Elektronische Gesundheitskarte und Telematikinfrastruktur

Feature: Highspeed-Konnektor

Version:	1.3.0
Revision:	793536
Stand:	12.12.2023
Status:	freigegeben
Klassifizierung:	öffentlich
Referenzierung:	gemF_Highspeed-Konnektor

Dokumentinformationen

Änderungen zur Vorversion

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

Dokumentenhistorie

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
1.0.0 CC	30.08.21		zur Abstimmung freigegeben	gematik
1.0.0	16.03.22		freigegeben	gematik
1.1.0	31.08.22		Einarbeitung Änderungsliste HSK_Maintenance_22.1	gematik
1.2.0	10.07.23	5.2.1.2	Einarbeitung Änderungsliste HSK_Maintenance_23.0 und _23.1, redaktionelle Anpassung (doppelte Afo), Übernahme der HSK-Anteile aus gemF_TI-Gateway	gematik
1.3.0	12.12.23		Änderungsliste HSK_Maintenance_23.3 und _23.5	gematik

Inhaltsverzeichnis

1 Einordnung des Dokuments

Das Dokument ergänzt vorhandene Spezifikationen für das Zulassungsobjektes eines im Rechenzentrum betriebenen Highspeed-Konnektors.

1.1 Zielsetzung

Mit dem Highspeed-Konnektor soll die Grundlage für eine hochverfügbare und skalierbare Konnektorlösung zum Betrieb in einem zertifizierten Rechenzentrum geschaffen werden.

1.2 Zielgruppe

Das Dokument richtet sich an Hersteller, Betreiber, BSI und die Gesellschafter der gematik.

1.3 Abgrenzungen

1.4 Methodik

1.4.1 Epic und User Story

Epics und zugeordnete User Stories werden durch eine eindeutige ID gekennzeichnet.

Epic und UserStory werden im Dokument wie folgt dargestellt:
<Jira-ID> - <Zusammenfassung des Jira-Issue>
Text / Beschreibung
[<=]

Dabei umfasst die Anforderung sämtliche zwischen Jira-ID und Textmarke [<=] angeführten Inhalte.

1.4.2 Anforderungen

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

Da in dem Beispielsatz „Eine leere Liste DARF NICHT ein Element besitzen.“ die Phrase „DARF NICHT“ semantisch irreführend wäre (wenn nicht ein, dann vielleicht zwei?), wird in diesem Dokument stattdessen „Eine leere Liste DARF KEIN Element besitzen.“ verwendet. Die Schlüsselworte werden außerdem um Pronomen in Großbuchstaben ergänzt, wenn dies den Sprachfluss verbessert oder die Semantik verdeutlicht.

Anforderungen werden im Dokument wie folgt dargestellt:
<AFO-ID> - <Titel der Afo>

Text / Beschreibung
[<=]

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

2 Epic und User Story

2.1 STB-169 Highspeed-Konnektor 2.0

Definition der Zulassungsgrundlagen für eine rechenzentrumsbasierte TI-Zugangslösung auf Basis der funktionalen Anforderungen für den Konnektor PTV 5:

- Zielgruppe sind in erster Linie Krankenhäuser und große Einrichtungen
- perspektivisch soll die Lösung erweitert werden, um einen TI-Zugang als Service anzubieten.

2.1.1 Betrieb auf Standard-Hardware/Ablaufumgebungen

Der Highspeed-Konnektor soll auf Standard-Hardware betrieben werden. Damit wird eine Unabhängigkeit von den Produktlebenszyklen der Serverhersteller erreicht. Je nach Leistungsanforderungen des Betreibers wird eine geeignete Hardware ausgewählt.

2.1.2 Breitband-Zugang zur TI

Die Bandbreite des Zugangs zur TI lässt sich nach Anforderungen des Betreibers skalieren.

2.1.3 Leistungsfähiges Modul für Identitäten

Der Identitätsspeicher muss so leistungsfähig sein, dass auch große Installationen mit einer Identität betrieben werden können. (ein HSM statt viele gSMC-K)

3 Einordnung in die Telematikinfrastruktur

Der Highspeed-Konnektor kann die Funktion des Konnektors für große Institutionen (wie Krankenhäuser) übernehmen, bei denen aktuell durch die Institution eine Vielzahl von Einbox- oder Rechenzentrums-Konnektoren betrieben werden muss und daher das Bedürfnis nach einer performanteren Lösung besteht.

Der Highspeed-Konnektor setzt die Spezifikation des Konnektors bis auf die Bereiche um, die in diesem Dokument explizit ausgenommen werden. Zusätzlich werden Anforderungen spezifisch für den Highspeed-Konnektor gestellt.

Die Lösung stellt keinen allgemeinen neuen Zugang zur TI dar, sondern soll explizit nur in großen Institutionen den Betrieb von vielen Einbox-Konnektoren, wie sie heute dort betrieben werden, 1 zu 1 ersetzen. Der Betrieb findet nach wie vor in direkter Verantwortung der LE-Institution statt. Die Nutzung des eines gehosteten Highspeed-Konnektors im Rahmen einer Auftragsdatenverarbeitung ist jedoch nicht ausgeschlossen.

4 Technisches Konzept

Die Konnektorsoftware wird auf Standard-Serverhardware betrieben. Es können geeignete Virtualisierungs- und Container-Lösungen zum Einsatz kommen.

Die Konnektorsoftware kann modularisiert werden (z.B. Anwendungskonnektor, Netzkonnektor, Fachmodule). Es muss sichergestellt sein, dass die Schnittstellen der Module nur von den dafür vorgesehenen Gegenstellen benutzt werden und die Vertraulichkeit der Kommunikation zwischen den Modulen gewährleistet ist (z.B. durch beidseitig authentisierte und verschlüsselte Transportkanäle).

Die gSMC-K kann durch zertifizierte (z. B. FIPS 140-1 und 140-2 oder CC) HSM oder TPM-Lösungen ersetzt werden. Die Anforderungen an die Personalisierung der gSMC-K gelten analog für die Personalisierung des HSM.

Um den Missbrauch der SMC-B zu verhindern, muss der Zugriff des Betreibers auf die SMC-B ausgeschlossen sein z.B. durch eine Trennung von Besitz und Wissen.

4.1 Anbindung über SZZP an die TI

Der Highspeed-Konnektor wird direkt über einen SZZP (light) des AZPD (Arvato) an die TI angebunden.

- Es muss technisch (im Betrieb) und organisatorisch (im Rahmen der Inbetriebnahme) durchgesetzt werden, dass nur der geprüfte Highspeed-Konnektor auf die gesicherten Fachdienste und die zentralen Dienste der TI zugreifen kann. An der technischen Umsetzung dieser Forderung ist auch der SZZP (light) beteiligt.
- Der Betreiber des Highspeed-Konnektors muss am ITSM der TI teilnehmen. Da der Betreiber anderen Teilnehmern des ITSM keinen Service anbietet, gelten nur ein Teil der Anforderungen zum ITSM für den Betreiber des Highspeed-Konnektors.
- Der Betreiber des Highspeed-Konnektors muss nicht in vollem Umfang an den Prozessen zur Informationssicherheit und zum Datenschutz der TI teilnehmen. Er muss jedoch der gematik Kontaktdaten für Ansprechpartner zu Informationssicherheit und Datenschutz benennen und zudem schwere Vorfälle melden.
- Es muss ein VSDM-Intermediär eines VPN-Zugangsdienst genutzt werden.
- Durch die Anbindung an die TI über SZZP entfällt die Registrierung und VPN-Verbindung zum VPN-Zugangsdienst.
- Verbindungen der Clients zu offenen Fachdiensten und weiteren Anwendungen (WANDA) erfolgen direkt über den SZZP-light-plus und nicht über den HSK. Dem Betreiber werden entsprechend zwei Subnetze seitens TI zur Verfügung gestellt. Die Betriebsumgebung muss ein entsprechendes Routing zur Verfügung stellen.
- Der Hersteller muss sich bzgl. der Anbindung mit dem AZPD abstimmen.

4.2 Sicherheitsnachweis

4.2.1 Hersteller

Die Sicherheit des Produktes wird insgesamt durch drei Prüfverfahren nachgewiesen:

- eine Beschleunigte Sicherheitszertifizierung durch das BSI,
- eine Prüfung durch eine Common-Criteria-Prüfstelle mit Konnektor-Erfahrung und
- ein Produktgutachten.

Zudem ist ein Nachweis zu den sicheren Softwareentwicklungsprozessen des Herstellers notwendig (siehe folgender Absatz).

4.2.1.1 Sichere Software-Entwicklung

A_22046 - Sichere Software Entwicklungsumgebung
Der Hersteller des Highspeed-Konnektors MUSS die Entwicklung in der CC-evaluierten Entwicklungsumgebung durchführen. Wenn die Entwicklung nicht in einer während der Konnektor-Evaluierung (Aspekt ALC) mit geprüften Umgebung stattfindet, MUSS der Hersteller ein Sicherheitsgutachten über seine sicheren Softwareentwicklungsprozesse einreichen.**[**<=**]**

4.2.2 Anbieter/Betreiber

Für die Anbieterzulassung wird die Sicherheit über ein Sicherheitsgutachten nachgewiesen.

5 Spezifikation

5.1 Produkteigenschaften (Funktional und Sicherheit)

Für den Highspeed-Konnektor gelten folgende Anforderungen, auch wenn sie sich an den Konnektor, das "Fachmodul ePA im KTR-Consumer" oder den Basis- bzw. KTR-Consumer richten:

A_21853-01 - Feste Kopplung von Konnektor und SZZP
Der Konnektor MUSS eine kryptographische Kopplung mit dem SZZP light plus unterstützen, durch die ausschließlich der Konnektor - und explizit nicht der Administrator der Betriebsumgebung - über die Schnittstellen des SZZP light plus Zugang in die geschützten Bereiche der TI bekommen. Die Kopplung muss aktiviert sein, wenn der Highspeed-Konnektor unter einer Anbieterzulassung Highspeed-Konnektor betrieben wird. Die Kopplung MUSS deaktiviert sein, wenn der Highspeed-Konnektor unter einer Anbieterzulassung TI-Gateway betrieben wird. Die Konfiguration MUSS durch den Hersteller erfolgen.**[**<=**]**

A_21882 - Authentisierung für Kopplung von Konnektor und SZZP
Der Konnektor MUSS das Auslösen der Kopplung mit einem SZZP gesondert von der Administrations-Schnittstelle vor Zugriff schützen, sodass dies grundsätzlich von der Rolle des Konnektor-Administrators getrennt werden kann.
[<=**]**

A_21883 - Kopplung von Konnektor und SZZP nur durch Hersteller
Der Hersteller des Konnektors MUSS im Rahmen der Inbetriebnahme des Konnektors die Kopplung zwischen Konnektor und SZZP vornehmen und die Zugangsdaten - vom Konnektor und vom SZZP - für das Auslösen der Kopplung geheim halten.
[<=**]**

TIP1-A_4730-02 - Kommunikation mit NET_TI_GESICHERTE_FD
Der Konnektor MUSS sicherstellen, dass IP-Pakete mit einer Absenderadresse aus dem Adressbereich NET_TI_GESICHERTE_FD verworfen werden, wenn sie nicht vom SZZP der TI stammen.
Der Konnektor MUSS die Kommunikation mit Systemen des Netzwerksegments NET_TI_GESICHERTE_FD für folgende Fälle unterstützen:

- [1] vom Konnektor kommend
- [37] vom Fachmodul kommend

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

- [2] von „Aktive Komponenten" kommend
- [3] in Richtung Konnektor gehend

Der Konnektor MUSS sicherstellen, dass die aus einer unterstützten Kommunikation mit Systemen aus dem Netzwerksegment NET_TI_GESICHERTE_FD bestimmten IP-Pakete ausschließlich zum SZZP der TI geleitet werden.
[<=**]**

TIP1-A_4731-02 - Kommunikation mit NET_TI_ZENTRAL
Der Konnektor MUSS sicherstellen, dass IP-Pakete mit einer Absenderadresse aus dem Adressbereich NET_TI_ZENTRAL verworfen werden, wenn sie nicht vom SZZP der TI stammen.
Der Konnektor MUSS die Kommunikation mit Systemen des Netzwerksegments NET_TI_ZENTRAL für folgende Fälle unterstützen:

- [4] vom Konnektor kommend

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

- [5] von „Aktive Komponenten" kommend
- [6] in Richtung Konnektor gehend

Der Konnektor MUSS sicherstellen, dass die aus einer unterstützten Kommunikation mit Systemen aus dem Netzwerksegment NET_TI_ZENTRAL bestimmten IP-Pakete ausschließlich zum SZZP der TI geleitet werden.
[<=]

TIP1-A_4732-02 - Kommunikation mit NET_TI_DEZENTRAL
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

[<=]

Nachfolgende Anforderung ist durch Prozessprüfung im Rahmen der Anbieterzulassung zu gewährleisten, da die Umsetzung in den Komponenten des Betreibers erfolgt:

TIP1-A_4733-02 - 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 vom SZZP der TI stammen.
Der Konnektor MUSS die Kommunikation mit Systemen des Netzwerksegments ANLW_AKTIVE_BESTANDSNETZE für folgende Fälle unterstützen:

- [10] vom Konnektor kommend nur für die DNS-Namensauflösung mittels DNS_SERVERS_BESTANDSNETZE
- [11b] 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 angeschlossene Netze des Gesundheitswesens mit WANDA Basic (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 zum SZZP der TI geleitet werden.
[<=]

Die Namensauflösung für Bestandsnetze durch den HSK ist dann relevant, wenn Clients keine Namensauflösung im Internet machen können.

TIP1-A_4797-04 - HSK: DNS-Forwards des DNS-Servers
Der DNS-Server des Highspeed-Konnektors MUSS die folgenden DNS-Forwards durchführen:

Tabelle 1: TAB_KON_687_03 DNS-Forwards des DNS-Servers

Domain	Forwarders	Bemerkungen
Namensraum TI, *.DNS_TOP_LEVEL_DOMAIN_TI	DNS_SERVERS_TI	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).
Namensraum TI, Top Level Domains ti-wa (PU) und ti-wa-test (RU und TU).	DNS_SERVERS_TI	DNS Forward Rule zur Auflösung aller DNS-Namen innerhalb des Namensraums der TI mit der Top Level Domains ti-wa (für die PU) und ti-wa-test (für die RU und TU).
Lokale Zone „konlan.“	autoritativer Nameserver des Konnektors	DNS Forward Rule zur Auflösung aller DNS-Namen innerhalb der Zone „konlan.“

[<=]

TIP1-A_4805-03 - HSK: 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 2: TAB_KON_654-02 - Konfigurationsparameter Namensdienst

ReferenzID	Belegung	Bedeutung und Administrator-Interaktion
DNS_SERVERS_TI	Liste von IP-Adressen der DNS-Server	Liste von DNS-Servern, die zur Namensauflösung des Namensraums der TI verwendet werden
DNS_TOP_LEVEL_DOMAIN_TI	DNS Domainname	Top Level Domain des Namensraumes TI

[<=]

Da der Highspeed-Konnektor keinen VPN-Zugangsdienst nutzt, verwendet er auch keine CRL.

TIP1-A_4701-03 - TUC_KON_035 „Zertifikatsdienst initialisieren"
In der Bootup-Phase MUSS der Konnektor den Zertifikatsdienst durch Aufruf des TUC_KON_035 „Zertifikatsdienst initialisieren" initialisieren.

Tabelle 3: TAB_KON_772 TUC_KON_035 „Zertifikatsdienst initialisieren"

Element	Beschreibung
Name	TUC_KON_035 „Zertifikatsdienst initialisieren"
Beschreibung	Der TUC beschreibt den gesamten Ablauf der Initialisierung des TrustStore im Rahmen der betrieblichen Prozesse: Prüfung der Aktualität, Integrität und Authentizität der Einträge im TrustStore.
Auslöser	• Bootup des Konnektors
Vorbedingungen	keine
Eingangsdaten	keine
Komponenten	Konnektor
Ausgangsdaten	• Status der Initialisierung des TrustStore
Nachbedingungen	Keine
Standardablauf	Für den übergebenen Status der Initialisierung des TrustStore werden folgende Schritte durchgeführt: 1. Falls in den letzten 24 Stunden keine Aktualisierung der TSL im Truststore stattgefunden hat, aktualisiert der Konnektor die TSL durch den Aufruf von TUC_KON_032 „TSL aktualisieren".

	2. Falls im Zeitraum von CERT_BNETZA_VL_UPDATE_INTERVAL keine Aktualisierung der BNetzA VL stattgefunden hat, aktualisert der Konnektor die BNetzA VL durch den Aufruf von TUC_KON_031 „BNetzA-VL aktualisieren". 3. Der Konnektor prüft die Gültigkeitsdauer der Zertifikate aller gesteckten Karten (inkl. gSMC-K bzw. Konnektor-Identitäten im HSM) mittels Aufruf von: für gSMC-K TUC_KON_033{checkSMCK; doInformClients=Ja; crypt = ECC} TUC_KON_033{checkSMCK; doInformClients=Ja; crypt = RSA} für jede gesteckte G2.0 Karte TUC_KON_033{cardSession; doInformClients=Ja; crypt = RSA} für jede gesteckte ab G2.1 Karte TUC_KON_033{cardSession; doInformClients=Ja; crypt = ECC} TUC_KON_033{cardSession; doInformClients=Ja; crypt = RSA} 4. Der Konnektor liest von der gSMC-K bzw. vom HSM den öffentlichen Schlüssel des CVC-Root-Zertifikats und speichert diesen im TrustStore [gemSpec_gSMC-K_ObjSys#5.3.10].
Varianten/ Alternativen	Keine
Fehlerfälle	Keine
Nichtfunktionale Anforderungen	Keine
Zugehörige Diagramme	Keine

Tabelle 4: TAB_KON_605 Fehlercodes TUC_KON_035 „Zertifikatsdienst initialisieren"

Fehlercode	ErrorType	Severity	Fehlertext
Neben den Fehlercodes der aufgerufenen technischen Use Cases können keine weiteren Fehlercodes auftreten.			

[<=]

Da der Konnektor keinen direkten Zugang zum Internet hat, entfällt der TSL-Download aus dem Internet.

TIP1-A_4693-03 - TUC_KON_032 „TSL aktualisieren"
Der Konnektor MUSS den technischen Use Case TUC_KON_032 „TSL aktualisieren" umsetzen.

Tabelle 5: TAB_KON_766 TUC_KON_032 „TSL aktualisieren“

Element	Beschreibung
Name	TUC_KON_032 „TSL aktualisieren“
Beschreibung	Dieser TUC prüft die Aktualität der TSL und initialisiert ggf. den TSL-spezifischen Bereich des TrustStores neu. Zusätzlich wird bei einem Wechsel des TI-Vertrauensankers das neue TSL-Signer-CA-Zertifikat in einem sicheren Speicherort im Konnektor hinterlegt. Im Fall der Veröffentlichung eines CVC-Root-CA-Zertifikats werden das CVC-Root-CA-Zertifikat und die Cross-CV-Zertifikate aus der TSL in den Truststore eingestellt.
Auslöser	• Aufruf durch andere TUCs
Vorbedingungen	• Ein gültiger TI-Vertrauensanker ist vorhanden • Das XML-Schema der TSL-Datei liegt vor
Eingangsdaten	• importedTSL – *optional* (TSL aus aus manuellem Import) (Optional) • baseTime – *optional; default: aktuelles Datum* (Referenzzeitpunkt) () • hashTSL - *optional* (Hashwert-Datei der TSL im System; gilt nur für TSL(ECC-RSA))
Komponenten	Konnektor
Ausgangsdaten	• result (Status der Prüfung) • newHashTSL - *optional; verpflichtend für TSL(ECC-RSA)* (Hashwert-Datei der TSL im System; gilt nur für TSL(ECC-RSA))
Nachbedingungen	• Aktuelle TSL-Informationen inkl. des Vertrauensankers der BNetzA VL und sämtlicher CVC-Root-CA- und Cross-CV-Zertifikate liegen im Truststore vor. • Ein ggf. gelieferter neuer Vertrauensanker der TI ist in einem sicheren Speicherort gespeichert
Standardablauf	1. Der Konnektor prüft und aktualisiert ggf. die TSL durch Aufruf von TUC_PKI_001. Der Konnektor verwendet bei der Aktualisierung der TSL standardmäßig die Download-Punkte in der TI. Der durch den dort aufgerufenen TUC_PKI_011 „Prüfung des TSL-Signer-Zertifikates“ benötigte aktuelle TI-Vertrauensanker befindet sich auf der gSMC-K in der Datei EF.C.TSL_CA_1 oder in einem sicheren Speicherort im Konnektor. Es ist dasjenige Zertifikat zu verwenden, welches zum Referenzzeitpunkt gültig ist

	und ab dem Aktivierungsdatum (`StatusStartingTime` des neuen TSL-Signer-CA-Zertifikats) aktiviert ist. 2. Ggf. vorhandene CVC-Root-CA-Zertifikat und Cross-CV-Zertifikate werden genauso wie und zusammen mit den anderen CA-Zertifikaten aus der TSL extrahiert. 3. Alle Informationen aus der TSL werden im TSL-spezifischen Bereich des TrustStores gespeichert 4. Der Konnektor löst TUC_KON_256 { topic = „CERT/TSL/UPDATED”; eventType = Op; severity = Info; doLog = true; doDisp = false } aus. 5. CERT_CRL_DOWNLOAD_ADDRESS wird mit den CRL-Download-Adressen aus der TSL überschrieben.
Varianten/ Alternativen	(→1) Wird die *importedTSL* manuell übergeben (in den Eingangsdaten), so wird diese statt des Downloads verwendet und an TUC_PKI_001 übergeben. Innerhalb der PKI TUCs findet dann kein Download der TSL statt. (→1) Wird durch den von TUC_PKI_001 aufgerufenen TUC_PKI_013 „Import neuer Vertrauensanker“ ein neuer TI-Vertrauensanker (ein neues TSL-Signer-CA-Zertifikat) in der *importedTSL* gefunden, so wird dieser, wie dort beschrieben, extrahiert und in einem sicheren Speicherort gespeichert. Vor Erreichen des Aktivierungsdatums werden die TSLs ausschließlich mit dem alten TSL-Signer-Zertifikat signiert. Ab dem Aktivierungsdatum werden die TSLs mit einem TSL-Signer-Zertifikat signiert, das von der neuen TSL-Signer-CA ausgestellt wurde.
Fehlerfälle	(→1) Tritt beim manuellen Import der Datei ein Fehler auf, wird TUC_KON_256 { topic = „CERT/TSL/IMPORT“; eventType = Op; severity = Error; parameters = „$Fehlerbeschreibung“; doLog = true; doDisp = false } ausgelöst. Fehlercode 4128. (→1) Tritt beim periodischen Update der TSL beim Aufruf des TUC_PKI_001 oder eines durch ihn aufgerufenen TUCs ein Fehler auf, geht der Konnektor in den Betriebszustand EC_TSL_Update_Not_Successful. Der Konnektor geht erst in den Betriebszustand EC_TSL_Update_Not_Successful, wenn weder der Downloadversuch aus der TI noch der Downloadversuch aus dem Internet erfolgreich war. Die vorhandenen TSL-Vertrauensanker werden weiter verwendet. Fehlercode 4127.

Nichtfunktionale Anforderungen	keine
Zugehörige Diagramme	keine

Tabelle 6: TAB_KON_598 Fehlercodes TUC_KON_032 „TSL aktualisieren"

Fehlercode	ErrorType	Severity	Fehlertext
Neben den Fehlercodes der aufgerufenen technischen Use Cases können folgende weitere Fehlercodes auftreten:			
4127	Security	Error	Import der TSL-Datei fehlgeschlagen
4128	Technical	Error	der manuelle Import der TSL-Datei schlägt fehl

[<=]

Da die Einschränkung des Zugriffs auf die Komponenten in der VAU im Falle eines Hardwaredefekts eine schnelle Reparatur durch den Betreiber verbietet (A_21987), sollte die Verfügbarkeit des Highspeed-Konnektors durch Redundanz abgesichert sein.

A_21884 - Redundanter Aufbau Highspeed-Konnektor
Der Anbieter des Highspeed-Konnektors SOLL die Lösung redundant betreiben, damit bei Ausfall einer technischen Komponente die - zwecks Betreiberausschluss notwendigerweise durch den Hersteller vorzunehmende - technische Wartung nicht zu erhöhten Ausfallzeiten führt.**[<=]**

A_21854 - Nutzung des VSDM-Intermediärs
Der Konnektor MUSS über einen Intermediär auf die VSDM-Dienste zugreifen.**[<=]**

Die Anforderungen zum Ex- und Import werden angepasst, um die Verwendung von Standardkomponenten zu erleichtern:

TIP1-A_4814-02 - Export- Import von Konfigurationsdaten
Der Administrator MUSS die gesamten Konfigurationsdaten des Anwendungskonnektors ex- und importieren können. Dazu gehören die Konfigurationsparameter des Konnektors, die persistenten Daten wie im Informationsmodell des Konnektors (Tabelle TAB_KON_507 Informationsmodell Entitäten) definiert und die Pairing Informationen der Kartenterminals.
Für die Konfigurationsdaten des Netzkonnektors MUSS eine Möglichkeit zur Sicherung und Wiederherstellung existieren.

Der Konnektor MUSS sicherstellen, dass der Exportvorgang nur von einem am Konnektor angemeldeten User mit mindestens der Rolle Administrator ausgelöst werden kann.
Der Konnektor MUSS sicherstellen, dass der Importvorgang nur von einem am Konnektor angemeldeten User mit der Rolle Super-Administrator ausgelöst werden kann.
Sowohl Ex- als auch Import MÜSSEN protokolliert werden durch TUC_KON_271 „Schreibe Protokolleintrag" {
topic = „MGM/CONFIG_EXIMPORT";
eventType = Op;
severity = Info;
parameters = („User=$AdminUsername,
Mode=[Export/Import]")}.

[<=]

A_22338 - Tägliche Aktualisierung der TSL
Der Highspeed-Konnektor MUSS täglich durch Aufruf von TUC_KON_032 die TSL aktualisieren**[<=]**

5.1.1 Schnittstellen

Der Highspeed-Konnektor stellt für den LE exakt die selben Schnittstellen bereit wie ein Einbox-Konnektor. Dies betrifft also die SOAP- und LDAP-Operationen. Der Netzwerkverkehr zu offenen Diensten, kann durch den Highspeed-Konnektor oder direkt über den SZZP (light) geroutet werden. Für den Administrator gibt es die Administrationsschnittstelle wie beim Einbox-Konnektor. Zusätzlich gibt es eine Administrationsschnittstelle nur für den Hersteller die zur Kopplung mit dem SZZP und ggf. dem HSM dient (siehe A_21883). Es sind keine weiteren Schnittstellen gestattet.

A_21988-01 - Highspeed-Konnektor - Keine zusätzlichen Schnittstellen
Der Highspeed-Konnektor DARF NICHT Schnittstellen besitzen, die ein Einbox-Konnektor nicht auch besitzt, sofern diese nicht explizit gefordert oder erlaubt sind. Dies betrifft auch Zugänge die ggf. durch die Server-Hardware-Basis grundsätzlich gegeben wären. Der Highspeed-Konnektor verhält sich nach außen in der Art seiner Schnittstellen somit wie ein Einbox-Konnektor.
[<=]

5.1.2 Sichere Trennung von logischen Konnektorinstanzen

Der Highspeed-Konnektor kann mehrere einzelne Konnektorinstanzen virtualisieren. Die Virtualisierung muss dazu genutzt werden, Wechselwirkung zwischen den Instanzen zu unterbinden. Das gilt innerhalb des Highspeed-Konnektors für die Virtualisierung einzelner Dienste als auch bei der Adressierung vollständiger Konnektorinstanzen durch den Nutzer. Solch eine Virtualisierung muss dazu genutzt werden, die Mandantentrennung abzusichern.

A_22041 - Highspeed-Konnektor: Sichere Trennung virtueller Instanzen
Der Highspeed-Konnektor MUSS virtuelle Instanzen von Konnektoren sicher voneinander trennen, sodass zum einen kein Zugriff von einer Instanz auf die andere möglich ist und zum anderen eine feste Zuordnung von Mandanten zu Konnektorinstanzen durchgesetzt wird.**[<=]**

TIP1-A_4820-02 - HSK: Instanzen erstellen und löschen
Der HSK, der virtuelle Instanzen unterstützt, MUSS über eine Administratorrolle verfügen, die eine virtuelle Instanz in einem HSK löschen und erstellen kann. Der HSK MUSS es ermöglichen, diese Rolle von der Administration innerhalb einzelner HSK-Instanzen zu trennen.
Beim Löschen einer HSK-Instanz muss die gesamte Konfiguration dieser Instanz und alle internen Speicher, Protokolle inklusiv der Sicherheitsprotokolle sowie der Vertrauensraum inklusiv der CERT_IMPORTED_CA_LIST gelöscht werden.
Das Löschen der HSK-Instanz MUSS zusammen mit dem username des auslösenden Administrators im HSK protokolliert werden.
Beim Erstellen einer HSK-Instanz MUSS beim Start der Instanz der aktuelle

Vertrauensraum eingebunden werden.
[<=]

A_23159 - Prozess zum Erstellen und Löschen von HSK-Instanzen
Der Betreiber des HSK MUSS einen Prozess etablieren, der den Auftrag zum Erstellen und Löschen einer HSK-Instanz, dessen Prüfung und dessen Umsetzung mit den dabei beteiligten Personen dokumentiert. Der Prozess muss geeignet sein, die unberechtigte Löschung von Instanzen zu verhindern.**[<=]**

5.1.3 Administration und Betriebsfunktionen

A_23359 - Administration des HSK-Basis Systems
Der Highspeed-Konnektor MUSS eine Administration für das Basissystem bereitstellen und folgende separate Administratoren-Rollen umsetzen:

- Hersteller (HSK-Basis)
  - Aktivierung der kryptographischen Kopplung zum SZZP-light-plus
  - Konfiguration des Schlüssels für die Verbindung zum SZZP-light-plus
  - Konfiguration der Kopplung zum HSM und Management HSM
  - Leserechte auf das Logging des Basissystems ohne die Logs der HSK-Instanzen
  - Nutzer mit Rolle "Hersteller" erzeugen/ändern/löschen
- Basissystem-Administrator
  - Verwaltung der instanzenübergreifenden HSK-Konfigurationen inkl. Einspielen Updates
  - Ressourcenkonfiguration von HSK-Instanzen
  - Leserechte auf das Logging des Basissystems ohne die Logs der HSK-Instanzen
  - Backup/Restore von HSK-Instanzen (Snapshots)
  - Löschen von HSK-Instanzen
  - Nutzer mit Rolle "HSK-Admin" erzeugen/ändern/löschen
  - im technisch unterstützten 4 Augenprinzip Nutzer mit Rolle "Zugangsmodul" erzeugen/ändern/löschen
- Zugangsmodul (technischer user)
  - Erzeugen und löschen von HSK-Instanzen
  - Zuordnen von IP-Adressen zu Konnektor-Instanzen
  - Backup/Restore von HSK-Instanzen
  - Ressourcenkonfiguration von HSK-Instanzen

[<=]

TIP1-A_4810-02 - Benutzerverwaltung der Managementschnittstelle
HSK-Instanzen MÜSSEN eine Benutzerverwaltung für die Managementschnittstelle enthalten, in der anmeldeberechtigte Administratoren-Benutzer definiert werden können. Die Benutzerverwaltung MUSS die Administrator-Rollen Lokaler-Administrator und Super-

Administrator unterstützen.
Die Benutzerverwaltung kann weitere Rollen unterstützen.
Den Administrator-Rollen MÜSSEN folgende Rechte zugewiesen sein:

- Lokaler-Administrator:
  - ausschließlicher Zugriff über lokalen Endpunkt der Managementschnittstelle
  - Verwaltung aller Konfigurationsdaten und Durchführung aller Administratoraktionen mit Ausnahme von:
    - Benutzerverwaltung gemäß Tabelle TAB_KON_655
- Remote-Administrator:
  - ausschließlicher Zugriff über remote-Endpunkt der Managementschnittstelle
  - Verwaltung aller Konfigurationsdaten und Durchführung aller Administratoraktionen mit Ausnahme von:
    - Benutzerverwaltung gemäß Tabelle TAB_KON_655
    - Konfigurationseinstellungen und Administratoraktionen gemäß Tabelle TAB_KON_851
- Super-Administrator:
  - ausschließlicher Zugriff über lokalen Endpunkt der Managementschnittstelle
  - Benutzerverwaltung gemäß Tabelle TAB_KON_655
  - Verwaltung aller Konfigurationsdaten und Durchführung aller Administratoraktionen

Tabelle 7: TAB_KON_655 Konfigurationen der Benutzerverwaltung (Super-Administrator)

ReferenzID	Belegung	Bedeutung und Administrator-Interaktion
MGM_USER_LIST	Liste von Benutzernamen und deren Kontaktdaten	Liste von Benutzern und deren Kontaktdaten. Benutzerkonten MÜSSEN angelegt, geändert und gelöscht werden können. Das Passwort eines Benutzerkontos MUSS neu gesetzt werden können.
MGM_ADMIN_RIGHTS	Liste von Zugriffsrechten eines Benutzers	i. Eindeutige Zuordnung eines Benutzerkontos zu einer Rolle. Die Benutzerverwaltung MUSS sicherstellen, dass zu jeder Zeit mindestens ein Benutzerkonto mit der Rolle Super-Administrator vorhanden ist. Gewähren/Entziehen von Rechten für Benutzerkonten: ii. Zugriffsrechte bezüglich der Konfigurationsbereiche. iii. Recht zum Aufbau einer Remote-Management-Session und/oder zur Konfiguration des Remote-Management gemäß TAB_KON_663 (USER_INIT_REMOTESESSION). iv. Recht für einen Werksreset (USER_RESET_PERMISSION)

Die Benutzerverwaltung MUSS es jedem Benutzer ermöglichen Konfigurationsänderungen gemäß Tabelle TAB_KON_656 vorzunehmen:

Tabelle 8: TAB_KON_656 Konfigurationen der Benutzerverwaltung

ReferenzID	Belegung	Bedeutung und Administrator-Interaktion
MGM_USER_INFO	Kontaktdaten	Der angemeldete Benutzer MUSS seine Kontaktdaten ändern können. Der Benutzername DARF NICHT änderbar sein.

[<=]

A_23258 - Rollenausschlüsse Highspeedkonnektor
Der Highspeed-Konnektor MUSS folgende Einschränkungen bei der Zuordnung von Rollen zu Nutzern durchsetzen:

- Ein Nutzer mit der Rolle Hersteller darf keine andere Rolle haben.
- Ein Nutzer mit der Rolle Zugangsmodul darf keine andere Rolle haben.

[<=]

A_23395 - Backup & Restore von Instanzen (Konfigurationsdaten)
Der Highspeed-Konnektor MUSS ein Backup und Restore der Konfigurationen seiner Instanzen ermöglichen, wobei die Backups entweder den HSK (und seine VAU) nicht verlassen oder mit Schlüsselmaterial des HSK oder der SMC-B hinsichtlich Vertraulichkeit und Integrität so geschützt sind, dass diese nicht unberechtigt eingesehen oder geändert werden dürfen. Unberechtigt ist jeder außer der Inhaber der Instanz (LEI) und der ggf. von ihm berechtigte DVO.**[<=]**

A_23397 - Sicherung und Wiederherstellung HSK-Basissystem
Der HSK MUSS eine Möglichkeit bieten, die Konfiguration oder den Systemzustand des Basissystems zu sichern und wieder herzustellen.
[<=]

A_23477 - Protokollierung Infomodell - Clientsysteme
Der HSK MUSS im Sicherheitsprotokoll der jeweiligen Instanz protokollieren, wenn ClientsystemIDs und ClientsystemCredentials konfiguriert, geändert oder gelöscht werden.**[<=]**

5.1.3.1 Eingeschränkte Nutzung des KSR

Der Highspeed-Konnektor nutzt den KSR um Updates für Kartenterminals zu laden und auf angeschlossenen Kartenterminals zu installieren. Die Software des Highspeed-Konnektors wird nicht über den KSR aktualisiert, sondern durch Upload am Highspeed-Konnektor. Der Highspeed-Konnektor kann in Teilen aktualisiert werden, bspw. das zugrundeliegende Betriebssystem oder die Virtualisierungsfunktionalität unabhängig vom eigentlichen Anwendungskonnektor. In jedem Fall muss die Integrität und Authentizität der Highspeed-Konnektor-Updates vor deren Anwendung geprüft werden.

TIP1-A_4832-03 - TUC_KON_280 „Konnektoraktualisierung durchführen“
Der Highspeed-Konnektor MUSS den technischen Use Case TUC_KON_280 „Konnektoraktualisierung durchführen“ umsetzen.

Tabelle 9: TAB_KON_664 – TUC_KON_280 „Konnektoraktualisierung durchführen“

Element	Beschreibung
Name	TUC_KON_280 „Konnektoraktualisierung durchführen“
Beschreibung	Dieser TUC aktualisiert den Konnektor oder Teile des Konnektors mit einem Update, dessen Update-Dateien direkt übergeben wurden
Auslöser	• Der Administrator hat ein lokales Updatepaket bezogen und zur Anwendung übergeben.
Vorbedingungen	
Eingangsdaten	• Updatepaket (herstellerspezifisch, von lokaler Datenquelle, mit enthaltenen FirmwareFiles)
Komponenten	Konnektor,
Ausgangsdaten	Keine
Nachbedingungen	Der Konnektor arbeitet basierend auf der übergebenen, im Updatepaket enthaltenen neuen Version.
Standardablauf	Der Konnektor MUSS das zur Anwendung übergebene Updatepaket wie folgt anwenden: 1. Integrität und Authentizität jeder der Im Updatepaket enthaltenen FirmwareFiles prüfen (Mechanismus ist herstellerspezifisch) 2. Bei Aktualisierung des Anwendungskonnektors: Prüfen auf Zulässigkeit des Updates basierend auf der Firmware-Gruppe (siehe [gemSpec_OM#2.5] Bei Aktualisierung der zugrundeliegenden Systemanteile: Prüfung auf Basis eines herstellerspezifischen Mechanismus, dass alte, ggf. Schwachstellen aufweisende Versionen nicht erneut eingespielt werden können. (Der Rollback bei Fehlern im Update-Prozess ist davon ausgenommen.) 3. Anwenden der zur Verfügung stehenden FirmwareFiles a. Herstellerspezifischer Mechanismus zur Aktualisierung der internen Konnektorsoftware durch die FirmwareFiles inklusive anschließender Prüfung auf Erfolg. b. Bestehende Konfigurationsdaten des Konnektors MÜSSEN erhalten bleiben und sofern erforderlich und möglich automatisch auf die Definitionen der neuen Firmware angepasst werden.

	c. Ist ein händischer Anpassungs- oder Ergänzungsbedarf der Konfigurationsdaten erforderlich, so MUSS der Administrator hierüber geeignet informiert werden
Varianten/Alternativen	
Fehlerfälle	(→1) Integritätsprüfung eines FirmwareFiles fehlgeschlagen, Fehlercode: 4183 (→ 2) Firmwaregruppenprüfung fehlgeschlagen, Fehlercode: 4185 (→3a) Interne Aktualisierung fehlgeschlagen, dann: 1. Rollback auf vorherige Version 2. Abbruch mit Fehlercode: 4184
Nichtfunktionale Anforderungen	
Zugehörige Diagramme	

Tabelle 10: TAB_KON_665 Fehlercodes TUC_KON_280 „Konnektoraktualisierung durchführen"

Fehlercode	ErrorType	Severity	Fehlertext
Neben den Fehlercodes der aufgerufenen technischen Use Cases können folgende weitere Fehlercodes auftreten:			
4183	Security	Error	Integritätsprüfung UpdateFiles fehlgeschlagen.
4184	Security	Error	Anwendung der UpdateFiles fehlgeschlagen (<Details>).
4185	Security	Error	Firmware-Version liegt außerhalb der gültigen Firmware-Gruppe

[<=]

A_23476 - Zentrale Umsetzung von KSR-Client, NTP und Namensdienst
Der HSK MUSS die Funktionen KSR-Client, NTP und Namensdienst auf zentral für alle HSK-Instanzen oder einen Cache für alle Instanzen implementieren.
[<=]

5.1.4 Integration in das TI-Gateway

Hinweis zum Datenschutz: Der nutzende Leistungserbringer muss mit Vertragsabschluss einwilligen, dass die Daten über seine HSK-Instanzen zugreifbarer SMC-B im TI-Gateway verarbeitet werden und dem Portal-Nutzer der zugeordneten HSK-Instanzen angezeigt werden. Die Daten anderer Karten dürfen vom HSK nicht an das Zugangsmodul gesendet werden.
Durch die obige Anforderung soll die Last auf den zentralen Diensten KSR, NTP und Namensdienst begrenzt werden.

A_23303 - TLS mit Client-Authentisierung verpflichtend für Clientsystemanbindungen
Der Highspeed-Konnektor in einem TI-Gateway MUSS im Modus [ANCL_ TLS_ MANDATORY = enabled] und [ANCL_ CAUT_ MANDATORY = enabled] und [ANCL_ CAUT_ MODE = CERTIFICATE] betrieben werden, was global am Basissystem des HSK durch die Rolle "Hersteller" im Rahmen der Inbetriebnahme konfiguriert werden muss und nicht durch andere Administrator-Rollen (Basissystem-Administrator, Zugangsmodul, Administratoren von HSK-Instanzen) deaktivierbar sein darf.**[<=]**

A_23475 - Nachnutzung HSM durch TI-GW-Zugangsmodul
Der Highspeed-Konnektor in einem TI-Gateway KANN sein HSM dem TI-GW-Zugangsmodul verfügbar machen.**[<=]**

A_23474 - Nachnutzung HSM durch TI-GW-Zugangsmodul - Absicherung und Prüfung
Der Highspeed-Konnektor in einem TI-Gateway MUSS, wenn sein HSM auch für das TI-GW-Zugangsmodul nutzbar ist, diese Schnittstelle absichern, sodass keine Zugriffe auf den HSK oder die Schlüssel des HSK im HSM durch das TI-Gateway oder dessen Betreiber möglich sind, und die Schnittstelle eindeutig als Außenschnittstelle im Rahmen der Sicherheitsnachweisverfahren ausweisen und dort prüfen lassen.**[<=]**

A_23360 - TI-Gateway - Kopplung Zugangsmodul und HSK
Der HSK in einem TI-Gateway MUSS das Zugangsmodul (bzw. Clients in der Rolle "Zugangsmodul") mittels eines beidseitig authentisierten und hinsichtlich Vertraulichkeit und Integrität geschützten Kanals anbinden, wobei der HSK seine, im HSM gespeicherte Identität (z.B. I.AK.AUT) als Server-Authentisierung nutzen muss.**[<=]**

A_23469 - Unterstützung AK.AUT und individuelle Identität an der Management-Schnittstelle
Der Highspeed-Konnektor in einem TI-Gateway MUSS beim initialen Verbindungsaufbau zur Management-Schnittstelle einer HSK-Instanz immer seine AK.AUT Identität als TLS-Server-Identität verwenden und über die Konfiguration der Instanz auch Instanz-individuelle erzeugte (vgl. A_21699*) oder importierte (vgl. A_21697*) Identitäten für die Management-Schnittstelle unterstützen.**[<=]**

A_23432 - Verpflichtendes Auto-Update
Der Highspeed-Konnektor in einem TI-Gateway MUSS im Modus [`MGM_KSR_AUTO_UPDATE`=Enabled] und [`MGM_KSR_UTODOWNLOAD`=Enabled] betrieben werden, was global am Basissystem des HSK durch die Rolle "Hersteller" im Rahmen der Inbetriebnahme konfiguriert werden muss und nicht durch andere Administrator-Rollen (Basissystem-Administrator, Zugangsmodul, Administratoren von HSK-Instanzen) deaktivierbar sein darf.**[<=]**

A_23444 - Verifikation gesteckter SMC-B
Der Highspeed-Konnektor in einem TI-Gateway MUSS von gesteckten und freigeschalteten SMC-B die Gültigkeit und Echtheit prüfen und das Ergebnis der Prüfung für das TI-Gateway-Zugangsmodul zugreifbar machen. Die Prüfung muss die

Zertifikatsprüfung incl OCSP sowie die Verwendung eines Privaten Schlüssels umfassen. Die Prüfung muss nach der Freischaltung sowie einmal täglich erfolgen.**[**<=**]**

A_23446 - Messung von Verfügbarkeitsdaten
Der Highspeed-Konnektor in einem TI-Gateway MUSS Verfügbarkeitsdaten für aller aktiven Kartenterminals, die Erreichbarkeit von KIM und eRP Fachdiensten und freigeschaltete SMC-B erheben und dem TI-Gateway-Zugangsmodul zugreifbar machen. **[**<=**]**

5.1.5 HTTP-Forwarder

Für HSK v1.1.x ist kein vollständiger HTTP-Forwarder gefordert, sondern nur A_23882:

A_23882 - HSK OCSP-Adressierung
Der Highspeed-Konnektor MUSS OCSP-Responder im Namensraum der TI direkt adressieren. OCSP-Anfragen außerhalb des Namensraum MUSS der Highspeed-Konnektor an den OCSP-Proxy der TI-Plattform mit einer neu gebildeten Ziel-URL richten. Die Ziel-URL ist nach folgendem Schema zu bilden:
<URL des OCSP-Proxy>/<bisherige Ziel URL des OCSP Requests>**[**<=**]**

Die URL des OCSP-Proxy kann bei der gematik erfragt werden und über das Basissystem konfigurierbar gemacht werden. Die Parameter `CERT_OCSP_FORWARDER_ADDRESS` und `CERT_OCSP_FORWARDER_PORT` können für die Anzeige genutzt werden.

Für nachfolgende Version des HSK ist ein HTTP-Forwarder umzusetzen:

A_23488 - HSK, http-Forwarder - Funktion
Der http-Forwarder MUSS einen http-Forwarder implementieren, der an ihn gerichtete http-Anfragen in der Funktion eines Forwarding-Proxy weiterleitet und die zurückgelieferten http-Antworten an den Absender sendet.
Alle Anfragen, deren Ziel nicht im Namensraum der TI liegt, MÜSSEN an den OCSP-Proxy der TI-Plattform mit einer neu gebildeten Ziel-URL weitergeleitet werden. Die Ziel-URL ist nach folgendem Schema zu bilden:
<URL des OCSP-Proxy>/<bisherige Ziel URL des OCSP Requests>
[<=**]**

Der HSK muss auf Ebene des Basissystems oder als vorgelagerte Komponente einen http-Forwarder bereitstellen.

Der http-Forwarder dient zur Erschwerung einer Profilbildung unter Ausnutzung von Informationen aus OCSP-Anfragen und der IP-Adresse der HSK-Instanzen. Hierfür fungiert diese Komponente in der Funktion eines http-Forwarding-Proxy, der an ihn gerichtete OCSP-Anfragen an die entsprechenden OCSP-Responder weiterleitet sowie die zurückgelieferten OCSP-Antworten an den Absender sendet.

A_23478 - HSK, http-Forwarder - Absenderadresse
Der http-Forwarder MUSS http-Anfragen mit der IP-Adresse des http-Forwarders als Absenderadresse weiterleiten.**[**<=**]**

A_23479 - HSK, http-Forwarder - kein Cache
Der http-Forwarder DARF Datenverkehr NICHT in einem Cache zwischenspeichern.**[**<=**]**

A_23480 - Anonymisierung
Der http-Forwarder MUSS weitergeleitetem http-Anfragen anonymisieren; insbesondere DARF die IP-Adresse des ursprünglichen http-Klienten NICHT in der weitergeleiteten Anfrage enthalten sein.**[**<=**]**

5.1.6 HSK NTP-Synchronisation

TIP1-A_4793-03 - Konfigurierbarkeit des Konnektor NTP-Servers (Highspeed-Konnektor)
Der Administrator MUSS die in TAB_KON_643-HSK aufgelisteten Parameter über die Managementschnittstelle konfigurieren können.

Tabelle 11: TAB_KON_643-HSK Konfiguration des Konnektor NTP-Servers

ReferenzID	Belegung	Bedeutung
NTP_TIMEZONE	Zeitzone	Der Administrator MUSS die Zeitzone des Konnektors einstellen können. Default-Wert: Central European Time/Mitteleuropäische Zeit (CET/MEZ)
NTP_TIME	Zeit	Der Administrator MUSS die Zeit des Konnektors (NTP_TIME) über die Managementschnittstelle manuell einstellen können.
NTP_SERVER_ ADDR	IP-Adressen	Die Adressen des primären und sekundären Stratum-1-Zeitserver der zentralen TI-Plattform für die Synchronisation mit dem NTP-Server des Konnektors.

[<=]

TIP1-A_4789-02 - Zustandsvariablen des Konnektor Zeitdiensts
TAB_KON_640 listet die zu verwendenden Zustandsvariablen des Konnektor NTP-Servers. Diese Werte DÜRFEN NICHT durch den Administrator geändert werden.

Tabelle 12: TAB_KON_640 Zustandswerte für Konnektor NTP-Server

ReferenzID	Belegung	Zustandswerte
NTP_WARN_PERIOD	30	Anzahl an Tagen nach der ersten erfolglosen Zeitsynchronisierung nach der eine Warnung an den Betreiber erfolgen soll
NTP_GRACE_PERIOD	50	Anzahl an Tagen nach der ersten erfolglosen Zeitsynchronisierung nach welcher der Konnektor in einen kritischen Betriebszustand übergehen muss.
NTP_MAX_ TIMEDIFFERENCE	3600	Maximale Zeitabweichung in Sekunden zwischen Systemzeit und Zeit des Stratum-1-Zeitservers zum Zeitpunkt der Zeitsynchronisierung.

[<=]

GS-A_3942-01 - Produkttyp Highspeed-Konnektor, Stratum 2
Der Produkttyp Highspeed-Konnektor MUSS einen Stratum-2-NTP-Server implementieren, der sich bei bestehender Verbindung mit Stratum-1-NTP-Servern der zentralen TI synchronisieren MUSS.
[<=]

A_24061 - HSK: Konfiguration NTP-Server
Der NTP-Server im HSK MUSS in der Lage sein, sich mit Strata 1 bis 3 zu synchronisieren.**[<=]**

5.1.7 Anforderungen an den Hersteller des HSK

A_23470 - Rollentrennung HSM-Personalisierung und Betrieb TI-Gateway
Der Hersteller des HSK MUSS sicherstellen, dass Personen die an der Personalisierung des HSM des HSK beteiligt sind nicht zeitgleich am Betrieb des TI-Gateways (Rolle Betreiber) beteiligt sind und dass entsprechende Prozesse definiert und etabliert sind, die dies dauerhaft gewährleisten und eine regelmäßige Validierung der Umsetzung durchsetzen. Die Umsetzung des Rollenausschluss MUSS die Weisungsbefugnis von Vorgesetzten berücksichtigen. Das heißt, dass kein Vorgesetzter direkte Weisungsbefugnis sowohl für Personen im Bereich der HSM-Personalisierung des HSK-Herstellers als auch für Personen mit der Rolle Betreiber beim TI-Gateway innehaben darf (ausgenommen ist das Management des Unternehmens).**[<=]**

5.2 Betrieblich

Im Rahmen der Anbieter-/Betreiberzulassung muss nachgewiesen werden:

5.2.1 Betriebsumgebung

5.2.1.1 Initialisierung des Vertrauensraumes

A_22336 - Initialisierung mit ECC-Vertrauensraum
Der Hersteller des Highspeed-Konnektors MUSS diesen mit dem ECC-Vertrauensraum initialisieren.**[<=]**

Wenn keine gSMC-K verwendet wird, soll der initiale Anker für den Vertrauensraum auf dem HSM personalisiert werden.

Es gelten diesbezüglich GS-A_4640 und GS-A_4641 aus gemSpec_PKI.

A_17548-02 - TSL-Signer-CA Zertifikat sicher speichern
Der Konnektor MUSS den aktuellen TI-Vertrauensanker im sicheren Datenspeicher speichern.
[<=]

5.2.1.2 HSM

TIP1-A_4503-03 - Verpflichtung zur Nutzung von gSMC-K oder HSM
Der Konnektor MUSS das geheime Schlüsselmaterial zur Geräteidentität (ID.AK.AUT, ID.SAK.AUT) und der Rolle SAK (C.SAK.AUTD_CVC) über Smartcards des Typs gSMC-K gemäß [gemSpec_gSMC-K_ObjSys] oder ein HSM nutzen. Der Konnektor MUSS mit einer gSMC-K oder einem HSM bestückt sein. Er KANN mit mehr als einer gSMC-K oder HSM bestückt sein.
[<=]

A_17598-01 - Qualität des HSM
Die Highspeed-Konnektoren MÜSSEN privates Schlüsselmaterial zu Zertifikaten der Telematikinfrastruktur in einem HSM, dessen Eignung durch eine erfolgreiche Evaluierung nachgewiesen wurde, integritätsgeschützt und vertraulich speichern. Als Evaluierungsschema kommen dabei Common Criteria oder Federal Information Processing Standard (FIPS) in Frage. Die Prüftiefe MUSS mindestens (a) FIPS 140-2 Level 3, oder (b) Common Criteria EAL 4 entsprechen.
[<=]

Es ist nicht gefordert, das HSM im FIPS-Modus zu betreiben.

A_21885 - Personalisierung des HSM mit Konnektoridentitäten durch Hersteller
Der Hersteller des Konnektors MUSS, wenn er ein HSM für die Speicherung der Konnektoridentitäten verwendet, das HSM mittels sicherer Prozesse und in seiner gesicherten Produktionsumgebung personalisieren.**[<=]**

Entsprechend werden relevante Anforderungen zur Personalisierung einer gSMC-K dem Prüfverfahren Sicherheitsgutachten für den Hersteller des Highspeed-Konnektors zugeordnet. Im Falle der Nutzung von gSMC-Ks sind diese Anforderungen mit einer entsprechenden Begründung als "nicht relevant" im Gutachten zu bewerten.

Die Nutzung eines HSMs für die Identitäten der LEI ist für zukünftige Versionen des Highspeed-Konnektors angedacht. Aktuell müssen hier weiterhin SMC-Bs verwendet werden.

A_22590 - HSK: Kein Abruf von Zertifikatsprofilen C.NK.VPN bei Nutzung HSM
Der Hersteller des Highspeedkonnektors DARF NICHT Zertifikate mit dem Profil C.NK.VPN beziehen, wenn er ein HSM statt einer gSMC-K verwendet und das HSM personalisiert.**[<=]**

A_21987-01 - Zugriff auf das HSM nur durch den Hersteller
Der Highspeed-Konnektor MUSS administrative Zugriffe auf das HSM, die Kopplung mit dem HSM und die Kopplung mit dem SZZP durch andere als den Hersteller unterbinden.
[<=]

A_21886 - Feste Kopplung von Konnektor und HSM
Der Konnektor MUSS, wenn ein HSM verwendet wird, fest kryptographisch mit dem HSM gekoppelt sein, sodass eine hinsichtlich Vertraulichkeit und Integrität geschützte, beidseitig authentisierte Verbindung zwischen Konnektor und HSM besteht und ausschließlich der Konnektor die auf dem HSM gespeicherten Identitäten nutzen kann.
[<=]

5.2.1.3 Vertrauenswürdige Ausführungsumgebung

Die Vertrauenswürdigen Ausführungsumgebung (VAU) dient der datenschutzrechtlich zulässigen und sicheren Verarbeitung von schützenswerten Klartextdaten innerhalb des HSK.

Die VAU ist die Gesamtheit aus der für eine Klartextverarbeitung erforderlichen Software, dem für eine Klartextverarbeitung genutzten physikalischen System sowie den für die Integrität einer Klartextverarbeitung erforderlichen organisatorischen und physischen Rahmenbedingungen.

Die VAU grenzt sich von allen weiteren, im betrieblichen Kontext bei einem Anbieter, der den HSK betreibt, vorhandenen Systemen und Prozessen dadurch ab, dass die sensiblen Klartextdaten von Komponenten innerhalb der VAU aus erreichbar sind oder sein können, während sie dies von außerhalb der VAU nicht sind. Sensible Daten verlassen die VAU ausschließlich gemäß wohldefinierten (Zugriffs-)Regeln und in verschlüsselter Form.

Die schützenswerten sensiblen Daten sind alle Versichertendaten (personenbezogene Daten und Schlüssel), die im HSK verarbeitet werden.

Die VAU muss einen Schutz dieser Daten leisten, der gerade auch gegen Innentätern beim Anbieter/Betreiber wirkt.

Dieser Schutz vor unberechtigtem Zugriff auf schützenswerte Klartextdaten kann auf unterschiedliche Art und Weise erreicht werden. Dabei können technische Maßnahmen in Software (im Code des Produkts oder hardwarenahe Mechanismen), Maßnahmen zum physischen Schutz und organisatorische Maßnahmen genutzt bzw. kombiniert werden. Ein ausschließlich organisatorischer Schutz ist jedoch nie ausreichend, denn es muss wie o.g. stets der Innentäter, der am Betrieb des Produkts beteiligt ist betrachtet werden, der an der Durchsetzung von organisatorischen Maßnahmen beteiligt ist und diese somit ggf. umgehen kann und Zugriff direkt auf die Hardware bekäme.

Auch wenn der Schutz der Daten vorrangig ist, muss dennoch ebenso die Betreibbarkeit der Lösungen mit betrachtet werden. Daher sollen Lösungen ermöglicht werden, bei denen der Betreiber einfache Wartungsarbeiten durchführen kann, ohne dass dafür jedes Mal Ausfallzeiten für das Produkt anfallen. Der dadurch grundsätzlich gegebene Zugriff des Betreibers auf die Hardware, muss für die Auswahl der Schutzmaßnahmen berücksichtigt werden.

Die Anforderungen im Folgenden sollen Herstellern und Anbietern eine gewisse Freiheit bei der Wahl der Maßnahmen geben, jedoch für bestimmte Szenarien detailliertere Vorgaben machen unter denen diese Szenarien dann realisierbar sind. Dies sind dann Anforderungen konkret im Kontext des Highspeed-Konnektors sowie auch dessen Betrieb innerhalb des TI-Gateways.

A_17346-02 - HSK: VAU - Zwingende Verwendung der VAU
Der Highspeed-Konnektor MUSS Schlüssel und Medizinischen Daten eines Versicherten ausschließlich innerhalb der VAU verarbeiten und sie so vor Zugriff durch Unbefugte bei ihrer Verarbeitung im Klartext schützen.
[<=]

A_17347-02 - HSK: VAU - Keine persistente Speicherung von Versichertendaten
Der Highspeed-Konnektors DARF Schlüssel und medizinische Daten eines Versicherten NICHT persistent speichern, auch nicht verschlüsselt.
[<=]

A_17348-02 - HSK: VAU - Schutz ePA-Akten- und Kontextschlüssel
Der Highspeed-Konnektor MUSS sicherstellen, dass die Akten- und Kontextschlüssel der Versicherten die VAU nur verlassen (unabhängig davon, ob sie verschlüsselt oder unverschlüsselt sind), wenn sie ans ePA-Aktensystem übermittelt werden und die Übermittlung zum ePA-Aktensystem in einem sicheren Kanal erfolgt.
[<=]

A_17350-02 - HSK: VAU - Isolation von anderen Datenverarbeitungsprozessen des Anbieters
Der Highspeed-Konnektor MUSS die in der VAU ablaufenden Datenverarbeitungsprozesse von allen sonstigen Datenverarbeitungsprozessen des Anbieters/Betreibers trennen und damit gewährleisten, dass der Anbieter/Betreiber vom Zugriff auf die in der VAU verarbeiteten, schützenswerten Daten ausgeschlossen ist.
[<=]

A_17351-02 - HSK: VAU - Ausschluss von Manipulationen an der Software
Die VAU des Highspeed-Konnektors MUSS die Integrität der eingesetzten Software schützen und damit insbesondere unbemerkte Manipulationen an der Software durch den

Anbieter/Betreiber ausschließen.
[<=]

A_17352-02 - HSK: VAU - Ausschluss von Manipulationen an der Hardware
Die VAU des Highspeed-Konnektors MUSS die Integrität der eingesetzten Hardware schützen und damit insbesondere unberechtigten physischen Zugriff auf die VAU-Hardware und unbemerkte Manipulationen an der VAU-Hardware - auch durch den Anbieter/Betreiber - ausschließen.**[<=]**

A_17353-02 - HSK: VAU - Kontinuierliche Wirksamkeit des Manipulationsschutzes
Die VAU des Highspeed-Konnektors MUSS den Ausschluss von Manipulationen an der Hardware und der Software durch den Anbieter/Betreiber mit Mitteln umsetzen, deren dauerhafte und kontinuierliche Wirksamkeit gewährleistet werden kann.
[<=]

A_17354-02 - HSK: VAU - Physischer Zugang
Die VAU des Highspeed-Konnektors MUSS mit technischen Mitteln sicherstellen, dass kein unberechtigter Zugriff auf die Hardware der VAU möglich ist und dass

a. niemand - berechtigt oder unberechtigt und auch nicht der Anbieter/Betreiber - während der Verarbeitung personenbezogener medizinischer Daten physischen Zugriff auf die Hardware der Systeme erlangen kann, auf denen eine VAU ausgeführt wird
   und / oder
b. auf dem System durch Verschlüsselung auf CPU-Level keine Klartextdaten verarbeitet werden, so dass auch bei physischem Zugriff auf die Hardware
   i. kein Zugriff auf verarbeitete personenbezogenen medizinischen Daten im Klartext möglich ist,
   ii. keine Deaktivierung der Maßnahmen, die vor Zugriff auf Klartextdaten schützen, möglich ist.

Durch die Umsetzung von Punkt b werden berechtigte Zugriffe auf die Systeme durch den Anbieter entsprechend A_24295* möglich.**[<=]**

A_17355-02 - HSK: VAU - Extraktion Klartextdaten bei physischem Zugang unterbinden
Die VAU des Highspeed-Konnektors MUSS mit technischen Mitteln sicherstellen, dass ein physischer Zugang zu Hardware-Komponenten der VAU nur erfolgen kann, wenn gewährleistet ist, dass aus ihnen keine Nutzdaten im Klartext extrahiert werden können. Dies kann erfüllt werden, indem bei physischem Zugang automatisch sämtliche sensiblen Daten aus dem Speicher gelöscht werden oder gar keine Klartextdaten auf dem System verarbeitet werden und dies auch durch physischen Zugang nicht umgangen oder deaktiviert werden kann.**[<=]**

A_17356-03 - HSK: VAU - Löschen aller Daten beim Beenden von Verarbeitungsvorgängen
Die VAU des Highspeed-Konnektors MUSS beim Beenden von Verarbeitungsvorgängen sämtliche Daten dieses Verarbeitungsvorgangs löschen, sobald diese Daten nicht mehr benötigt werden. Insbesondere müssen beim Beenden einer virtuellen HSK-Instanz sämtliche transienten Daten dieser Instanz gelöscht werden. Löschen bedeutet, dass auch keine sensiblen Daten mehr im flüchtigen Speicher gehalten werden. Ein Persistieren von sensiblen Daten ist entsprechend A_17347-* zu keinem Zeitpunkt zulässig.
[<=]

A_17351-01 - HSK: Ausschluss von Manipulationen an der Software der VAU
Die VAU des Highspeed-Konnektors MUSS die Integrität der eingesetzten Software schützen und damit insbesondere Manipulationen an der Software durch den Anbieter/Betreiber ausschließen.
[<=]

A_17352-01 - HSK: Ausschluss von Manipulationen an der Hardware der VAU
Die VAU des Highspeed-Konnektors MUSS die Integrität der eingesetzten Hardware schützen und damit insbesondere Manipulationen an der Hardware durch den Anbieter/Betreiber ausschließen.
[<=]

A_17353-01 - HSK: Kontinuierliche Wirksamkeit des Manipulationsschutzes der VAU
Die VAU des Highspeed-Konnektors MUSS den Ausschluss von Manipulationen an der Hardware und der Software durch den Anbieter/Betreiber mit Mitteln umsetzen, deren dauerhafte und kontinuierliche Wirksamkeit gewährleistet werden kann.
[<=]

A_17354-01 - HSK: Kein physischer Zugang des Anbieters zu Systemen der VAU
Die VAU des Highspeed-Konnektors MUSS mit technischen Mitteln sicherstellen, dass niemand, auch nicht der Anbieter/Betreiber , während der Verarbeitung personenbezogener medizinischer Daten Zugriff auf physische Schnittstellen der Systeme erlangen kann, auf denen eine VAU ausgeführt wird.
[<=]

A_17355-01 - HSK: Nutzdatenbereinigung vor physischem Zugang zu Systemen der VAU
Die VAU des Highspeed-Konnektors MUSS mit technischen Mitteln sicherstellen, dass ein physischer Zugang zu Hardware-Komponenten der Verarbeitungskontexte nur erfolgen kann, nachdem gewährleistet ist, dass aus ihnen keine Nutzdaten extrahiert werden können.
[<=]

A_17356-02 - HSK: Löschen aller Daten beim Beenden des Verarbeitungskontextes
Die VAU des Highspeed-Konnektors MUSS beim Beenden eines Verarbeitungskontextes sämtliche Daten dieses Verarbeitungskontextes sicher löschen.
[<=]

A_23495-01 - HSK: VAU - Protokollierung bei physischem Zugang zu Systemen der VAU
Der Highspeed-Konnektor MUSS sämtliche Zugriffe auf die Hardware der VAU protokollieren - sei es die vorgesehene berechtigte Öffnungen oder das Auslösen der Sensoren/Alarme des physischen Zugangsschutzes (vgl. A_17352-*, A_17354-*, A_17355-*).
[<=]

A_24294 - HSK: VAU - Physischer Zugang bei laufender Verarbeitung
Der Hersteller des Highspeed-Konnektors MUSS, wenn sein HSK-Produkt physischen Zugang zur Hardware bei laufender Datenverarbeitung durch berechtigte Mitarbeiter des Anbieters entsprechend A_17354-* Punkt b zulässt, folgendes umsetzen:

- Dieser Zugang des Anbieters MUSS im Sicherheitskonzept des Herstellers berücksichtigt werden, wobei dies auch Innentäter beim Anbieter einbeziehen muss.
- In den Nutzungsbedingungen für Anbieter (bspw. "Secure User Guidance") MÜSSEN

- die zulässigen Wartungsarbeiten, die der Anbieter durchführen darf, inkl. Maximaldauer benannt werden (diese sind auch konkret im Produktgutachten aufzuführen),
- die für berechtigte physische Zugriffe des Anbieters notwendigen zusätzlichen organisatorischen Maßnahmen definiert werden und
- auf die zwingende Prüfung der Umsetzung dieser zusätzlichen Maßnahmen entsprechend GS-A_4984-01 und A_24295 hingewiesen werden.

[<=]

5.2.1.4 Unabhängigkeit von dem Betreiber des Aktensystems

A_21248-02 - Anbieter HSK - Unabhängigkeit des Betreibers eines ePA-Aktensystems vom Betreiber eines HSK

Der Anbieter des ePA-Aktensystems und der Anbieter des HSK MÜSSEN dafür Sorge tragen, dass ihr beauftragter Betreiber für das ePA-Aktensystem unabhängig vom beauftragten Betreiber des Highspeed-Konnektors ist, d.h. es sind mindestens jeweils eigenständige Rechtspersönlichkeiten mit eigenständigen operativen Geschäfts- und Betriebsführungen und es ist eine strikte Vermeidung von Personenidentitäten bzw. Doppelrollen in den Funktionen Geschäftsführung, leitende Mitarbeiter und Zugangsberechtigte zum Betriebsort des Highspeed-Konnektor bzw. des ePA-Aktensystems gewährleistet.

[<=]

5.2.1.5 Anforderungen aus gemSpec_DS_Anbieter

Grundsätzlich ist der Betrieb des Highspeed-Konnektors in einem Krankenhaus oder einer großen Einrichtung vergleichbar mit dem Betrieb vieler Einbox-Konnektoren, die in der selben Umgebung auch direkt von der Einrichtung, bzw. ihrem Dienstleister betrieben werden. Es erfolgt somit weiterhin ein Betrieb des (Highspeed-)Konnektors durch die Leistungserbringerinstitution. Daher wird trotz der notwendigen Anbieterzulassung für den Anbieter/Betreiber des Highspeed-Konnektors ein nur geringer Umfang der Anforderungen zur betrieblichen Sicherheit gefordert. Dieser umfasst hauptsächlich die Herstellung von direkten Kommunikationswegen mit dem koordinierenden ISMS und Meldungen von Vorfällen an dieses.

5.2.2 ITSM Integration

Der Betreiber des Highspeed-Konnektors nimmt am ITSM teil. Da der Betreiber des Highspeed-Konnektors keinen Service für andere ITSM-Teilnehmer anbietet, gelten nur ein Teil der Anforderungen (siehe Anbietertypsteckbrief).

5.2.2.1 Mitwirkungspflichten ITSM

Für den Betreiber des Highspeed-Konnektors ergeben sich Mitwirkungspflichten am ITSM.

Dafür werden Änderungen an der Tabelle *Tab_KPT_Betr_TI_002 Mitwirkungspflichten der TI-ITSM-Teilnehmer* und zusätzlich an der Tabelle *Tab_KPT_Betr_TI_003 Mitwirkungsverpflichtung im TI-ITSM* aus *[gemKPT_Betr]* vorgenommen.

5.2.3 Auftragsdatenverarbeitung/AVV

A_21989 - Auftragsdatenverarbeitung zwischen LEI und Anbieter Highspeed-Konnektor
Der Anbieter des HSK MUSS, wenn er nicht der nutzende Leistungserbringer ist, mit jeder nutzenden LEI eine Auftragsdatenverarbeitung vertraglich in Form eines AVV nach DSGVO regeln. Diese vertragliche Regelung muss insbesondere auch umfassen, dass der Anbieter oder ein von ihm beauftragter Betreiber nicht auf die fachlichen Anwendungsfälle (SOAP-Operationen) des Konnektors und seiner Fachmodule zugreift.**[**<=**]**

5.2.4 Weitere Betriebliche Anforderungen

Der Highspeed-Konnektor wird im Gegensatz zum Einbox-Konnektor nicht über den VPN-Zugangsdienst, sondern über den SZZP-light+ an die TI angebunden. In dieser Anbindungsvariante wird dem Highspeed-Konnektor keine DNS-Informationen zu den NTP-Servern in der TI bereitgestellt. Deshalb muss der Highspeed-Konnektor die Möglichkeit der manuellen Konfiguration über eine entsprechende Konfigurationsoberfläche bereitstellen.

TIP1-A_4795-03 - TUC_KON_352 „Initialisierung Zeitdienst" (Highspeed-Konnektor)
Der Highspeed-Konnektor MUSS in der Bootup-Phase TUC_KON_352 "Initialisierung Zeitdienst" durchlaufen.

Tabelle 13: TAB_KON_644-HSK – TUC_KON_352 „Initialisierung Zeitdienst"

Element	Beschreibung
Name	TUC_KON_352 „Initialisierung Zeitdienst"
Beschreibung	Der Highspeed-Konnektor muss zum Bootup den konnektoreigenen NTP-Server mit einem NTP-Server der zentralen TI-Plattform synchronisieren. falls MGM_LU_ONLINE=Enabled.
Anwendungsumfeld	Synchronisierung der Systemzeit zur Startzeit
Eingangsanforderung	Keine
Auslöser	• Bootup • Event NETWORK/VPN_TI/UP
Vorbedingungen	Verbindung zum VPN-Konzentrator zur TI muss aufgebaut sein

Eingangsdaten	NTP-Server der zentralen TI-Plattform
Komponenten	Highspeed-Konnektor
Ausgangsdaten	Keine
Standardablauf	Falls MGM_LU_ONLINE=Enabled: • Der Highspeed-Konnektor verwendet die konfigurierten Adressen der NTP-Server der zentralen TI-Plattform (NTP_SERVER_ ADDR) • gemäß [NTPv4] • Falls keine Antwort erfolgt ist oder falls der Zeitserver nicht erreichbar ist, wird Fehler 4177 ausgelöst. Zur Feststellung werden die NTPv4 eigenen Timeoutwerte berücksichtigt.
Varianten/Alternativen	Keine
Fehlerfälle	4177: Der NTP-Server des Highspeed-Konnektors empfängt keine Systemzeit
Nichtfunktionale Anforderungen	Keine
Zugehörige Diagramme	Keine

Tabelle 14: TAB_KON_645-HSK Fehlercodes TUC_KON_352 „Initialisierung Zeitdienst"

Fehlercode	ErrorType	Severity	Fehlertext
4177	Technical	Warning	Der NTP-Server des Highspeed-Konnektors konnte nicht synchronisiert werden.

[<=]

TIP1-A_5152-01 - Aktualisieren der Infrastrukturinformationen aus der TI
Der Betreiber des Highspeed-Konnektors MUSS einen Prozess etablieren, mit dem Änderungen in der Bestandsnetze.xml innerhalb von einem Arbeitstag umgesetzt werden können.
[<=]

Dieser betriebliche Prozess sollte vom Highspeed-Konnektor folgendermaßen unterstützt werden:

A_22571 - Benachrichtigung und Bereitstellung der Bestandsnetze.xml
Der Highspeed-Konnektor KANN eine Benachrichtigung des Betreibers über eine neue Bestandsnetze.xml und die Bereitstellung der heruntergeladenen Bestandsnetze.xml für den Betreiber umsetzen.**[<=]**

5.2.4.1 Betriebsdatenmeldedienst

Der Highspeed-Konnektor liefert wie auch schon der Konnektor Betriebsdaten gemäß des vereinbarten Datennutzungskonzeptes und nutzt dazu das gleiche Schema „conn/OperatingData.xsd".

A_23764-01 - Highspeed-Konnektor:Betriebsdaten - Konfiguration CI-ID und URL-Schnittstelle ContentUploadXML
Der Anbieter Highspeed-Konnektor MUSS die folgenden Parameter des Highspeed-Konnektor-Basissystems konfigurieren:

- Configuration-Item Identifier (CI-ID*)
- URL zu der Schnittstelle I_OpsData_Update::contentUploadXML nach Vorgabe der gematik

*<CI-ID> = Identifiziert die Produktinstanz, siehe Anforderung [A_17764 - Verwendung CI-ID] in [gemRL_Betr_TI#6.1.1]
[<=]

A_23769-01 - Highspeed-Konnektor: Betriebsdaten - Konfiguration Betriebsstättenart
Der Highspeed-Konnektor MUSS die Konfiguration der Betriebsstättenart gemäß Vorgaben zum Element SiteType aus dem Schema „conn/OperatingData.xsd" durchsetzen. Der Konnektor KANN die Einstellung entweder als einfache Auswahlliste in der Managementoberfläche der Highspeed-Konnektor-Instanz konfigurierbar bereit stellen (die Konfiguration muss initial leer sein und der Highspeed-Konnektor MUSS durchsetzen, dass die Konfiguration ausgeführt wird) oder er KANN die Information automatisch aus der Profession-OID der SMC-B gemäß GS-A_4443* ermitteln.
Wenn der Konnektor die Information automatisch aus der Profession-OID der SMC-B ermittelt, MUSS er folgendes Mapping der Profession-OID auf das Element SiteType aus dem Schema „conn/OperatingData.xsd" vornehmen:

Tabelle 15: TAB_KON_940 Mapping Profession-OID auf SiteType

Profession-OID	SiteType
1.2.276.0.76.4.50	ARZTPRAXIS
1.2.276.0.76.4.51	ZAHNARZTPRAXIS
1.2.276.0.76.4.53	KRANKENHAUS
1.2.276.0.76.4.54 1.2.276.0.76.4.55 1.2.276.0.76.4.56	APOTHEKE
alle anderen OIDs	SONSTIGE

Wenn der Konnektor die Information automatisch aus der Profession-OID der SMC-B ermittelt und dabei mehrere SMC-Bs vorfindet, MUSS er die OIDs aller SMC-Bs auslesen, jeweils den SiteType festlegen und als Betriebstättenart den ermittelten SiteType mit der höchsten Position in der folgenden Liste setzen:

1. KRANKENHAUS
2. ARZTPRAXIS oder ZAHNARZTPRAXIS (gleichgestellt)
3. APOTHEKE
4. SONSTIGE

[<=]

A_23846-01 - Highspeed-Konnektor:Betriebsdaten - Konfiguration CI-ID
Der Highspeed-Konnektor MUSS die Configuration-Item Identifier (CI-ID*) im Highspeed-Konnektor-Basissystem konfigurierbar als Datentyp String bereit stellen.

*<CI-ID> = Identifiziert die Produktinstanz, siehe Anforderung [A_17764 - Verwendung CI-ID] in [gemRL_Betr_TI#6.1.1]
[<=]

A_23847-01 - Highspeed-Konnektor:Betriebsdaten - Konfiguration URL Schnittstelle ContentUploadXML
Der Highspeed-Konnektor MUSS die URL zu der Schnittstelle I_OpsData_Update::contentUploadXML im Highspeed-Konnektor-Basissystem konfigurierbar als Datentyp String bereit stellen.
[<=]

Mit der Konfigurierbarkeit in A_23764*, A_23846* und A_23847* ist beispielsweie eine Einstellung in der Managementoberfläche oder eine Konfigurationsdatei gemeint.

A_23761 - Highspeed-Konnektor:Betriebsdaten - Bereitstellung von Betriebsdaten - Basissystem
Die Highspeed-Konnektor-Instanz MUSS Betriebsdaten, reduziert um die folgenden Werte

- ContractID
- UpdateMode
- TI-Connection Mode
- Internetmode
- Connector::VPNTISTATUS
- Connector::VPNSISStatus
- TrustStatus::CRL

und ergänzt um die Betriebsstättenart täglich an die Betriebsdatenerfassung gemäß [gemSpec_SST_LD_BD] an die Schnittstelle I_OpsData_Update::contentUploadXML übermitteln.
Den Configuration-Item Identifier (CI-ID*) und die URL zu der Schnittstelle I_OpsData_Update::contentUploadXML ermittelt die Highspeed-Konnektor-Instanz aus der Konfiguration des Highspeed-Konnektor-Basissystems.

*<CI-ID> = Identifiziert die Produktinstanz, siehe Anforderung [A_17764 - Verwendung CI-ID] in [gemRL_Betr_TI#6.1.1]**[<=]**

A_21137 - Konnektor:Betriebsdaten - Formatierung der Betriebsdaten
Der Konnektor MUSS die Betriebsdaten als XML-Dokument gemäß dem Schema „`conn/OperatingData.xsd`“ mit

- dem MimeType "text/xml" und
- dem Type "OperatingDataConnector"

senden.**[<=]**

A_21225 - Konnektor:Betriebsdaten - Annotations im XML-Schema
Der Konnektor MUSS die XML Elemente der Betriebsdaten gemäß der Annotations im Schema OperatingData.xsd befüllen.**[<=]**

A_23762 - Highspeed-Konnektor:Betriebsdaten - Fehlerbehandlung
Liefert I_OpsData_Update einen Fehler, MUSS der Highspeed-Konnektor das Senden der Betriebsdaten 3 Mal im Abstand von 5 Minuten erneut versuchen.
[<=]

A_23763 - Highspeed-Konnektor:Betriebsdaten - contentUploadXML nicht vorhanden
Meldet I_OpsData_Update, dass die Schnittstelle contentUploadXML nicht vorhanden ist, DARF der Konnektor die Operation NICHT sofort wiederholen. Erst zum nächsten regulären Termin soll wieder gesendet werden.
[<=]

A_23857 - Highspeed-Konnektor:Betriebsdaten - Vermeiden von Spitzenlasten beim Senden von Betriebsdaten
Der Highspeed-Konnektor MUSS Spitzenlasten durch paralleles Senden von Betriebsdaten vermeiden.
Dazu MÜSSEN die im Einsatz befindlichen Highspeed-Konnektoren eines Herstellers ihre Sende-Versuche gleichmäßig über den Tag verteilen.
[<=]

A_21140 - Konnektor:Betriebsdaten - Keine personenbezogenen und medizinischen Daten senden
Der Konnektor DARF NICHT personenbezogene, personenbeziehbare oder medizinische Daten senden.**[<=]**

6 Test Konzept

Für den Highspeed-Konnektor gelten neben den gewohnten Anforderungen aus gemKPT_Test, die sich an dezentrale Komponenten richten, weitere Anforderungen, die sich ergeben, wenn der Highspeed-Konnektor in RU und TU nicht physikalisch in der gematik verfügbar ist.

6.1 Zugang und Verfügbarkeit

Der Hersteller eines Highspeedkonnektors muss der gematik mindestens fünf (virtuelle) Instanzen des Highspeedkonnektors für Testzwecke exklusiv zur Verfügung stellen. Einzelne Hardwarekomponenten (z.B. SZZP, HSM) können mit anderen Instanzen geteilt werden, wenn eine logische Trennung erfolgt. Wenn unterschiedliche Versionen testrelevant sind, sollen hierfür eigene virtuelle Instanzen bereitgestellt werden. Eine Instanz des Highspeedkonnektors muss mit der TU der TI verbunden sein. Die Nutzung eines Intermediärs muss herstellerseitig gewährleistet werden. Die vier weiteren Instanzen müssen mit dem SZZP der lokalen Testumgebung der gematik verbunden werden.

Der Hersteller muss der gematik einen VPN Zugang zum Highspeedkonnektor ermöglichen, über den die Clientsystemschnittstellen, die Admin-Schnittstellen und die Kartenterminal-Schnittstellen zugänglich sind. Für die vier Instanzen des Highspeedkonnektors, welche mit dem SZZP der lokalen Testumgebung der gematik verbunden sind, muss auch der ganze Netzwerkverkehr Richtung TI (über den SZZP) über den VPN Tunnel zur gematik ermöglicht werden.

Der Hersteller muss der gematik einen Admin-Zugang ermöglichen, über den die Konfigurations- und Überwachungstätigkeiten des Betreibers und DVOs möglich sind, insbesondere zur Einrichtung von Clientsystemen und Kartenterminals sowie Logeinsichten. Außerdem muss der Hersteller es der gematik ermöglichen, Dateien (z.B. TSL, BNetzA-VL, Zertifikate) über die Adminoberfläche des Highspeedkonnektors einzuspielen.

Die REST-Schnittstelle zur Administration des Highspeedkonnektors, muss der gematik offengelegt und zugängig gemacht werden.

A_22577 - Highspeed-Konnektor: Bereitstellung TU-Anbindung
Der Hersteller eines Highspeed-Konnektors MUSS die Anbindung seines Produktes an die TU über einen SZZP inklusive vollständiger Erreichbarkeit aller Dienste bereitstellen.**[**<=**]**

A_22574 - Zugang zum Highspeed Konnektor
Der Hersteller eines Highspeed-Konnektors MUSS nach der Anbindung seines Produktes in der TU dem Test der gematik einen Zugang auf die Managementschnittstelle zu seinem Produkt einrichten.**[**<=**]**

TIP1-A_2805 - Zeitnahe Anpassung von Produktkonfigurationen
Der Hersteller oder Anbieter von Produkten MUSS sicherstellen, dass in der Testumgebung die Produkte (außer Smartcards) sich in ihren Konfigurationen zeitnah (möglichst kleiner 1 Arbeitstag) anpassen lassen.**[**<=**]**

6.2 Logging

TIP1-A_7330 - Tracedaten von echten Außenschnittstellen
Die testdurchführende Instanz SOLL seine eigenverantwortlichen Tests an den Außenschnittstellen des Testobjekts und nicht an internen Loopback Devices durchführen.
[<=]

TIP1-A_7331 - Bereitstellung von Tracedaten an Außenschnittstelle
Die testdurchführende Instanz SOLL bei eigenverantwortlichen Tests an denen an der Außenschnittstelle des Produkts Daten transferiert werden der gematik einen Mitschnitt zur Verfügung stellen, der die folgenden Punkte erfüllt:
• vollständig sein (komplette Paketgröße und gesamte MTU-Size)
• tatsächlichen Daten (insbesondere Messdaten, wie z. B. Zeitstempel) enthalten
• ein auswertbares Format, (z. B. pcap oder pcapng) haben
• und bei Mitschnitt verschlüsselter Protocol-Layer (z.B. TLS-Layer) und Nutzung eines Simulators als Peer, das Mastersecret als separate Datei bereitstellen.
[<=]

6.3 Interoperabilität

TIP1-A_6529 - Produkttypen: Mindestumfang der Interoperabilitätsprüfung
Die testdurchführende Instanz (TDI) MUSS zum Nachweis der Interoperabilität alle für das jeweilige Produkt relevanten anwendungsfallbasierten Tests mit der Mindestanzahl von Produkten gemäß Tabelle 13: Tab_Test_033 Mindestumfang der Interoperabilitätsprüfung durchführen.**[<=]**

Es werden Änderungen an der Tabelle *Tab_Test_033 Mindestumfang der Interoperabilitätsprüfung* aus *[gemKPT_Test]* vorgenommen.

Tabelle 16: Tab_Test_033(_HSK) Mindestumfang der Interoperabilitätsprüfung

Zu testendes Objekt:	eGK G2[1]	eGK G2.1[13]	SMC-B	HBA	ZOD	HBA-qSig	Primärsystem	E-Mail-Client (auch PVS)	Web-Browser	Clientmodul KIM	eHealth-KT[12]	Konnektor	Konnektor-Highspeed	VPN-ZugD	Zentrales Netz TI	Namensdienst	Zeitdienst	TSL-Dienst	KSR	Störungsampel	OCSP-Datenbereitstellung	TSP X.509 nonQES	TSP X.509 QES	Intermediär VSDM	VSDM-FD	SG Bestandsnetze	Fachdienst KIM	Verzeichnisdienst	KTR-AdV	ePA-Aktensystem	ePA-Frontend des Versicherten	Schlüsselgenerierungsdienst	Signaturdienst	E-Rezept Fachdienst	IDP-Dienst	Sektorale IDP	E-Rezept FdV	Apothekenverzeichnisdienst
Konnektor (PTV4)	2	1	2	2	1[18]	1[18]	3			1[18]	3[18]	2[2]	ffpvt	1				1	1		1	1	1	1	3			1		3[18]	2[7,18]	1						
Konnektor (PTV4+)	2	1	2	2	1[18]	1[18]	3			1[18]	3[18]	2[2]	ffpvt	2				1	1		1	1	1	2	3			1		3[18]	2[7,18]	1						
Konnektor (PTV5)	2	1	2	2	1[18]	1[18]	3			1[18]	3[18]	2[2]	ffpvt	2				1	1		1	1	1	2	3			1		3[18]	2[7,18]	1						
Konnektor Highspeed	2	1	2	2	1[18]	1[18]	1			3[18]	3[18]	3[2]	ffpvt	-				1	1		1	1	1	1	3			1		3[18]	2[7,18]	1						
eHealth-Kartenterminal	2	1	2	2	1[18]	1[18]						2	ffpvt																								
Mobiles Kartenterminal	2	1	2	2			3																														
VPN-Zugangsdienst												2	ffpvt		1	1	1	1		1		1															
Zentrales Netz der TI														1		1	1	1	1	1	1																
Namensdienst															1		1	1		1																	
Zeitdienst														1	1	1		1		1																	
Konfigurationsdienst												2	ffpvt		1	1	1			1																	
Verzeichnisdienst										2		2	ffpvt			1	1	1		1																	
Sicherheits-Gateway Bestandsnetze															1	1	1	1		1																	
Intermediär VSDM												2	ffpvt		1	1	1	1		1		1			3												
Fachdienst KIM										6																5[5]	1										
Clientmodul KIM								3		5		3	ffpvt													6	1										
KTR-AdV	1[3]	1	1												1	1	1	1		1		1		1	1												
ePA-Aktensystem	1	1	2									2[18]	ffpvt		1	1	1	1		1		1					1		2[19]	4[6,18]							
ePA-Frontend des Versicherten	1	1										2[6,18]	ffpvt									1[21]							3[18,20]		1	1[21]					
KTR-Consumer															1	1	1	1		1		1				1[9]	1		1								
Basis-Consumer															1	1	1	1		1		1				1	1										
Signaturdienst																				1		1								1							
Schlüsselgenerierungsdienst												2[18]	ffpvt		1	1	1	1		1		1							1	3[18]							
IDP-Dienst							3								1	1	1	1		1		1	1										1		1	1	
Sektorale IDP																				1															1		
E-Rezept Fachdienst							3								1	1	1	1		1	1													1		2[4]	
E-Rezept Frontend des Versicherten																											1						1	1		1
Apothekenverzeichnisdienst																																			2	

[1] soweit noch verfügbar
[2] QES-Signatur-Erstellen bzw. überprüfen
[3] eGK mit VSD-Update und eGK mit Sperrung (pro unterstütztem Mandanten)
[4] es muss jeweils die aktuelle und die vorletzte Majorversion von iOS bzw. Android mit dem neusten Patchlevel getestet werden
[5] verschiedene Fachdienste KIM müssen untereinander interoperabel sein
[6] FdVs in den Ausprägungen Android, iOS, Desktop Client des Herstellerkonsortiums sowie eine Ausprägung eines anderen FdV-Herstellers.
[7] Ergebnisse eines Dokumentenhandlings via KON oder FdV muss auf der jeweils anderen Seite sicht- und prozesszierbar sein. Es sind FdVs in zwei verschiedenen Ausprägungen (Android, iOS oder Desktop Client zu verwenden).
[8] Ergebnisse eines Dokumentenhandlings via KON oder FdV muss auf der jeweils anderen Seite sicht- und prozesszierbar sein.
[9] Nur, wenn die Option KTR-Consumer mit einem KIM-CM gewählt ist.
[12] incl. Gerätekarten gSMC-K und gSMC-KT
[13] Ein IOP-Test ist erst ab dem Zeitpunkt notwendig, ab dem die gematik G2.1-Karten anbietet
[18] Soweit verfügbar
[19] nur Operationen checkRecordExists und getExportPackage
[20] Der Hersteller des ePA-Frontend des Versicherten testet die Interoperabilität gegen das ePA-Aktensystem seines Herstellerkonsortiums. Der Anbieterwechsel ist mit zwei weiteren Aktensystemen zu prüfen.
[21] Soweit alternative Authentisierung unterstützt wird

7 Anhang A – Verzeichnisse

7.1 Abkürzungen

Kürzel	Erläuterung
HSK	Highspeed-Konnektor
KTR	Kostenträger
AVV	Auftragsverarbeitungsvertrag (AV-Vertrag)
LEI	Leistungserbringerinstitution
VAU	Vertrauenswürdige Ausführungsumgebung

7.2 Referenzierte Dokumente

7.2.1 Dokumente der gematik

Die nachfolgende Tabelle enthält die Bezeichnung der in dem vorliegenden Dokument referenzierten Dokumente der gematik zur Telematikinfrastruktur.

[Quelle]	**Herausgeber: Titel**
[gemGlossar]	gematik: Glossar der Telematikinfrastruktur
gemSpec_DS_Anbieter	gematik: Spezifikation Datenschutz- und Sicherheitsanforderungen der TI an Anbieter
[gemSpec_gSMC-K_ObjSys]	gematik: Spezifikation der gSMC-K Objektsystem
[gemKPT_Betr]	gematik: Betriebskonzept Online-Produktivbetrieb
[gemKPT_Test]	gematik: Testkonzept der TI
[gemKPT_Betriebsdaten_Kon]	gematik: Datennutzungskonzept Betriebsdaten Konnektor