

CGM VPN-ZUGANGSDIENST

LEISTUNGSBESCHREIBUNG



Synchronizing Healthcare



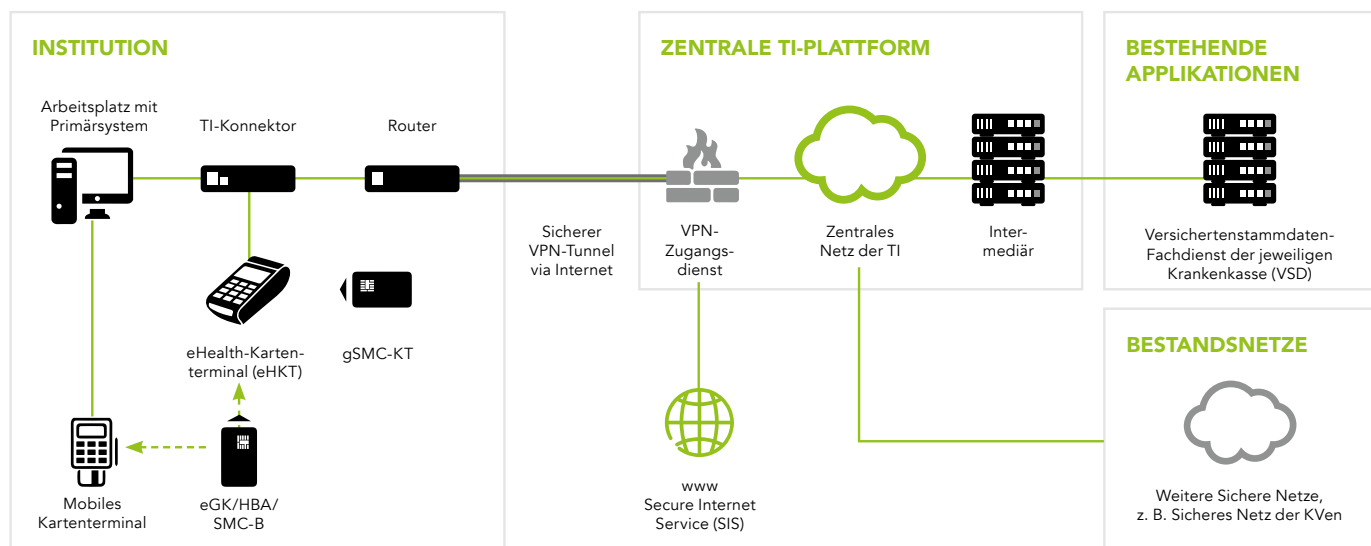
CompuGroup
Medical

VPN-ZUGANGSDIENST

Ausschließlich über einen VPN-Zugangsdienst, der für die Telematikinfrastruktur (TI) zugelassen ist, kann eine sichere Anbindung der Institutionen und Primärsysteme an die Telematikinfrastruktur erfolgen.

Der VPN-Zugangsdienst ist die Gegenstelle des Konnektors in der TI. Er ermöglicht den Leistungserbringern den Zugang zur TI und ist für den Secure Internet Service (SIS) sowie den

Zugang zu aktuellen Bestandsnetzen, wie z. B. dem Sicheren Netz der Kassenärztlichen Vereinigungen (SNK), vorbereitet. Als Transportinfrastruktur zwischen dem Institutionsnetzwerk des Leistungserbringers auf der einen Seite und dem VPN-Zugangsdienst auf der anderen Seite wird in der Regel das öffentliche Internet genutzt. Es wird ein sicherer Tunnel über das Internet aufgebaut.



DER SICHERE ZUGANG ZUR TI: CGM VPN-ZUGANGSDIENST

Digitale Kommunikation ist aus dem Institutionsalltag nicht mehr wegzudenken. Schon heute ist vieles möglich, wie z. B. die zahlreichen Online-Anwendungen im Sicheren Netz der Kassenärztlichen Vereinigungen zeigen.

Und zukünftig wird digitale Kommunikation noch sicherer und attraktiver: Im Rahmen der Telematikinfrastruktur wird beim VPN-Zugangsdienst eine verschlüsselte VPN-Verbindungen zur Nutzung digitaler Dienste aufgebaut: zur

Telematikinfrastruktur (TI) selbst sowie optional zum **Secure Internet Service (SIS)**, über den auch **CGM-Mehrwertdienste** erreichbar sind.

Nur über einen VPN-Zugangsdienst, der von der gematik für die TI zugelassen ist, darf der Konnektor eine sichere Verbindung zur Telematikinfrastruktur aufbauen. Die CGM bietet seit 2017 als erster TI-Provider ihren VPN-Zugangsdienst zuverlässig, leistungsstark und sicher im Produktivbetrieb an.

LEISTUNGSMERKMALE DES CGM VPN-ZUGANGSDIENSTES

Der VPN-Zugangsdienst der CGM bindet alle Primärsysteme sicher in die Telematikinfrastruktur im Gesundheitswesen ein:

AUFGABEN

Der VPN-Zugangsdienst ist eine zentrale Komponente der TI und dient als Verbindung zwischen Leistungserbringern und zentralen Diensten der TI. Er erfüllt vielfältige Aufgaben:

- Der VPN-Zugangsdienst ist in zwei Dienste aufgeteilt: den Zugang zur Telematikinfrastruktur (TI) und den Zugang zur Nutzung eines sicheren Internetzugangs (SIS).
- Er verbindet die Primärsysteme mit der zentralen Telematikinfrastruktur des deutschen Gesundheitswesens.
- Die Kommunikation der Leistungserbringer mit dem VPN-Zugangsdienst erfolgt über den Konnektor, der sich als dezentrale Komponente in einer Leistungserbringerinstitution befindet.

ANWENDUNGEN

- Aktualisierung der Versichertenstammdaten (VSDM)
- Secure Internet Service (SIS)
- Bestandsnetze (z. B. das Sichere Netz der KVen (SNK))

ZUKÜNFTIGE ANWENDUNGEN

- Notfalldatenmanagement (NFDm)
- eMedikationsplan (eMP)
- Versand von elektronischen Arztbriefen (eArztbrief)
- Sichere Kommunikation zwischen Leistungserbringern (KOM-LE)
- Elektronische Patientenakte (ePA)
- Elektronisches Rezept (eRezept)
- Elektronische Fallakte (eFA)
- Telekonsile
- Elektronisches Patientenfach
- Elektronische Arbeitsunfähigkeitsbescheinigung (eAU)

SCHNITTSTELLEN UND SICHERHEIT

Die Kommunikation aller Beteiligten erfolgt durch verschiedene verschlüsselte technische Komponenten, wodurch ein unbefugter Zugriff Dritter ausgeschlossen ist.

- Der Zugang sowohl zur TI als auch zum SIS erfolgt durch beidseitige, zertifikatsbasierte Authentisierung am VPN-Konzentrator.
- Durch kryptografische Maßnahmen ist die Vertraulichkeit und Integrität der zu übertragenen Daten sichergestellt.
- Durch Authentifizierungs- und Autorisierungsmaßnahmen können ausschließlich registrierte und freigeschaltete Leistungserbringer die Dienste der TI und des SIS nutzen.
- Die Komponenten der TI, so auch der VPN-Zugangsdienst, werden nach aktuellen IT-Sicherheitsvorschriften vom Bundesamt für Sicherheit in der Informationstechnik (BSI) kontrolliert und fortlaufend überwacht sowie von der gematik geprüft und zur Zulassung zertifiziert.
- Der nach ISO 27001:2013 zertifizierte VPN-Zugangsdienst wird mit einer geografischen Redundanz in mehreren ebenfalls zertifizierten Rechenzentren betrieben. Alle Komponenten sind je Standort zusätzlich redundant vorhanden.
- Die Schutzziele Integrität, Vertraulichkeit, Verfügbarkeit und Authentizität des Information Security Management Systems (ISMS) werden eingehalten.
- Für TI und SIS werden unterschiedliche Einwahlknoten betrieben, die dasselbe Schutzniveau aufweisen, deren Zugangszonen jedoch physisch getrennt sind. Ein Datenverkehr zwischen TI und SIS ist nicht erlaubt.
- Der Zugang zum VPN-Zugangsdienst wird durch hochverfügbare Paketfilter abgesichert, die ausschließlich Daten des VPNs passieren lassen. Andere eingehende Daten werden unterbunden.
- Zur Früherkennung von Angriffen wird ein „Intrusion Detection System“ (IDS) eingesetzt.
- Durch geeignete Sicherheitsmaßnahmen der Firewalls schützt der VPN-Zugangsdienst sich und die Komponenten der TI vor Bedrohungen aus dem Internet.

CGM VPN-ZUGANGSDIENST

SIE HABEN NOCH FRAGEN ODER INFORMATIONSBEDARF?

Wir oder Ihr CGM zertifizierter Dienstleister vor Ort (DVO) stehen Ihnen jederzeit gerne zur Verfügung.

CompuGroup Medical Deutschland AG
Business Area Connectivity
Maria Trost 21 | 56070 Koblenz

cgm.com/ti

Version: 3 / Oktober 2024

CGMCOM-CONTI_28391_1024_RRH

Synchronizing Healthcare



CompuGroup
Medical