

Elektronische Gesundheitskarte und Telematikinfrastruktur

Feature: TI-Gateway

Version: 1.1.0
Revision: 957849
Stand: 04.08.2023
Status: freigegeben
Klassifizierung: öffentlich
Referenzierung: gemF_TI-Gateway

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	15.02.23		freigegeben	gematik
1.1.0	04.08.23		Übernahme von Inhalten gemF_TI- Gateway --> gemSpec_Perf, gemKPT_Betr, gemF_Highspeed- Konnektor; redaktionelle Anpassungen	gematik

Inhaltsverzeichnis

1 Einordnung des Dokuments.....	5
1.1 Zielsetzung.....	5
1.2 Zielgruppe.....	5
1.3 Abgrenzungen.....	5
1.4 Methodik Anforderungen.....	5
2 Einordnung in die Telematikinfrastuktur.....	7
3 Technisches Konzept.....	8
4 Rollenkonzept TI-Gateway.....	9
4.1 Reseller.....	9
4.2 Betreiber.....	10
4.3 Hersteller des HSK.....	10
4.4 HSK-Instanz Administrator z.B. Dienstleister vor Ort (DVO).....	10
4.5 Remote-Administrator.....	11
4.6 Kunde - Leistungserbringer.....	11
4.7 Rollenkombinationen & Rollenausschlüsse.....	12
5 Spezifikation Zugangsmodul.....	14
5.1 Onboarding und Registrierung.....	14
5.1.1 Nutzerportal.....	15
5.1.2 Initiale Authentifizierung der HSK-Instanz.....	17
5.1.3 Betriebsfunktionen für den Leistungserbringer.....	20
5.2 VPN.....	20
5.3 Routing und Firewall.....	22
5.4 Sicherheit & Datenschutz.....	23
5.5 Rohdaten-Performance-Reporting.....	26
5.5.1 Umfang.....	26
5.5.2 Lieferintervalle.....	26
5.5.3 Format.....	26
5.6 Lastanforderungen.....	26
6 Anforderungshaushalt TI-Gateway.....	27
6.1 Neue Anforderungen.....	27
6.1.1 Anbietererklärung.....	27
6.1.2 Sicherheitsgutachten.....	27
6.2 Betrieb.....	29
6.2.1 Servicezerlegung.....	29

6.2.2 Mitwirkungsverpflichtung im TI-ITSM gemäß [gemRL_Betr_TI].....	29
6.2.3 Spezifische Ausprägungen und Verpflichtungen einzelner Rollen.....	29
6.2.4 Supportkonzept.....	29
6.2.4.1 Spezifische Ausprägungen.....	29
6.2.4.2 Organisatorische Service Level.....	29
6.2.4.3 Technische Service Level / Performance-Kenngrößen.....	29
6.2.5 gemKPT_Betr: Anhang A.....	29
6.2.6 gemSpec_Perf#3.x.1 Leistungsanforderungen TI-Gateway.....	29
6.2.6.1 gemSpec_Perf#3.x.1.1 Lastmodell TI-Gateway.....	29
6.2.6.2 gemSpec_Perf#3.x.1.2 Bearbeitungszeiten TI-Gateway.....	29
6.2.6.3 gemSpec_Perf#3.x.1.3 Performancevorgaben TI-Gateway.....	30
7 Änderungen an gemILF_PS.....	31
8 Beispiele und Referenzimplementierungen.....	32
9 Anhang A - Verzeichnisse.....	33
9.1 Abkürzungen.....	33
9.2 Referenzierte Dokumente.....	33
9.2.1 Dokumente der gematik.....	33
9.2.2 Weitere Dokumente.....	33

1 Einordnung des Dokuments

Die Schnittstelle zwischen der zentralen Infrastruktur der TI und der dezentralen Umgebung bildet derzeit die dezentrale Komponente Konnektor, die eine gesicherte Verbindung zum VPN-Zugangsdienst der TI aufbaut. Um im Sinne der TI2.0 Komplexität aus der dezentralen Umgebung zu entfernen, wurde das Produkt TI-Gateway definiert, welches die Funktion von Zugangsdienst und Teilfunktionen des Konnektors in einem Dienst zusammenfasst. Dieses Feature-Dokument beschreibt das TI-Gateway (Anbieter TI-Gateway, Produkt Zugangsmodul und Anpassungen am Produkt Highspeed-Konnektor) und beinhaltet Blattanforderungen, die nicht bereits Teil anderer Spezifikationen der gematik sind. Der vollständige Anforderungshaushalt ergibt sich aus den Steckbriefen für den Anbieter TI-Gateway und den Produkten, die Teil des TI-Gateway sind.

1.1 Zielsetzung

Dieses Dokument soll ein Verständnis für das TI-Gateway vermitteln und die Anforderungslage vervollständigen. Dadurch sollen Hersteller und Anbieter in die Lage versetzt werden, das Produkt herzustellen bzw. dessen Betrieb zu ermöglichen.

1.2 Zielgruppe

Hersteller, Anbieter, Nutzer und andere Stakeholder.

1.3 Abgrenzungen

Das Dokument beinhaltet nur neue bzw. geänderte Anforderungen. Die vollständige Anforderungslage für die Produkttypen des TI-Gateways und den Anbieter des TI-Gateways ergeben sich aus den Produkttypsteckbriefen, dem Anbietersteckbrief und den darin referenzierten Anforderungen.

1.4 Methodik 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 Einordnung in die Telematikinfrastruktur

Das TI-Gateway ist ein zentraler Dienst der Telematikinfrastruktur, der Leistungserbringern anstelle eines Konnektors ermöglicht,

- eHealth-Kartenterminals (und darüber TI-Smartcards) zu nutzen,
- Services zu nutzen, wie sie vom Anwendungskonnektor und den Fachmodulen des Konnektors angeboten werden und
- über das Netzwerk auf offene Fachdienste und WANDA zuzugreifen.

Anbieter des TI-Gateways können darüber hinaus ihren Kunden weitere Services anbieten, müssen dann jedoch transparent machen, dass diese nicht Teil des zugelassenen TI-Gateways sind. (siehe A_23472)

Durch die Verschiebung der Funktionalitäten, die heute vom Konnektor im lokalen Netz des Nutzers bereitgestellt werden, in einen im Rechenzentrum betriebenen Dienst stehen zwangsläufig gewisse Funktionen nicht mehr zur Verfügung. Dies sind konkret:

- Schutz des lokalen Netzes des Nutzers gegenüber Angriffen aus dem Internet (bei Konnektor ausschließlich bei Anbindung "in Reihe" gegeben)
- Sicherer Internet Service (SIS)
- Zeitdienst für das lokale Netz
- DHCP Server für das lokale Netz
- VSDM im Offline-Betrieb
- VSDM im Standalone-Betrieb (nur bei Nutzung von zwei Konnektoren gegeben)

Nutzer bzw. die von ihnen beauftragten IT-Dienstleister (DVO) müssen entsprechend alternative Lösungen für die Funktionen umsetzen, die zuvor über den Konnektor genutzt wurden (sofern die Funktionen benötigt werden). Dies gilt insbesondere für die Absicherung des lokalen Netzes gegen das Internet, falls vor der Nutzung des TI-Gateway ein Konnektor in Anbindungsart "in Reihe" installiert war.

3 Technisches Konzept

Die Anbieterzulassung für das TI-Gateway setzt eine Produktzulassung Zugangsmodul und eine Produktzulassung Highspeed-Konnektor (HSK) voraus. Die Komponente http-Proxy ist als Teil des Produkttyps HSK umzusetzen. Die Anbieterzulassung für das TI-Gateway umfasst die Produkte Intermediär-VSDM, wobei ein bereits unter der Anbieterzulassung VPN-Zugangsdienst betriebener Intermediär nachgenutzt werden kann.

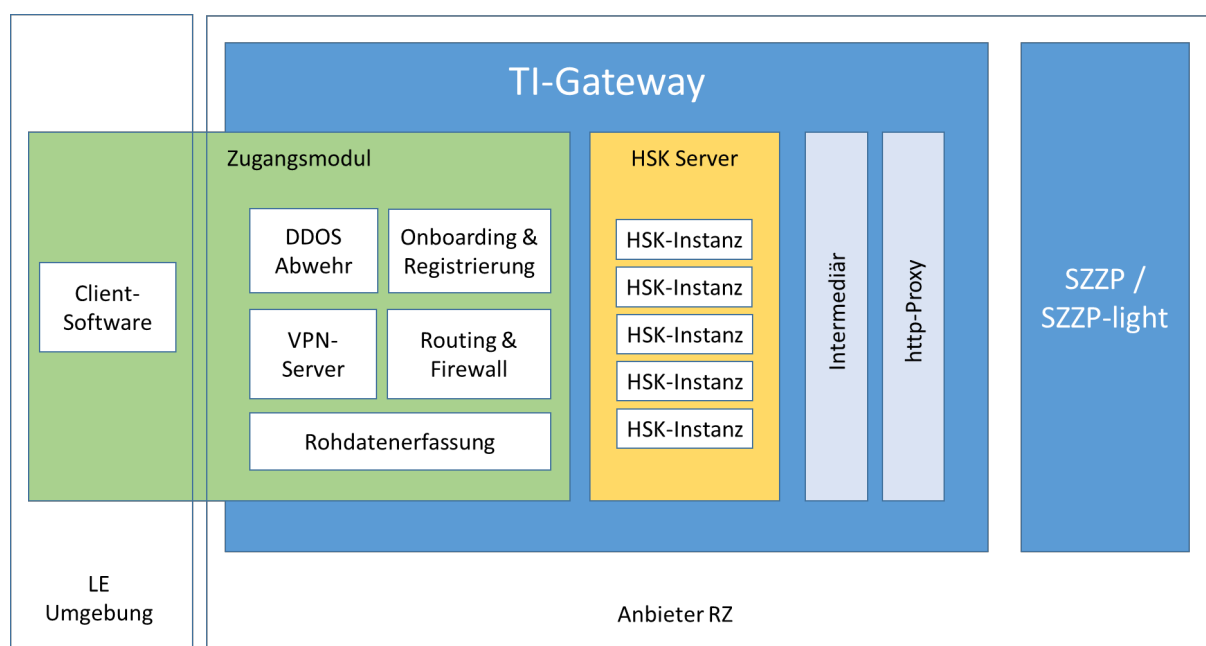


Abbildung 1: Anbindung TI-Gateway

Das Zugangsmodul ermöglicht und sichert

- den Zugriff für die fachliche Nutzung auf die HSK-Instanz
- den Zugriff für die Administration einer HSK-Instanz
- den Zugriff auf offene Fachdienste und WANDA der Telematikinfrastruktur

Der HSK stellt bereit

- die Basisdienste der Telematikinfrastruktur für LE-Umgebungen
- die Fachmodule
- die Kartenterminalintegration für die LE-Umgebung

Die Produkte Intermediär und http-Proxy bieten Funktionalitäten, die bei Nutzung von Konnektoren durch den VPN-Zugangsdienst abgedeckt werden.

Die Anbindung an die Telematikinfrastruktur erfolgt über einen SZZP oder SZZP-light. Die Anbindung über ein SZZP-light-plus, die bei einer Anbieterzulassung HSK vorgeschrieben ist, wird für das TI-Gateway nicht unterstützt.

4 Rollenkonzept TI-Gateway

Die gematik lässt ein Unternehmen als Anbieter des TI-Gateways zu. Der Anbieter erbringt Betriebsleistung und Service unter Verwendung zugelassener Produkte. Der Anbieter kann dazu Unterauftragnehmer beauftragen (siehe auch gemKPT_Betr.) Die Beziehungen der Firmen untereinander wird im Rollenkonzept nicht betrachtet.

Damit Mitarbeiter des Anbieters oder seiner Unterauftragnehmer nicht auf medizinische Informationen oder unberechtigt auf personenbezogene Daten zugreifen, werden die betrieblichen Tätigkeit in verschiedenen Rollen zugeordnet und es wird geregelt, welche Rollen ein Mitarbeiter innehaben kann.

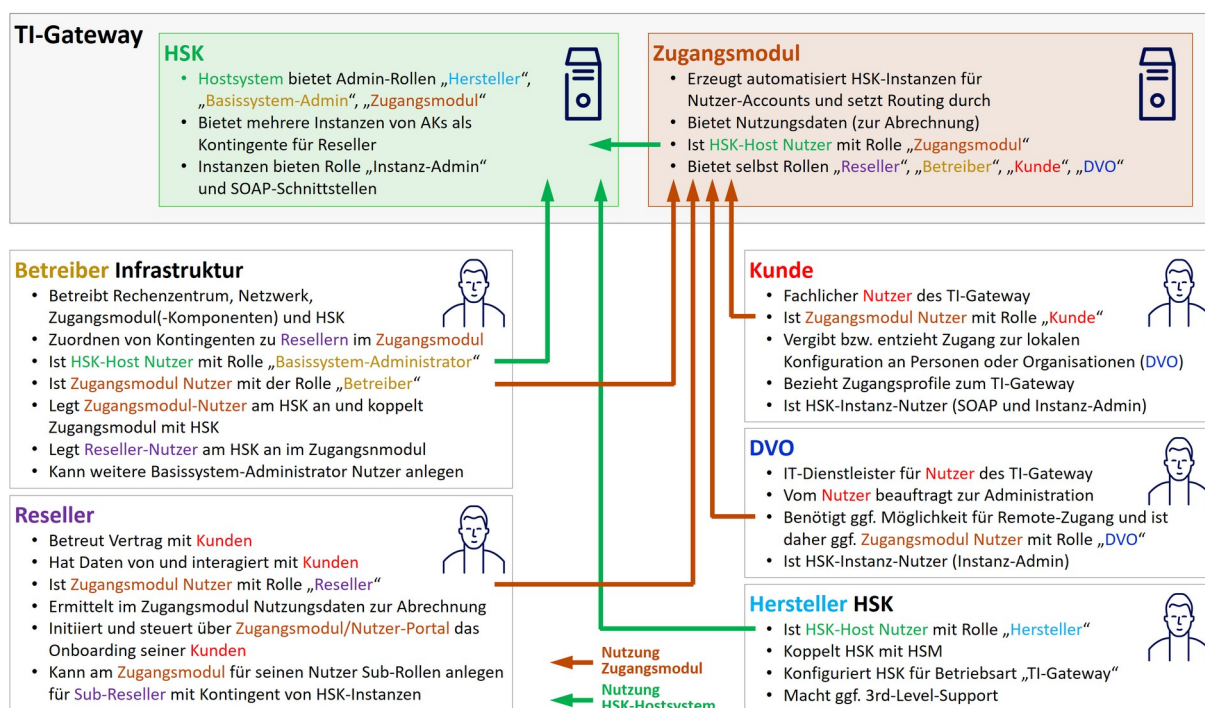


Abbildung 2: Übersicht Rollen und Komponenten

4.1 Reseller

Der Reseller betreut den Kunden kaufmännisch und qualifiziert einen Neukunden bevor im Onboardingprozess dem Kunden eine HSK-Instanz erzeugt/zugeordnet wird.

Der Reseller steuert das Onboarding von LE-Institutionen inklusive dem Erzeugen von HSK-Instanzen im „Werkzustand“ (automatisiert) über die Onboarding- & Registrierungskomponente des Zugangsmoduls. Der Reseller beauftragt die Löschung von HSK-Instanzen durch den Infrastrukturbetreiber (4-Augen-Prinzip).

Im Rahmen des Onboardings werden auch automatisiert der Administrations-Zugang an den Leistungserbringer bzw. den von diesem beauftragten lokalen Administrator (DVO) vergeben (Zugangsdaten abrufbar über das Nutzer-Portal) und die HSK-Instanzen zugewiesen. Der Reseller hat auf diese Daten keinen Zugriff. Dieser Prozess ist automatisiert und erfordert keinen manuellen Eingriff des Resellers oder Betreibers.

Der Reseller hat keinen Zugriff auf medizinische Daten oder die fachliche Konfiguration von HSK-Instanzen.

Der Reseller kann am Zugangsmodul abrechnungsrelevante Information einsehen bzw. abrufen.

Der Reseller hat keinen Zugriff auf das HSK-Basissystem oder die HSK-Instanzen.

4.2 Betreiber

Der Betreiber überwacht und steuert technische Komponenten des TI-Gateways inkl. der RZ-Infrastruktur darum.

Der Betreiber greift auf das HSK-Basissystem über die Admin-Rolle "Basissystem-Admin" zu. Dazu gehört die Installation von Softwareupdates und das Erzeugen und Wiederherstellen von Backups der HSK-Instanzen (Snapshots). Dabei hat der Betreiber keinen Zugriff auf den Inhalt und die Konfiguration der HSK-Instanzen und deren fachliche Logs und er hat ebenso keinen Zugriff auf medizinische Daten. Der Infrastrukturbetreiber führt die Löschaufträge des Resellers von HSK-Instanzen aus.

Der Betreiber überwacht und administriert das Zugangsmodul.

Der Infrastrukturbetreiber kann technische Parameter wie die Ressourcenauslastung überwachen und technische Parameter wie die Ressourcenzuweisung für HSK-Instanzen ändern. Diese Aufgabe kann auch an den Reseller für dessen jeweiliges Kontingent von HSK-Instanzen übertragen werden.

4.3 Hersteller des HSK

Der Hersteller interagiert mit dem HSK-Basissystem mit der Rolle Hersteller. In dieser Funktion konfiguriert er den HSK für die Betriebsart "TI-Gateway" und koppelt den HSK mit dem HSM.

Der Hersteller stellt Softwareupdates bereit und wird für 3rd-Level-Support/Debugging hinzugezogen.

Der Hersteller des HSK hat keinen Zugriff auf Logs aus den HSK-Instanzen. Wenn diese für den Support notwendig sind, müssen diese von einer Administrator-Rolle pseudonymisiert bereitgestellt werden.

4.4 HSK-Instanz Administrator z.B. Dienstleister vor Ort (DVO)

Die Administration der HSK-Instanz wird vom Leistungserbringer oder einem von ihm beauftragten Dienstleister durchgeführt (DVO). Diese Rolle entspricht somit dem lokalen Administrator, wie er auch beim Einboxkonnektor agiert.

Der DVO greift aus der Leistungserbringerumgebung oder über einen eigenständigen Zugang auf die Administrationsschnittstelle der HSK-Instanz zu. Im Fall des eigenständigen Zugangs steuert der LE über das Nutzer-Portal des Zugangsmoduls welche Person/Organisation(DVO) auf seine Instanz zugreifen kann. Der DVO authentifiziert sich in jedem Fall direkt am Admin-Interface der HSK-Instanz.

Der LE/DVO nimmt die initiale Anbindung der HSK-Instanz an die LEI vor (Pairing der KTs und Konfiguration der Primärsysteme, beidseitige Authentisierung). Auch ein späteres Hinzufügen von neuen Primärsystemen hat stets einen lokalen Anteil auf Grund der notwendigen Konfiguration in Clientsystem und HSK-Instanz für die beidseitige Authentisierung und Zugriffssteuerung (Infomodell).

Der lokale Administrator kann fachliche Logs der HSK-Instanz einsehen.

Die Erreichbarkeit der Administrations-Schnittstelle der HSK-Instanz muss für den LE von seinen Systemen aus jederzeit gegeben sein. Dabei müssen zwei unabhängige Sicherungsschichten umgesetzt werden, eine für den Zugang zum Administrations-Interface und eine durch Authentisierung an der HSK-Instanz.

Eine Erreichbarkeit der fachlichen Schnittstellen (SOAP, LDAP, CETP, SICCT) über ein anders Netz bzw. einen anderen Zugang als den VPN-Zugang ist ausgeschlossen. Der Nutzer kann einem DVO den Zugriff auf die Administrationsschnittstelle seiner HSK-Instanz auch jederzeit wieder über das Nutzer-Portal entziehen.

4.5 Remote-Administrator

Der Remote-Administrator übernimmt kontinuierliche Überwachungs- und Wartungsaufgaben. Der Remote-Administrator ist eine eingeschränkte Administrator-Rolle, die nicht über alle Rechte verfügt. Insbesondere kann der Remote-Administrator keine neuen Clientsysteme anlegen oder bestehende Clientsystem-Identitäten ändern. Dadurch ist ausgeschlossen, dass ein Remote-Administrator als Innentäter sich selbst als Clientsystem konfiguriert und somit dauerhaft remote mittels der Identität der jeweiligen LEI auf die TI und ihre Fachdienste zugreifen kann (bspw. ePA).

Der Remote-Administrator darf keinen Zugriff auf die SOAP/CETP-Schnittstellen haben (Ausschluss durch Netzwerk und/oder Authentifizierung)

Die Rolle entspricht dem bisherigen Remote-Administrator bei Inboxkonnektoren. Die Rolle ist optional.

4.6 Kunde - Leistungserbringer

Der Kunde, also der Leistungserbringer ist der Nutzer der fachlichen Schnittstellen(SOAP, LDAP, CETP, SICCT) einer konkreten HSK-Instanz und Inhaber einer SMC-B-Identität. Der Kunde hat Administrativen Zugang zu seiner HSK-Instanz.

Der Nutzer des Zugangsmoduls mit der Rolle Kunde

- bezieht ein Zugangsprofile zum TI-Gateway und
- vergibt/entzieht den Remote-Zugang zum Admin-Interface seiner HSK-Instanz für DVO.

Der Kunde hat einen Vertrag mit dem Anbieter des TI-Gateway und beauftragt ggf. einen DVO.

Weitere Rollen

Die Hersteller von anderen Komponenten (Intermediär, Zugangsmodul) haben abgesehen von ggf. Support für die von ihnen entwickelten Komponenten keine Rolle im Betrieb.

4.7 Rollenkombinationen & Rollenausschlüsse

Durch die Beschränkung der Rollen, die ein Mitarbeiter eines Anbieters TI-Gateway und seiner Unterauftragnehmer innehat, soll der Zugang zu medizinischen und personenbezogenen Versichertendaten verhindert werden.

Personen können mehrere der oben genannten Rollen ausführen. Folgende Rollen können dabei kombiniert werden

Erlaubte Rollenkombination

Szenario \ Rollen						
	Betreiber	Reseller	Hersteller	lokaler Admin/DVO	remote Admin	Leistungserbringer
Reseller mit DVO	✗	✓	✗	✓	✗	✗
Reseller mit Support	✗	✓	✗	✗	✓	✗
LE als Admin	✗	✗	✗	✓	✗	✓
Betreiber mit Support	✓	✗	✗	✗	✓	✗
Reseller und Betreiber	4-Augen Prinzip für Löschen von Instanz	4-Augen Prinzip für Löschen von Instanz	✗	✗	✗	✗

Abbildung 3: Szenarien mit erlaubten Rollenkombinationen

A_23237 - Rollenausschluss Betreiber - DVO

Der Anbieter des TI-Gateways MUSS sicherstellen, dass Personen aus dem Betrieb des TI-Gateways (Rolle Betreiber) nicht zeitgleich als lokale Administratoren von HSK-Instanzen des TI-Gateway (Rolle DVO) tätig werden 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 mit der Rolle Betreiber als auch für Personen mit der Rolle DVO innehaben darf (ausgenommen ist das Management des Unternehmens).[<=]

A_23238 - Rollenausschluss Hersteller - andere Rollen

Der Anbieter des TI-Gateways MUSS sicherstellen, dass keine Personen, die in der Herstellung (Entwicklung/Implementierung) des HSK und/oder des Zugangsmoduls tätig ist, Aufgaben eines Betreibers, Resellers oder DVOs übernimmt und dass entsprechende Prozesse definiert und etabliert sind, die dies dauerhaft gewährleisten und eine regelmäßige Validierung der Umsetzung durchsetzen.[<=]

Die Einschränkung aus den obigen Anforderung muss vertraglich zwischen Anbieter und seinen Unterauftragnehmern festgelegt werden. Die Unterauftragnehmer müssen diese Einschränkung vertraglich mit ihren Mitarbeitern festlegen.

A_23239 - Rollenkombination Betreiber - Reseller

Der Anbieter des TI-Gateway MUSS sicherstellen dass für das Löschen von HSK-Instanzen ein 4 Augen Prinzip unter Mitwirkung des Resellers zur Anwendung kommt.[<=]

5 Spezifikation Zugangsmodul

5.1 Onboarding und Registrierung

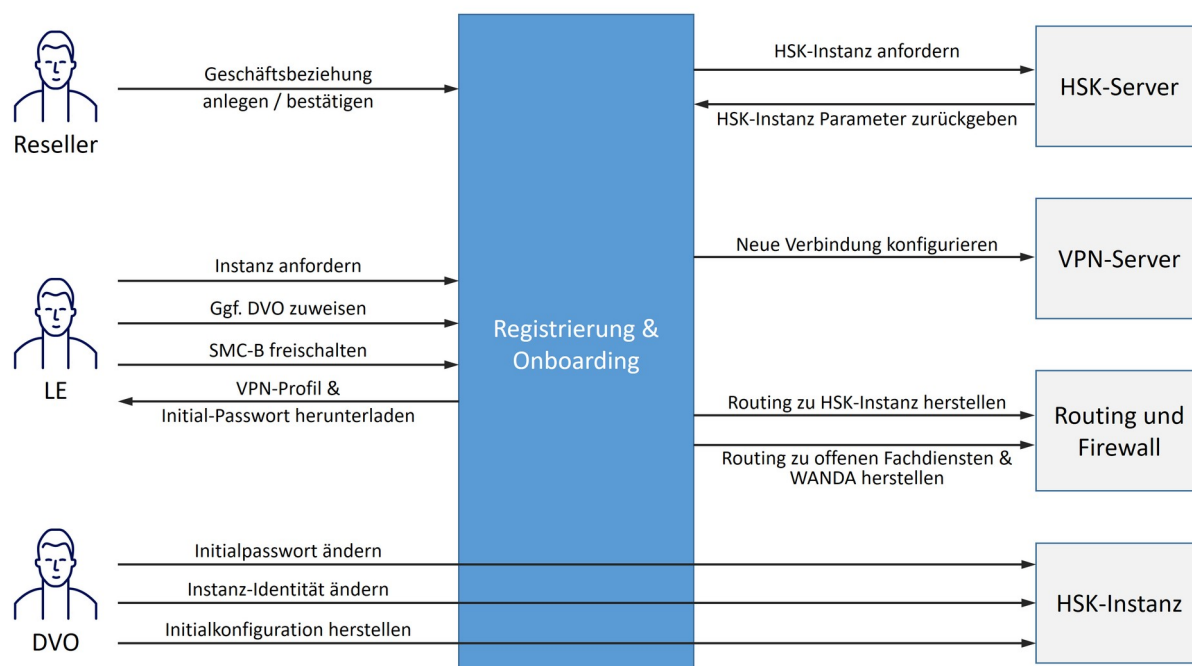


Abbildung 4: Onboarding und Registrierung

Der Anwender soll von dem System durch den Registrierungs- und Onboardingprozess geführt werden. Der Prozess soll in der Regel ohne Intervention eines Administrators auf Seiten des TI-Gateways durchgeführt werden. Im Folgenden wird der Prozess exemplarisch beschrieben. Die Konkrete Umsetzung darf davon abweichen, solange die formulierten Anforderungen erfüllt werden. Die Automatisierung manueller Schritte ist ausdrücklich erwünscht.

Der Reseller oder im Falle einer Selbstregistrierung der Leistungserbringer startet den Registrierungsprozess.

Der Leistungserbringer richtet eine Zwei-Faktor-Authentisierung (2FA) für seinen Zugang ein.

Nach erfolgreicher Registrierung erfolgt das Onboarding:

1. Das Onboarding-Modul löst am HSK-Server die Erzeugung einer HSK-Instanz aus. Darauf erhält das Onboarding-Modul die virtuelle IP-Adresse der HSK-Instanz und das initiale Admin-Passwort.
2. Das Onboarding-Modul generiert die benötigten VPN-Profile mit Credentials und der Inner-IP für die LE-Umgebung. Der LE wählt, ob er ein VPN-Profil für ein VPN-Gateway, mehrere VPN-Profile für Software-VPN-Clients auf verschiedenen Rechnern oder separate VPN-Profile für Kartenterminals benötigt.

3. Das Onboarding-Modul konfiguriert den VPN-Server und das Routing für diese LE-Umgebung zu der zugehörigen HSK-Instanz. Wenn ein über VPN angeschlossener DVO auf die HSK-Instanz zugreifen soll, gibt der LE diesen Netzwerkzugriff frei.

4. Der Nutzer oder sein DVO lädt die Zugangsdaten für die initiale Einrichtung aus dem Onboarding-Modul. Er richtet die lokale Umgebung inkl. des VPN-Clients ein. Über eine VPN-Kanal konfiguriert der DVO die HSK-Instanz. Dabei prüft der DVO zunächst das HSK-AK.AUT-Zertifikat. Anschließend ändert der DVO das Passwort zum Administrations-Zugang der Instanz, prüft auf ein "sauberes" (= leeres) Informationsmodell und erzeugt oder importiert eine individuelle TLS-Identität für die Instanz, welche dann in den Clientsystemen verteilt wird. Somit kann später bei jeder Server-Authentifizierung konkret die Instanz der LEI verifiziert werden (statt nur der HSK). Ansätze zur Authentifizierung der konkreten HSK-Instanz über eigene AK.AUT-Identitäten pro Instanz sind ebenso zulässig. Der DVO richtet initial mindestens das Informationsmodell für ein Kartenterminal mit einer SMC-B ein.

5. Das Onboarding-Modul prüft die SMC-B (Nutzung SMC-B über KT und HSK-Instanz; ggf. lokale Onboarding-Softwarekomponente notwendig, welche die Aufrufe der Konnektor-Operation steuert). Im Falle einer gültigen SMC-B schaltet das Onboarding-Modul das Routing aus dem LE-Netz zu WANDA und offenen Fachdiensten frei.

5.1.1 Nutzerportal

A_23241 - Nutzer-Portal für Leistungserbringer

Das Zugangsmodul MUSS ein Nutzer-Portal zur Interaktion des Leistungserbringers mit dem TI-Gateway bereitstellen, welches über eine Verbindung mit prüfbarer Authentizität des Servers und Schutz der Vertraulichkeit und Integrität erreicht wird. Wird das Nutzer-Portal über einen Web-Browser erreicht, MUSS es sich mit einem Extended Validation TLS-Zertifikat eines Herausgebers gemäß [CAB Forum] authentisieren und OCSP-Stapling [RFC-6066] umsetzen.【<=】

Das Zugangsmodul kann eine lokale Softwarekomponente umfassen. Das Zugangsmodul interagiert mit dem HSK über einen technischen User mit der Rolle Zugangsmodul.

A_23242 - TI-Gateway Zugangsmodul - Zwei-Faktor-Authentifizierung für Leistungserbringer

Das Zugangsmodul MUSS den Leistungserbringer für den Zugang zum Nutzer-Portal mit zwei Faktoren authentifizieren und dabei sowohl durchsetzen, dass die Faktoren aus verschiedenen Kategorien stammen:

- Wissen: Passwort (ORP.4.A22 des BSI-Grundschriftkompendiums ist zu beachten), PIN (min. 6-stellig);
- Besitz: Chipkarte, TAN-Generator, pushTAN, hardwaregebundenes kryptographische Token;
- Biometrie: Android: Biometric Class 3 (ehemals "Strong") oder äquivalent, iOS: Face-ID, Fingerabdruck;

als auch, dass die Faktoren nicht unabhängig voneinander angreifbar sind.

【<=】

Informationen zu Biometrie-Klassen unter Android sind unter <https://source.android.com/docs/compatibility/cdd> zu finden.

A_23338 - TI-Gateway Zugangsmodul - Schutz der Zugangsdaten

Das Zugangsmodul MUSS die Nutzer-Portal-Zugangsdaten/-faktoren der Nutzer geschützt vor unberechtigter Kenntnisaufnahme und Manipulation - auch von Administratoren - speichern. Das Zugangsmodul MUSS Änderungen von Zugangsdaten/-faktoren von

Nutzern mit zwei Faktor Authentisierung nur erfolgreicher Zwei-Faktor-Authentisierung zulassen.【<=】

A_23339 - TI-Gateway Zugangsmodul - Maßnahmen bei vergessenen oder verlorenen Zugangsfaktoren

Wenn das Zugangsmodul Maßnahmen zum Zurücksetzen von Zugangsfaktoren für das Nutzer-Portal implementiert, DARF es NICHT die Sicherheit der Zwei-Faktor-Authentisierung aushebeln.【<=】

Dies kann bspw. über ein registriertes E-Mail-Konto des Nutzers geschehen, sofern dieses in dem Sinne als dritter Faktor fungiert, also nicht bereits in die 2FA eingebunden ist und jeweils nur ein Faktor zurückgesetzt werden kann, also nicht beide gleichzeitig.

A_23363 - TI-Gateway Zugangsmodul - Freischaltung von HSK-Instanzen für Nutzer

Das Zugangsmodul MUSS durchsetzen, dass HSK-Instanzen erst erzeugt werden, wenn diesbezüglich ein Vertrag abgeschlossen wurde (Freigabe durch Reseller).【<=】

Die obige Anforderung zielt darauf ab, dass neue Nutzer vertrieblich qualifiziert werden, bevor sie Zugang zu einer HSK-Instanz bekommen. Damit soll ausgeglichen werden, dass die technische Berechtigungsprüfung mit der SMC-B erst später im Onboardingprozess erfolgen kann.

A_23353 - TI-Gateway Zugangsmodul - Erzeugung HSK-Instanz und VPN-Profil

Das Zugangsmodul MUSS für registrierte Nutzer folgendes erzeugen und für den Nutzer bereithalten:

- Eine oder mehrere HSK-Instanzen - entsprechend der Freigabe des Resellers - am HSK des TI-Gateway, wobei als Rückgabeparameter das initiale Passwort für den Instanz-Administrator und die Routinginformationen für die jeweilige Instanz erhalten wird.
- Ein VPN-Profil bestehend aus Daten, die für den Aufbau der VPN-Verbindung notwendig sind. (bspw. Client-Schlüssel und -Zertifikat, Informationen zu Adressierung und Routing, Vertrauensanker zur Authentifizierung des VPN-Konzentrators durch den Client).

【<=】

Als Variante zur Zustellung des VPN-Profiles über das Nutzerportal kann auch ein Provisionierungssystem angebunden werden, wenn z.B. vorkonfigurierte VPN-Gateway-Hardware zum Einsatz kommt.

Für den Fall, dass seine VPN-Schlüssel korrumpiert wurden, gilt:

A_23439 - TI-Gateway Zugangsmodul - Wechsel von VPN-Profilen

Das TI-GW-Zugangsmodul MUSS dem LE ermöglichen, bestehende VPN-Profile zu deaktivieren und neue VPN-Profile zu generieren.

【<=】

A_23281 - Schutz der privaten VPN-Schlüssel und initialer Passwörter bei zentraler Speicherung

Das Zugangsmodul MUSS das VPN-Profil eines Nutzers sowie das initiale Instanz-Administrator-Passwort ausschließlich dem authentifizierten Nutzer (Leistungserbringer) oder dem authentifizierten DVO, der vom Nutzer ausgewählt wurde, zugänglich machen. Die privaten Schlüssel für die VPN-Clientauthentisierung, die VPN-Serverauthentisierung und das initiale Instanz-Administrator-Passwort MÜSSEN bei der zentralen Speicherung vor unberechtigtem Zugriff und Manipulation - auch von Administratoren beim Zugangsmodul - geschützt sein, wobei dies neben organisatorischen Maßnahmen auch durch technische Maßnahmen unterstützt sein muss. So ist bspw. eine persistente Speicherung im Klartext und ohne Maßnahmen zum Erkennen von Änderungen unzulässig (siehe dazu auch A_23366*).【<=】

Es ist zulässig, dass DVOs über ein VPN an das TI-Gateway angeschlossen werden und nach Freigabe durch den LE als Administrator auf die HSK-Instanz des LE zugreifen. (Siehe 5.3 Routing und Firewall)

A_23385 - TI-Gateway Zugangsmodul - Sichere Übermittlung VPN-Profil an DVOs

Das Zugangsmodul MUSS das VPN-Profil eines DVOs vertraulich und integer an den authentifizierten DVO übermitteln. Dies muss jedoch nicht zwingend über das selbe Nutzerportal geschehen wie für Leistungserbringer. [≤]

A_23243 - Netzzugang zur TI nach SMC-B Prüfung

Das Zugangsmodul MUSS die SMC-B der LE-Institution inkl. Besitz des privaten Schlüssels und Online-Sperrstatus prüfen bevor es die Netzwerkverbindung zu WANDA und offenen Fachdiensten freigibt. Für diese Authentisierung wird die Identität HCI.AUT verwendet. [≤]

5.1.2 Initiale Authentifizierung der HSK-Instanz

Im Rahmen der Ersteinrichtung der HSK-Instanz muss sich der Nutzer bzw. der vom Nutzer beauftragte DVO bei der ersten Verbindung mit der Management-Schnittstelle davon überzeugen, dass er tatsächlich mit einem echten TI-Highspeed-Konnektor kommuniziert. Dafür muss die Authentizität des HSK über dessen TI-Identitäten (AK.AUT) geprüft werden. Hierbei kann eine HSK-weit genutzte Identität verwendet werden, diese muss also nicht Instanz-individuell sein. Erst nach dem Etablieren dieser Vertrauensbeziehung können nachfolgende Prüfschritte und die Ersteinrichtung stattfinden, wobei dann bspw. auch individuelle Identitäten und Zertifikate für spätere Verbindungen zur SOAP- und Management-Schnittstelle erzeugt werden.

Der einfachste Fall - wie er auch bei Inbox-Konnektoren vorliegt - ist eine über den Webbrowser bediente Administrations-GUI. Diese hat für die Zertifikatsprüfung den Nachteil, dass Webbrowser keine TI-Zertifikate positiv validieren. Im Falle von Inboxkonnektoren können entsprechende Warnungen des Browsers durch die manuelle Prüfung von im Browser anzeigbaren Zertifikatsdaten sowie vor allem die gleichzeitige Kontrolle über Konnektor, Netzwerk und Client akzeptiert werden. Dies ist beim TI-Gateway nicht möglich. Es ist ein essentieller Schritt bei der ersten Verbindung die Authentizität technisch vollständig zu prüfen.

Allein mit einem Webbrowser ist dies also beim TI-Gateway nicht möglich (oder nur höchst umständlich). Daher ist ein zusätzlicher Software-Client notwendig, der mindestens die Prüfung des TI-Zertifikats übernimmt und entweder weiter gefasst ist und auch die Management-GUI umfasst oder zumindest eine Validierung des anschließend im Browser mit einer Warnung angezeigten Zertifikats ermöglicht (Abgleich von Fingerprint des im Software-Client geprüften Zertifikats gegen den im Browser anzeigbaren Fingerprint). Letztere Variante ermöglicht anschließend eine Nutzung des Browsers für die Administration. In der Minimal-Version ist der Software-Client ein Kommandozeilen-Tool.

Sofern ein Browser involviert ist, sind die dadurch gegebenen Implikationen von Herstellern und Anbietern zu berücksichtigen, wie die in Webbrowsern nicht vorhandene Unterstützung von Zertifikaten und Schlüsseln, die auf Brainpool-Kurven basieren. Auch wenn nur einmalig bei der initialen Verbindung das C.AK.AUT in Zusammenspiel mit einem Webbrowser verwendet werden soll (weil anschließend Instanz-individuelle self-signed-Zertifikate erzeugt oder importiert werden), ist dies technisch nicht möglich, wenn das C.AK.AUT auf Brainpool-Kurven basiert.

Die geschilderte Prüfung der Authentizität gegen eine TI-Identität muss lediglich einmalig als initialer Schritt stattfinden. Über die so gebildete Vertrauensbeziehung ist die

Erzeugung oder der Import individueller Nicht-TI-Identitäten möglich, wie es auch Einbox-Konnektoren heute schon unterstützen. Diese Identitäten können dann in Form von Allow-Listen in die genutzten Clientsysteme importiert werden, sodass spätere Authentifizierungen gegen diese Prüfbasis durchgeführt werden. Erzeugung und Import individueller Nicht-TI-Identitäten kann für eine einfache Handhabung in das Tool integriert werden.

Grundsätzlich ergibt sich somit initial folgender Ablauf:

- Nutzer bzw. DVO (im Folgenden nur DVO) hat VPN-Profil, Initial-Passwort und Software-Client heruntergeladen
- DVO hat den VPN-Client installiert / eingerichtet und den VPN-Tunnel aufgebaut
- DVO kennt IP-Adresse seiner HSK-Instanz und kann diese von seinem Clientsystem aus über den VPN-Tunnel erreichen
- DVO nutzt den Software-Client, welcher parametrisiert mit der IP-Adresse der HSK-Instanz einen TLS-Verbindungsaufbau zur Management-Schnittstelle der Instanz durchführt und das C.AK.AUT prüft
- Der Software-Client gibt im Positiv-Fall das Prüfergebnis sowie den SHA-256 Wert des geprüften C.AK.AUT aus
- DVO verbindet sich über Webbrowser mit der HSK-Instanz
- Der Webbrowser gibt eine Warnung zur unsicheren Verbindung aus
- DVO lässt sich über die weiteren Informationen das Zertifikat und dort den SHA-256 Wert anzeigen
- DVO vergleicht die SHA-256 Werte und akzeptiert im Positiv-Fall die Verbindung im Browser
- Es findet die Ersteinrichtung unter Berücksichtigung weiterer Prüfungen im Webbrowser statt (siehe A_23340*).

Da der Software-Client die Zertifikatsprüfung durchführt, muss genau dieser Aspekt durch einen Gutachter technisch geprüft werden (A_23341*).

Für den Highspeed-Konnektor ist in diesem Zusammenhang A_23469* und A_23470* in [gemF_Highspeed-Konnektor] zu beachten.

A_23341 - TI-Gateway Zugangsmodul - Client-Software für Prüfung HSK-TLS-Zertifikat

Das TI-GW-Zugangsmodul MUSS eine Client-Software umfassen, welche unter Angabe der IP-Adresse der HSK-Instanz einen TLS-Verbindungsaufbau zur Management-Schnittstelle dieser Instanz durchführt, dabei das C.AK.AUT Zertifikat des HSK wie folgt prüft:

- Prüfung der Signatur des Zertifikats gegen ein aktuell gültiges Komponenten-CA-Zertifikate [GEM.KOMP-CAX.der] vom TSL-Downloadpunkt <https://download.tsl.ti-dienste.de/SUB-CA/>,
- Prüfung auf zeitliche Gültigkeit des Zertifikats,
- Prüfung auf die Zertifikatstyp-OID oid_ak_aut,
- Prüfung auf Sperrstatus "good" mittels des OCSP-Responders der Komponenten-CA im Internet
(RSA: <http://download.crl.ti-dienste.de/ocsp> | ECC:
<http://download.crl.ti-dienste.de/ocsp/ec>),

ein entsprechend aussagekräftiges Prüfergebnis ausgibt und im Positiv-Fall zusätzlich den SHA-256 Wert des Zertifikats ausgibt, mit dem sich das Admin-Interface der HSK-Instanz

bei nachfolgenden Verbindungen Identifiziert (C.AK.AUT oder ggf. über Client-SW bereits importiertes oder erzeugtes individuelles Zertifikat).【<=】

Die Internet-Schnittstelle des OCSP-Responders der Komponenten-CA für die RU/TU finden sich hier:

- RSA: <http://download-testref.crl.ti-dienste.de/ocsp>
- ECC: <http://download-testref.crl.ti-dienste.de/ocsp/ec>

A_23340 - TI-Gateway Zugangsmodul - Beschreibung Authentifizierung & Verifikation HSK-Instanz

Der Anbieter TI-Gateway MUSS seinen Nutzern (Leistungserbringer bzw. deren DVO) Informationen zur Hand geben, dass beim initialen Verbindungsaufbau zur Administrationsschnittstelle der HSK-Instanz deren Authentizität überprüft werden muss und wie dies möglich ist. Dies umfasst mindestens

- die technische Prüfung des TLS-Zertifikats C.AK.AUT des HSK mittels des Software-Clients (siehe A_23341*)
- Bei Verwendung eines Webbrowsers zur Administration:
 - der Abgleich des SHA-256 Werts des im Browser bei der Verbindung zur Management-Schnittstelle der HSK-Instanz mit einer Sicherheitswarnung angezeigten Zertifikats gegen den durch den Software-Client angezeigten SHA-256 Wert
- die Verifikation, dass die HSK-Instanz zur Änderung des Passworts für den Admin-Account auffordert,
- die Änderung des Passworts des Admin-Accounts,
- die Verifikation, dass keine weiteren Admin-Nutzer in der HSK-Instanz angelegt sind,
- die Verifikation, dass das Informationsmodell der HSK-Instanz leer/unkonfiguriert ist bei der Ersteinrichtung,
- Import der individuellen HSK-Instanz-Identität in die "Allowlist" der Clientsysteme und den ggf. für die Administration genutzten Webbrowser
 - entweder durch die Erzeugung oder den Import einer HSK-Instanz-individuellen Server-Identität
 - oder durch die Nutzung der AK.AUT-Identitäten sofern diese HSK-Instanz-individuell sind, also genau eine AK.AUT-Identität immer genau einer HSK-Instanz zugeordnet ist.

Zudem MUSS der Nutzer darauf hingewiesen werden im Nutzer-Portal zu prüfen, dass initial keine Freischaltung für Remote-Zugänge zur HSK-Instanz aus DVO-Netzen konfiguriert sind.

【<=】

Die oben in A_23340* dargestellten Prüfungen sind wie bereits zu Beginn des Abschnitts geschildert einmalig beim initialen Verbindungsaufbau durchzuführen. Anschließende Zertifikats-Prüfungen erfolgen gegen eine Allowlist wie im letzten Punkt von A_23340* beschrieben.

5.1.3 Betriebsfunktionen für den Leistungserbringer

A_23302 - Anzeige Verfügbarkeit und Service Level

Der Produkttyp TI-Gateway-Zugangsmodule MUSS dem Leistungserbringer die aktuelle Verfügbarkeit des Services und die erreichten Werte für die Service-Level zur Verfügbarkeit anzeigen. [≤]

Umgesetzt werden kann diese Anforderung über das Nutzer-Portal oder über eine lokale Softwarekomponente. Bei einer lokalen Softwarekomponente muss die Internet-Verfügbarkeit überwacht werden, um nicht die Verfügbarkeit der TI-Gateway Services zu verzerren. Verfügbarkeitsdaten werden vom HSK ermittelt und dem Zugangsmodule bereitgestellt (siehe A_23446).

5.2 VPN

Der VPN-Service des TI-Gateway-Zugangsmoduls ermöglicht es Leistungserbringerumgebungen eine VPN-Verbindung zum TI-Gateway aufzubauen. Es sind unterschiedliche VPN-Lösungen und -Clients erlaubt, solange sie den folgenden Sicherheits-Mindestanforderungen genügen.

A_23351 - TI-Gateway-Zugangsmodule - Verbindungen ausschließlich über VPN

Das Zugangsmodule MUSS sicherstellen, dass Verbindungen zur Nutzung von HSK-Instanzen des HSK des TI-Gateways ausschließlich über einen VPN-Kanal akzeptiert werden. [≤]

A_23379 - TI-Gateway-Zugangsmodule - VPN - Protokoll

Das Zugangsmodule MUSS Nutzer mittels eines VPN-Kanals anbinden, welcher auf den Protokollen IPsec/IKEv2 oder WireGuard beruht und dafür VPN-Server und VPN-Client bereitstellen. [≤]

Als VPN-Protokolle sind aktuell IPsec/IKEv2 oder WireGuard vorgesehen.

Hinweis bzgl. WireGuard

Das WireGuard-Protokoll und die darin genutzten kryptographischen Algorithmen befinden sich derzeit noch in einer detaillierteren Sicherheitsbewertung, weshalb diese aktuell noch mit einem Vorbehalt versehen sind.

Dies betrifft die Anforderungen

- A_23379* (Protokoll),
- A_23375* und A_23377* (Curve25519),
- A_23376* (ChCha20Poly1305) und
- A_23378* (BLAKE2s).

Andere Protokolle sind nicht grundsätzlich ausgeschlossen, müssen jedoch mit der gematik abgestimmt werden. In Bezug auf das WireGuard-Protokoll siehe auch:

- "Whitepaper Wire Guard" <https://www.wireguard.com/papers/wireguard.pdf>
- "Mechanised Cryptographic Proof" <https://hal.inria.fr/hal-02100345v3/document>

Es kann für eine LEI sowohl eine VPN-Verbindung zu einem VPN-Router aufgebaut werden, als auch mehrere VPN-Verbindungen zu einzelnen Rechnern und Kartenterminals. Dabei müssen unterschiedliche VPN-Client-Identitäten zum Einsatz kommen.

A_23375 - TI-Gateway-Zugangsmodule - VPN - Authentisierung

Das Zugangsmodule MUSS für den VPN-Kanal eine zwingende beidseitige Authentisierung am Server und Client durchsetzen, wobei jeweils sowohl die eigene Authentisierung als auch die Authentifizierung des Gegenübers mindestens anhand statischer asymmetrische Schlüsselpaare stattfinden muss und dabei für die Schlüsselpaare asymmetrische Algorithmen aus der Menge {RSA3072, ECC-NIST-P-256, ECC-Brainpool256r1, ECC-Curve25519} verwendet werden müssen. [≤]

A_23376 - TI-Gateway-Zugangsmodule - VPN - Transportschutz

Das Zugangsmodule MUSS für den VPN-Kanal am Server und am Client einen Transportschutz für alle übermittelte Daten bzgl. Vertraulichkeit und Integrität durchsetzen unter Verwendung symmetrischer Chiffren aus der Menge {AES128, AES256, ChaCha20Poly1305}. [≤]

A_23377 - TI-Gateway-Zugangsmodule - VPN - Ephemere Sitzungs-Schlüssel

Das Zugangsmodule MUSS für den VPN-Kanal Forward-Secrecy Server- und Client-seitig durchsetzen mit ephemeren ECDH-Schlüsseln aus der Menge {ECC-NIST-P-256, ECC-Brainpool256r1, ECC-Curve25519}. [≤]

A_23378 - TI-Gateway-Zugangsmodule - VPN - Hash-Funktionen

Das Zugangsmodule MUSS für alle im Rahmen des Aufbaus und Betriebs des VPN-Kanals notwendigen Hashwertberechnungen Hashfunktionen aus der Menge {SHA256, BLAKE2s} im Server und im Client verwenden. [≤]

A_23380 - TI-Gateway-Zugangsmodule - VPN - Prüfung Sperrstatus Clients

Das Zugangsmodule MUSS bei der Client-Authentifizierung durch den Server im Rahmen des VPN-Verbindungsaufbaus den Sperrstatus der Client-Identität prüfen (Vergleich A_23261*). [≤]

A_23381 - TI-Gateway-Zugangsmodule - VPN - Abbruch Verbindungsaufbau im Fehlerfall

Das Zugangsmodule MUSS durchsetzen, dass sowohl im Server als auch im Client, wenn Fehler im Rahmen der beidseitigen Authentisierung oder des Schlüsselaustauschs auftreten, jeweils ein Abbruch des Verbindungsaufbaus stattfindet. [≤]

A_23364 - TI-Gateway-Zugangsmodule - VPN-Client - Server-Authentifizierung

Der VPN-Client eines TI-Gateway-Zugangsmoduls MUSS den VPN-Server gegen eine ihm vorliegende Prüfbasis authentifizieren. [≤]

Die Prüfbasis hängt vom gewählten Authentifizierungsverfahren ab: Schlüssel, Zertifikat, CA-Zertifikat...

A_23365 - TI-Gateway-Zugangsmodule - VPN-Client - VPN-Protokoll

Der Hersteller des VPN-Client eines TI-Gateway-Zugangsmoduls MUSS das VPN-Protokoll im Client entsprechend A_23375*, A_23376*, A_23377*, A_23378*, A_23379* und A_23381* umsetzen und dies im Rahmen des Sicherheitsnachweis (Produktgutachten) mindestens durch entsprechende Tests inkl. Negativ-Testfälle im Blackbox-Ansatz verifizieren lassen. [≤]

Idealer Weise können bestehende Sicherheitsnachweise zum VPN-Client nachgenutzt werden.

A_23382 - TI-Gateway VPN-Client - Nutzerinformation

Der Anbieter des TI-Gateways MUSS seine Nutzer verständlich zum sicheren Umgang mit den privaten VPN-Client-Schlüsseln und zur korrekten Installation und Nutzung des VPN-Clients informieren. [≤]

A_23245 - VPN-Server Konfiguration durch Onboarding-Modul

Der VPN-Server des Zugangsmoduls MUSS ausschließlich Verbindungen annehmen, für die er vom Onboarding-Modul ein VPN-Profil erhalten hat. [≤]

5.3 Routing und Firewall

A_23246 - Routing zur zugewiesenen HSK-Instanz

Das TI-GW-Zugangsmodul MUSS sicherstellen, dass eine LE-Institution nur die Interfaces der ihr zugewiesenen HSK-Instanz erreichen kann. [≤]

Einem Kunden können mehrere HSK-Instanzen zugewiesen werden, aber eine HSK-Instanz kann nur einem Kunden zugewiesen sein. Siehe auch A_23390

A_23370 - Zugang zum Administrationsinterface einer HSK-Instanz

Das TI-GW-Zugangsmodul MUSS sicherstellen, dass das Administrationsinterface einer HSK-Instanz nur aus dem Netz der zugeordneten LE-Institution und einem möglicherweise vom Leistungserbringer freigegebenen DVO-Netz möglich ist. [≤]

Für den Zugang zum Administrationsinterface sind zwei unabhängige Sicherungsschichten umzusetzen. Eine Schicht kontrolliert den Zugang zum Administrationsinterface, die zweite Schicht ist die Authentisierung an der HSK-Instanz.

A_23394 - Routing zum fachlichen Interface einer HSK-Instanz

Das TI-GW-Zugangsmodul MUSS sicherstellen, dass das fachliche Interface (SOAP, LDAP, CETP) einer HSK-Instanz nur aus dem Netz der zugeordneten LE-Institution möglich ist - also auch explizit nicht aus einem möglicherweise vom Leistungserbringer für die Administration freigegebenen DVO-Netz. [≤]

A_23371 - DVO-Netzzugang entziehen

Das TI-GW-Zugangsmodul MUSS es einem Leistungserbringer ermöglichen, den Zugang zum Administrationsinterface aus einem DVO-Netz auch wieder zu entziehen. [≤]

5.4 Sicherheit & Datenschutz

TIP1-A_5389-01 - TI-GW-Zugangsmodul, zyklische Prüfung der C.HCI.AUT Zertifikate

Das Zugangsmodul MUSS die Gültigkeit (inkl. Online-Sperrstatus) aller aktiven C.HCI.AUT (SM-B-AUT-Zertifikat) einmal täglich prüfen. [≤]

TIP1-A_5390-01 - TI-GW-Zugangsmodul, gesperrtes C.HCI.AUT Zertifikat

Das Zugangsmodul MUSS, wenn die zyklische Prüfung ergeben hat, dass eine HSK-Instanz keinen Zugriff auf ein gültiges C.HCI.AUT (SM-B-AUT-Zertifikat) hat, das mit dieser Instanz assoziierte Routing zu offenen Fachdiensten und Wanda unverzüglich entfernen und den Leistungserbringer benachrichtigen. Die Anzahl der auf diese Weise gesperrten Zugänge muss an die gematik reported werden. [≤]

Die eigentliche Gültigkeitsprüfung der SM-B wird durch den HSK durchgeführt (A_23444). Die Freischaltung der offenen Fachdienste und Wanda wird durch A_23243* geregelt.

A_23248 - DDoS-Protection

Das TI-GW-Zugangsmodule und der Anbieter des TI-Gateway MÜSSEN Angriffe auf die Verfügbarkeit des TI-Gateways (DDoS) an seinen Schnittstellen zum Internet abwehren und dabei die Empfehlungen des BSI sowie, wenn ein qualifizierter Dienstleister zum Schutz vor DDoS-Angriffen beauftragt wird, die Kriterien des BSI zur Auswahl qualifizierter Dienstleister berücksichtigen.【<=】

Empfehlungen des BSI zur Abwehr von DDoS-Angriffen sind unter https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Gefahren/DDoS/ddos_node.html und Kriterien für entsprechende Dienstleister sind unter https://www.allianz-fuer-cybersicherheit.de/Webs/ACS/DE/Informationen-und-Empfehlungen/Informationen-und-weiterfuehrende-Angebote/Qualifizierte-Dienstleister/qualifizierte-dienstleister_node.html zu finden.

A_23249 - Erkennung und Abwehr unberechtigter Zugriffe

Das TI-GW-Zugangsmodule MUSS Maßnahmen zum Erkennen und zur Abwehr unberechtigter Zugriffe aus dem Internet sowie aus angeschlossenen LEI- und DVO-Netzen umsetzen (bspw. durch Paketfilter, Netflow, IDS/IPS, ALG).【<=】

Auch aus per VPN angeschlossenen Netzen von Leistungserbringerinstitutionen sowie ggf. DVOs dürfen nur erlaubte Kommunikationen/Protokolle/Funktionen möglich sein. Insbesondere kann vor der Prüfung der SMC-B nicht sicher davon ausgegangen werden, dass tatsächlich Leistungserbringer über einen VPN-Kanal mit dem TI-Gateway interagieren.

A_23392 - Sperrung VPN-Zugänge bei detektierten Angriffen

Das TI-GW-Zugangsmodule MUSS, wenn über Netze von angeschlossenen Nutzern (LEI/DVO) Angriffe detektiert werden, die Nutzer dieser Zugänge unverzüglich darüber informieren und Maßnahmen bis hin zur Sperrung der betroffenen VPN-Zugänge umsetzen. Eine vollständige Sperrung des Zugangs muss dabei immer das letzte Mittel sein.【<=】

A_23393 - Prozesse zur schnellen Kommunikation und Entsperrung von VPN-Zugängen

Der Anbieter TI-Gateway MUSS Prozesse zur Behandlung und Klärung erkannter Angriffe aus Nutzer-Netzen etablieren, sodass eine schnelle Kommunikation mit betroffenen Kunden und eine Klärung der Situation möglich ist und eine Sperrung möglichst, vermieden werden kann, sofern dies sicherheitstechnisch vertretbar ist. Ebenso müssen Situationen, die zu einer Sperrung geführt haben, schnellst möglich geklärt werden können um den Zugang wieder zu entsperren.【<=】

TIP1-A_4338-01 - TI-GW-Zugangsmodule, Sicherung zum Transportnetz Internet durch Paketfilter

Das TI-GW-Zugangsmodule MUSS das TI-Gateway zum Transportnetz Internet durch einen zustandslosen Paketfilter (ACL) absichern, welcher ausschließlich die erforderlichen Protokolle weiterleitet. Der Paketfilter MUSS frei konfigurierbar sein auf der Grundlage von Informationen aus OSI Layer 3 und 4, das heißt Quell- und Zieladresse, IP-Protokoll sowie Quell- und Zielport.【<=】

TIP1-A_4339-01 - TI-GW-Zugangsmodule, Platzierung Paketfilters Internet

Der Paketfilter des TI-GW-Zugangsmoduls zum Schutz der VPN-Konzentratoren in Richtung Transportnetz Internet DARF NICHT auf den VPN-Konzentratoren implementiert werden.【<=】

A_23342 - TI-GW-Zugangsmodule - Richtlinien für den Paketfilter zum Internet

Der Paketfilter des TI-GW-Zugangsmoduls MUSS die Weiterleitung von IP-Paketen an der Schnittstelle zum Internet auf genau die Protokolle beschränken, die für die verwendete VPN-Technologie und das Nutzer-Portal zwingend erforderlich sind. Ein Verbindungsaufbau aus dem TI-GW-Zugangsmodule in Richtung Internet MUSS

unterbunden werden. Ausnahmen davon bspw. für die Erreichbarkeit von Update-Servern sind mit dem Gutachter abzustimmen, von diesem zu bewerten und im Falle der Abnahme (positiven Bewertung) durch den Gutachter nachvollziehbar im Gutachten zu dokumentieren. [≤]

A_23457 - Weiterleitung gesammelter Informationen zu Bedrohungen an zentrales Security Monitoring

Der Anbieter TI-Gateway MUSS die Informationen über potenzielle Bedrohungen, die durch die Umsetzung von A_23248*, A_23249*, A_23342* und TIP1-A_4338* gesammelt werden an ein zentrales Security Monitoring (siehe GS-A_5557* und A_20719*) zur übergreifenden Erkennung und Analyse weiterleiten. [≤]

TIP1-A_4292-01 - TI-GW-Zugangsmodul, Härtung des VPN-Konzentrators

Die VPN-Konzentratoren des Zugangsmoduls MÜSSEN so konfigurieren werden, dass ausschließlich die erforderlichen Netzwerkprotokolle und kryptographischen Methoden akzeptiert werden. [≤]

A_23343 - TI-GW-Zugangsmodul - Kein direkter Zugriff auf zentrale Dienste und gesicherte Fachdienste

Das TI-GW-Zugangsmodul MUSS einen direkten Zugriff aus dem Internet und den Netzen angeschlossener Nutzer auf gesicherte Fachdienste und zentrale Dienste verhindern. [≤]

A_23344 - TI-GW-Zugangsmodul - Verbindungen bei Komponentenausfall beenden

Das TI-GW-Zugangsmodul MUSS sicherstellen, dass alle bestehenden VPN-Verbindungen beendet werden und keine neuen Verbindungen zugelassen werden, wenn nachgelagerte Komponenten vollständig ausgefallen sind und dadurch die Nutzung des TI-Gateways nicht mehr möglich ist. [≤]

A_23345 - TI-GW-Zugangsmodul - Härtung Zugänge

Das TI-GW-Zugangsmodul MUSS sicherstellen, dass es ausschließlich definierte und gehärtete Schnittstellen anbietet - auch für die Administration - ohne Low-Level-Zugänge mit Systemrechten. [≤]

A_23366 - TI-GW-Zugangsmodul - Nutzung HSM

Das TI-GW-Zugangsmodul MUSS für die Erzeugung von Zufallszahlen und Schlüsseln ein nach FIPS 140-2 Level 3 oder Common Criteria EAL 4 zertifiziertes HSM verwenden und geheime Schlüssel in diesem HSM vor Zugriff geschützt speichern, so dass nur das TI-GW-Zugangsmodul selbst die Schlüssel nutzen kann. Dies bezieht sich mindestens auf folgende Schlüssel:

- Geheime Schlüssel zur Authentisierung gegenüber dem HSK
- Schlüssel zum Schutz von Vertraulichkeit und Integrität persistent gespeicherter Daten (bspw. die privaten Schlüssel von VPN-Konzentratoren)

[≤]

A_23473 - TI-GW-Zugangsmodul - Nachnutzung HSM des HSK

Das TI-GW-Zugangsmodul KANN das HSM des Highspeed-Konnektors nachnutzen, sofern der Highspeed-Konnektor dies entsprechend A_23474* und A_23475* zulässt. HSM-Administrator bleibt in diesem Fall jedoch der Hersteller des HSK. [≤]

A_23390 - TI-Gateway-Zugangsmodul - Eigene HSK-Instanz pro Kunde

Das TI-GW-Zugangsmodul MUSS jedem Nutzer seine eigene virtuelle HSK-Instanz zuweisen, sodass nie unterschiedliche Nutzer die selbe HSK-Instanz verwenden. [≤]

Es ist weiterhin möglich, dass Leistungserbringer bspw. in Gemeinschaftspraxen oder einem MVZ eine einzige HSK-Instanz gemeinsam verwenden. In diesem Fall treten die Leistungserbringer gegenüber dem TI-Gateway-Anbieter als ein einziger Nutzer auf. Dies ist analog zur Nutzung eines Inbox-Konnektors mit einem VPN-Zugang durch mehrere Leistungserbringer, wobei diese ebenso gegenüber dem VPN-Zugangsdienst-Anbieter als ein Nutzer erscheinen.

Die Nutzung mehrerer Instanzen durch einen einzigen Nutzer ist problemlos, solange die Nutzung jeder Instanz entsprechend A_23390* exklusiv durch diesen Nutzer stattfindet.

A_23354 - TI-Gateway-Zugangsmodul - Kopplung HSK, Prüfung Identität des HSK

Das Zugangsmodul in einem TI-Gateway MUSS bei der beidseitigen Authentisierung mit dem HSK die Identität (I.AK.AUT) des HSK prüfen und seine eigenen Clientsystem-Credentials hinsichtlich Vertraulichkeit und Integrität geschützt speichern. [≤]

A_23362 - TI-Gateway-Zugangsmodul - Kopplung HSK, Geschützter Import Clientsystem-Credentials

Der Anbieter TI-Gateway MUSS einen sicheren Prozess zur Erzeugung und/oder Import der Clientsystem-Credentials des Zugangsmoduls für die Verbindung zum HSK etablieren, der die Vertraulichkeit und Integrität der Clientsystem-Credentials wahrt und gewährleistet, dass Clientsystem-Credentials nicht dauerhaft außerhalb des Zugangsmoduls oder HSK vorliegen. [≤]

Die Administration des Zugangsmoduls lässt somit nur den Import der Clientsystem-Credentials zu, nicht jedoch das Auslesen dieser.

A_23261 - Sperrbarkeit von Institutionen

Der Anbieter TI-Gateway und das Zugangsmodul MÜSSEN über organisatorische und technische Maßnahmen verfügen, um einzelne angeschlossene Institutionen vom Zugang zur TI auszuschließen, unter anderem auch auf Weisung der gematik. [≤]

Die gematik muss den Zugang von Leistungserbringerinstitutionen bspw. für den Fall der Verwendung veralteter, schwachstellenbehafteter Versionen anderer TI-Komponenten sperren lassen können, da solche Komponenten eine Bedrohung für die gesamte TI darstellen können.

A_23490 - TI-Gateway-Zugangsmodul - Keine Unterbrechung TLS-Kanal zur HSK-Instanz-Administration

Das TI-GW-Zugangsmodul DARF NICHT die TLS-Verbindung des Nutzers bzw. DVOs zur Management-Schnittstelle der jeweiligen HSK-Instanz unterbrechen. Die Verbindung ist immer Ende-zu-Ende vom Nutzer bzw. DVO, der sich somit auch immer direkt an der HSK-Instanz authentisiert. [≤]

5.5 Rohdaten-Performance-Reporting

verschoben nach [gemSpec_Perf::2.5.2 Rohdaten-Performance-Reporting (Rohdatenerfassung v.02)]

5.5.1 Umfang

verschoben nach [gemSpec_Perf::2.5.2.1 Umfang]

5.5.2 Lieferintervalle

verschoben nach [gemSpec_Perf::2.5.2.2 Lieferintervalle]

5.5.3 Format

verschoben nach [gemSpec_Perf::2.5.2.3 Format]

Neue Anforderungen in Kapitel "3.x.2.2 Format"

verschoben nach [gemSpec_Perf::2.5.2.2 Format]

5.6 Lastanforderungen

verschoben nach [gemSpec_Perf::3.10.1.3 Performancevorgaben TI-Gateway]

6 Anforderungshaushalt TI-Gateway

Dem Anbietertyp TI-Gateway sind Betriebliche Anforderungen aus den Spezifikationen gemSpec_DS_Anbieter, gemRL_Betr_TI, gemKPT_Betr, gemKPT_Test, gemSpec_Perf, gemSpec_Krypt und gemSpec_Net zugewiesen.

6.1 Neue Anforderungen

6.1.1 Anbietererklärung

A_18737-01 - Sperrung von Zugängen zur TI

Der Anbieter TI-Gateway MUSS nach Weisung der gematik Zugänge zur TI sperren. [≤]

A_23472 - Auftragsverarbeitung bei weiteren Diensten

Der Anbieter TI-Gateway MUSS für weitere Services, bei denen medizinische oder personenbezogene Daten verarbeitet werden, einen Vertrag zur Auftragsverarbeitung mit seinen Kunden schließen und diesen transparent machen, dass solche Services nicht im Rahmen der Anbieterzulassung des TI-Gateways geprüft wurden.

[≤]

Auf Grund der Informationsflüsse ist es sinnvoll das KIM-Clientmodul in das TI-Gateway zu integrieren.

TIP1-A_4323-01 - TI-Gateway, http-Forwarder - Verteilung

Der Anbieter des TI-Gateways MUSS pro Standort mindestens einen http-Forwarder bereitstellen, der sich netzwerktechnisch in der Service-Zone TI befindet.

[≤]

A_23481 - http-Forwarder - IP-Adresse

Der Anbieter des HSK oder TI-Gateways MUSS jedem http-Forwarder eine IP-Adresse aus dem Adressbereich der Service-Zone des Standortes zuweisen. [≤]

A_23487 - Aktualisierbarkeit von VPN-Clients

Der Anbieter des TI-Gateways MUSS Maßnahmen umsetzen, um die Aktualität der eingesetzten VPN-Clients und weiterer ggf. ausgelieferter Client-Software sicherzustellen.

[≤]

6.1.2 Sicherheitsgutachten

Es sind wie beschrieben Konstellationen möglich und zulässig, bei denen ein Anbieter TI-Gateway nicht selbst alle Anforderungen erfüllt, sondern in der Zusammenarbeit zwischen Reseller und Infrastrukturbetreiber Anforderungen von einer Partei erfüllt und nachgewiesen werden und von der anderen Partei dies im Rahmen der Anbieterzulassung nachgenutzt wird. Es muss jedoch stets nachgewiesen werden, dass in Summe alle Anforderungen erfüllt sind und keine Lücken durch gegenseitige Verweise auf die Verantwortung des anderen entstehen.

A_23352 - Anforderungsabdeckung von zugekaufter Leistung

Der Anbieter des TI-Gateways MUSS, wenn er zur Erfüllung von Anforderungen Leistungen einer andern Partei (Infrastrukturbetreiber oder Reseller) erwirbt bzw. nachnutzt, nachweisen, dass diese Anforderungen für ihn von der anderen Partei erfüllt werden, was mindestens einen Verweis auf den bestehenden Nachweis der anderen

Partei zur Erfüllung der nachgenutzten Anforderung und die vertragliche Regelung zur Erbringung eben dieser Leistung durch die andere Partei für den Zulassungsnehmer beinhalten muss. [≤]

TIP1-A_4482-01 - TI-Gateway, Kommunikation LE-Institutionen

Der Anbieter des TI-Gateways MUSS sicherstellen, dass eine direkte Netzwerkkommunikation zwischen LE-Institutionen über das TI-Gateway nicht möglich ist. [≤]

Die geeignete und robuste technische Umsetzung obliegt dem Anbieter (Firewalls, VLANs).

TIP1-A_4341-01 - TI-Gateway, Erkennung von Angriffen

Der Anbieter des TI-Gateways MUSS durch technische und organisatorische Maßnahmen sicherstellen, dass Angriffe aus dem Internet auf das TI-Gateway erkannt werden. Als geeignete Maßnahmen werden angesehen:

- Auswertung von Logfiles
- Auswertung von Netflow
- Intrusion Detection Systeme (IDS)

[≤]

Der Anbieter muss dabei berücksichtigen, dass sowohl Bestandskunden, als auch Neukunden, deren SMC-B noch nicht geprüft wurde, möglicherweise ein Angreifer sind.

GS-A_4847-01 - Produkttyp TI-Gateway, DNSSEC im Namensraum Transportnetz

Anbieter des TI-Gateways MÜSSEN den Namensraum Transportnetz per DNSSEC sichern. [≤]

Der Hersteller muss die für sein Produkt erforderlichen Protokolle angeben wie in TIP1-A_4340-01.

A_23494 - 4-Augen-Prinzip bei Wartung HSK

Der Anbieter des TI-Gateway MUSS Zugriffe auf den HSK (vgl. gemF_Highspeed-Konnektor#5.2.1.4) auf Wartungsarbeiten in Notfällen beschränken, ein striktes 4-Augen-Prinzip für diese Zugriffe etablieren und durchsetzen sowie solche Zugriffe protokollieren. Zugriffe auf den HSK durch den Anbieter sind ausschließlich für Wartungsarbeiten beim Ausfall von Hardware-Komponenten wie Netzteilen vorgesehen - sofern solche Wartungen beim eingesetzten HSK überhaupt für den Betreiber möglich sind -, welche zum Ausfall des HSK und zu einer verringerten Verfügbarkeit oder Performance des TI-Gateway führen. [≤]

A_23496 - Erkennen und Melden von Unregelmäßigkeiten bei physischem Zugriff auf HSK

Der Anbieter des TI-Gateway MUSS Prozesse definieren und etablieren, die Unregelmäßigkeiten bzgl. physischer Zugriffe auf den HSK erkennen lassen. Dies umfasst die Prüfung von Protokollen des HSK bzgl. des Auslösens von Alarmen zum physischen Zugang (vgl. A_23495*) und dem Herunterfahren des HSK. Erkannte Unregelmäßigkeiten sind als erheblicher Sicherheitsvorfall zu werten und im Rahmen von GS-A_5555* an die gematik zu melden. [≤]

A_23361 - TI-Gateway - Zulässige Produkttypversionen Highspeed-Konnektor

Der Anbieter TI-Gateway MUSS eine Highspeed-Konnektor-Version einsetzen, die für die Verwendung im TI-Gateway zugelassen ist. [≤]

6.2 Betrieb

6.2.1 Servicezerlegung

verschoben nach [gemKPT_Betr::3.5.2 Servicezerlegung]

6.2.2 Mitwirkungsverpflichtung im TI-ITSM gemäß [gemRL_Betr_TI]

verschoben nach [gemKPT_Betr::3.5.3 Mitwirkungsverpflichtung im TI-ITSM gemäß [gemRL_Betr_TI]]

6.2.3 Spezifische Ausprägungen und Verpflichtungen einzelner Rollen

verschoben nach [gemKPT_Betr::3.4.4 Spezifische Ausprägungen und Verpflichtungen einzelner Rollen]

6.2.4 Supportkonzept

6.2.4.1 Spezifische Ausprägungen

verschoben nach [gemKPT_Betr::3.6.3 Spezifische Ausprägungen]

6.2.4.2 Organisatorische Service Level

verschoben nach [gemKPT_Betr::5.2.2 Spezifische Ausprägungen]

6.2.4.3 Technische Service Level / Performance-Kenngrößen

verschoben nach [gemKPT_Betr::5.3.2.13 TI-Gateway-Zugangsmodule (PDT72)]

6.2.5 gemKPT_Betr: Anhang A

verschoben nach [gemKPT_Betr::7.1.1 Produkttypen (PDT-IDs)]

6.2.6 gemSpec_Perf#3.x.1 Leistungsanforderungen TI-Gateway

6.2.6.1 gemSpec_Perf#3.x.1.1 Lastmodell TI-Gateway

verschoben nach [gemSpec_Perf::3.10.1.3.1 Lastmodell TI-Gateway]

6.2.6.2 gemSpec_Perf#3.x.1.2 Bearbeitungszeiten TI-Gateway

verschoben nach [gemSpec_Perf::3.10.1.3 Bearbeitungszeiten TI-Gateway]

6.2.6.3 gemSpec_Perf#3.x.1.3 Performancevorgaben TI-Gateway

verschoben nach [gemSpec_Perf::3.10.1.3 Performancevorgaben TI-Gateway]

7 Änderungen an gemILF_PS

Zertifikatsbasierte Clientsystemauthentifizierung muss jetzt vom Primärsystem unterstützt werden.

TIP1-A_4962-01 - Nutzung von TLS-Authentisierungsmethoden

Das Primärsystem MUSS die TLS-Authentisierungsmethoden der Stufen 2 und 4 aus Tabelle Tab_ILF_PS_Konfigurationsvarianten_HTTP und Stufe 2 aus Tabelle Tab_ILF_PS_Konfigurationsvarianten_CETP unterstützen, d. h. TLS mit Server-Authentisierung mit bzw. ohne Client-Authentisierung.

Das PS MUSS für TLS-gesicherte Verbindungen mindestens TLS-Version 1.2 verwenden, es KANN auch TLS Version 1.3 verwenden.

[<=]

8 Beispiele und Referenzimplementierungen

<Optional: Beispiele für Aufrufsequenzen, ausgetauschte Daten, etc. zur Unterstützung der Implementierung>

9 Anhang A - Verzeichnisse

9.1 Abkürzungen

Kürzel	Erläuterung

9.2 Referenzierte Dokumente

9.2.1 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

9.2.2 Weitere Dokumente

[Quelle]	Herausgeber (Erscheinungsdatum): Titel