LEISTUNGSBESCHREIBUNG
CGM MANAGED TI

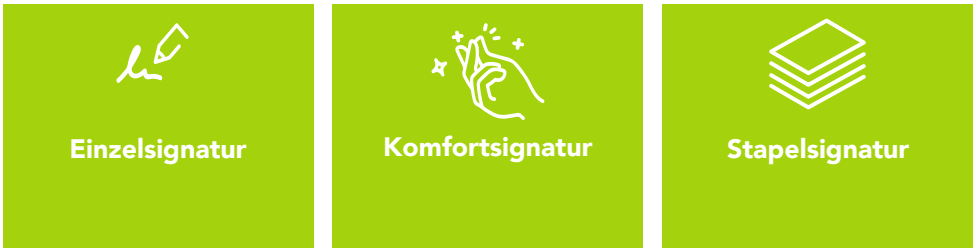
CGM TI
Connecting Healthcare

1. ÜBERBLICK CGM MANAGED TI

1.1 TI-Zugang im Rechenzentrum

Die Telematikinfrastruktur (TI) ist die Plattform für digitale Gesundheitsanwendungen im deutschen Gesundheitswesen und vernetzt die beteiligten Leistungserbringer. CGM MANAGED TI bietet allen Gesundheitsprofis komfortabel die Möglichkeit, sich an die TI anzubinden und so sicher miteinander relevante Informationen auszutauschen und dadurch Mehrwerte bei der Gesundheitsversorgung zu schaffen, beispielsweise durch den Zugriff auf Patientendaten in der elektronischen Patientenakte (ePA) oder den sicheren Austausch von medizinischen Daten über Kommunikation im Medizinwesen (KIM).
CGM MANAGED TI ersetzt vollständig die Funktionen eines TI-Konnektors vor Ort in der Institution des Leistungserbringers und bietet dabei den vollen Zugriff auf die derzeit verfügbaren Fachanwendungen und -dienste der TI:

Darüber hinaus steht der Basisdienst qualifizierte elektronische Signatur (QES) zur Nutzung weiterer TI-Anwendungen zur Verfügung:



Voraussetzung zur Nutzung der genannten Anwendungen und Basisdienste ist eine entsprechende Unterstützung der gematik-Schnittstellen durch das eingesetzte Primärsystem.

1.2 Anbindungsvarianten

CGM MANAGED TI steht in zwei Varianten zur TI-Anbindung über das hochsichere, redundante sowie zertifizierte (TIER IV, ISO 27001, ISO 9001) CGM-Rechenzentrum zur Verfügung. Die Wahl der Anbindungsart hängt von den örtlichen Gegebenheiten ab, unter anderem von der Größe der Institution oder der möglichen Erfordernis einer mobilen Nutzung der TI. Im Rahmen der TI-Anbindung wird sichergestellt, dass die gewählte Anbindungsart den individuellen Anforderungen der Institution entspricht.

CGM MANAGED TI-Anbindung über die CGM VPN-Box bzw. CGM FIREWALL:
Zugriff auf den TI-Zugang im sicheren CGM-Rechenzentrum mit VPN-Verbindungsaufbau über die CGM VPN-Box bzw. CGM FIREWALL in der Institution des Leistungserbringers.

Softwarebasierte CGM MANAGED TI-Anbindung:
Softwarebasierter Zugriff auf den TI-Zugang im sicheren CGM-Rechenzentrum in der Institution des Leistungserbringers.

1.3 Inkludierte Leistungen im Überblick

- TI-Zugang über das CGM-Rechenzentrum
- Höchste Sicherheitsstandards durch ein nach TIER IV, ISO 27001 sowie ISO 9001 zertifiziertes, hochsicheres und hochverfügbares Rechenzentrum in Deutschland
- Sichere Verbindung des Primärsystems* und zugelassener stationärer E-Health-Kartenterminals am Nutzungsort des Leistungserbringers mit dem CGM-Rechenzentrum über IPSec-IKEv2-basierte VPN-Tunnel
- Anbindung von allen Primärsystemen (On-Premise und in der Cloud), bei denen Mandant-, Clientsystem- und Arbeitsplatz-IDs zum Zeitpunkt der Installation anpassbar sind
- Vor-Ort-Installation der VPN-Tunnel auf der CGM VPN-Box bzw. CGM FIREWALL bzw. bei der softwarebasierten Anbindungsvariante auf den E-Health-Kartenterminals und TI-Arbeitsplätzen, für die eine CGM MANAGED TI-Anbindung beauftragt wurde
- Konfiguration der Komponenten vor Ort durch einen CGM-zertifizierten Dienstleister vor Ort (DVO)
- Automatisches Einspielen von zugelassenen Updates und PTV-Upgrades für kommende TI-Anwendungen
- Umstellung auf das CGM TI-GATEWAY nach Zulassung
- Konfiguration der CGM FIREWALL Cybersecurity-Features durch einen CGM-zertifizierten Dienstleister vor Ort (nur bei Beauftragung der CGM FIREWALL)

* Die Anbindung des Primärsystems setzt eine aktive Schnittstelle für den CGM-Konnektor KoCoBox MED+ bzw. CGM VPN-Zugangsdienst voraus. Es ist Softwarefirmen nach § 332a SGB V ab dem 30. Dezember 2023 untersagt, zusätzliche Entgelte für die Freischaltung bzw. den Betrieb dieser Schnittstelle zu erheben.

1.4 Abgrenzung zu konventionellen Vor-Ort-Installationen

Durch den Managed-Service-Ansatz liegt die Verantwortung für Betrieb, Pflege und Überwachung des TI-Zugangs im CGM-Rechenzentrum gesamtheitlich bei CGM und nicht mehr beim Leistungserbringer:

- Pflege, Wartung und Support der TI-Zugänge erfolgt zentral im CGM-Rechenzentrum
- Updates und Upgrades der TI-Zugänge werden automatisch durch CGM im CGM-Rechenzentrum eingespielt
- Hohe Verfügbarkeit und Schutz vor Systemausfällen erfolgt durch 24/7-Monitoring im CGM-Rechenzentrum und Redundanzabsicherung
- Vorhalten eines geschützten Bereiches für den Konnektor (Konnektorschrank) beim Leistungserbringer in der Institution nicht mehr erforderlich
- Entfall der regelmäßigen Überprüfung der Sicherheitsmerkmale des eingesetzten Konnektors (Prüfung auf Unversehrtheit der Gehäusesiegel)

Bei CGM MANAGED TI in Verbindung mit der CGM FIREWALL profitiert der Leistungserbringer zusätzlich von einem ergänzendem Schutz für sein Institutionsnetzwerk. Die CGM FIREWALL schützt das Netzwerk der Institution vor Angriffen von außen und setzt dank ihrer Grundkonfiguration wesentliche Bestandteile der Anforderungen der IT-Sicherheitsrichtlinie optimal um.

1.5 Detailbeschreibungen zu CGM MANAGED TI-Anbindungsvarianten

1.5.1 CGM MANAGED TI über die CGM FIREWALL

Die VPN-Verbindung zum sicheren TI-Zugang im CGM-Rechenzentrum wird über die CGM FIREWALL aufgebaut. Durch die Anbindung jedes Endgeräts in der Institution des Leistungserbringers an die CGM FIREWALL ist die Absicherung des Institutionsnetzwerks (CGM FIREWALL-Leistungsbeschreibung siehe **cgm.com**/ti-download) zusammen mit der sicheren Verbindung zur TI über das CGM-Rechenzentrum abgebildet.

1.5.2 CGM MANAGED TI-Anbindung über die CGM VPN-Box

Die gelieferte CGM VPN-Box fungiert ausschließlich als VPN-Router für den VPN-Verbindungsaufbau in das CGM-Rechenzentrum aus der Institution des Leistungserbringers. Die CGM FIREWALL-Leistungsbeschreibung findet in diesem Fall keine Anwendung. Anstelle der bei der CGM FIREWALL verwendeten Lizenzierungsstufe wird eine Lizenz mit geringerem Funktionsumfang angewendet, die keine Sicherheitsfunktionen enthält.

Es findet keine Zuweisung von CGM-Vorlagen für die Firewall-Grundkonfiguration statt. Es werden keine Ausnahmen auf Kundenwunsch hinzugefügt und alle ausgehenden Verbindungen erlaubt. Die Vorgaben der IT-Sicherheitsrichtlinie werden damit nicht erfüllt. Weitere Sicherheitsfunktionen wie Content Scanning, Botnet Detection, Intrusion Prevention Service, Portblocking, Geolocation Filter sowie Contentfilter sind in dieser Lizenzierungsstufe nicht enthalten und können nicht genutzt oder konfiguriert werden.

1.5.3 Softwarebasierte CGM MANAGED TI-Anbindung

Der Verbindungsaufbau vom Endgerät des Leistungserbringers mit TI-fähiger Primärsoftware in das CGM-Rechenzentrum wird über einen IPSec-IKEv2-VPN-Tunnel vom Endgerät selbst durchgeführt. Jedes Endgerät erhält hierbei bei Installation ein dediziertes, eindeutiges VPN-Profil, das von CGM zugeteilt wird. Dieses Profil wird über von CGM gelieferte Installationssoftware im Betriebssystem des Endgeräts hinterlegt. Der Leistungserbringer aktiviert das Profil durch einmalige Eingabe von Nutzernamen und Passwort oder Hinterlegen eines Zertifikats im Zertifikatsspeicher des Endgeräts und nutzt es ab dann automatisch. Es handelt sich dabei um einen Split-Tunnel, der nur TI-Anfragen an den TI-Zugang über den VPN-Tunnel verschlüsselt an das CGM-Rechenzentrum leitet. Stationäre E-Health-Kartenterminals bauen ebenfalls über einen IPSec-IKEv2-VPN-Tunnel die Verbindung ins CGM-Rechenzentrum auf. Anfragen, die keinen TI-Bezug haben, werden wie bisher über die bestehenden Kommunikationswege geleitet und stehen in keinem Bezug zur CGM MANAGED TI-Installation.

2. SYSTEMVORAUSSETZUNGEN

2.1 Installation und Betrieb

- Performanter (>=6 MBit) Internetzugang
- VPN-passthrough-fähiger Internetrouter (bei allen gängigen Routermodellen möglich)
- Bei softwarebasierter CGM MANAGED-TI-Anbindung: Windows-Betriebssysteme mit mindestens Windows 10, weitere Unix-basierte Betriebssysteme wie macOS oder Linux-Distributionen in einer aktuell vom Betriebssystemhersteller noch unterstützten Version
- TI-fähiges Primärsystem (On-Premise oder cloudbasiert); CGM MANAGED TI ist mit allen gematik-konformen Softwaresystemen kompatibel
- Stationäre E-Health-Kartenterminals (Worldline ORGA 6141 ab Firmware 3.8.0 bzw. ORGA Neo ab Firmware 3.9.0; CHERRY ST-1506 ab Firmware 3.0.0)
- Security Module Card Typ B (SMC-B) mit gültigem TI-Zertifikat für die Registrierung und Authentisierung der Verbindung in die TI
- Netzwerkinfrastruktur (z. B. Switch, LAN-Kabel) zur Anbindung der Endgeräte an die CGM VPN-Box bzw. CGM FIREWALL (entfällt bei softwarebasierter CGM MANAGED TI-Anbindung)
- Korrekte Angabe von individuellen Voraussetzungen der Institution (Anzahl TI-Arbeitsplätze, Anzahl stationäre E-Health-Kartenterminals) bei Bestellung durch den Leistungserbringer
- Passwörter und Zugänge zu bisher eingesetzten TI-Komponenten

- Vereinbarung gemäß Art. 26 Abs. 1 DSGVO für eine gemeinsame Verarbeitung personenbezogener Daten
- CGM PROTECT-Vereinbarung zur Auftragsverarbeitung (entfällt bei softwarebasierter CGM MANAGED TI-Anbindung)

2.2 Empfohlene Systemlandschaft

- Elektronischer Heilberufsausweis (eHBA) zur Nutzung von QES
- CGM KIM zur sicheren Kommunikation in der TI (www.meine-ti.de/kim)

3. SICHERHEIT

3.1 Verschlüsselte Verbindungen

Alle Verbindungen zwischen den Endgeräten des Leistungserbringers bzw. der CGM VPN-Box/CGM FIREWALL und dem CGM-Rechenzentrum sind mittels IPsec-IKEv2 verschlüsselt. Somit ist sichergestellt, dass die übermittelten Daten für Dritte nicht zugänglich sind. Die Komponenten vor Ort, insbesondere stationäre E-Health-Kartenterminals und SMC-B- / eHBA-Karten, müssen dabei den Vorgaben der gematik GmbH entsprechen und verbleiben in der Verantwortung des Leistungserbringers.

3.2 Rechenzentrumssicherheit

Das CGM-Rechenzentrum, das die TI-Zugänge verwaltet und aufbaut, ist nach TIER IV, dem höchsten Sicherheits- und Verfügbarkeitsstandard, sowie ISO 27001 und ISO 9001 zertifiziert. Zudem befindet sich das CGM-Rechenzentrum in Deutschland und erfüllt damit auch alle datenschutzrechtlichen Vorgaben für die Datenverarbeitung im deutschen Gesundheitswesen.

3.3 Ausfallsicherheit

Alle TI-Zugänge werden inkl. ihrer Konfigurationen von Backup-Mechanismen gesichert. Im Falle eines Ausfalls werden diese Backups kostenlos auf einem anderen TI-Zugang eingespielt.

4. KOMPONENTEN IM DETAIL

4.1 Endgeräte des Leistungserbringers

Um die Primärsoftware des Leistungserbringers für die Anbindung an die TI nutzen zu können, ist entweder die TI-fähige Primärsoftware auf dem Endgerät am Nutzungsort des Leistungserbringers installiert (On-Premise-Lösung) oder wird über das Endgerät im Internet aufgerufen (Cloud-Lösung). Für den Verbindungsaufbau der Endgeräte bzw. der CGM VPN-Box/CGM FIREWALL werden zunächst die ausgehenden Ports UDP/500 und UDP/4500 benötigt. Nach VPN-Tunnelaufbau setzt das Betriebssystem bzw. die CGM VPN-Box/CGM FIREWALL automatisch die VPN-Routen aus dem dedizierten VPN-Profil, das die CGM zur Verfügung stellt. TI-Anfragen werden dann in das CGM-Rechenzentrum geleitet. Anfragen, die keine TI-Relevanz haben, werden über das Standardgateway der Institution des Leistungserbringers verarbeitet.

4.1.1 TI-fähiges Primärsystem (Cloud-Lösung)

Der Verbindungsaufbau vom Endgerät des Nutzers in das CGM-Rechenzentrum wird nicht direkt vom Endgerät ausgehend durchgeführt, sondern von der TI-fähigen Cloud-Lösung selbst initiiert. Der Cloud-Betreiber erhält dafür ein spezifisches VPN-Profil von CGM, über das er die Verbindung ins sichere CGM-Rechenzentrum für alle seine Nutzer aufbauen kann. Das VPN-Profil für TI-Anfragen des Leistungserbringers für den Verbindungsaufbau der zentralen Cloud-Lösung an das CGM-Rechenzentrum ist obligat durch den Cloud-Betreiber zu nutzen, damit der Leistungserbringer eindeutig identifiziert werden kann. Voraussetzung für die Anbindung einer Cloud-Lösung ist eine Kooperationsvereinbarung des Cloud-Betreibers mit der CGM Deutschland AG. Bei einer CGM MANAGED TI-Anbindung eines Leistungserbringers über die CGM VPN-Box/CGM FIREWALL werden bei Nutzung einer TI-fähigen Cloud-Lösung alle Verbindungen der stationären E-Health-Kartenterminals über die CGM VPN-Box/CGM FIREWALL abgebildet.

4.1.2 Zugelassene stationäre E-Health-Kartenterminals

Der Verbindungsaufbau von für die TI zugelassenen stationären E-Health-Kartenterminals am Nutzungsort des Leistungserbringers zum CGM-Rechenzentrum erfolgt ebenfalls über VPN. Dafür muss das stationäre E-Health-Kartenterminal entsprechend der Installationsanleitung mit dem Router verbunden sein (LAN) und über einen Stromanschluss verfügen. Bei einer CGM MANAGED TI-Anbindung eines Leistungserbringers über die CGM VPN-Box/CGM FIREWALL werden durch CGM IP-Adressen für die stationären E-Health-Kartenterminals vorgegeben. Die anzubindenden stationären E-Health-Kartenterminals müssen dann im LAN des Leistungserbringers genau diese IP-Adressen erhalten, um mit dem TI-Zugang im CGM-Rechenzentrum kommunizieren zu können.

Bei einer softwarebasierten CGM MANAGED TI-Anbindung für stationäre E-Health-Kartenterminals stellt CGM dem Installierenden ein dediziertes, eindeutiges VPN-Profil für jedes Kartenterminal online zur Verfügung, das anhand der Installationsanleitung des E-Health-Kartenterminal-Herstellers installiert wird. Nach der Installation des VPN-Profils baut das stationäre E-Health-Kartenterminal bedarfsweise selbstständig die Verbindung in das CGM-Rechenzentrum auf.

4.2 CGM-Rechenzentrum

Das in Deutschland ansässige CGM-Rechenzentrum ist nach TIER IV[1] zertifiziert, hat daher eine **originäre Verfügbarkeit von 99,995 %** und entspricht den höchsten Standards für Rechenzentren. Der logische Betrieb des Rechenzentrums und aller enthaltenen Komponenten wird ausschließlich durch CGM sichergestellt. CGM gewährleistet, dass der TI-Zugang in den von der gematik GmbH geforderten Zeiträumen verfügbar ist. CGM garantiert weiterhin, dass nur durch die gematik GmbH zugelassene TI-Komponenten genutzt werden. Die Pflege, Wartung und der Support der Komponenten im CGM-Rechenzentrum sind Bestandteil der Leistungen von CGM MANAGED TI und werden von CGM durchgeführt.

[1] Vgl. https://www.tuvit.de/de/leistungen/rechenzentren-colocation-cloud-infrastrukturen/trusted-site-infrastructure/

5. INSTALLATIONSLEISTUNGEN

Die Installation von CGM MANAGED TI und ggf. die Konfiguration der CGM FIREWALL Cybersecurity-Features erfolgt durch von der CGM zertifizierte Dienstleister vor Ort (DVO). Um eine zeitsparende und erfolgreiche CGM MANAGED TI-Installation sicherzustellen, ist es unverzichtbar, dass zum vereinbarten Installationstermin alle erforderlichen technischen und organisatorischen Voraussetzungen erfüllt sind. Hintergrundinformationen dazu stehen in dieser Leistungsbeschreibung sowie in der CGM MANAGED TI Kundencheckliste (Versand mit der Auftragsbestätigung) zur Verfügung. Die Installation in der Institution erfolgt mit Terminvorgabe durch CGM/DVO (routenoptimierte Planung). Die Installation umfasst folgende Leistungen:

- Terminvereinbarung
- An- und Abfahrt
- Bei vorheriger TI-Anbindung über den CGM-Konnektor KoCoBox MED+ Rückbau des bisher genutzten Konnektors inkl. der notwendigen Veranlassung der Sperrung sowie einer sicheren Rückführung (Entsorgung)
- Anbindung an die TI über das sichere Rechenzentrum der CGM
- Freischaltung des TI-Zugangs im CGM-Rechenzentrum
- Installation der VPN-Profile auf den Endgeräten des Leistungserbringers bzw. auf der CGM VPN-Box/CGM FIREWALL
- Ggf. Herauslösen und Einbringen einer Institutionskarte (SMC-B)
- Einrichtung der TLS-Verschlüsselung (Vorgabe gemäß IT-Sicherheitsrichtlinie und Voraussetzung zur Nutzung der Komfortsignatur) an bis zu 5 TI-Arbeitsplätzen, sofern vom eingesetzten Primärsystem unterstützt
- Einstellungen des TI-Integrationsmoduls des Primärsystems
- Bei Tausch einer SMC-B Bekanntmachung des neuen Sicherheitsschlüssels der Institution (SMC-B) im CGM KIM-Clientmodul für bereits vorhandene Telematik-ID
- Lieferung und Inbetriebnahme der CGM VPN-Box/CGM FIREWALL
- Funktionstest
- Erstellung des Abnahmeprotokolls als Nachweis für die durchgeführte Installation
- Einweisung der Mitarbeitenden in der Institution des Leistungserbringers

Die Anpassung einer vorhanden KIM-Konfiguration ist kein Bestandteil von CGM MANAGED TI und muss separat beim CGM DVO oder dem Softwareanbieter beauftragt werden.

Weicht die Anzahl von benötigten gSMC-KTs während der Installation von der beauftragten Anzahl ab, werden die abweichenden Mengen über das Abnahmeprotokoll erfasst und mittels Nachlasses bzw. Nachberechnung behandelt.

Eine CGM MANAGED TI-Anbindung von TI-Arbeitsplätzen mit einer CHERRY-Tastatur ist nicht möglich. Um die betroffenen TI-Arbeitsplätze anbinden zu können, ist die Anschaffung eines neuen E-Health-Kartenterminals erforderlich.

Wenn in Ihrer Institution bereits eine CGM FIREWALL installiert ist, wird die VPN-Verbindung in das CGM-Rechenzentrum über Ihre bestehende CGM FIREWALL aufgebaut, wodurch die Lieferung einer CGM VPN-Box entfällt.

6. SERVICE LEVEL AGREEMENT (SLA)

6.1 Anwendersupport

Der Anwendersupport ist in den Allgemeinen Geschäftsbedingungen (AGB), den Besonderen Geschäftsbedingungen (Bes.GB) sowie im CGM CONNECTIVITY SLA geregelt, zu finden unter **cgm.com**/ti-download. Für die Anbindung über die CGM VPN-Box bzw. CGM FIREWALL gelten darüber hinaus auch die Bes.GB CGM PROTECT, die ebenfalls unter **cgm.com**/ti-download einsehbar sind.

6.2 Verfügbarkeit CGM MANAGED TI

Für die TI-Zugänge gewährleistet CGM zur Hauptzeit eine Verfügbarkeit von 99,8 % und zur Nebenzeit von 99 %. Als Hauptzeit gilt Montag bis Freitag von 6 bis 22 Uhr, ausgenommen bundeseinheitliche Feiertage. Alle übrigen Stunden der Woche sind Nebenzeit. Angekündigte Wartungsfenster sowie Störungen, die außerhalb der Betriebssphäre von CGM liegen oder von CGM nicht zu vertreten sind (höhere Gewalt, Verschulden Dritter), werden nicht als Ausfallzeit gewertet. Wartungsfenster liegen bevorzugt in Nebenzeiten.

6.3 Störfallklassen und Reaktionszeiten

Störfallklassen und Reaktionszeiten sind dem CGM Connectivity Service Level Agreement (SLA) zu entnehmen, zu finden unter **cgm.com**/ti-download.

SecurITy made in Germany

Trust Seal
www.teletrust.de/itsmig

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

cgm.com/ti

CGMCOM-26723_CONTI_0524_RRH

Synchronizing Healthcare

CompuGroup Medical