Elektronische Gesundheitskarte und Telematikinfrastruktur

Errata zu Release 3.0.0 Online-Produktivbetrieb (Stufe 3) Erprobung und Produktivbetrieb

führt zu

Release 3.0.0-1

Version:	1.0.1
Stand:	06.02.2019
Status:	freigegeben
Klassifizierung:	öffentlich
Referenzierung:	[gemErrata_R3.0.0-1]

Betroffene Produkttypen	**Neue Produkttypversion**
gemProdT_Kon PTV3	3.3.1-0

ID	Dokument	Quelle Dokument und/oder Kapitel	Beschreibung der Änderung	**Anpassungen** an Afos; TUCs, Tabellen, Korrekturen	von Änderung betroffene Dokumente
C_6670	gemSpec_Kon	TIP1-A_4797	**Fachlicher Fehler, Konnektor, DNS Forwarder für Domain ti-wa** Es fehlt eine Forwarding Regel für die Domain ti-wa.	TIP1-A_4797 Tabelle TAB_KON_687 DNS-Forwards des DNS-Servers wird um eine neue Zeile ergänzt. Domain: Namensraum TI, Top Level Domain ti-wa. Forwarders: DNS_ SERVERS_ TI Bemerkungen: DNS Forward Rule zur Auflösung aller DNS-Namen innerhalb des Namensraums der TI mit der Top Level Domain ti-wa (für die PU) und ti-wa-test (für die RU und TU). Zeile Domain = "Namensraum TI (*.DNS_TOP_ LEVEL_DOMAIN_TI)" wird geändert. Bemerkungen alt: DNS Forward Rule zur Auflösung aller DNS-Namen innerhalb des Namensraums der TI. Bemerkungen neu: DNS Forward Rule zur Auflösung aller DNS-Namen innerhalb des Namensraums der TI mit der Top Level Domain telematik (für die PU) und telematik-test (für die RU und TU).	gemSpec_Kon gemProdT_Kon_PTV3
C_6674	gemSpec_Net gemSpec_Kon	GS-A_4029 GS-A_4850 TIP1-A_4981 TIP1-A_5407 TIP1-A_5530 Tabelle 278: TAB_KON_680 Mapping der Netzwerksegmente	**NET_AADG als separater IP-Adresskreis entfernen** Nach der Einführung des Adressbereiches NET_AADG im IP-Adresskonzept der TI (gemSpec_Net) muss dieser Parameter als separates IP-Netzsegment wieder entfernt werden. Ein Konsistenzfehler zum bestehenden PP des Konnektors wird damit korrigiert.	C_6674_Anlage	gemSpec_Net gemSpec_Kon gemProdT_Kon_PTV3
C_6655	gemSpec_Kon	TAB_KON_504	**Erlaubte Operationen im Zustand EC_FIREWALL_NOT_RELIABLE** Die ursprünglichen Festlegungen zum Fehlerzustand EC_Firewall_Not_Reliabel forderten die Verfügbarkeit einiger weniger Operationen u.a. der Administrierbarkeit des Konnektors. Diese Funktionalitäten sind jedoch in den aktuellen Konnektoren nicht vorgesehen, da dies den Vorgaben aus dem Zertifizierungsverfahren für einen solchen Fehlerzustand widerspricht (es ist dann gar keine Operation mehr erlaubt, sondern höchstens die Möglichkeit eines Werksresets). Da der Konnektor diesen Fehlerzustand nur bei schwerwiegenden Fehlern des Konnektors (bspw. Hardwarefehler) erreicht, in denen der Konnektor wahrscheinlich nicht mehr in einen betriebsfähigen Zustand gebracht werden kann, ist es unverhältnissmäßig, Änderungen an den bestehenden Implementierungen zu fordern. Um Konsistenz zu den Sicherheitsvorgaben von BSI und Prüfstelle herzustellen, wird die Spezifikation nun so angepasst, dass an den bereits zertifizierten Umsetzungen keine Änderungen nötig sind. Dies ist aus funktionaler Sicht akzeptabel und steht nicht mehr im Widerspruch mit den Sicherheitsvorgaben.	siehe C_6655_Anlage	gemSpec_Kon gemProdT_Kon_PTV3
C_6656	ws-trust-1.3.xsd		**Korrektur - Schemadatei hat falschen Namensraumbezeichner** In der OASIS-Spezifikation http://docs.oasis-open.org/ws-sx/ws-trust/200512/ws-trust-1.3-os.html wird der Namensraum des Schemas in Abschnitt "1.3 Namespace" explizit zu "http://docs.oasis-open.org/ws-sx/ws-trust/200512" angegeben. In der von OASIS veröffentlichten Schemadatei unter http://docs.oasis-open.org/ws-sx/ws-trust/200512/ws-trust-1.3.xsd wird abweichend der Targetnamespace "http://docs.oasis-open.org/ws-sx/ws-trust/200512/" verwendet. Der Unterschied "/" erscheint zwar beim Lesen unscheinbar, bedeutet aber technisch zwei verschiedene Namensräume. In http://docs.oasis-open.org/ws-sx/ws-trust/v1.3/errata01/os/ws-trust-1.3-errata01-os.html klingt mit "ER019, Wrong target namespace in WSDL for WS-Trust 1.3" die notwendige Fehlerkorrektur an. In der Datei ws-trust-1.3.xsd muss der Fehler behoben werden.	In der Datei ws-trust-1.3.xsd wird der Targetnamespace von "http://docs.oasis-open.org/ws-sx/ws-trust/200512/" auf "http://docs.oasis-open.org/ws-sx/ws-trust/200512" korrigiert.	ws-trust-1.3.xsd gemProdT_Kon_PTV3

Änderungsbedarf:

Anpassung der Spezifikation um Konsistenz zu den Sicherheitsvorgaben zu schaffen.

Änderungen in [gemSpec_Kon] Version 5.4.0

3.3 Betriebszustand

[...]

TIP1-A_4510: Sicherheitskritische Fehlerzustände
Der Konnektor MUSS bei eingetretenem Fehlerzustand aus Tabelle Tab_ Kon_503 Betriebszustand_Fehlerzustandsliste mit Severity=Fatal dafür sorgen, dass von den Operationen der Basisdienste und Technische Use Cases (TUCs) der Basisdienste, die relevant für Fachanwendungen sind, nur erlaubte Operationen und TUCs gestartet und ausgeführt werden.
Welche Operationen und TUCs je eingetretenem Fehlerzustand ausgeführt werden dürfen, legt Tabelle „TAB_KON_504 Ausführungserlaubnis für Dienste in kritischen Fehlerzuständen“ fest: Jede Erlaubnis ist dort durch ein „x“ definiert.
Sind mehrere Fehlerzustände gleichzeitig eingetreten, dürfen nur die Operationen und TUCs ausgeführt werden, die für alle eingetretenen Fehlerzustände erlaubt sind. Der Konnektor muss Anfragen, die auf Grund eines kritischen Fehlerzustandes nicht ausgeführt oder abgebrochen werden, mit einem Fehler (Fehlercode 4002) beantworten.

Tabelle : TAB_KON_502 Fehlercodes „Betriebszustand“

Fehlercode	ErrorType	Severity	Fehlertext
4002	Security	Fatal	Der Konnektor befindet sich in einem kritischen Betriebszustand

<==

[...]

Tabelle : 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_Period	EC_TSL_Trust_Anchor_Out_Of_Date	~~EC_Firewall_Not_Reliable~~ (Spalte gelöscht)	EC_Secure_Key_Store_Not_Available	EC_FW_Not_Valid_Status_Blocked
Technische Use Cases (TUCs) der Basisdienste relevant für Fachanwendung und die Kommunikation mit Weiteren Anwendungen und SIS												
Zugriffsberechtigungsdienst												
TUC_KON_000	PrüfeAufrufkontext	-	x	x	x	x	x	x	x	~~x~~	x	x
Dienstverzeichnisdienst												
TUC_KON_041	Einbringen der Endpunkt informationen	-	-	-	x	x	x	x	x	~~x~~	x	x

Erlaubte Operationen im Zustand EC_FIREWALL_NOT_RELIABLE

		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_Period	EC_TSL_Trust_Anchor_Out_Of_Date	~~EC_Firewall_Not_Reliable~~ (Spalte gelöscht)	EC_Secure_Key_Store_Not_Available	EC_FW_Not_Valid_Status_Blocked
während der Bootup-Phase												
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	System ereignis 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												

Erlaubte Operationen im Zustand EC_FIREWALL_NOT_RELIABLE

	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_Period	EC_TSL_Trust_Anchor_Out_Of_Date	~~EC_Firewall_Not_Reliable~~ (Spalte gelöscht)	EC_Secure_Key_Store_Not_Available	EC_FW_Not_Valid_Status_Blocked
TUC_KON_110 Kartenbasierte TLS-Verbindung aufbauen	-	-	-	-	-	-	-	-	-	-	-
Verbindung zum VPN-Konzentrator											
TUC_VPN-ZD_0001 „IPsec Tunnel TI aufbauen”	-	-	-	-	-	-	-	-	-	-	-
TUC_VPN-ZD_0002 „IPsec Tunnel 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									-		
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
CheckCertificate Expiration	-	-	-	-	-	x	x	x	~~x~~	x	x
VerifyCertificate	-	-	-	-	-	x	-	x	~~x~~	x	x
Zeitdienst											

Erlaubte Operationen im Zustand EC_FIREWALL_NOT_RELIABLE

		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_Period	EC_TSL_Trust_Anchor_Out_Of_Date	~~EC_Firewall_Not_Reliable~~ (Spalte gelöscht)	EC_Secure_Key_Store_Not_Available	EC_FW_Not_Valid_Status_Blocked
	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

In den kritischen Fehlerzuständen, in denen keine TLS-Verbindung ins LAN aufgebaut werden (EC_Random_Generator_Not_Reliable, EC_Software_Integrity_Check_Failed, EC_Security_Log_Not_Writable, EC_Time_Sync_Pending_Critical, EC_Time_Difference_Intolerable), kann keine Verbindung zu den Kartenterminals aufgebaut werden. Infolge sind hier keine Kartenoperationen zugelassen.

Wenn keine Verbindung zum VPN-Konzentrator des SIS aufgebaut werden kann, ist infolge das Internet nicht über den Konnektor erreichbar. Wenn keine Verbindung zum VPN-Konzentrator der TI aufgebaut werden kann, sind Bestandsnetze nicht erreichbar.

A_16203 Nutzbarkeit im Zustand EC_FIREWALL_NOT_RELIABLE

Im Zustand EC_Firewall_Not_Reliable DARF der Konnektor NICHT nutzbar sein. Möglichkeiten zur Behebung des Zustandes EC_Firewall_Not_Reliable sind mit dem CC - Evaluierer und Zertifizierer abzustimmen.

<== {*Prüfverfahren: sich.tech.Eig.:CC-Evaluierung*}

Die Architektur der TI ist so angelegt, dass die Fehlerzustände mit Severity=Fatal in den Tabellen TAB_KON_504 und TAB_KON_503 mit vernachlässigbarer Wahrscheinlichkeit von externen Einflüssen abhängen. Die SLAs für Dienste der zentralen TI-Plattform sind so gefasst, dass diese schwerwiegend verletzt werden müssten, um dadurch einen Konnektor in einen solchen kritischen Zustand zu bringen (externer Fehler aus Sicht des Konnektors). Dass beispielsweise der TSL-Dienst über den Zeitraum der Grace-Period-TSL (typisch: 7 Tage) nicht erreichbar ist (ErrorCondition EC_TSL_Out_Of_Date _Beyond_Grace_Period), kann nur bei massiver Verletzung der für zentrale Dienste festgelegten SLAs eintreten.

Grund der Änderung

Nach der Einführung des Adressbereiches NET_AADG im IP-Adresskonzept der TI [gemSpec_Net] muss dieser Parameter als separates IP-Netzsegment wieder entfernt werden. Ein Konsistenzfehler zum bestehenden PP des Konnektors wird damit korrigiert.

gemSpec_Net

GS-A_4029

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 (TI_Dezentral_SIS) (siehe Erläuterung)	2M	100.64.0.0/11	Dezentral (Dezentral SIS)	Anbieter Zentrales Netz TI
Konnektoren	2M	100.64.0.0/11	Konnektoren TI (Konnektoren SIS)	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-Zugangsdienst	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_Fach~~Anwendungsdienste	256K	100.100.0.0/14	Fachdienste	Anbieter Zentrales Netz TI
Offene ~~Fachd~~Dienste	32K	100.102.0.0/17	Offene Fachdienste oder Dienste eines SÜV	Anbieter Offene Fachdienste oder Dienste eines SÜV
	Der Anbieter Zentrales Netz TI weist jedem Offenen Fachdienst ein /26 Adressblock aus dem Bereich 100.102.0.0/17 zu			
	32K	100.102.128.0/17	aAdG und aAdG-NetG-TI	Anbieter aAdG und aAdG-NetG-TI
	Der Anbieter Zentrales Netz TI weist den aAdG und aAdG-NetG-TI bei Bedarf ein /26 Adressblock aus dem			

	Bereich 100.102.128.0/17 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	100.101.0.0/16 100.103.0.0/16	Reserve	Anbieter Zentrales Netz TI
TI_Dezentral_SIS (siehe Erläuterung)	256k	100.104.0.0/14	Dezentral SIS	Anbieter Zentrales Netz TI
Konnektoren	128k	100.104.0.0/15	Konnektoren SIS	Anbieter Zugangsdienst
Reserveblock	128k	100.106.0.0/15	Reserve	Anbieter Zentrales Netz TI
TI_Betriebsreserve	1.5M	100.108.0.0/14 100.112.0.0/12	Reserve	Anbieter Zentrales Netz TI

GS-A_4850

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 (TI_Test_Dezentral_SIS) (siehe Erläuterung)	512K	172.16.0.0/13	Dezentral TI (Dezentral SIS)	Anbieter Zentrales Netz TI
Konnektoren	512K	172.16.0.0/13	Konnektoren TI (SIS)	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-Zugangsdienst	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_~~Fach~~Anwendungsdienste	256K	172.28.0.0/14	Fachdienste	Anbieter Zentrales Netz TI
Offene ~~Fachd~~Dienste	32K	172.30.0.0/17	Offene Fachdienste oder Dienste	Anbieter Offene Fachdienste oder Dienste eines SÜV
	Der Anbieter Zentrales Netz TI			

	weist jedem Offenen Fachdienst ein /26 Adressblock aus dem Bereich 172.30.0.0/17 zu		eines SÜV	
	32K	172.30.128.0/17	aAdG und aAdG-NetG-TI	Anbieter aAdG und aAdG-NetG-TI
	Der Anbieter Zentrales Netz TI weist den aAdG und aAdG-NetG-TI bei Bedarf ein /26 Adressblock aus dem Bereich 172.30.128.0/17 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			
(TI_Test_Dezentral_SIS) (siehe Erläuterung)	172.29.0.0/16		Dezentral SIS	Anbieter Zentrales Netz TI
Konnektoren	64K	172.29.0.0/16	Konnektoren SIS	Anbieter Zugangsdienst
Reserveblöcke	128K	172.29.0.0/ 16172.31.0.0/16	Reserve	Anbieter Zentrales Netz TI

gemSpec_Kon

TIP1-A_4981

Tabelle 10: TAB_KON_812 Umgebungsabhängige Konfigurationsparameter

Betriebs umgebung	Konfigurations parameter	Konfigurations wert	Beschreibung
PU	NET_TI_ ZENTRAL	siehe [gemSpec_Net#Tab_ Adrkonzept_Produktiv]	Siehe TAB_KON_680. Dieser Wert MUSS für den Administrator über die Managementschnittstelle einsehbar, DARF aber NICHT änderbar sein.
	NET_TI_ GESICHERTE_FD	siehe [gemSpec_Net#Tab_ Adrkonzept_Produktiv]	Siehe TAB_KON_680. Dieser Wert MUSS für den Administrator über die Managementschnittstelle einsehbar, DARF aber NICHT änderbar sein.
	NET_TI_ OFFENE_FD	siehe [gemSpec_Net#Tab_ Adrkonzept_Produktiv]	Siehe TAB_KON_680. Dieser Wert MUSS für den Administrator über die Managementschnittstelle einsehbar, DARF aber NICHT änderbar sein.
	~~NET_AADG~~	~~siehe [gemSpec_Net#Tab_ Adrkonzept_Produktiv] Eintrag aAdG und aAdG NetG-TI~~	~~Siehe TAB_KON_680. Dieser Wert MUSS für den Administrator über die Managementschnittstelle einsehbar, DARF aber NICHT änderbar sein.~~
	DNS_TOP_ LEVEL_DOMAIN_TI	telematik.	Siehe TAB_KON_731. Dieser Wert MUSS für den Administrator über die Managementschnittstelle einsehbar, DARF aber NICHT änderbar sein.
RU/TU	NET_TI_ ZENTRAL	siehe [gemSpec_Net# Tab_Adrkonzept_Test]	Siehe TAB_KON_680. Dieser Wert MUSS für den Administrator über die Managementschnittstelle mit dem Konfigurationswert voreingestellt und änderbar sein.
	NET_TI_ GESICHERTE_FD	siehe [gemSpec_Net# Tab_Adrkonzept_Test]	Siehe TAB_KON_680. Dieser Wert MUSS für den Administrator über die Managementschnittstelle mit dem Konfigurationswert voreingestellt und änderbar sein.
	NET_TI_ OFFENE_FD	siehe [gemSpec_Net# Tab_Adrkonzept_Test]	Siehe TAB_KON_680. Dieser Wert MUSS für den Administrator über die Managementschnittstelle mit dem Konfigurationswert voreingestellt und änderbar sein.
	~~NET_AADG~~	~~siehe [gemSpec_Net#Tab_ Adrkonzept_Produktiv]~~	~~Siehe TAB_KON_680. Dieser Wert MUSS für den Administrator über die~~

		~~Eintrag aAdG und aAdG-NetG-TI~~	~~Managementschnittstelle mit dem Konfigurationswert voreingestellt und änderbar sein.~~
	DNS_TOP_ LEVEL_ DOMAIN_TI	telematik-test.	Siehe TAB_KON_731. Dieser Wert MUSS für den Administrator über die Managementschnittstelle einsehbar, aber nicht änderbar sein.

TIP1-A_5407

Der Konnektor MUSS für die Kommunikation aus den Adressbereichen NET_LEKTR-Umgebung mit den Adressbereichen NET_TI_OFFENE_FD, ~~NET_AADG~~ und ANLW_BESTANDSNETZE eine Network Address Port Translation (NAPT) gemäß [RFC3022#2.2, 3, 4.1-4.3] vornehmen.
Für die Umsetzung der Private Local Address aus den Adressbereichen der Einsatzumgebung MUSS die IP-Adresse VPN_TUNNEL_TI_INNER_IP als Global Address genutzt werden.
Der Konnektor MUSS für die Kommunikation aus den Adressbereichen der NET_LEKTR-Umgebung mit dem Internet über den VPN-Tunnel SIS eine Network Address Port Translation (NAPT) gemäß RFC3022#2.2, 3, 4.1-4.3 vornehmen. Für die Umsetzung der Local Address MUSS die IP-Adresse VPN_TUNNEL_SIS_INNER_IP als Global Address genutzt werden.

TIP1-A_5530

Der Konnektor MUSS sicherstellen, dass IP-Pakete mit einer Absenderadresse aus dem Adressbereich NET_TI_OFFENE_FD ~~und NET_AADG~~ verworfen werden, wenn sie nicht aus dem VPN-Tunnel der TI (VPN_TI) stammen.
Der Konnektor MUSS die Kommunikation mit Systemen des Netzwerksegments NET_TI_OFFENE_FD ~~und NET_AADG~~ für folgende Fälle unterstützen:

- [33] von „Aktive Komponenten“ kommend
- [36] vom Fachmodul kommend

Der Konnektor MUSS insbesondere die Kommunikation an seinen Außenschnittstellen mit Systemen des Netzwerksegments NET_TI_OFFENE_FD ~~und NET_AADG~~ für folgende Fälle blockieren:

- [34] vom Konnektor kommend
- [35] in Richtung Konnektor gehend

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

Änderung im beschreibenden Text

Tabelle 278: TAB_KON_680 Mapping der Netzwerksegmente

ReferenzID im Konnektor	Adressbereich für die TI-Produktivumgebung	Adressbereich für die TI-Testumgebung	Adressbereich für die TI-Referenzumgebung
NET_SIS	TI_Dezentral_SIS - Konnektoren	TI_Test_Dezentral_SIS - Konnektoren	Ist durch den Testbetriebsverantwortlichen zu definieren.
NET_TI_DEZENTRAL	TI_Dezentral - Konnektoren	TI_Test_Dezentral - Konnektoren	Ist durch den Testbetriebsverantwortlichen zu definieren.
NET_TI_ZENTRAL	TI_Zentral - Zentrale Dienste	TI_Test_Zentral - Zentrale Dienste	Ist durch den Testbetriebsverantwortlichen zu definieren.
NET_TI_OFFENE_FD	~~TI_Fach~~Anwendungsdienste - Offene Fachdienste - aAdG und aAdG-NetG-TI	~~TI_~~Test_~~Fach~~Anwendungsdienste - Offene Fachdienste - aAdG und aAdG-NetG-TI	Ist durch den Testbetriebsverantwortlichen zu definieren.
~~NET_AADG~~	~~aAdG und aAdG-NetG-TI~~	~~TI_Test_Fachdienste - Offene Fachdienste~~	~~Ist durch den Testbetriebsverantwortlichen zu definieren.~~
NET_TI_GESICHERTE_FD	~~TI_Fach~~Anwendungsdienste - Gesicherte Fachdienste	~~TI_~~Test_~~Fach~~Anwendungsdienste - Gesicherte Fachdienste	Ist durch den Testbetriebsverantwortlichen zu definieren.
NET_LEKTR	Liste der Netzwerke die in der Einsatzumgebung über den Konnektor erreichbar sind. Ein Eintrag der Liste enthält die Netzwerkadresse und den Netzwerkprefix.		
ANLW_BESTANDSNETZE	Liste der an die TI angeschlossenen Bestandsnetze (u. a. das Sichere Netz der KVen). Ein Eintrag der Liste enthält die Netzwerkadresse und den Netzwerkprefix.		
ANLW_AKTIVE_BESTANDSNETZE	Liste der an die TI angeschlossenen und aktivierten Bestandsnetze		