TI-Gateway

Das TI-Gateway ist als Teil der zentralen Infrastruktur der TI ein „sicherer Zugangsdienst als Schnittstelle zur dezentralen Infrastruktur“ i.S.v. § 306 Abs. 2 Nr. 2 lit. a SGB V.

Das TI-Gateway fasst die einige Services des Konnektors und die Services des VPN-Zugangsdienstes zusammen.

Der Dienst ermöglicht es den Leistungserbringer:innen:

- eHealth-Kartenterminals mit Smartcards anzusteuern,
- Services anolog zu denen des Anwendungskonnektors und der Fachmodule des Konnektors zu nutzen,
- über das VPN auf offene Fachdienste und WANDA zuzugreifen.

Im Unterschied zu einem Konnektor in der medizinischen Institution entfallen folgende Funktionalitäten:

- Schutz des Netzes gegenüber dem Internet im Rahmen einer sog. Reihenschaltung,
- Sicherer Internet Service (SIS),
- Zeitdienst,
- DHCP Server,
- VSDM Standalone/Offline.

Architektur

Das TI-Gateway setzt sich aus den Produkttypen **Highspeed-Konnektor** (HSK), einem **Zugangsmodul** sowie dem **Intermediär VSDM** zusammen. Letzterer kann bei vorhandener Zulassung vom Anbieter des TI-Gateway nachgenutzt werden. Ein **http-Proxy** ist zudem als Teil des HSK umzusetzen.

Die Anbindung an die TI erfolgt über einen **SZZP** oder einen **SZZP-light**. Die Anbindung über einen kryptografisch gekoppelten SZZP-light+ - wie bei der Anbieterzulassung HSK - wird nicht unterstützt.

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 TI.

Der **HSK** stellt

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

bereit.

Der **VSDM-Intermediär** und der **http-Proxy** bieten Funktionalitäten, die bei Nutzung eines

Konnektors durch den VPN-Zugangsdienst abgedeckt wurden.

Die Clients (Primärsysteme) kommunizieren mit dem TI-Gateway (Zugangsmodul) über TLS. Die gegenseitige Authentisierung muss lokal konfiguriert werden vom DVO.

Zudem muss ein Software-Client (zum Download) vom Anbieter des TI-Gateways bereitgestellt werden, um bei der ersten Verbindung (zur Einrichtung des HSK-Instanz u.a.) zum Zugangsmodul die Authentizität technisch vollständig prüfen zu können, was alleine über einen Browser nicht gewährleistet werden kann.

Der **VPN-Service** des Zugangsmoduls ermöglicht eine VPN-Verbindung aus der LE-Umgebung zum TI-Gateway. Zudem bietet das Zugangsmodul **Firewall**-Funktionalitäten (bspw. DDoS-Protection und Paketfilter (ACL)) an.

Unterschied zum HSK

Die Anbieterzulassung HSK wurde für den Eigenbetrieb durch das Krankenhaus entwickelt. Um die betrieblichen Anforderungen auf ein Minimum reduzieren zu können, wurde die kryptographische Kopplung zum SZZP-light+ spezifiziert. Eine strikte Trennung zwischen Leistungserbringer und Betreiber ist im Anwendungsfall Krankenhaus nicht nötig. Die Anbieterzulassung TI-Gateway definiert einen Zugangsdienst im Sinne des §306 SGB V. Um dem gerecht zu werden, muss der Betreiber vom Zugriff auf die medizinischen Daten ausgeschlossen werden, was durch eine Kombination von organisatorischen und technischen Maßnahmen erreicht wird. Für die technischen Maßnahmen wurden Anforderungen an das Zugangsmodul definiert. Nicht zuletzt muss dir Anbieter TI-Gateway betriebliche Anforderungen an Datenschutz und Informationssicherheit erfüllen wie alle Zentralen Dienste.

Unterschied zu jetzigen TIaaS-Angeboten (akquinet oder Red Medical u.a.)

- da das TI-Gateway die Rolle eines Zugangsdienstes übernimmt, liegt nach den Regelungen des SGB V die datenschutzrechtliche Verantwortung beim Anbieter. Somit wird verhindert, dass der LE für Fehler verantwortlich ist, die außerhalb seines Einflussbereiches liegen.
- Bei den aktuellen Lösungen wird das Netz der LEI über VPN in das Rechenzentrum des Anbieters verlegt, ohne dass die Sicherheit dieser Verbindung unabhängig geprüft wird. Die Anforderungen an das Zugangsmodul wurden formuliert, damit die Sicherheit durch ein Gutachter prüfbar wird.
- Bei den aktuellen Lösungen kann nicht verhindert werden, dass ein böswilliger Mitarbeiter beim Betreiber massenhaft Zugang zu medizinischen Daten bekommt, indem er z.B. einen Client als Angreifer in das Informationsmodell aller Konnektoren konfiguriert. Durch das Rollenkonzept mit Rollenausschlüssen wird dieses Risiko mitigiert.
- mit dem Nutzerportal wird eine Komponente eingefügt, die für administrative Funktionen in einer TI2.0 gebraucht wird.
- die bisherigen Lösungen sind nicht gut genug skalierbar, um als flächendeckende Alternative zu Einboxkonnektoren zu dienen.

Die im Markt als RZ-Konnektoren vertriebenen Bündel von Einboxkonnektoren (bei Secunet

Doppelkonnektoren) sind durch die Spezifikation der Einboxkonnektoren abgedeckt. Zusatzanforderungen sind im Anhang der Finanzierungsvereinbarung der DKG. Konnektorhosting ist weiterhin zulässig im Rahmen der Hoheit des LE über die Organisation seiner Institution. Allerdings bleibt die orginäre Verantwortung bis zu den Schnittstellen des Konnektors hierfür beim LE, auch für die VPN-Verbindung ins Rechenzentrum und die Verarbeitung im Rechenzentrum, auf die der LE keinen direkten Einfluss hat (→ Notwendigkeit der AV). Das TI-Gateway macht Vorgaben für die VPN-Strecke und die Verarbeitung im RZ, die geprüft werden, was einen Übergang der Verantwortung auf den Anbieter ermöglicht. Ein Verbot der bestehenden Rechenzentrumslösungen ist nicht geplant. Die gematik strebt jedoch an, diese Lösungen mit Mitteln des Marktes durch zugelassene TI-Gateways zu verdrängen.

Sicherheit

Die Clients kommunizieren mit dem TI-Gateway (Zugangsmodul) über TLS.

Über die Verwendung zugelassener Produkte und organisatorische Maßnahmen, die bei der Zulassung im Rahmen eines Sicherheitsgutachtens überprüft werden (Rollenkonzept!), wird sichergestellt, dass Mitarbeiter des Anbieters nicht unberechtigt auf medizinische Daten zugreifen können.

Somit kann davon ausgegangen werden, dass keine unberechtigte Kommunikation über den SZZP stattfindet. (Dies ist beim HSK im „Eigenbetrieb“ nicht so, weshalb hier der SZZP-Zugang technisch abgesichert werden musste mit dem Nachteil erhöhter Komplexität und erheblicher Verzögerungen).

Mehrwegangebote

Der TI-Zugang wird mit dem TI-Gateway als „Managed Service“ über die jeweiligen Betriebsdienstleister bezogen. Dieser umfasst zunächst die reine Verbindung zur TI über den High-Speed-Konnektor. Schrittweise soll dies um weitere Mehrwertdienste ergänzt werden können. Der Leistungsempfänger erhält damit weitere Funktionen, bspw. wie das KIM-Client-Modul, die Nachrichtenvalidierung, die Anbindungsmöglichkeit für Mobilgeräte oder perspektivisch auch die Nutzung von Fernsignaturdiensten.