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:

Mit Änderungsmeldung C_6097 werden folgende Dokumente angepasst:

gemSpec_Kon

gemProdT_Kon_PTV3

Änderungen in gemSpec_Kon

2.9 Standalone-Szenario

Gemäß §291~~a~~ SGB V Absatz 2b müssen „Diese Dienste [zur Online-Aktualisierung der Versichertendaten auf der eGK] […] auch ohne Netzanbindung an die Praxisverwaltungssysteme der Leistungserbringer online genutzt werden können."

Dies bedeutet, dass der Konnektor ohne ein steuerndes Clientsystem ereignisgetrieben Fachanwendungen ausführen können muss. Aus Fachsicht „steht der Konnektor alleine", ohne Clientsysteme. Die konkreten Aktionen, die Fachanwendungen in diesen Fällen ausführen, sowie deren Auslöser werden in den jeweiligen Fachmodulspezifikationen beschrieben.

Ein solcher alleinstehender Konnektor mit Zugang zur TI muss zur Durchführung der Fachanwendungen durch einen weiteren Konnektor unterstützt werden, der in direkter Verbindung zum Clientsystem steht, selbst aber keine Online-Anbindung besitzt. ~~Die im Gesetz geforderte informationstechnische Trennung (Online-Bereich vs. Offline-Bereich im lokalen Netz des Leistungserbringers) kann auch durch eine logische Separation innerhalb eines Konnektors erreicht werden, die der Administrator zuschalten kann (siehe Kapitel 0). Ist dieser Modus aktiviert, so garantiert der Konnektor, dass keine Daten aus Richtung der TI zum Clientsystem gelangen (und umgekehrt). In dieser Betriebsart ist demnach statt zwei Konnektoren nur ein Konnektor notwendig.~~

4.1.7 Verschlüsselungsdienst

4.1.7.1 Funktionsmerkmalweite Aspekte

~~⌦ **TIP1-A_4615 Enc: Keine Onlineprüfung bei Logischer Separation**~~

~~Ist MGM_LOGICAL_SEPARATION=Enabled DARF der Verschlüsselungsdienst des Konnektors für Aufrufe an der Außenschnittstelle NICHT den Revocationsstatus von Zertifikaten prüfen, d. h. der Konnektor muss sich nach Außen verhalten, als wäre MGM_LU_ONLINE=Disabled.~~ ~~⌫~~

© gematik – öffentlich_Entwurf

4.1.8 Signaturdienst

4.1.8.1 Funktionsmerkmalweite Aspekte

4.1.8.1.1 Dokumentensignatur

~~⌦ TIP1-A_4626 Sig: Keine Onlineprüfung bei Logischer Separation~~

~~Ist MGM_LOGICAL_SEPARATION=Enabled DARF der Signaturdienst des Konnektors für Aufrufe an der Außenschnittstelle NICHT den Revocationsstatus von Zertifikaten prüfen, d. h. der Konnektor muss sich nach Außen verhalten, als wäre MGM_LU_ONLINE=Disabled.~~ ~~⌫~~

4.1.12 LDAP-Proxy

4.1.12.4.1 TUC_KON_290 „LDAP-Verbindung aufbauen“

TAB_KON_805 - TUC_KON_290 „LDAP-Verbindung aufbauen“

Element	Beschreibung
Vorbedingungen	• MGM_LU_ONLINE=Enabled • ~~MGM_LOGICAL_SEPARATION=Disabled~~

4.1.12.4.2 TUC_KON_291 „Verzeichnis abfragen“

TAB_KON_815 - TUC_KON_291 „Verzeichnis abfragen“

Element	Beschreibung
Vorbedingungen	• MGM_LU_ONLINE=Enabled • ~~MGM_LOGICAL_SEPARATION=Disabled~~ • Eine LDAPv3-Verbindung LDAP-Client sowie eine LDAPv3 Verbindung vom Konnektor zum VZD wurden aufgebaut (TUC_KON_290 „LDAP-Verbindung aufbauen“)

4.1.12.4.3 TUC_KON_292 „LDAP-Verbindung trennen“

TAB_KON_816 - TUC_KON_292 „LDAP-Verbindung trennen“

Element	Beschreibung
Vorbedingungen	• MGM_LU_ONLINE=Enabled • ~~MGM_LOGICAL_SEPARATION=Disabled~~ • Eine LDAPv3-Verbindung LDAP-Client sowie eine LDAPv3 Verbindung vom Konnektor zum VZD wurden aufgebaut (TUC_KON_290 „LDAP-Verbindung aufbauen“)

4.1.12.4.4 TUC_KON_293 „Verzeichnisabfrage abbrechen“

TAB_KON_817 - TUC_KON_293 „Verzeichnisabfrage abbrechen“

© gematik – öffentlich_Entwurf

Element	Beschreibung
Vorbedingungen	• MGM_LU_ONLINE=Enabled • ~~MGM_LOGICAL_SEPARATION=Disabled~~ • Ein Search Request wurde vom Konnektor empfangen und an den VZD weitergeleitet (TUC_KON_291 „Verzeichnis Abfragen“). Der Request wurde vom VZD noch nicht beantwortet.

4.2.1 Anbindung LAN/WAN

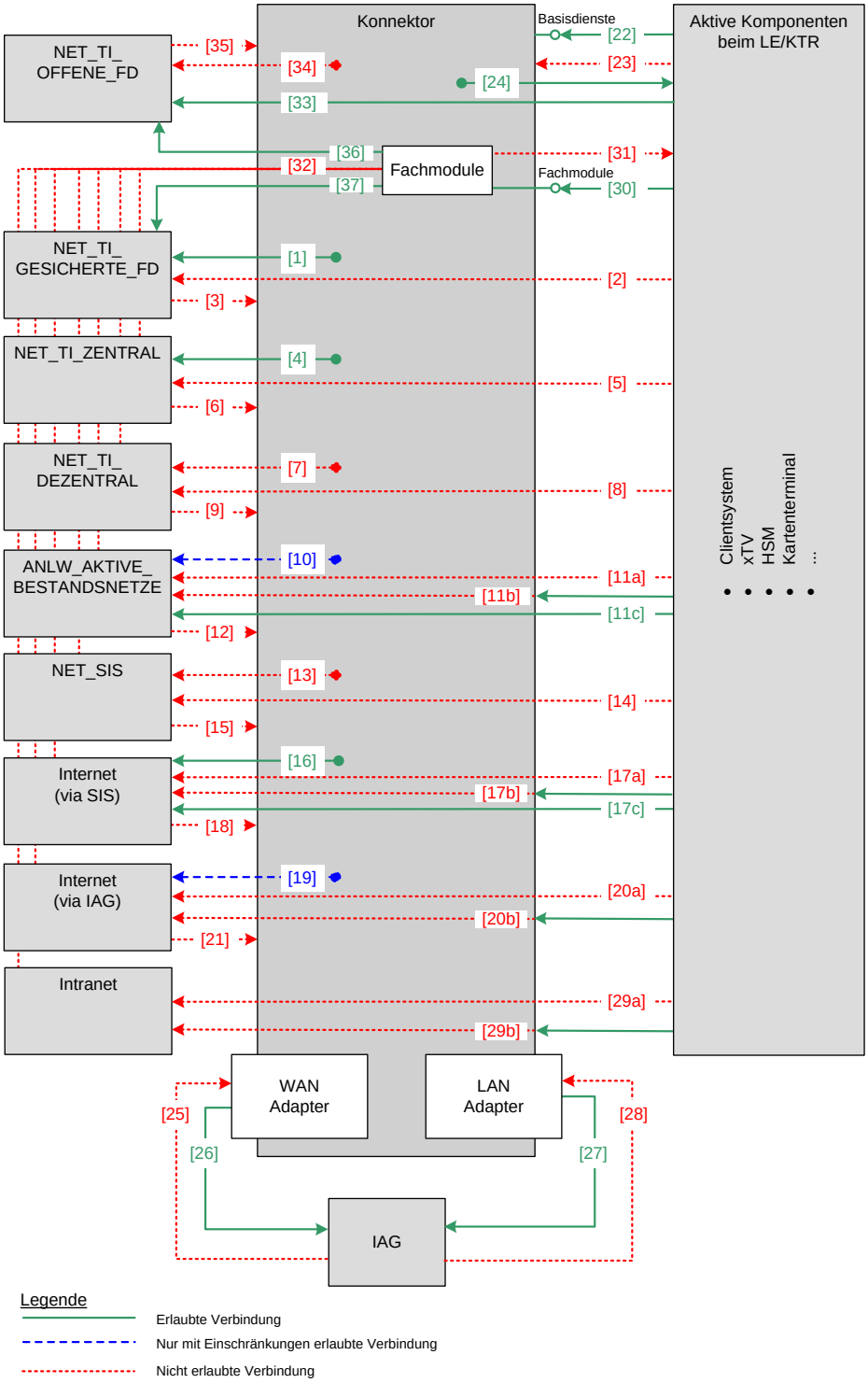
4.2.1.1.2 Routing und Firewall

Darstellung der Kommunikationsregeln des Konnektors

Diese Abbildung dient der Veranschaulichung der im Konnektor verwendeten Kommunikationsregeln welche in den nachfolgenden Afo definiert werden.

alt:

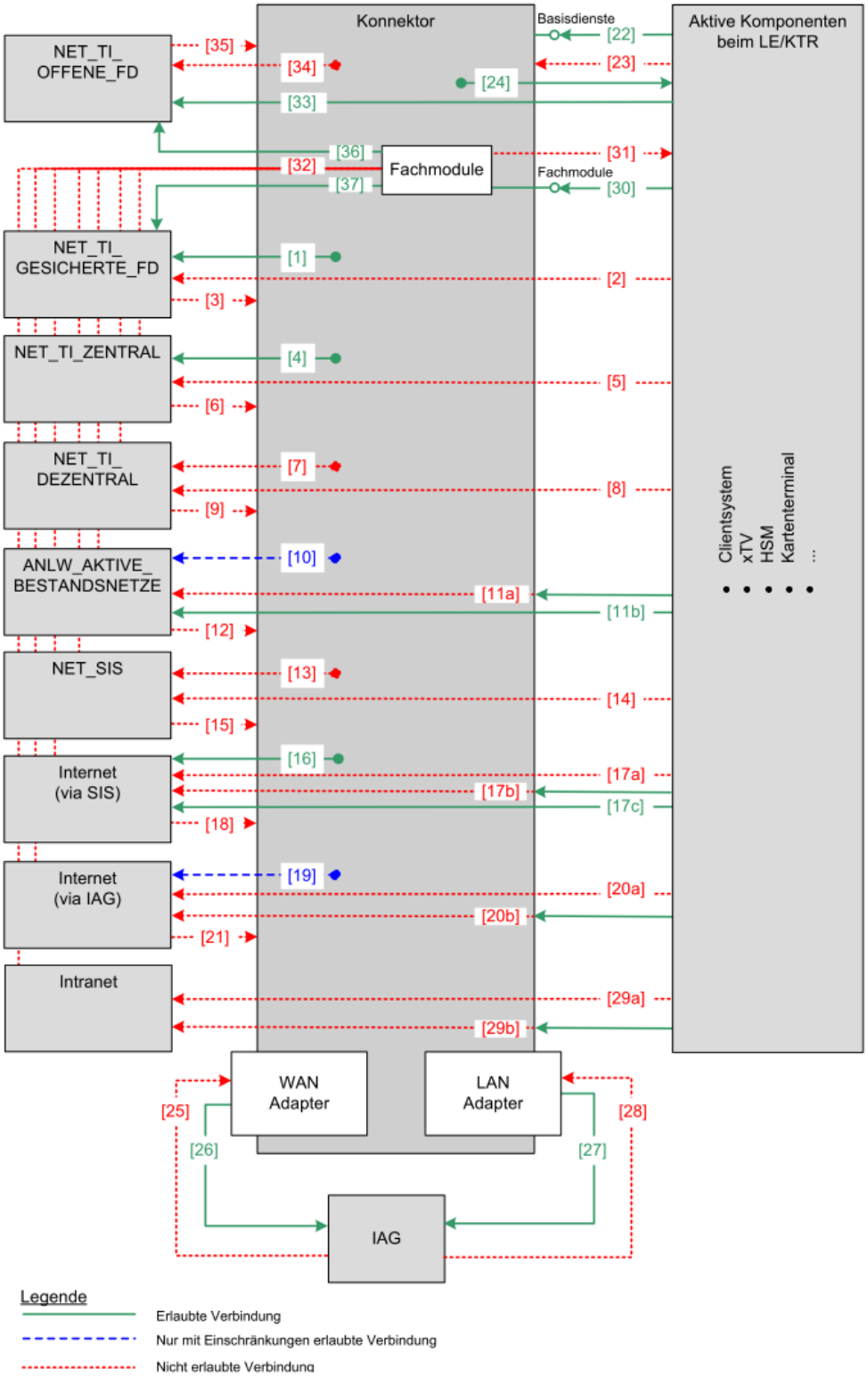
© gematik – öffentlich_Entwurf



PIC_KON_115 Kommunikationsregeln Konnektor

© gematik – öffentlich_Entwurf

neu:



PIC_KON_115 Kommunikationsregeln Konnektor

⌦ TIP1-A_4733 Kommunikation mit ANLW_AKTIVE_BESTANDSNETZE

© gematik – öffentlich_Entwurf

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 ~~und MGM_LOGICAL_SEPARATION=Disabled)~~ vom Konnektor kommend nur für die DNS-Namensauflösung mittels DNS_SERVERS_BESTANDSNETZE
- [11b~~c~~] 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] wenn (MGM_LOGICAL_SEPARATION=Enabled) für freigegebene Bestandsnetze (ANLW_AKTIVE_BESTANSNETZE) von „Aktive Komponenten“ kommend~~
- [11c~~b~~] für nicht freigegebene Bestandsnetze (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_4735 Kommunikation mit dem Internet (via SIS)

Der Konnektor MUSS sicherstellen, dass IP-Pakete mit einer Absenderadresse aus dem Adressbereich NET_TI_ZENTRAL, NET_TI_GESICHERTE_FD; NET_TI_OFFENE_FD, NET_TI_DEZENTRAL, ANLW_AKTIVE_BESTANDSNETZE, ANLW_LAN_ADDRESS_SEGMENT, aus einem der Netzwerksegmente in ANLW_LEKTR_INTRANET_ROUTES oder ANLW_WAN_NETWORK_SEGMENT verworfen werden, wenn sie aus dem VPN-Tunnel der SIS (VPN_SIS) stammen.

Der Konnektor MUSS die Kommunikation mit Systemen des Netzwerksegments Internet (via SIS) für folgende Fälle unterstützen:

- [16] wenn (MGM_LU_ONLINE=Enabled ~~und MGM_LOGICAL_SEPARATION=Disabled~~ und ANLW_INTERNET_MODUS=SIS) vom Konnektor kommend
- [17c] wenn (MGM_LU_ONLINE=Enabled ~~und MGM_LOGICAL_SEPARATION=Disabled~~ und ANLW_INTERNET_MODUS=SIS) von „Aktive Komponenten“ kommend

© gematik – öffentlich_Entwurf

Der Konnektor MUSS insbesondere die Kommunikation an seinen Außenschnittstellen mit Internet (via SIS) für folgende Fälle blockieren oder umleiten:

- [17a] blockieren, wenn (MGM_LU_ONLINE=Enabled ~~und MGM_LOGICAL_SEPARATION=Disabled~~ und ANLW_INTERNET_MODUS=KEINER) von „Aktive Komponenten“ kommend
- [17b] umleiten, wenn (MGM_LU_ONLINE=Enabled ~~und MGM_LOGICAL_SEPARATION=Disabled~~ und ANLW_INTERNET_MODUS=IAG) von „Aktive Komponenten“ kommend; ➔ Der Konnektor MUSS an Hosts im Internet gerichtete IP-Pakete gemäß [RFC792] umleiten (ICMP Redirect).
- [18] blockieren, wenn von SIS kommend in Richtung Konnektor (und die dahinterliegenden „Aktive Komponenten“)

Der Konnektor MUSS sicherstellen, dass die für die Kommunikation mit dem Internet (via SIS) bestimmten IP-Pakete ausschließlich in den VPN-Tunnel des SIS (VPN_SIS) geleitet werden. ⌫

⌦ **TIP1-A_4736 Kommunikation mit dem Internet (via IAG)**

Der Konnektor MUSS sicherstellen, dass eingehende IP-Pakete von der Kommunikation mit dem Internet mit der Empfängeradresse ungleich (ANLW_LAN_IP_ADDRESS oder aus einem der Netzwerksegmente in ANLW_LEKTR_INTRANET_ROUTES wenn ANLW_WAN_ADAPTER_MODUS=DISABLED) oder (ANLW_WAN_IP_ADDRESS wenn ANLW_WAN_ADAPTER_MODUS=ENABLED) verworfen werden.

Der Konnektor MUSS sicherstellen, dass ausgehende IP-Pakete für die Kommunikation mit dem Internet mit der Absenderadresse ungleich (ANLW_LAN_IP_ADDRESS oder aus einem der Netzwerksegmente in ANLW_LEKTR_INTRANET_ROUTES wenn ANLW_WAN_ADAPTER_MODUS=DISABLED) oder (ANLW_WAN_IP_ADDRESS wenn ANLW_WAN_ADAPTER_MODUS=ENABLED) verworfen werden.

Der Konnektor MUSS die Kommunikation mit Systemen des Netzwerksegments Internet (via IAG) für folgende Fälle unterstützen:

- [19] vom Konnektor kommend zu den folgenden Systemen für das Protokoll IPsec
    - VPN_KONZENTRATOR_TI_IP_ADDRESS
    - VPN_KONZENTRATOR_SIS_IP_ADDRESS
- [19] vom Konnektor kommend zu den folgenden Systemen für HTTP und HTTPS
    - CERT_CRL_DOWNLOAD_ADDRESS
    - hash&URL-Server
    - Registrierungsserver

© gematik – öffentlich_Entwurf

- o Remote-Managementserver
- o DNS_ROOT_ANCHOR_URL (benötigte IP-Adressen um den DNSSEC Trust Anchor im Namensraum Internet zu verifizieren)

- [19] vom Konnektor kommend zu den folgenden Systemen für das Protokoll DNS
  - o beliebige Hosts

Der Konnektor MUSS insbesondere die Kommunikation an seinen Außenschnittstellen mit Internet (via IAG) für folgende Fälle blockieren oder umleiten:

- [20a] blockieren, wenn (ANLW_INTERNET_MODUS=KEINER oder MGM_LU_ONLINE=Disabled ~~oder MGM_LOGICAL_SEPARATION=Enabled~~) von „Aktive Komponenten“ kommend
- [20b] mittels ICMP Redirect gemäß [RFC792] zum Default Gateway umleiten, wenn die Zieladresse des IP-Pakets nicht innerhalb der Adressbereiche (NET_TI_ZENTRAL, NET_TI_OFFENE_FD, NET_TI_GESICHERTE_FD und ANLW_AKTIVE_BESTANDSNETZE) ist und ANLW_INTERNET_MODUS=IAG und von „Aktive Komponenten“ kommend.
- [21] blockieren, wenn von IAG kommend in Richtung Konnektor (und die dahinterliegenden „Aktive Komponenten“)⌧

4.2.4 VPN-Client

4.2.4.2 Durch Ereignisse ausgelöste Reaktionen

⌦ **TIP1-A_4782 SIS VPN-Client Stop Events**

Beim Auftreten einer der nachfolgenden Events MUSS der Konnektor den VPN-Tunnel zum SIS beenden:

- ~~MGM/LOGICAL_SEP_CHANGED mit (Active=Enabled)~~
- MGM/LU_CHANGED/LU_ONLINE mit (Active=Disabled)⌧

4.2.4.3.2 TUC_KON_322 „Verbindung zu dem VPN-Konzentrator des SIS aufbauen“

⌦ **TIP1-A_4784 TUC_KON_322 „Verbindung zu dem VPN-Konzentrator des SIS aufbauen“**

Der Konnektor MUSS den technischen Use Case TUC_KON_322 „Verbindung zu dem VPN-Konzentrator der SIS aufbauen“ umsetzen.

TAB_KON_637 - TUC_KON_322 „Verbindung zu dem VPN-Konzentrator der SIS aufbauen“

⌦ **TIP1-A_4784 TUC_KON_322 „Verbindung zu dem VPN-Konzentrator des SIS aufbauen“**

© gematik – öffentlich_Entwurf

Der Konnektor MUSS den technischen Use Case TUC_KON_322 „Verbindung zu dem VPN-Konzentrator der SIS aufbauen“ umsetzen.

Tabelle 1: TAB_KON_637 - TUC_KON_322 „Verbindung zu dem VPN-Konzentrator der SIS aufbauen“

Element	Beschreibung
Name	TUC_KON_322 Verbindung zu dem VPN-Konzentrator der SIS aufbauen
Beschreibung	Es muss ein IPsec-Tunnel zum VPN-Konzentrator der SIS aufgebaut werden
Auslöser	Bootup-Phase TUC_KON_305 „LAN-Adapter initialisieren“ TUC_KON_306 „WAN-Adapter initialisieren“ Event NETWORK/VPN/CONFIG_CHANGED Optional: Event MGM/LU_CHANGED/LU_ONLINE Manueller Aufruf über Managementschnittstelle
Vorbedingungen	ANLW_INTERNET_MODUS = SIS Die Verbindung VPN-Konzentrator TI ist aufgebaut Der TUC_KON_304 „Netzwerk-Routen einrichten“ muss erfolgreich durchgeführt worden sein.
Eingangsdaten	Keine
Komponenten	Konnektor
Ausgangsdaten	Der virtuelle Adapter VPN_SIS mit der IP-Adresse VPN_TUNNEL_SIS_INNER_IP wurde zur Verfügung gestellt. • Innere Tunnel-IP-Adresse des VPN-Konzentrators SIS • VPN_KONZENTRATOR_SIS_IP_ADDRESS • DNS_SERVER_SIS
Standardablauf	1) Wenn der Auslöser Event NETWORK/VPN/CONFIG_CHANGED ist, muss der VPN-Tunnel SIS abgebaut werden. 2) Wenn der VPN-Tunnel SIS noch aktiv ist, ist der Ablauf abgeschlossen. Anderenfalls ist mit Ablaufschritt 3) fortzufahren. 3) Prüfen, ob (MGM_LU_ONLINE=Enabled). falls nicht ist der TUC ohne Ausgabe einer Fehlermeldung zu beenden. ~~4) Prüfen, ob (MGM_LOGICAL_SEPARATION=Disabled), falls nicht ist der TUC mit einer Fehlermeldung zu beenden.~~ 5) entfällt 6) Prüfen, ob die im Konnektor hinterlegte CRL noch gültig ist. falls nicht, MUSS der TUC_KON_040 „CRL aktualisieren“

© gematik – öffentlich_Entwurf

Element	Beschreibung
	aufgerufen werden, Anschließend erneut prüfen, ob die im Konnektor hinterlegte CRL nun gültig ist. Falls die CRL noch nicht gültig ist, ist der TUC mit Fehler zu beenden. 7) Aufrufen von TUC_VPN-ZD_0002 “IPsec Tunnel SIS aufbauen” 8) Aufrufen von TUC_KON_304 „Netzwerk-Routen einrichten“ Sobald der Tunnel erfolgreich aufgebaut wurde, ist der folgende Event zu generieren: TUC_KON_256 {"NETWORK/VPN_SIS/UP"; Op; Info;IP= $VPN_TUNNEL_SIS_INNER_IP}
Varianten / Alternativen	Keine
Fehlerfälle	(→ 3) Keine Online-Verbindung zulässig; 4172 ~~(→ 4) Keine Online-Verbindung zulässig; 4172~~ (→ 6) CRL ist Abgelaufen (outdated);4173 (→ 7) VPN Tunnel konnte nicht aufgebaut werden; Fehlercode: 4176

4.2.5 Zeitdienst

4.2.5.5.1 Sync_Time

⌦ TIP1-A_4791 Operation sync_Time

Der NTP-Server des Konnektors MUSS an der Client-Schnittstelle eine Operation sync_Time anbieten**.**

Tabelle 2 TAB_KON_642 Operation sync_Time

Name	I_NTP_Time_Information:sync_Time
Beschreibung	Der Konnektor MUSS anfragenden Clients (z.B. Ärztearbeitsplatz) per NTP-Version 4 die Systemzeit liefern
Aufrufparameter	Vgl. [NTPv4]
Rückgabe	Vgl. [NTPv4]
Vorbedingungen	MGM_LU_ONLINE=Enabled ~~und MGM_LOGICAL_SEPARATION=Disabled~~
Nachbedingungen	Der anfragende Client hat die korrekte Zeit geliefert bekommen.
Hinweise	Keine
Fehler	Der Aufruf schlägt fehl (bleibt unbeantwortet), wenn

© gematik – öffentlich_Entwurf

Name	I_NTP_Time_Information:sync_Time
	MGM_LU_ONLINE=Disabled ~~oder MGM_LOGICAL_SEPARATION=Enabled~~

⌫

4.2.6 Namensdienst und Dienstlokalisierung

4.2.6.1 Funktionsmerkmalseite Aspekte

⌦ TIP1-A_4797 DNS-Forwards des DNS-Servers

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

Tabelle 3: 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. ~~Wenn (MGM_LOGICAL_SEPARATION=Enabled) gesetzt ist MUSS der Konnektor diesen Namensraum ausschließlich für interne Dienste und die internen Fachanwendungen auflösen.~~

4.3.6 Leistungsumfänge und Standalone-Szenario~~s~~

~~**⌦ TIP1-A_4823 Konnektor mit logischer Trennung**~~

~~Die Managementschnittstelle MUSS es einem Administrator ermöglichen Konfigurationsänderungen gemäß Tabelle TAB_KON_660 vorzunehmen:~~

~~Die Aktivierung der logischen Trennung DARF sich NICHT auf die Anzahl benötigter Kartenterminals auswirken. Alle mit deaktivierter logischer Trennung mit einem Kartenterminal verfügbaren Funktionen des Konnektors müssen auch mit aktivierter logischer Trennung weiterhin mit nur einem Kartenterminal zur Verfügung stehen.~~

~~**Tabelle 4 TAB_KON_660 Konnektor mit logischer Trennung**~~

~~ReferenzID~~	~~Belegung~~	~~Bedeutung und Administrator-Interaktion~~
~~MGM_LOGICAL_SEPARATION~~	~~Enabled / Disabled~~	~~Der Administrator MUSS die logische Separation zwischen TI und lokalem Netz der Einsatzumgebung aktivieren / deaktivieren können.~~ ~~Default-Wert: Disabled~~ ~~Bei Veränderung MUSS TUC_KON_256 gerufen werden {"MGM/LOGICAL_SEP_CHANGED"; Op; Info; „Active=$MGM_LOGICAL_SEPARATION"}~~

© gematik – öffentlich_Entwurf

~~MGM_LOGICAL_SEPARATION wirkt hauptsächlich in den Funktionsmerkmalen:~~

- ~~„Zertifikatsdienst“ (Kapitel **Fehler! Verweisquelle konnte nicht gefunden werden.**)~~
- ~~„Anbindung LAN/WAN“ (Kapitel 0)~~
- ~~„VPN-Client“ (Kapitel 0)~~
- ~~„Zeitdienst“ (Kapitel **Fehler! Verweisquelle konnte nicht gefunden werden.**)~~

© gematik – öffentlich_Entwurf

Anhang E - Übersicht Konfigurationsparameter und Zustandswerte

Tabelle 5 – TAB_KON_689 Konfigurationsparameter und Zustandswerte des Konnektors

Zustandswert?	ReferenzID	Belegung	Bedeutung und Administrator-Interaktion bzw. Zustandswerte
Leistungsumfänge und Standalone-Szenario~~s~~			
	~~MGM_LOGICAL_SEPARATION~~	~~Enabled / Disabled~~	~~Der Administrator MUSS die logische Separation zwischen TI und lokalem Netz der Einsatzumgebung aktivieren / deaktivieren können.~~ ~~Default-Wert: Disabled~~ ~~Bei Veränderung MUSS TUC_KON_256 gerufen werden {"MGM/LOGICAL_SEP_CHANGED"; Op; Info; „Active=$ MGM_LOGICAL_SEPARATION"}~~

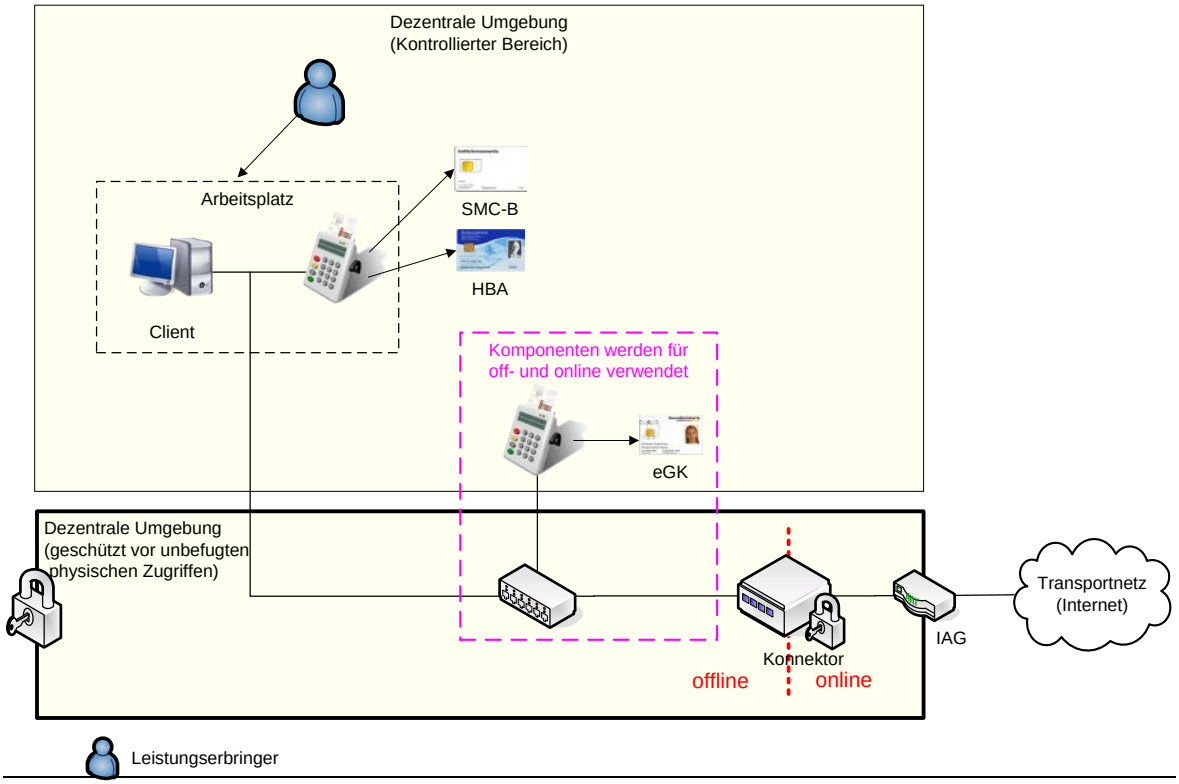
Anhang F - Übersicht Events

Tabelle 6 – TAB_KON_777 Events Interne Mechanismen

Topic Ebene1	Topic Ebene2	Topic Ebene3	Typ	Schwere	Prot	An Clients	Parameter	Bedeutung	Auslöser (TUC/Op)
Leistungsumfänge und Standalone-Szenario~~s~~									
~~MGM~~	~~LOGICAL_SEP_CHANGED~~		~~Op~~	~~Info~~	~~x~~	~~x~~	~~Active=$MGM_LOGICAL_SEPARATION~~	~~Festlegung des Konnektors zur logischen Separierung wurde geändert~~	~~Administrator~~

Anhang K – Szenarien im dezentralen Umfeld

~~Szenario 8: Standalone Konnektor - Logische Trennung~~



~~Abbildung 1 Standalone-Szenario mit logischer Trennung im Konnektor~~

~~Beschreibung des Szenarios~~

~~Dieses Szenario stellt eine Variante des Standalone-Szenarios dar, bei dem eine logische Trennung im Konnektors konfiguriert wurde.~~

~~Im Standalone-Szenario besteht eine Trennung zwischen den Praxissystemen der dezentralen Umgebung, welche offline (also, ohne Anbindung an die zentrale TI-Plattform) betrieben werden und den für das Update der eGK durch die Fachanwendung VSDM notwendigen Komponenten, welche online (also, mit Verbindung in die zentrale TI-Plattform) betrieben werden.~~

~~Die logische Trennung im Standalone-Szenario zeichnet sich dadurch aus, dass ein Standalone-Szenario ohne einen separaten Konnektor und ohne ein separates eHealth-Kartenterminal realisiert werden kann. Der Konnektor stellt dabei sicher, dass nur die Fachlogik von VSDM auf die Online-Funktionen der TI zugreifen kann. Den Praxissystemen steht alleinig die Offline-Funktionalität des Konnektors zur Verfügung.~~

~~Im Offline-Modus sind einzelne Funktionen des Konnektors nicht verfügbar, andere haben einen eingeschränkten Funktionsumfang. So kann z.B. eine QES erzeugt oder geprüft aber dabei keine aktuelle Statusauskunft (OCSP-Response) für die eingesetzten Zertifikate~~

© gematik – öffentlich_Entwurf

~~eingeholt werden. Dies hat zur Folge, dass bei Erzeugung einer QES keine Statusauskunft für das Signaturzertifikat in die Signatur eingebettet werden kann und bei einer Prüfung der QES nur eine eventuell in die Signatur eingebettet Statusauskunft des Zertifikats berücksichtigt werden kann.~~

~~Der Nutzer muss in diesem Fall selber entscheiden, ob der gebotene Funktionsumfang für seinen Anwendungsfall ausreichend ist.~~

~~Voraussetzungen~~

~~Folgende zusätzliche Punkte müssen erfüllt sein, um dieses Szenario umzusetzen:~~

- ~~Konfiguration im Konnektor: Logische Trennung~~
- ~~Konfiguration im Konnektor: eHealth-Kartenterminal, welches für von der Fachlogik von VSDM für das Update der eGK mit Online-Verbindung verwendet werden soll.~~

~~Auswirkung~~

- ~~Standalone-Szenario mit minimalem Systemausbau~~
- ~~Eingeschränkte Funktionalität der TI für Praxissysteme (nur Offline-Funktionalität)~~
- ~~Notwendige Prüfung des Nutzers, ob eingeschränkte Funktionalität (insbesondere bei Sicherheitsfunktionen) akzeptabel ist.~~
- ~~Keine Verfügbarkeit des sicheren Internetzugangs der TI (als Teil der Einschränkungen im Offline-Modus).~~

© gematik – öffentlich_Entwurf