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

Alle Anbieter von Diensten in der TI und Anbieter anderer Anwendungen des Gesundheitswesens mit Anschluss an die TI und Zugriff auf Dienste der TI MÜSSEN für ihre über die TI erreichbaren Systeme die zugewiesenen IP-Bereiche nutzen. Bei einem Anbieter anderer Anwendungen des Gesundheitswesens mit Anschluss an die TI und Zugriff auf Dienste der TI können es vom Anbieter bereitgestellte öffentliche IP-Adressen sein. Änderungen an diesen Bereichen MÜSSEN die Anbieter einzelner TI-Dienste bei dem Anbieter Zentrales Netz TI beantragen und bei Verwendung eigener öffentlicher IP-Adressen mit dem Anbieter Zentrales Netz TI abstimmen.⌫

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

Alle Anbieter von Diensten in der TI und Anbieter anderer Anwendungen des Gesundheitswesens mit Anschluss an die TI und Zugriff auf Dienste 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_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.

Ein Anbieter anderer Anwendungen des Gesundheitswesens mit Anschluss an die TI und Zugriff auf Dienste der TI MUSS für die Adressierung ihrer Systeme in Richtung SZZP die mit dem Anbieter Zentrales Netz TI abgestimmten IP-Adressen nutzen.⌫

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

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

Tabelle 2: 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	Anzahl Hauseinführungen	Anzahl der Hauseinführungen vom Zentralen Netz zum SZZP	1 oder 2
4a	Anzahl der angebundenen Standorte	Anzahl der angebundenen Standorte (z.B. bei Verteilung auf mehrere RZ)	1 oder 2
5	Anschlussbandbreite	Anschlussbandbreite: Typ 1: 1 bis 100 Mbit/s Typ 2: 1 Mbit/s bis 1 Gbit/s	Typ 1 oder Typ 2
6	Anzahl SZZPs	Anzahl der SZZPs	1 oder 2
7	Hochverfügbarkeitsprotokolle	Möglicherweise vom Produkttyp eingesetzte Hochverfügbarkeitsprotokolle zwischen Netzkomponenten des Produkttyps mit Anschluss an die TI durch SZZPs	VRRP, HRSP u.a.
8	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_4013 Nutzung von UDP/TCP-Portbereichen

Produkttypen von Fachanwendungen und Zentralen Diensten der TI-Plattform und Anbieter anderer Anwendungen des Gesundheitswesens mit Anschluss an die TI und

Zugriff auf Dienste der TI MÜSSEN die zugeordneten bzw. abgestimmten UDP/TCP-Portbereiche für die Kommunikation in der TI nutzen.⌫

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

Die Anbieter von Produkttypen der TI und Anbieter anderer Anwendungen des Gesundheitswesens mit Anschluss an die TI, und Zugriff auf Dienste der TI, MÜSSEN die Nutzung der zugeteilten und mit den Anbietern anderer Anwendungen des Gesundheitswesens mit Anschluss an die TI und Zugriff auf Dienste der TI abgestimmten UDP/TCP-Portbereiche dokumentieren und diese Dokumentation dem Anbieter Zentrales Netz TI bei Änderungen und auf Anforderung zur Verfügung stellen.⌫

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

Produkttypen die innerhalb der TI NTP-Clients implementieren und Anbieter anderer Anwendungen des Gesundheitswesens mit Anschluss an die TI und Zugriff auf Dienste der TI, MÜSSEN das NTP-Protokoll Version 4 gemäß [RFC5905] unterstützen.⌫

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

Produkttypen die innerhalb der TI NTP-Clients implementieren und Anbieter anderer Anwendungen des Gesundheitswesens mit Anschluss an die TI und Zugriff auf Dienste der TI, die einen NTP-Client für die TI Implementieren, MÜSSEN gemäß [RFC5905] den Association Mode Client verwenden und das Polling-Intervall nach dem clock discipline algorithm dynamisch einstellen.⌫

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

Produkttypen die innerhalb der TI DNS-Resolver implementieren und Anbieter anderer Anwendungen des Gesundheitswesens mit Anschluss an die TI und Zugriff auf Dienste der TI, 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 Bestandsnetze.

Der Nameserver des Konnektors muss für den Namensraum der TI die Caching Nameserver (TI) des für ihn zuständigen VPN-Zugangsdienstes abfragen. Für die Namensräume von Bestandsnetzen muss der Nameserver die Nameserver des entsprechenden Bestandsnetzes 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.⌫

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

Bestandsnetze und Anbieter anderer Anwendungen mit Anschluss an die TI und Zugriff auf Dienste der TI, ohne Zugriff auf Dienste der TI, MÜSSEN bei Anschluss an die TI für diesen Anschluss und Kommunikation mit der TI eigene, öffentliche IPv4-Adressbereiche nutzen.⌫

⌦ **GS-A_5583 aAdG-NetG - Verwaltung des Namensraums**

Ein Anbieter eines an die TI angeschlossenen Netzes des Gesundheitswesens mit aAdG-NetG MUSS den Namensraum des an die TI angeschlossenen Netzes des Gesundheitswesens mit anderen Anwendungen des Gesundheitswesens selber verwalten und dafür Caching Nameserver (recursion available) im an die TI angeschlossenen Netz des Gesundheitswesens mit anderen Anwendungen des Gesundheitswesens bereitstellen.⌫

⌦ **GS-A_5584 Meldung Anbieter eines an die TI angeschlossenen Netzes des Gesundheitswesens mit aAdG-NetG zu Netzwerkinformationen**

Ein Anbieter eines an die TI angeschlossenen Netzes des Gesundheitswesens mit aAdG-NetG MUSS dem Anbieter des zentralen Netzes der TI die Informationen über den Namen des an die TI angeschlossenen Netzes des Gesundheitswesens mit anderen Anwendungen des Gesundheitswesens, den verwendeten öffentlichen IP-Adressraum, den Namensraum sowie den Caching Nameserver bereitstellen.⌫

⌦ **GS-A_5585 Meldung Anbieter eines an die TI angeschlossenen Netzes des Gesundheitswesens mit aAdG-NetG zu Policyinformationen**

Ein Anbieter eines an die TI angeschlossenen Netzes des Gesundheitswesens mit aAdG-NetG MUSS dem Anbieter des Sicherheitsgateways Bestandsnetze, über dass das Netz des Anbieters an die TI angebunden wird, Informationen zu den am Sicherheitsgateway freizuschaltenden Protokollen und Ports für das an die TI anzuschließende Netz des Gesundheitswesens mit anderen Anwendungen des Gesundheitswesens bereitstellen.⌫

⌦ **GS-A_5586 Meldung Anbieter eines an die TI angeschlossenen Netzes des Gesundheitswesens mit aAdG-NetG zur technischen Anschlussvariante**

Ein Anbieter eines an die TI angeschlossenen Netzes des Gesundheitswesens mit aAdG-NetG MUSS mit dem Anbieter des Sicherheitsgateways Bestandsnetze, über dass das Netz des Anbieters an die TI angebunden wird, abstimmen, wie der netztechnische Anschluss an das Sicherheitsgateway erfolgen soll und diesen bereitstellen.⌫

Änderungsbedarf in gemSpec_TSL

In diesem Dokument wird die Anforderung WA-A_2030 aus dem Integrationsleitfaden als TIP1-A_5120 übernommen.

6.3 TSL_Download

⌦ **TIP1-A_5120 Clients des TSL-Dienstes: HTTP-Komprimierung unterstützen**

Clients (~~Die~~ Produkttypen der TI, aAdG und aAdG-NetG-TI), die Dateien vom TSL-Dienst herunterladen, SOLLEN die Komprimierung der Daten über HTTP „Content Coding“ [RFC7231] mit dem Algorithmus gzip unterstützen. ⌫

A1 – Abkürzungen

Kürzel	Erläuterung
aAdG	andere Anwendungen des Gesundheitswesens (mit Zugriff auf Dienste der TI)
aAdG-NetG	andere Anwendungen des Gesundheitswesens ohne Zugriff auf Dienste der TI in angeschlossenen Netzen des Gesundheitswesens
aAdG-NetG-TI	andere Anwendungen des Gesundheitswesens mit Zugriff auf Dienste der TI aus angeschlossenen Netzen des Gesundheitswesens

Änderungsbedarf in gemSpec_PKI

In diesem Dokument wird die Anforderung GS-A_4957 angepasst und die Anforderungen WA-A_2033, WA-A_2111 und WA-A_2112 aus dem Integrationsleitfaden in das Dokument übernommen.

9.1.1.1.1 OCSP-Request

⌦ **GS-A_4957 Beschränkungen OCSP-Request**

Komponenten (Produkttypen der TI, aAdG und aAdG-NetG-TI), die Zertifikate prüfen, DÜRFEN (abweichend von [RFC2560]) je OCSP-Request NICHT mehr als den Status für genau ein Zertifikat abfragen.Ist hierbei die Verwendung der OCSP-Extension „Nonce“ zulässig, DARF diese die Länge von 256 Bit NICHT überschreiten.⌫

⌦ **WA-A_2033 Nutzung der OCSP-Responder der TI**

Eine aAdG oder aAdG-NetG-TI MUSS die OCSP-Responder der TI nutzen.⌫

8.1.1 Initialisierung TI-Vertrauensraum

⌦ **GS-A_4641 Initiale Einbringung TI-Vertrauensanker**

Die Produkttypen der TI, die Zertifikate prüfen, MÜSSEN die initiale Einbringung des aktuell gültigen TSL-Signer-CA-Zertifikat als TI-Vertrauensanker in die Komponente nachweislich sicher vor Manipulation vornehmen.⌫

⌦ **WA-A_2111 Initiale Einbringung TI-Vertrauensanker in andere Anwendungen**

Der Anbieter einer aAdG oder aAdG-NetG-TI MUSS sicherstellen, dass die initiale Einbringung des aktuell gültigen TSL-Signer-CA-Zertifikats als TI-Vertrauensanker in Dienste der aAdG oder der aAdG-NetG-TI nachweislich sicher vor Manipulation vorgenommen wird.⌫

⌦ **GS-A_4748 Initiale Einbringung TSL-Datei**

Die Produkttypen der TI, die Zertifikate prüfen, MÜSSEN die initiale Einbringung der TSL-Datei in die Komponente nachweislich sicher vor Manipulation vornehmen.⌫

⌦ **WA-A_2112 Initiale Einbringung TSL-Datei in andere Anwendungen**

Der Anbieter einer aAdG oder aAdG-NetG-TI MUSS sicherstellen, dass die initiale Einbringung der TSL-Datei in Dienste der aAdG oder der aAdG-NetG-TI nachweislich sicher vor Manipulation vorgenommen wird.⌫

B1 – Abkürzungen

Kürzel	Erläuterung
aAdG	andere Anwendungen des Gesundheitswesens (mit Zugriff auf Dienste der TI)
aAdG-NetG	aAndere Anwendungen des Gesundheitswesens ohne Zugriff auf Dienste der TI in angeschlossenen Netzen des Gesundheitswesens
aAdG-NetG-TI	andere Anwendungen des Gesundheitswesens mit Zugriff auf Dienste der TI aus angeschlossenen Netzen des Gesundheitswesens

Änderungsbedarf in gemRL_TSL_SP_CP

In diesem Dokument wird die Anforderungen WA-A_2113 aus dem Integrationsleitfaden aufgenommen.

Anhang A - Certificate Policy für Komponentenzertifikate

Ergänzend zu Abschnitt 5.3.4 gelten folgende Anforderungen bezogen auf die Zuordenbarkeit und Verwendung von Komponentenzertifikaten:

⌦ **GS-A_4330 Einbringung des Komponentenzertifikats**

Der Betreiber einer Produktinstanz oder der Hersteller eines Produkts MUSS das korrekte Einbringen des Komponentenzertifikats in die Produktinstanz sicherstellen. ⌫

⌦ **WA-A_2113 Einbringung des Komponentenzertifikats in andere Anwendungen**

Der Anbieter einer aAdG oder aAdG-NetG-TI MUSS das korrekte Einbringen des Komponentenzertifikats in Dienste der aAdG oder der aAdG-NetG-TI sicherstellen.⌫

C1 – Abkürzungen

Kürzel	Erläuterung
aAdG	andere Anwendungen des Gesundheitswesens (mit Zugriff auf Dienste der TI)
aAdG-NetG	andere Anwendungen des Gesundheitswesens ohne Zugriff auf Dienste der TI in angeschlossenen Netzen des Gesundheitswesens
aAdG-NetG-TI	andere Anwendungen des Gesundheitswesens mit Zugriff auf Dienste der TI aus angeschlossenen Netzen des Gesundheitswesens

Änderungsbedarf in gemSpec_VZD

In diesem Dokument wird die Anforderung TIP1-A_5566 angepasst.

Das Dokument wird in Gänze - inklusive dieser Änderungen - vorgelegt.

Änderungsbedarf in gemSpec_Kon

Als redaktionelle Anpassung in den nicht normativen Texten der gemSpec_Kon wird die bisherige Formulierung ”Bestandsnetz” durch die neue Formulierung ”angeschlossenes Netz des Gesundheitswesens mit aAdG-NetG” ersetzt.

Notwendige textuelle Anpassung in Anforderungen:

Tabelle 3: TAB_KON_504 Ausführungserlaubnis für Dienste in kritischen Fehlerzuständen

	EC_Software_Integrity_Check_Failed	EC_Random_Generator_Not_Reliable	EC_Security_Log_Not_Writable	EC_Time_Sync_Pending_Critical	EC_Time_Difference_Intolerable	EC_CRL_Out_Of_Date	EC_TSL_Out_Of_Date_Beyond_Grace_	EC_TSL_Trust_Anchor_Out_Of_Date	EC_Firewall_Not_Reliable	EC_Secure_KeyStore_Not_Available	EC_FW_Not_Valid_Status_Blocked
Technische Use Cases (TUCs) der Basisdienste relevant für Fachanwendung und die Kommunikation mit ~~Bestandsnetz~~Weitere Anwendungen und SIS											
Zugriffsberechtigungsdienst											
TUC_KON_000 PrüfeAufrufkontext	-	x	x	x	x	x	x	x	x	x	x
Dienstverzeichnisdienst											
TUC_KON_041 Einbringen der Endpunktinformationen während der Bootup-Phase	-	-	-	x	x	x	x	x	x	x	x

	EC_Software_Integrity_Check_Failed	EC_Random_Generator_Not_Reliable	EC_Security_Log_Not_Writable	EC_Time_Sync_Pending_Critical	EC_Time_Difference_Intolerable	EC_CRL_Out_Of_Date	EC_TSL_Out_Of_Date_Beyond_Grace_	EC_TSL_Trust_Anchor_Out_Of_Date	EC_Firewall_Not_Reliable	EC_Secure_KeyStore_Not_Available	EC_FW_Not_Valid_Status_Blocked
Kartenterminaldienst											
TUC_KON_051 Mit Anwender über Kartenterminal interagieren	-	-	-	-	-	x	x	x	-	-	x
Kartendienst											
TUC_KON_005 Card-to-Card authentisieren	-	-	-	-	-	x	x	x	-	-	x
TUC_KON_006 Datenzugriffsaudit eGK schreiben	-	-	-	-	-	x	x	x	-	-	x
TUC_KON_018 eGK-Sperrung prüfen	-	-	-	-	-	x	x	x	-	-	x
TUC_KON_024 Karte zurücksetzen	-	-	-	-	-	x	x	x	-	-	x
TUC_KON_026 Liefere CardSession	-	-	-	-	-	x	-	x	-	-	-
TUC_KON_200 SendeAPDU	-	-	-	-	-	x	x	x	-	-	x
TUC_KON_202 LeseDatei	-	-	-	-	-	x	x	x	-	-	x
TUC_KON_203 SchreibeDatei	-	-	-	-	-	x	x	x	-	-	x
TUC_KON_209 LeseRecord	-	-	-	-	-	x	x	x	-	-	x
Systeminformationsdienst											
TUC_KON_256 Systemereignis absetzen	-	x	x	x	x	x	x	x	x	x	x
Verschlüsselungsdienst											
TUC_KON_072 Daten symmetrisch verschlüsseln	-	-	-	x	x	x	x	x	-	-	x
TUC_KON_073 Daten symmetrisch entschlüsseln	-	-	-	x	x	x	x	x	-	-	x
Zertifikatsdienst											
TUC_KON_034 Zertifikatsinformationen extrahieren	-	-	-	x	x	x	x	x	-	-	x
Protokollierungsdienst											
TUC_KON_271 Schreibe Protokolleintrag	-	x	x	x	x	x	x	x	x	x	x
TLS-Dienst											
TUC_KON_110 Kartenbasierte TLS-Verbindung aufbauen	-	-	-	-	-	-	-	-	-	-	-
Verbindung zum VPN-Konzentrator											
TUC_KON_321 Verbindung zu dem VPN-Konzentrator der TI aufbauen	-	-	-	-	-	-	-	-	-	-	-
TUC_KON_322 Verbindung zum dem VPN-Konzentrator des SIS aufbauen	-	-	-	-	-	-	-	-	-	-	-
Operationen der Basisdienste											
Kartendienst											
VerifyPin	-	-	-	-	-	x	x	x	-	-	x
UnblockPin	-	-	-	-	-	x	x	x	-	-	x
ChangePin	-	-	-	-	-	x	x	x	-	-	x
GetPinStatus	-	-	-	-	-	x	x	x	-	-	x
Systeminformationsdienst											

	EC_Software_Integrity_Check_Failed	EC_Random_Generator_Not_Reliable	EC_Security_Log_Not_Writable	EC_Time_Sync_Pending_Critical	EC_Time_Difference_Intolerable	EC_CRL_Out_Of_Date	EC_TSL_Out_Of_Date_Beyond_Grace_	EC_TSL_Trust_Anchor_Out_Of_Date	EC_Firewall_Not_Reliable	EC_Secure_KeyStore_Not_Available	EC_FW_Not_Valid_Status_Blocked
Schnittstelle der Ereignissenke	-	x	x	x	x	x	x	x	x	x	x
GetCardTerminals	-	x	x	x	x	x	x	x	x	x	x
GetCards	-	x	x	x	x	x	x	x	x	x	x
GetResourceInformation	-	x	x	x	x	x	x	x	x	x	x
Subscribe	-	x	x	x	x	x	x	x	x	x	x
RenewSubscription	-	x	x	x	x	x	x	x	x	x	x
Unsubscribe	-	x	x	x	x	x	x	x	x	x	x
GetSubscription	-	x	x	x	x	x	x	x	x	x	x
Verschlüsselungsdienst											
EncryptDocument	-	-	-	-	-	x	x	x	-	-	x
DecryptDocument	-	-	-	-	-	x	x	x	-	-	x
Signaturdienst											
SignDocument	-	-	-	-	-	x	x	x	-	-	x
VerifyDocument	-	-	-	-	-	x	x	x	-	-	x
GetJobNumber	-	-	-	-	-	x	x	x	-	-	x
StopSignature	-	-	-	-	-	x	x	x	-	-	x
Authentifizierungsdienst											
ExternalAuthenticate	-	-	-	-	-	x	x	x	-	-	x
Zertifikatsdienst											
ReadCardCertificate	-	-	-	-	-	x	x	x	x	x	x
CheckCertificateExpiration	-	-	-	-	-	x	x	x	x	x	x
VerifyCertificate	-	-	-	-	-	x	-	x	x	x	x
Zeitdienst											
I_NTP_Time_Information	-	-	-	-	-	x	x	x	-	x	-
Konnektormanagement											
Softwareaktualisierung	x	x	x	x	x	x	x	x	x	x	x
Protokolleinsicht	x	x	x	x	x	x	x	x	x	x	x
Werksreset	x	x	x	x	x	x	x	x	x	x	x
Sonstiges	-	x	x	x	x	x	x	x	x	x	x

⌦ TIP1-A_4732 Kommunikation mit NET_TI_DEZENTRAL

Der Konnektor MUSS sicherstellen, dass die Adressen aus dem Adressbereich NET_TI_DEZENTRAL nur für die Kommunikation mit der TI/den ~~Bestandsnetzen~~ weiteren Anwendungen des Gesundheitswesens in Form der inner IP (VPN_TUNNEL_TI_INNER_IP) des VPN-Tunnel der TI (VPN_TI) verwendet wird.

Der Konnektor MUSS die Kommunikation mit Systemen des Netzwerksegments NET_TI_DEZENTRAL für folgende Fälle unterstützen:

- keine

Der Konnektor MUSS insbesondere die Kommunikation an seinen Außenschnittstellen mit Systemen des Netzwerksegments NET_TI_DEZENTRAL für folgende Fälle blockieren:

- [7] vom Konnektor kommend (zur Verhinderung des Zugriffs auf fremde Konnektoren)
- [8] von „Aktive Komponenten“
- [9] in Richtung Konnektor gehend ⌫

⌦ **TIP1-A_4733 Kommunikation mit ANLW_AKTIVE_BESTANDSNETZE**

Der Konnektor MUSS sicherstellen, dass IP-Pakete mit einer Absenderadresse aus dem Adressbereich ANLW_AKTIVE_BESTANDSNETZE verworfen werden, wenn sie nicht aus dem VPN-Tunnel der TI (VPN_TI) stammen.

Der Konnektor MUSS die Kommunikation mit Systemen des Netzwerksegments ANLW_AKTIVE_BESTANDSNETZE für folgende Fälle unterstützen:

- [10] wenn (MGM_LU_ONLINE=Enabled vom Konnektor kommend nur für die DNS-Namensauflösung mittels DNS_SERVERS_BESTANDSNETZE
- [11b] wenn (MGM_LU_ONLINE=Enabled und MGM_LOGICAL_SEPARATION=Disabled) von „Aktive Komponenten“ kommend

Der Konnektor MUSS insbesondere die Kommunikation an seinen Außenschnittstellen mit Systemen des Netzwerksegments ANLW_AKTIVE_BESTANDSNETZE für folgende Fälle blockieren:

- [11a] für nicht freigegebene ~~Bestandsnetze~~angeschlossene Netze des Gesundheitswesens mit aAdG-NetG (ANLW_BESTANDSNETZE abzüglich ANLW_AKTIVE_BESTANDSNETZE) von „Aktive Komponenten“ kommend;
- [12] in Richtung Konnektor gehend (und den dahinterliegenden „Aktive Komponenten“)

Der Konnektor MUSS sicherstellen, dass die aus einer unterstützten Kommunikation mit Systemen aus dem Netzwerksegment ANLW_AKTIVE_BESTANDSNETZE bestimmten IP-Pakete ausschließlich in den VPN-Tunnel der TI (VPN_TI) geleitet werden. ⌫

⌦ **TIP1-A_4745 Eingeschränkte Nutzung von „Ping“**

Die Firewall des Konnektor MUSS TCP-Port-7(Echo)-Pakete verwerfen.

Die Firewall des Konnektor MUSS ICMP-Echo-Request (Typ 8) und ICMP-Echo-Response (Typ 0) ausschließlich für die folgenden Kommunikationen zulassen:

- vom Konnektor zu den VPN-Konzentratoren für SIS und TI über das Transportnetz (via IAG)
- vom Konnektor zu dem CRL-Webservern (im Transportnetz) über das Internet (via SIS) und das Transportnetz (via IAG)
- vom Konnektor zu dem IAG der Einsatzumgebung
- vom Konnektor zu NET_TI_ZENTRAL
- vom Konnektor zu NET_TI_GESICHERTE_FD
- vom Konnektor zu NET_TI_OFFENE_FD
- vom Konnektor zum lokalen Netzwerk (Adressen aus ANLW_LAN_NETWORK_SEGMENT oder Adressen aus einem der Netzwerksegmente in ANLW_LEKTR_INTRANET_ROUTES)
- vom lokalen Netzwerk (Adressen aus ANLW_LAN_NETWORK_SEGMENT (jedoch ohne die ANLW_LAN_IP_ADDRESS) oder Adressen aus einem der Netzwerksegmente in ANLW_LEKTR_INTRANET_ROUTES) zum Konnektor
- vom lokalen Netzwerk in ANLW_AKTIVE_BESTANDSNETZE (die freigegebenen ~~Bestandsnetze~~angeschlossenen Netze des Gesundheitswesens mit aAdG-NetG)
- vom lokalen Netzwerk in das Internet (via SIS)

Die Firewall des Konnektors MUSS für alle anderen Kommunikationen ein ICMP-Echo-Request (Typ 8) verwerfen. ⌫

⌦ **TIP1-A_4761 Konfiguration Anbindung LAN/WAN**

Die Managementschnittstelle MUSS es einem Administrator ermöglichen Konfigurationsänderungen gemäß Tabelle 302: TAB_KON_624 – „Konfigurationsparameter der Anbindung LAN/WAN vorzunehmen.

Wenn (ANLW_INTRANET_ROUTES_MODUS = REDIRECT) gesetzt ist, MUSS der Konnektor jedes Paket aus einem konfigurierten Intranet mit einem ICMP-Redirect mit dem hinterlegten Next Hop beantworten und der Konnektor MUSS gewährleisten, dass keine IP-Pakete in eines oder mehrere der konfigurierten Intranet geroutet werden.

Wenn (ANLW_INTRANET_ROUTES_MODUS = BLOCK) gesetzt ist, MUSS der Konnektor alle IP-Pakete für ein Intranet (gemäß ANLW_LEKTR_INTRANET_ROUTES) ablehnen.

Tabelle 302: TAB_KON_624 – „Konfigurationsparameter der Anbindung LAN/WAN“

ReferenzID	Belegung	Bedeutung und Administrator-Interaktion
ANLW_ANBINDUNGS_MODUS	InReihe	Der Konnektor ist in Reihe zu dem IAG der Einsatzumgebung geschaltet. Wenn ANLW_WAN_ADAPTER_MODUS= ENABLED befindet sich der Konnektor in diesem Anbindungsmodus.

ReferenzID	Belegung	Bedeutung und Administrator-Interaktion
		Der Administrator MUSS diesen Wert einsehen und DARF ihn NICHT ändern können.
	Parallel	Der Konnektor ist parallel (zu allen bestehenden Systemen) ins Netzwerk der Einsatzumgebung angebunden. Wenn ANLW_WAN_ADAPTER_MODUS= DISABLED befindet sich der Konnektor in diesem Anbindungsmodus. Der Administrator MUSS diesen Wert einsehen und DARF ihn NICHT ändern können.
ANLW_INTERNET_MODUS	SIS	Der (am Konnektor LAN-seitig ankommende) Internet-Traffic wird per VPN an den SIS geschickt.
	IAG	Bei Anfragen ins Internet wird der Aufrufer per ICMP-Redirect (Type 5) auf die Route zum IAG verwiesen. Wenn (ANLW_ANBINDUNGS_MODUS = InReihe) DARF dieser Wert NICHT auswählbar sein - statt dessen MUSS dann der Wert SIS verwendet werden.
	KEINER	Es wird kein Traffic ins Internet geroutet
ANLW_INTRANET_ROUTES_MODUS	REDIRECT	Der Konnektor MUSS sicherstellen, dass dieser Wert nur gesetzt werden kann, wenn der Administrator zuvor ein oder mehrere Intranet (ANLW_LEKTR_INTRANET_ROUTES) definiert hat.
	BLOCK	Der Konnektor MUSS alle IP-Pakete für ein Intranet (gemäß ANLW_LEKTR_INTRANET_ROUTES) ablehnen.
ANLW_WAN_ADAPTER_MODUS	ENABLED	Dieser Parameter ändert den Interface-Status des WAN-Adapters. Der Administrator MUSS diesen Wert einsehen können. Der Administrator MUSS diesen Wert ändern können.
	DISABLED	Dieser Parameter ändert den Interface-Status des WAN-Adapters. Der Administrator MUSS diesen Wert ein-

ReferenzID	Belegung	Bedeutung und Administrator-Interaktion
		sehen können. Der Administrator MUSS diesen Wert ändern können.
ANLW_LEKTR_INTRANET_ROUTES	Tupel aus Netzwerksegment und dazugehörigem Next-Hop	Der Administrator MUSS in diese Liste Einträge hinzufügen, editieren und löschen können. Liste von Routen zur Erreichung der Clientsysteme und Kartenterminals vom Konnektor; jeweils mit IP-Netzwerk dazugehörigem Next Hop. Die Netzwerksegmente DÜRFEN NICHT mit den Netzbereichen - NET_SIS - NET_TI_DEZENTRAL NET_TI_ZENTRAL - NET_TI_OFFENE_FD - NET_TI_GESICHERTE_FD - ANLW_BESTANDSNETZE kollidieren.
ANLW_SERVICE_TIMEOUT	X Sekunden	Der Administrator MUSS die maximale Zeit konfigurieren können, in der ein Service antworten muss, bevor das System einen Timout-Fehler meldet. Default-Wert: 60 Sekunden
ANLW_IAG_ADDRESS	IP Adresse	ANLW_IAG_ADDRESS ist die Adresse des Default Gateways. Diese IP-Adresse MUSS innerhalb des ANLW_WAN_NETWORK_SEGMENT liegen. Die Adresse wird entweder über DHCP automatisch (DHCP_CLIENT_WAN_STATE=ENABLED oder DHCP_CLIENT_LAN_STATE=ENABLED) oder anderenfalls manuell durch den Administrator konfiguriert. Bei automatischer Konfiguration per DHCP MUSS der Administrator den Wert von ANLW_IAG_ADDRESS ausschließlich einsehen können.
ANLW_AKTIVE_BESTANDSNETZE	Liste von IP-Address-	Der Administrator MUSS manuell aus der empfangenen Liste der zur Verfügung

ReferenzID	Belegung	Bedeutung und Administrator-Interaktion
	Segmenten	stehenden ~~Bestandsnetzen~~angeschlossenen Netze des Gesundheitswesens mit aAdG-NetG (gemäß TUC_KON_283 „Infrastruktur Konfiguration aktualisieren“) einzelne deaktivieren, bzw. nach vorheriger Deaktivierung, freischalten können. Nur die freigegeben ~~Bestandsn~~Netze werden in dieser Variablen erfasst~~. Nur die freigegebenen Bestandsnetze~~ und sind aus den Netzwerken der Einsatzumgebung erreichbar. Wird eine Änderung an der Liste der freigegebenen ~~Bestandsnetze~~Netze vorgenommen, so MUSS der Konnektor für jedes dieser freigegebenen ~~Bestandsnetze~~Netze in DNS_SERVERS_BESTANDSNETZE ein DNS-Referer-Eintrag für jede der dazugehörigen Domains mit allen zugehörigen DNS-Servern im Konnektor hinterlegen. Die Werte hierzu werden der via TUC_KON_283 aktualisierten Bestandsnetze.xml entnommen. Für hier „nicht freigegebene“ oder zwischenzeitlich gelöschte ~~Bestandsnetze~~Netze DARF der Konnektor NICHT Referer-Einträge in DNS_SERVERS_BESTANDSNETZE enthalten. Die Einträge in DHCP_AKTIVE_BESTANDSNETZE_ROUTES sind entsprechend zu aktualisieren. Der Konnektor MUSS nach jeder Änderung dieser Variablen durch den Administrator den TUC_KON_304 „Netzwerk-Routen einrichten“ aufrufen.
ANLW_IA_BESTANDSNETZE	AN	Der Konnektor MUSS alle über TUC_KON_283 übermittelten ~~Bestandsnetze~~angeschlossenen Netze des Gesundheitswesens mit aAdG-NetG aktivieren. Eine spätere manuelle Deaktivierung über das Management-Interface durch den Administrator ist möglich. Dieses Verhalten ist als Standartverhalten zu konfigurieren.
	AUS	Der Konnektor MUSS alle über TUC_KON_283 übermittelten ~~Bestandsnetze~~angeschlossenen Netze des Gesundheitswesens mit aAdG-NetG anbieten, diese aber nicht aktivieren. Eine spätere

ReferenzID	Belegung	Bedeutung und Administrator-Interaktion
		manuelle Aktivierung erfolgt über das Mangement-Interface durch den Administrator.

⌫

⌦ **TIP1-A_4767 Konfiguration des DHCP-Servers**

Der Konnektor MUSS die Möglichkeit bieten die in Tabelle 306 und Tabelle 307 beschriebenen Parameter des DHCP-Servers über die Managementschnittstelle zu konfigurieren.

Tabelle 306: TAB_KON_628 „Basiskonfiguration des DHCP-Servers“

Referenz ID	Belegung	Bedeutung
DHCP_SERVER_NETWORK	IP-Adresse	IP-Netzwerk der Einsatzumgebung.
DHCP_SERVER_BROADCAST	IP-Adresse	Die Broadcast-Adresse des Konnektors am LAN-Interface
DHCP_SERVER_DYNAMIC_RANGE	von – bis IP-Adresse	Adressbereich für Adressen die dynamisch vergeben werden dürfen.
DHCP_SERVER_CLIENTGROUPS	Name der Clientgruppe; Liste an MAC-Adressen	Der Konnektor MUSS dem Administrator über die Managementschnittstelle die Möglichkeit bieten mindestens zwei Client-Gruppen zu verwalten.
DHCP_SERVER_DEFAULT_CLIENTGROUP	Client-Gruppe	Standardmäßig eingestellte Client-Gruppe. Wird verwendet falls DHCP-Anfrage keiner anderen Client-Gruppe zugeordnet werden kann.

Tabelle 307: TAB_KON_629 „Client-Gruppenspezifische Konfigurationsoptionen des Konnektor-DHCP-Servers“

ReferenzID	Belegung	Bedeutung
Die gesamte Parameterliste ist für jede Client-Gruppe getrennt konfigurierbar		
DHCP_OWNDNS_ENABLED	Enabled/Disabled	Der Administrator MUSS konfigurieren können, ob der konnektoreigene DNS-Server als Parameter übergeben wird. Default-Wert: Disabled
DHCP_DNS_ADDR	IP-Adressen der DNS-Server	Falls der konnektoreigene DNS-Server nicht übergeben werden soll, müssen die Adressen externer aus dem Netz der Einsatzumgebung erreichbaren DNS-Server als Parameter übergeben werden. Der Administrator MUSS diese Adressen konfigurieren können.
DHCP_NTP	Enabled/Disabled	Der Administrator MUSS konfigurieren

ReferenzID	Belegung	Bedeutung
		können, ob der Konnektor die Adresse des Konnektor internen NTP-Servers per DHCP an die Clients sendet. Default-Wert: Enabled
DHCP_OWNDGW_ENABLED	Enabled/Disabled	Der Administrator MUSS konfigurieren können, ob der Konnektor beim Client als Default-Gateway gesetzt werden soll. Default-Wert: Disabled
DHCP_DGW_ADDR	IP-Adresse des DGW	Falls der Konnektor nicht als Default Gateway gesetzt werden soll, muss die Adresse des zu verwendenden DGW als Parameter übergeben werden. Der Administrator MUSS die Adresse des DGW konfigurieren können.
DHCP_IP_NETMASK	Netzmaske	Der Administrator MUSS die Netmask des Clients konfigurieren können.
DHCP_DOMAINNAME	Domainname	Der Administrator MUSS den Domainnamen des Clients konfigurieren können.
DHCP_HOSTNAME	Liste von Tupel aus Hostname und Mac-Adresse	Der Administrator MUSS eine Liste von Hostname der Clients konfigurieren können (Einträge einfügen, ändern, löschen).
DHCP_STATIC_LEASE	Liste von Tupel aus IP- und Mac-Adresse	Der Administrator MUSS für jede MAC-Adresse Static Lease konfigurieren können.
DHCP_LEASE_TTL	X Minuten	Der Administrator MUSS Lease-Dauer der dynamischen Adressen konfigurieren können.
DHCP_AKTIVE_BESTANDSNETZE_ROUTES	Liste von Tupel: `Netzwerksegment je INTRANET und Adresse für Next Hop je` freigegebenem ~~Bestandsnetz~~angeschlossenen Netz des Gesundheitswesens mit aAdG-NetG	Der Administrator MUSS je freigegebenem ~~Bestandsnetz~~angeschlossenen Netz des Gesundheitswesens mit aAdG-NetG (aus ANLW_AKTIVE_BESTANDSNETZE) den an den Client zu übermittelnden Routen-Eintrag aktivieren oder deaktivieren können.
DHCP_INTRANET_ROUTES	Liste von Tupel: Netzwerksegment je INTRANET und Adresse für Next Hop in die definierten Intranets	Der Administrator MUSS je Intranet-Tupel (aus ANLW_LEKTR_INTRANET_ROUTES) den an den Client zu übermittelnden Routen-Eintrag aktivieren oder deaktivieren können.
DHCP_ROUTES	Tupel Netzwerksegment	Der Administrator MUSS Routen zur Verteilung an die Clients frei konfigurieren

ReferenzID	Belegung	Bedeutung
	und Adresse für Next Hop	können. Der Konnektor MUSS sicherstellen, diese Listeneinträge keine Überschneidungen mit folgenden Netzsegmenten haben: - dem Netzwerksegment ANLW_LAN_NETWORK_SEGMENT - dem Netzwerksegment ANLW_WAN_NETWORK_SEGMENT - jedes Netzsegmente in ANLW_BESTANDSNETZE ANLW_AKTIVE_BESTANDSNETZE ANLW_LEKTR_INTRANET_ROUTES Die Routen SOLLEN über DHCP Option 121 (Windows Vista oder höher) bzw. DHCP Option 249 (Windows XP und darunter) verteilt werden.
DHCP_OPTIONS	Liste an weiteren DHCP-Optionen.	Vom Administrator konfigurierbare Liste an weiteren DHCP-Options gemäß [RFC2132]

⌫

⌦ TIP1-A_4797 DNS-Forwards des DNS-Servers

Der DNS-Server des Konnektors MUSS die folgenden DNS-Forwards durchführen:

Tabelle 326: TAB_KON_687 DNS-Forwards des DNS-Servers

Domain	Forwarders	Bemerkungen
Namensraum TI (*.DNS_TOP_LEVEL_D) OMAIN_TI	DNS_SERVERS_TI	DNS Forward Rule zur Auflösung aller DNS-Namen innerhalb des Namensraums der TI.
Namensraum ~~Bestandsnetzea~~angeschlossene Netze des Gesundheitswesens mit aAdG-NetG (Domainnamen von ~~Bestandsnetzena~~angeschlossenen Netzen des Gesundheitswesens mit aAdG-NetG gemäß Bestandsnetze.xml)	DNS_SERVERS_BESTANDSNETZE (Je Domainnamen eines ~~Bestandsnetzes~~angeschlossenen Netzes des Gesundheitswesens mit aAdG-NetG alle zugehörigen DNS-Server IP-Adressen gemäß Bestandsnetze.xml)	Je ~~Bestandsnetz~~angeschlossenem Netz des Gesundheitswesens mit aAdG-NetG in ANLW_AKTIVE_BESTANDSNETZE wird eine DNS Forward Rule zur Auflösung von DNS-Namen innerhalb dieses ~~des Bestandsnetzes~~Netzes verwendet.
Namensraum lokale Einsatzumgebung (DNS_DOMAIN_LEKTR)	DNS_SERVERS_LEKTR	DNS Forward Rule zur Auflösung aller DNS-Namen innerhalb der DNS-Domain DNS_DOMAIN_LEKTR

Domain	Forwarders	Bemerkungen
Namensraum Internet	DNS_SERVERS_SIS	Wenn der VPN-Tunnel SIS aktiv ist, muss eine Forward Rule für den Namensraum Internet über die DNS_SERVERS_SIS existieren.
Namensraum Internet	DNS_SERVERS_INT	Wenn der VPN-Tunnel SIS nicht aktiv ist, muss eine Forward Rule für den Namensraum Internet über die DNS_SERVERS_INT existieren
Lokale Zone „konlan.“	autoritativer Nameserver des Konnektors	DNS Forward Rule zur Auflösung aller DNS-Namen innerhalb der Zone „konlan.“

⌫

⌦ TIP1-A_4805 Konfigurationsparameter Namensdienst und Dienstlokalisierung

Der Administrator MUSS die in TAB_KON_654 aufgelisteten Parameter über die Managementschnittstelle konfigurieren und die in TAB_KON_731 aufgelisteten Parameter ausschließlich einsehen können.

Nach jeder Änderung MUSS sichergestellt werden, dass die Änderungen sofort am autoritativen bzw. am Caching-Nameserver zur Verfügung stehen.

Tabelle 335: TAB_KON_654 - Konfigurationsparameter Namensdienst

ReferenzID	Belegung	Bedeutung und Administrator-Interaktion
DNS_SERVERS_INT	Liste von IP-Adressen der DNS-Server	Liste von DNS-Servern für das Transportnetz. Die IP-Adressen KÖNNEN auf einen öffentlich zugänglichen Adressbereich eingeschränkt sein.
DNS_DOMAIN_VPN_ZUGD_INT	DNS Domainname	DNS-Domainname für die Service Discovery der VPN-Konzentratoren des VPN-Zugangsdienstes
DNS_SERVERS_LEKTR	Liste von IP-Adressen der DNS-Server	Liste von DNS-Servern, die zur Namensauflösung von Namensräumen in der Einsatzumgebung verwendet werden. Der Administrator MUSS die Liste von DNS-Servern, die die DNS_DOMAIN_LEKTR auflösen, bearbeiten können. Die IP-Adressen der DNS-Server KÖNNEN auf den Adressbereich der ANLW_LAN_IP_ADDRESS eingeschränkt sein.
DNS_DOMAIN_LEKTR	DNS Domainname	DNS Domainname, der von einem DNS-Server der Einsatzumgebung aufgelöst wird. Der Name DARF NICHT mit einem „.“ beginnen und nicht mit einem „.“ enden.

ReferenzID	Belegung	Bedeutung und Administrator-Interaktion
DNS_KONLAN_RR	Liste von DNS Resource Records der Zone „konlan“	Der Administrator muss die einzelnen Resource Records (RR) der Domain „konlan.” bearbeiten können (erzeugen, lesen, ändern, löschen). Davon ausgenommen sind die „konlan.“ SOA und NS RR, der „konnektor.konlan.“ A RR sowie der zum NS RR zugehörige A RR.
DNS_TA_CONFIG	Ist abhängig von der gewählten Umsetzung	Der Administrator MUSS die aktuellen DNSSEC Trustanchor für den Namensraum Internet auf geeignetem Weg in den Konnektor übernehmen können.

Tabelle 336: TAB_KON_731 Einsehbare Konfigurationsparameter Namensdienst

ReferenzID	Belegung	Bedeutung
DNS_SERVERS_TI	Liste von IP-Adressen der DNS-Server	Liste von DNS-Servern, die zur Namensauflösung des Namensraums der TI verwendet werden
DNS_SERVERS_SIS	Liste von IP-Adressen der DNS-Server	Liste von DNS-Servern, die zur Namensauflösung des Namensraums Internet bei Nutzung des SIS verwendet werden
DNS_SERVERS_BESTANDSNETZE	Liste von IP-Adressen der DNS-Servern je Domäne je freigegebenem ~~Bestandsnetz~~angeschlossenen Netz des Gesundheitswesens mit aAdG-NetG	Liste von DNS-Servern je Domain eines dieser freigegebenen ~~Bestandsnetzes~~Netze.
DNS_TOP_LEVEL_DOMAIN_TI	DNS Domainname	Top Level Domain des Namensraumes TI

⌫

⌦ TIP1-A_5153 TUC_Kon_283 „Infrastruktur Konfiguration aktualisieren“

Der Konnektor MUSS den technischen Use Case TUC_Kon_283 „Infrastruktur Konfiguration aktualisieren“ umsetzen.

Tabelle 354: TAB_KON_799 – TUC_KON_283 „Infrastruktur Konfiguration aktualisieren“

Element	Beschreibung
Name	TUC_KON_283 Infrastruktur Konfiguration aktualisieren
Beschreibung	Dieser TUC liest die Infrastrukturdaten vom KSR ein.
Auslöser	Automatisch einmal täglich; BOOTUP, Administrator

Element	Beschreibung
Vorbedingungen	Der TUC_KON_304 „Netzwerk-Routen einrichten“ MUSS fehlerfrei durchgelaufen sein. Der TUC_KON_321 „Verbindung zu dem VPN-Konzentrator der TI aufbauen“ MUSS fehlerfrei durchgelaufen sein.
Eingangsdaten	Keine
Komponenten	Konnektor, Konfigurationsdienst
Ausgangsdaten	Keine

Standardablauf	Der Konnektor MUSS folgende Schritte durchlaufen:
	1. „Einlesen des Konfigurations-XML“:
	a. Der Konnektor MUSS eine TLS-Verbindung zum Konfigurationsdienst anhand des in MGM_KSR_KONFIG_URL angegebenen Parameters aufbauen. Dabei MUSS er das durch den Server präsentierte Zertifikat mittels TUC_KON_037 „Zertifikat prüfen“ {
	certificate = C.ZD.TSL-S;
	qualifiedCheck = not_required;
	offlineAllowNoCheck = true;
	policyList = oid_zd_tls_s;
	intendedKeyUsage =
	digitalSignature&keyEncipherment;
	intendedExtendedKeyUsage = id-kp-serverAuth;
	validationMode = OCSP}
	auf Gültigkeit prüfen.
	Das Server-Zertifikat C.ZD.TLS-S MUSS für den Konfigurationsdienst ausgestellt sein.
	b. Herunterladen der Konfigurationsdaten mittels I_KSRS_Download::get_Ext_Net_Config (MGM_KSR_KONFIG_URL, „Bestandsnetze.xml“)
	2. Beenden der TLS-Verbindung
	„Prüfen der Versionskennung auf Änderungen“:
	Wenn das Element /Infrastructure/Version der heruntergeladenen Datei keine höhere Versionsnummer als die aktuell im Konnektor hinterlegte Version trägt, muss der TUC ohne Fehler beendet werden.
	3. Aktualisieren der Gesamtnetzliste
	Alle in der Datei enthaltenen Netzsegmente sind nach ANLW_BESTANDSNETZE zu übernehmen. In Abhängigkeit von ANLW_IA_BESTANDSNETZE sind neue ~~Bestandsnetze~~angeschlossene Netze des Gesundheitswesens mit aAdG-NetG nach ANLW_AKTIVE_BESTANDSNETZE zu übernehmen. War der Aktivierungsstatus eines ~~Bestandsnetzes~~dieser Netze bereits durch den Administrator manuell konfiguriert, so muss dieser Status erhalten bleiben.
	4. „Aktualisieren von Konfigurationsinformationen“
	Haben sich Konfigurationsdaten zu einem in ANLW_AKTIVE_BESTANDSNETZE gelisteten Netz verändert, so
	a. sind die Änderungen entsprechend zu übernehmen und zu aktivieren (Anpassung ANLW_AKTIVE_BESTANDSNETZE, DHCP_AKTIVE_BESTANDSNETZE_ROUTES,

Element	Beschreibung
	DNS_SERVERS_BESTANDSNETZE). b. ist anschließend TUC_KON_304 „Netzwerk-Routen einrichten“aufzurufen 5. „Entfernen von nicht mehr gültigen ~~Bestandsnetzen~~angeschlossenen Netzen des Gesundheitswesens mit aAdG-NetG“ Ist ein Netz in der neuen Datei gegenüber der alten Datei nicht mehr vorhanden, so: a. a) sind alle diesbezüglichen Daten zu entfernen und die Änderungen direkt aktiv zu schalten (Anpassung ANLW_AKTIVE_BESTANDSNETZE, DHCP_AKTIVE_BESTANDSNETZE_ROUTES, DNS_SERVERS_BESTANDSNETZE). b. b) ist anschließend TUC_KON_304 „Netzwerk-Routen einrichten“aufzurufen.
Varianten/Alternativen	Keine
Fehlerfälle	(→ 1-5) Es ist ein unerwarteter Fehler aufgetreten; Fehlercode: 4198
Nichtfunktionale Anforderungen	Keine
Zugehörige Diagramme	Keine

Tabelle 355: Tab_Kon_726 Fehlercodes TUC_KON_283 „Infrastruktur Konfiguration aktualisieren“

Fehlercode	ErrorType	Severity	Fehlertext
Neben den Fehlercodes der aufgerufenen technischen Use Cases können folgende weitere Fehlercodes auftreten:			
4198	Technical	Error	Beim Übernehmen der ~~Bestandsnetze~~angeschlossenen Netze des Gesundheitswesens mit aAdG-NetG ist ein Fehler aufgetreten.

⌫

Änderungen in Datenschutz- und Sicherheitsdokumenten

Der Transfer der Datenschutz- und Sicherheitsanforderungen erfolgt in das neue Dokument "Spezifikation Datenschutz- und Sicherheitsanforderungen der TI an Anbieter“ unter Berücksichtigung des Anforderungsmodularisierungskonzepts für Datenschutz- und Sicherheitsanforderungen, das in einem separaten Verfahren freigegeben wird. Innerhalb des Modularisierungskonzepts wurden zwei spezielle Module für weitere Anwendungen vorgesehen. Das Dokument "Spezifikation Datenschutz- und Sicherheitsanforderungen der TI an Anbieter“ wird zeitgleich mit dieser Änderung veröffentlicht.

Änderungen in der Verfahrensbeschreibung Bestätigung weiterer elektronischer Anwendungen des Gesundheitswesens sowie für die Gesundheitsforschung

In der noch nicht veröffentlichten Verfahrensbeschreibung werden die Inhalte der Anforderungen WA-A_2001 und WA-A_2002 wie folgt aufgenommen:

4.3 Zulieferungen des Antragstellers

Alle Dokumente, die der Antragsteller im Bestätigungsverfahren liefern muss, sind in deutscher Sprache zu übermitteln und können als PDF-Datei geliefert werden.

Der Antragsteller muss für die Kommunikation, die im Zusammenhang mit dem Bestätigungsverfahren erforderlich ist, deutschsprachige Ansprechpartner zur Verfügung stellen.

Änderung je Anforderung aus gemLF_Int_WA

In der folgenden Tabelle wird für jede Anforderung aus dem Leitfaden Integration weiterer Anwendungen ihr Verbleib in R2.1.2 angegeben.

Folgende spezielle Situationen ergeben sich dabei:

1) Die Anforderung wird in die neue "Spezifikation Datenschutz- und Sicherheitsanforderungen der TI an Anbieter“ aufgenommen.
2) Die Anforderung ist aufgrund der Überarbeitung der Anforderungslage im Rahmen der neuen "Spezifikation Datenschutz- und Sicherheitsanforderungen der TI an Anbieter“ weggefallen.
3) Inhalt der Anforderung wird in die Verfahrensbeschreibung zur Bestätigung weiterer Anwendungen überführt.

Afo-ID in gemLF_Int_WA	Afo-ID in R2.1.2	Quelle	Bemerkung
WA-A_2001	n.a.	gemZul_Best_Anwendungen	(3)
WA-A_2002	n.a.	gemZul_Best_Anwendungen	(3)
WA-A_2003	GS-A_4831	gemSpec_Net	
WA-A_2004	GS-A_2076-01	gemSpec_DS_Anbieter	(1)
WA-A_2005	GS-A_5564	gemSpec_DS_Anbieter	(1)
WA-A_2006	GS-A_4479-01	gemSpec_DS_Anbieter	(1)
WA-A_2007	GS-A_4473-01	gemSpec_DS_Anbieter	(1)
WA-A_2008	n.a.	n.a.	(2)
WA-A_2009	n.a.	n.a.	(2)
WA-A_2010	GS-A_5551	gemSpec_DS_Anbieter	(1)

Afo-ID in gemLF_Int_WA	Afo-ID in R2.1.2	Quelle	Bemerkung
WA-A_2011	GS-A_5552	gemSpec_DS_Anbieter	(1)
WA-A_2012	GS-A_5578+ GS-A_5574	gemSpec_DS_Anbieter	(1)
WA-A_2013	GS-A_5553	gemSpec_DS_Anbieter	(1)
WA-A_2014	GS-A_5554	gemSpec_DS_Anbieter	(1)
WA-A_2015	GS-A_4523-01	gemSpec_DS_Anbieter	(1)
WA-A_2016	GS-A_4524-01	gemSpec_DS_Anbieter	(1)
WA-A_2017	GS-A_5555	gemSpec_DS_Anbieter	(1)
WA-A_2018	n.a.	n.a.	(2)
WA-A_2019	GS-A_3886	gemRL_Betr	
WA-A_2020	GS-A_4009	gemSpec_Net	
WA-A_2021	GS-A_4024	gemSpec_Net	
WA-A_2022	GS-A_4027	gemSpec_Net	
WA-A_2023	GS-A_4759	gemSpec_Net	
WA-A_2024	GS-A_4805	gemSpec_Net	
WA-A_2025	GS-A_4013	gemSpec_Net	
WA-A_2026	GS-A_4018	gemSpec_Net	
WA-A_2027	GS-A_3934	gemSpec_Net	
WA-A_2028	GS-A_3937	gemSpec_Net	
WA-A_2029	GS-A_3932	gemSpec_Net	
WA-A_2030	TIP1-A_5120	gemSpec_TSL	
WA-A_2031	GS-A_4957	gemSpec_PKI	
WA-A_2032	GS-A_4957	gemSpec_PKI	
WA-A_2033	WA-A_2033	gemSpec_PKI	
WA-A_2034	TIP1-A_5566	gemSpec_VZD	
WA-A_2035	TIP1-A_5568	gemSpec_VZD	
WA-A_2036	n.a.	n.a.	(2)
WA-A_2037	n.a.	n.a.	(2)
WA-A_2038	n.a.	n.a.	(2)
WA-A_2039	n.a.	n.a.	(2)
WA-A_2040	n.a.	n.a.	(2)
WA-A_2041	GS-A_5566	gemSpec_DS_Anbieter	(1)

Afo-ID in gemLF_Int_WA	Afo-ID in R2.1.2	Quelle	Bemerkung
WA-A_2042	n.a.	n.a.	(2)
WA-A_2043	n.a.	n.a.	(2)
WA-A_2044	n.a.	n.a.	(2)
WA-A_2045	n.a.	n.a.	(2)
WA-A_2046	n.a.	n.a.	(2)
WA-A_2047	n.a.	n.a.	(2)
WA-A_2048	n.a.	n.a.	(2)
WA-A_2049	n.a.	n.a.	(2)
WA-A_2050	n.a.	n.a.	(2)
WA-A_2051	n.a.	n.a.	(2)
WA-A_2052	GS-A_4468-01	gemSpec_DS_Anbieter	(1)
WA-A_2053	n.a.	n.a.	(2)
WA-A_2054	n.a.	n.a.	(2)
WA-A_2055	n.a.	n.a.	(2)
WA-A_2056	n.a.	n.a.	(2)
WA-A_2057	GS-A_4478-01	gemSpec_DS_Anbieter	(1)
WA-A_2058	n.a.	n.a.	(2)
WA-A_2059	n.a.	n.a.	(2)
WA-A_2060	n.a.	n.a.	(2)
WA-A_2061	n.a.	n.a.	(2)
WA-A_2062	GS-A_2214-01	gemSpec_DS_Anbieter	(1)
WA-A_2063	GS-A_4980-01	gemSpec_DS_Anbieter	(1)
WA-A_2064	GS-A_4981-01	gemSpec_DS_Anbieter	(1)
WA-A_2065	GS-A_4982-01	gemSpec_DS_Anbieter	(1)
WA-A_2066	GS-A_4983-01	gemSpec_DS_Anbieter	(1)
WA-A_2067	GS-A_4984-01	gemSpec_DS_Anbieter	(1)
WA-A_2068	n.a.	n.a.	(2)
WA-A_2069	n.a.	n.a.	(2)
WA-A_2070	n.a.	n.a.	(2)
WA-A_2071	n.a.	n.a.	(2)
WA-A_2072	n.a.	n.a.	(2)

Afo-ID in gemLF_Int_WA	Afo-ID in R2.1.2	Quelle	Bemerkung
WA-A_2073	GS-A_4508-01	gemSpec_DS_Anbieter	(1)
WA-A_2074	n.a.	n.a.	(2)
WA-A_2075	n.a.	n.a.	(2)
WA-A_2076	n.a.	n.a.	(2)
WA-A_2077	n.a.	n.a.	(2)
WA-A_2078	n.a.	n.a.	(2)
WA-A_2079	n.a.	n.a.	(2)
WA-A_2080	n.a.	n.a.	(2)
WA-A_2081	n.a.	n.a.	(2)
WA-A_2082	n.a.	n.a.	(2)
WA-A_2083	n.a.	n.a.	(2)
WA-A_2084	n.a.	n.a.	(2)
WA-A_2085	n.a.	n.a.	(2)
WA-A_2086	n.a.	n.a.	(2)
WA-A_2087	GS-A_5575	gemSpec_DS_Anbieter	(1)
WA-A_2088	GS-A_4526-01	gemSpec_DS_Anbieter	(1)
WA-A_2089	n.a.	n.a.	(2)
WA-A_2090	n.a.	n.a.	(2)
WA-A_2091	GS-A_4530-01	gemSpec_DS_Anbieter	(1)
WA-A_2092	n.a.	n.a.	(2)
WA-A_2093	GS-A_4532-01	gemSpec_DS_Anbieter	(1)
WA-A_2094	n.a.	n.a.	(2)
WA-A_2095	n.a.	n.a.	(2)
WA-A_2096	n.a.	n.a.	(2)
WA-A_2097	n.a.	n.a.	(2)
WA-A_2098	n.a.	n.a.	(2)
WA-A_2099	n.a.	n.a.	(2)
WA-A_2100	n.a.	n.a.	(2)
WA-A_2101	GS-A_5324-01+ GS-A_5324-02	gemSpec_DS_Anbieter	(1)
WA-A_2102	GS-A_5017-01	gemSpec_DS_Anbieter	(1)
WA-A_2103	n.a.	n.a.	(2)

Afo-ID in gemLF_Int_WA	Afo-ID in R2.1.2	Quelle	Bemerkung
WA-A_2104	n.a.	n.a.	(2)
WA-A_2105	GS-A_2355-01	gemSpec_DS_Anbieter	(1)
WA-A_2106	n.a.	n.a.	(2)
WA-A_2107	n.a.	n.a.	(2)
WA-A_2108	n.a.	n.a.	(2)
WA-A_2109	n.a.	n.a.	(2)
WA-A_2110	n.a.	n.a.	(2)
WA-A_2111	WA-A_2111	gemSpec_PKI	
WA-A_2112	WA-A_2112	gemSpec_PKI	
WA-A_2113	WA-A_2113	gemRL_TSL_SP_CP	
WA-A_2114	GS-A_5567	gemSpec_DS_Anbieter	(1)
WA-A_2115	GS-A_5568	gemSpec_DS_Anbieter	(1)
WA-A_2116	GS-A_5569	gemSpec_DS_Anbieter	(1)
WA-A_2117	GS-A_5570	gemSpec_DS_Anbieter	(1)
WA-A_2118	GS-A_5571	gemSpec_DS_Anbieter	(1)
WA-A_2119	GS-A_5572	gemSpec_DS_Anbieter	(1)
WA-A_2120	GS-A_5573	gemSpec_DS_Anbieter	(1)
WA-A_2121	WA-A_2121	gemKPT_Test	
WA-A_2122	WA-A_2122	gemKPT_Test	
WA-A_2123	WA-A_2123	gemKPT_Test	
WA-A_2124	WA-A_2124	gemKPT_Test	
WA-A_2125	GS-A_4760	gemSpec_Net	
WA-A_2126	GS-A_5583	gemSpec_Net	
WA-A_2127	GS-A_5584	gemSpec_Net	
WA-A_2128	GS-A_5585	gemSpec_Net	
WA-A_2129	GS-A_5586	gemSpec_Net	
WA-A_2130	GS-A_5576	gemSpec_DS_Anbieter	(1)
WA-A_2131	GS-A_5577	gemSpec_DS_Anbieter	(1)
WA-A_2132	GS-A_5565	gemSpec_DS_Anbieter	(1)
WA-A_2133	GS-A_5556	gemSpec_DS_Anbieter	(1)