Elektronische Gesundheitskarte und Telematikinfrastruktur

Feature: Highspeed-Konnektor

Version:	1.0.0 CC 2
Revision:	~~400613~~427233
Stand:	~~30.08~~16.12.2021
Status:	zur Abstimmung freigegeben
Klassifizierung:	öffentlich_Entwurf
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
			Kommentierung	
1.0.0 CC 2	16.12.21		zur Abstimmung freigegeben	gematik

Inhaltsverzeichnis

1 Einordnung des Dokuments

Das Dokument ergänzt vorhandene Spezifikationen für das ~~Zulassungsobjekt~~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.

Eine allgemeine neue Zugangslösung ("TIaaS") kann durch eine Weiterentwicklung der Festlegungen in diesem Dokument konzipiert werden.

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.

Innerhalb des geschützten Bereichs des Rechenzentrums können SMC-B und gSMC-K in lokalen Kartenlesern gesteckt und genutzt werden, es müssen keine eHealth-Kartenterminals verwendet werden. Die SMC-B-PIN kann über den Konnektor eingegeben werden, eine Eingabe direkt am Kartenterminal ist nicht notwendig.

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

~~Bei dieser Variante wird~~ 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~~technische 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~~, ein~~ und der http-Forwarder ~~und die Betriebsdatenmeldeprozesse~~ eines VPN-ZD genutzt werden.
- ~~Es wird kein VPN-Client im Highspeed-Konnektor benötigt.~~
- Durch die Anbindung an die TI über SZZP entfällt die Registrierung und VPN-Verbindung zum VPN-Zugangsdienst.

4.2 Sicherheitsnachweis

4.2.1 Hersteller

~~Für den Highspeed-Konnektor sollen große Teile der CC-zertifizierten Konnektorsoftware und der TR-zertifizierten Fachmodule des Einbox-Konnektors nachgenutzt werden. Entsprechend soll dieser Anteil auch durch die Prüfstelle geprüft werden, die auch die CC- bzw. TR-Evaluierung vorgenommen hat. Es wird daher für alle auch für den Einbox-Konnektor und seine Fachmodule bestehenden Anforderungen mit dem Prüfverfahren "CC-Evaluierung" und "TR-Zertifizierung" das Prüfverfahren "Prüfung durch CC-Prüfstelle" gewählt. Das Prüfverfahren ist dann analog zu einem Minor-Release-Verfahren. Als Prüfgrundlage – im Sinne der Definition des fachlichen Prüfumfangs – bleiben für die entsprechenden Anforderungen jedoch das Schutzprofile PP-0098 sowie dessen Erweiterung in den Security Targets und die Technischen Richtlinien TR-03154/55/57 führend.~~

~~Speziell für den Highspeed-Konnektor neu hinzukommende Anforderungen bspw. zur VAU und zur Kopplung mit dem SZZP und ggf. dem HSM müssen nicht zwingend durch die bisherigen CC-Evaluatoren geprüft werden. Hier wird entsprechend das Prüfverfahren "Produktgutachten" gewählt.~~

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 Hersteller 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 Entwicklungsumgebung 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 - Feste Kopplung von Konnektor und SZZP
Der Konnektor und der SZZP MÜSSEN kryptographisch miteinander gekoppelt werden, so dass ausschließlich der Konnektor - und explizit nicht der Administrator der Betriebsumgebung - über die Schnittstellen des SZZP Zugang in die TI bekommen kann.**[<=]**

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] wenn (MGM_LU_ONLINE=Enabled) 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 (VPN_TI) geleitet werden.
[<=]

A_22337 - TSL-Download aus dem Internet optional
Der Highspeed-Konnektor KANN auf die Umsetzung der Variante "Download aus dem Internet" von TUC_KON_032 verzichten**[<=]**

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 - technisch 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.

(für Fachmodule siehe Kapitel 4.3.4)
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]“)}.

[<=]

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). Zudem ist es für den Highspeed-Konnektor gestattet die gSMC-Ks (sofern kein HSM verwendet wird) und vom LE dafür freigegebene SMC-Bs lokal per USB-Kartenleser anzubinden, sofern dies innerhalb der VAU geschieht. Es sind keine weiteren Schnittstellen gestattet.

A_21988 - 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 (bspw. ggf. USB-Kartenleser). 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.**[<=]**

A_22039 - Highspeed-Konnektor: Lokaler Kartenleser für gSMC-K und SMC-B möglich
Der Highspeed-Konnektor KANN Karten vom Typ gSMC-K und SMC-B über einen lokalen Kartenleser (USB) anbinden. Eine PIN-Eingabe kann dann über die Administrationsoberfläche des Konnektors erfolgen. PINs dürfen im Konnektor jedoch nicht gespeichert oder gecacht werden.**[<=]**

A_22040 - Highspeed-Konnektor: Absicherung Anbindung lokaler Kartenleser
Der Highspeed-Konnektor MUSS, wenn lokale Kartenleser (USB) verwendet werden, diese innerhalb der VAU anbinden (kein Zugriff des Betreibers auf den Kartenleser) und zusätzlich die genutzte Schnittstelle härten, sodass im Sinne der mehrschichtigen Sicherheit zum einen unberechtigte Zugriffe auf die Schnittstelle durch die VAU verhindert werden und zum anderen solche Zugriffe nicht für Angriffe auf den Highspeed-Konnektor genutzt werden können.**[<=]**

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.**[<=]**

5.1.3 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 bzw. durch den Hersteller. Bei Upload am Highspeed-Konnektor muss die Integrität und Authentizität des Updatespakets 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 1: TAB_KON_664 – TUC_KON_280 „Konnektoraktualisierung durchführen"

Element	Beschreibung
Name	TUC_KON_280 „Konnektoraktualisierung durchführen"
Beschreibung	Dieser TUC aktualisiert den Konnektor 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. Prüfen auf Zulässigkeit des Updates basierend auf der Firmware-Gruppe (siehe [gemSpec_OM#2.5]
	3. Anwenden der zur Verfügung stehenden FirmwareFiles
	a. TUC_KON_256{
	topic = „KSR/UPDATE/START";
	eventType = Sec;
	severity = Info;
	parameters = („Target=Konnektor,
	Name=$MGM_KONN_HOSTNAME"
	)}
	(betroffene Fachmodule und Basisdienste reagieren und stoppen sich)

	b. Herstellerspezifischer Mechanismus zur Aktualisierung der internen Konnektorsoftware durch die FirmwareFiles inklusive anschließender Prüfung auf Erfolg.
	c. Bestehende Konfigurationsdaten des Konnektors MÜSSEN erhalten bleiben und sofern erforderlich und möglich automatisch auf die Definitionen der neuen Firmware angepasst werden.
	d. Ist ein händischer Anpassungs- oder Ergänzungsbedarf der Konfigurationsdaten erforderlich, so MUSS der Administrator hierüber geeignet informiert werden
	e. TUC_KON_256 {
	topic = „KSR/UPDATE/SUCCESS";
	eventType = Sec;
	severity = Info;
	parameters = („Target=Konnektor,
	Name= $MGM_KONN_HOSTNAME,
	NewFirmwareversion =
	UpdateInformation.FirmwareVersion,
	ConfigurationChanged=<Ja/Nein>,
	ManualInputNeeded=<Ja/Nein>„) }
	Der TUC endet in jedem Fall mit:
	TUC_KON_256 {
	topic = „KSR/UPDATE/END";
	eventType = Sec;
	severity = Info;
	parameters = („Target=Konnektor,
	Name=$MGM_KONN_HOSTNAME") }
	(betroffene Fachmodule und Basisdienste reagieren und starten sich)

Varianten/Alternativen	

Fehlerfälle	Fehler in den folgenden Schritten des Ablaufs führen zu:
	a) Aufruf von TUC_KON_256 {
	topic = „KSR/ERROR";
	eventType = $ErrorType;
	severity = $Severity;
	parameters = („Target=Konnektor,
	Name= $MGM_KONN_HOSTNAME,
	Error=$Fehlercode,
	Bedeutung=$Fehlertext") }
	
	b) Abbruch der Verarbeitung mit den ausgewiesenen Fehlercodes
	
	(→1) Integritätsprüfung eines FirmwareFiles fehlgeschlagen, Fehlercode: 4183
	(→ 2) Firmwaregruppenprüfung fehlgeschlagen, Fehlercode:

	4185 (→3b) Interne Aktualisierung fehlgeschlagen, dann: 1. Rollback auf vorherige Version 2. Abbruch mit Fehlercode: 4184
Nichtfunktionale Anforderungen	
Zugehörige Diagramme	

Tabelle 2: 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

[<=]

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.[<=]

GS-A_4640 - Identifizierung/Validierung des TI-Vertrauensankers bei der initialen Einbringung
Hersteller von Produkttypen der TI, die Zertifikate prüfen, MÜSSEN bei der initialen Einbringung das aktuell gültige TSL-Signer-CA-Zertifikat eindeutig identifizieren und

mittels Fingerprint validieren, bevor dieses Zertifikat als TI-Vertrauensanker in die Komponente eingebracht werden darf.
[<=]

5.2.1.2 HSM

TIP1-A_4503-02 - Verpflichtung zur Nutzung von gSMC-K oder HSM
Der Konnektor MUSS das geheime Schlüsselmaterial zur Geräteidentität (ID.NK.VPN, 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_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.

A_21987 - Zugriff auf die VAU nur durch den Hersteller
Die VAU des Highspeed-Konnektors MUSS Eingriffe in das System durch andere als den Hersteller unterbinden. Das betrifft im Besonderen administrative Zugriffe auf das HSM, die Kopplung des HSM und die Kopplung mit dem SZZP.**[<=]**

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_17598 - Qualität des HSM
Die Basis- und KTR-Consumer 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_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 VAU dient der datenschutzrechtlich zulässigen und sicheren Verarbeitung von schützenswerten Klartextdaten (Aktenschlüssel und Kontextschlüssel des Aktenkontos eines Versicherten) innerhalb des FM ePA.

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 bildet den Verarbeitungskontext der Vertrauenswürdigen Ausführungsumgebung.

Zur Vertrauenswürdigen Ausführungsumgebung gehören neben den Verarbeitungskontexten alle für ihre Erreichbarkeit und betriebliche Steuerung erforderlichen Komponenten.

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

Die schützenswerten sensiblen Daten sind der Akten- und Kontextschlüssel der Aktenkonten, für die der KTR zugriffsberechtigt ist.

Die Mehrzahl Verarbeitungskontexte ergibt sich aus der softwaretechnischen Trennung verschiedener Sitzungen. Somit wird jede Akte in Ihrem eigenen Verarbeitungskontext genutzt. Physische Maßnahmen bspw. zum Zutrittsschutz sind hingegen nur einmalig für die gesamte VAU erforderlich, also für jeden Verarbeitungskontext identisch.

A_17346 - FM ePA KTR-Consumer: Verarbeitungskontext der VAU
Der Verarbeitungskontext des Fachmoduls ePA im KTR-Consumer MUSS sämtliche physikalischen Systemkomponenten sowie sämtliche Softwarekomponenten umfassen, deren Sicherheitseigenschaften sich auf den Schutz des Akten- und Kontextschlüssel eines Versicherten vor Zugriff durch Unbefugte bei ihrer Verarbeitung im Klartext auswirken können.
[<=]

A_17347 - FM ePA KTR-Consumer: Verarbeitungskontext der VAU - Keine persistente Speicherung von Akten- und Kontextschlüssel
Der Verarbeitungskontext des Fachmoduls ePA im KTR-Consumer DARF den Akten- und Kontextschlüssel eines Versicherten NICHT persistent speichern, auch nicht verschlüsselt.**[<=]**

A_17348 - FM ePA KTR-Consumer: Verarbeitungskontext der VAU - Akten- und Kontextschlüssel verlassen VAU nie
Der Verarbeitungskontext des Fachmoduls ePA im KTR-Consumer 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.
[<=]

5.2.1.4 Ausschluss von nicht autorisierten Zugriffen aus dem Betriebsumfeld

Für den Highspeed-Konnektor gelten folgende Anforderungen an das "Fachmodul ePA im KTR-Consumer":

A_17350 - FM ePA KTR-Consumer: Isolation der VAU von Datenverarbeitungsprozessen des Anbieters
Die VAU des Fachmoduls ePA im KTR-Consumer MUSS die im Verarbeitungskontext ablaufenden Datenverarbeitungsprozesse von allen sonstigen Datenverarbeitungsprozessen des Anbieters trennen und damit gewährleisten, dass der Anbieter KTR-Consumer vom Zugriff auf die in der VAU verarbeiteten, schützenswerten Daten ausgeschlossen ist.**[<=]**

A_17351 - FM ePA KTR-Consumer: Ausschluss von Manipulationen an der Software der VAU
Die VAU des Fachmoduls ePA im KTR-Consumer MUSS die Integrität der eingesetzten Software schützen und damit insbesondere Manipulationen an der Software durch den Anbieter KTR-Consumer ausschließen.**[<=]**

A_17352 - FM ePA KTR-Consumer: Ausschluss von Manipulationen an der Hardware der VAU
Die VAU des Fachmoduls ePA im KTR-Consumer MUSS die Integrität der eingesetzten Hardware schützen und damit insbesondere Manipulationen an der Hardware durch den Anbieter KTR-Consumer ausschließen.**[<=]**

A_17353 - FM ePA KTR-Consumer: Kontinuierliche Wirksamkeit des Manipulationsschutzes der VAU
Die VAU des Fachmoduls ePA im KTR-Consumer MUSS den Ausschluss von Manipulationen an der Hardware und der Software durch den Anbieter KTR-Consumer mit Mitteln umsetzen, deren dauerhafte und kontinuierliche Wirksamkeit gewährleistet werden kann.**[<=]**

A_17354 - FM ePA KTR-Consumer: Kein physischer Zugang des Anbieters zu Systemen der VAU
Die VAU des Fachmoduls ePA im KTR-Consumer MUSS mit technischen Mitteln sicherstellen, dass niemand, auch nicht der Anbieter KTR-Consumer, während der Verarbeitung personenbezogener medizinischer Daten Zugriff auf physische Schnittstellen der Systeme erlangen kann, auf denen eine VAU ausgeführt wird.**[<=]**

A_17355 - FM ePA KTR-Consumer: Nutzdatenbereinigung vor physischem Zugang zu Systemen der VAU
Die VAU des Fachmoduls ePA im KTR-Consumer 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 - FM ePA KTR-Consumer: Löschen aller aktenbezogenen Daten beim Beenden des Verarbeitungskontextes
Die VAU des Fachmoduls ePA im KTR-Consumer MUSS beim Beenden eines Verarbeitungskontextes sämtliche Daten dieses Verarbeitungskontextes sicher löschen.**[<=]**

A_21990 - Kein Zugriff auf SM-B Identitäten und Kopplungs-Geheimnis durch Betreiber
Der Highspeed-Konnektor MUSS den Betreiber vom vollen Zugriff auf SM-B-Identitäten ausschließen. Im Fall einer SMC-B darf der Betreiber nicht sowohl Zugriff auf die Karte

als auch im Wissen der PIN haben. Im Fall einer Speicherung von SM-B-Identitäten in einem HSM darf der Betreiber nicht das HSK-HSM-Kopplungsgeheimnis kennen.**[<=]**

5.2.1.5 Unabhängigkeit von dem Betreiber des Aktensystems

A_21248-01 - Anbieter ePA-Aktensystem - Unabhängigkeit des Betreibers eines ePA-Aktensystems vom Betreiber eines KTR-Consumers

Der Anbieter des ePA-Aktensystems und der Anbieter des KTR-Consumers MÜSSEN dafür Sorge tragen, dass ihr beauftragter Betreiber für das ePA-Aktensystem unabhängig vom beauftragten Betreiber des KTR-Consumers 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 KTR-Consumers bzw. des ePA-Aktensystems gewährleistet.**[<=]**

5.2.1.6 Anforderungen aus gemSpec_DS_Anbieter

Grundsätzlich ist der Betrieb des Highspeed-Konnektors ~~im~~in einem Krankenhaus oder einer großen Einrichtung vergleichbar mit dem Betrieb vieler Einbox-Konnektoren, die in der selben Umgebung auch direkt ~~vom Krankenhaus~~von der Einrichtung, bzw. ~~deren~~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 ~~(Krankenhaus-IT-Dienstleister)~~ 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

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

6 Anhang A – Verzeichnisse

6.1 Abkürzungen

Kürzel	Erläuterung
HSK	Highspeed-Konnektor
KTR	Kostenträger
AVV	
LEI	Leistungserbringerinstitution
VAU	Vertrauenswürdige Ausführungsumgebung

6.2 Referenzierte Dokumente

6.2.1 Dokumente der gematik

Die nachfolgende Tabelle enthält die Bezeichnung der in dem vorliegenden Dokument referenzierten Dokumente der gematik zur Telematikinfrastruktur. ~~Der mit der vorliegenden Version korrelierende Entwicklungsstand dieser Konzepte und Spezifikationen wird pro Release in einer Dokumentenlandkarte definiert; Version und Stand der referenzierten Dokumente sind daher in der nachfolgenden Tabelle nicht aufgeführt. Deren zu diesem Dokument jeweils gültige Versionsnummern sind in der aktuellen, von der gematik veröffentlichten Dokumentenlandkarte enthalten, in der die vorliegende Version aufgeführt wird.~~

[Quelle]	**Herausgeber: Titel**
[gemGlossar]	gematik: Glossar der Telematikinfrastruktur
gemSpec_DS_Anbieter	
[gemSpec_gSMC-K_ObjSys]	

672

673 ### 6.2.2 Weitere Dokumente

[Quelle]	Herausgeber (Erscheinungsdatum): Titel

674