CGM TI
Connecting Healthcare

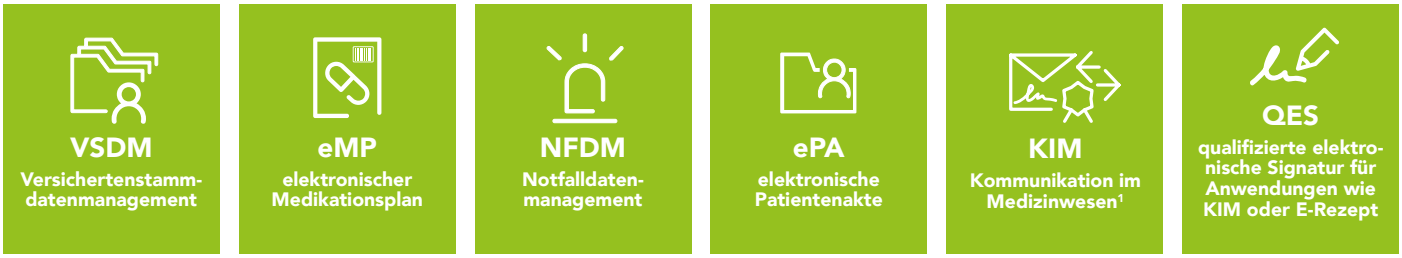
LEISTUNGSBESCHREIBUNG
CGM TI as a SERVICE

1. ÜBERBLICK

1.1 TI-Zugang im Rechenzentrum

Die Telematikinfrastruktur (TI) ist der Grundstein für das digitale Gesundheitswesen. CGM TIaaS 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 der elektronischen Patientenakte oder den sicheren Austausch von Therapieplänen „auf kurzem & datenschutzkonformen Dienstweg".
Mit CGM TIaaS können selbstverständlich auch cloudbasierte Softwarelösungen an die TI angeschlossen werden.

CGM TIaaS ersetzt dabei vollständig die Funktionen eines TI-Konnektors vor Ort in der Einrichtung des Leistungserbringers und bietet dabei den vollen Zugriff auf die derzeit verfügbaren und in Zukunft verpflichtenden Fachanwendungen und -dienste der TI zum Zeitpunkt der technischen Verfügbarkeit und Zulassung:



1.2 Leistungen im Überblick

- TI-Zugang über ein CGM-Rechenzentrum
- Höchste Sicherheitsstandards durch ein TIER-IV[2]-zertifiziertes, hochsicheres und hochverfügbares Rechenzentrum
- Sichere Verbindung aller anzubindenden Komponenten am Nutzungsort des Leistungserbringers mit dem CGM Rechenzentrum über einen IPSec-basierten VPN-Tunnel
- Bereitstellung von dedizierten VPN-Profilen für Arbeitsplatzrechner, mobile Endgeräte, Cloudzugänge und Kartenterminals
- Anbindung von Softwarelösungen on Premise und in der Cloud möglich, die eindeutige TI-Kontextparameter verwenden
- Installation bzw. Anbindung durch einen Dienstleister vor Ort (DVO) oder als Selbstinstallation des Leistungserbringers

Vorteile:

- **Maximale Reduktion der sensiblen technischen Infrastruktur beim Leistungserbringer**
- **Pflege, Wartung und Support der TI-Zugänge werden nicht mehr durch den Leistungserbringer bzw. IT-Dienstleister des Leistungserbringers erbracht**
- **Automatisches Einspielen von Updates und Upgrades durch CGM im Rechenzentrum**
- **kein Eingreifen/Überwachen der TI-Zugänge durch den Leistungserbringer**
- **Hohe Sicherheit und Schutz vor Systemausfällen**

[1] KIM-Postfächer sind über eine separate Beauftragung über https://meine-ti.de erhältlich

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

2. SYSTEMVORAUSSETZUNGEN

2.1 Installation und Betrieb

- performanter (>=6 MBit) Internetzugang
- VPN-passthrough-fähiger Internetrouter
- bei Windows-Betriebssystemen mindestens Windows 10
- bei Linux-Betriebssystemen mindestens Linux-Distributionen mit aktueller Charon-Bibliothek
- bei macOS-Betriebssystemen mindestens macOS 10.15 (Catalina)
- TI-fähiges Primärsystem (on-premise oder cloud-basiert). CGM TIaaS ist mit allen gematik-konformen Softwaresystemen kompatibel
- E-Health-Kartenterminals mit VPN-Funktionalität (Ingenico Orga 6141 ab Firmware 3.8.0; Cherry ST-1506 ab Firmware 3.0.0)
- SMC-B für die Freischaltung der Verbindung in die TI

2.2 Empfohlene Systemlandschaft

- Managed Firewall und Endpointprotection zum Schutz der Infrastruktur beim Leistungserbringer
- Elektronischer Heilberufsausweis (eHBA) zur Nutzung von QES und ePA
- CGM KIM zur sicheren Kommunikation in der TI (meine-ti.de)

3. SICHERHEIT

3.1 Verschlüsselte Verbindungen

Alle Verbindungen zwischen den Endgeräten des Leistungserbringers und dem CGM-Rechenzentrum sind mittels IPSec verschlüsselt. Somit ist sichergestellt, dass die übermittelten Daten für Dritte nicht zugänglich sind. Die Komponenten vor Ort, insbesondere Kartenterminals und SMC-B- / eHBA-Karten, müssen dabei den Vorgaben der gematik 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, zertifiziert und hat daher eine originäre Verfügbarkeit von 99,995%. Damit entspricht es den höchsten Standards für Rechenzentren. Zudem ist das Rechenzentrum in Deutschland angesiedelt und erfüllt damit auch alle datenschutzrechtlichen Vorgaben gemäß DSGVO für die Datenverarbeitung im Gesundheitswesen. Der logische Betrieb des Rechenzentrums und aller enthaltenen Komponenten wird ausschließlich durch CGM sichergestellt.
Weiter stellt die CGM sicher, dass der TI-Zugang in den von der gematik GmbH geforderten Zeiträumen verfügbar ist, sowie dass nur durch die gematik GmbH zugelassenen TI-Komponenten genutzt werden.
Die Pflege, Wartung und der Support der Komponenten im CGM-Rechenzentrum sind Bestandteil der Leistungen von TIaaS und werden von CGM durchgeführt.

4. KOMPONENTEN IM DETAIL

4.1 Endgeräte des Leistungserbringers

Um die Primärsoftware des Leistungserbringers für die Nutzung der Telematikinfrastruktur 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 (TI-fähige Cloud-Lösung). Für den Verbindungsaufbau der Endgeräte werden zunächst die Ports UDP/500 und UDP/4500 benötigt. Nach VPN-Tunnelaufbau setzt das Betriebssystem automatisch die VPN-Routen aus dem dedizierten VPN-Profil, das die CGM zur Verfügung stellt. Das Betriebssystem des Endgeräts leitet dann bei TI-Anfragen den Datenverkehr in das CGM-Rechenzentrum. Anfragen, die keine TI-Relevanz haben, werden über das Standardgateway des Betriebssystems verarbeitet.

4.1.1 TI-fähige On-Premise-Lösung

Der Verbindungsaufbau vom Endgerät des Leistungserbringers mit TI-fähiger Primärsoftwäre 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 und durch einmalige Eingabe von Nutzername und Passwort oder durch Hinterlegen eines Zertifikats im Zertifikatsspeicher des Endgeräts durch den Leistungserbringer aktiviert und ab dann automatisch genutzt. 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. Anfragen, die keinen TI-Bezug haben, werden wie vor der TIaaS-Installation bearbeitet. Weitere Verbindungsszenarien wie bspw. die Verbindung über hardwarebasierte VPN-Router werden im Zuge der regulären Weiterentwicklung von CGM TIaaS berücksichtigt.

4.1.2 TI-fähige 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. Für jeden Nutzer der Cloud-Lösung erhält der Cloud-Betreiber von CGM nach Bestellung von CGM TIaaS ein nutzerspezifisches VPN-Profil. 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.

4.1.3 Zugelassene E-Health-Kartenterminals

Der Verbindungsaufbau von für die TI zugelassenen Kartenterminals am Nutzungsort des Leistungserbringers zum CGM Rechenzentrum erfolgt ebenfalls über VPN. Dafür muss das Kartenterminal entsprechend der Installationsanleitung mit dem Router verbunden sein (LAN) und über einen Stromanschluss verfügen. Für die Installation des Kartenterminals stellt CGM dem Installierenden ein dediziertes, eindeutiges VPN-Profil für das Kartenterminal online zur Verfügung, das anhand der Installationsanleitung des Kartenterminal-Herstellers installiert wird. Nach der Installation des VPN-Profils baut das Kartenterminal bedarfsweise selbstständig die Verbindung in das CGM-Rechenzentrum auf.

5. INSTALLATIONSLEISTUNGEN

5.1 Installation mit Dienstleister vor Ort (DVO)

Die Installation von CGM TIaaS erfolgt durch von der CGM zertifizierte Dienstleister vor Ort (DVO). Diese Installation umfasst folgende Leistungen:

- Terminvereinbarung
- An- und Abfahrt
- Inbetriebnahme Kartenterminals (bei Neuerwerb)
- Installation der VPN-Profile auf Endgeräten des Leistungserbringers
- Anbindung an das Rechenzentrum
- Funktionstest
- Ausstellung Installationsprotokolls (förderungsbegründendes Dokument)

6. SERVICE LEVEL AGREEMENT (SLA)

6.1 Anwendersupport

Der Anwendersupport ist in den Allgemeinen Geschäftsbedingungen (AGB) und den besonderen Geschäftsbedingungen (BesGB) geregelt (s. u. www.cgm.com/ti-download).

6.2 Verfügbarkeit TIaaS

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

6.3 Störfallklassen und Reaktionszeiten

Der Anwendersupport ist in den Allgemeinen Geschäftsbedingungen (AGB) und den besonderen Geschäftsbedingungen (BesGB) geregelt (s. u. www.cgm.com/ti-download.)

6.3.1 Störfallklassen

Betriebsverhindernder Mangel (Priorität 1):

- Nutzung von TIaaS ist unmöglich oder schwerwiegend eingeschränkt.

Betriebsbehindernder Mangel (Priorität 2):

- Nutzung von TIaaS ist erheblich eingeschränkt.

Leichter Mangel (Priorität 3):

- Nutzung von TIaaS ist mit leichten Einschränkungen möglich.

6.3.2 Reaktionszeiten

Folgende Zeiten gelten für qualifizierte Meldungen ab dem Zeitpunkt des Eingangs bei CompuGroup Medical Deutschland AG

- Priorität 1: innerhalb von 4 Stunden
- Priorität 2: innerhalb von 8 Stunden
- Priorität 3: innerhalb von 20 Stunden

Qualifizierte Meldungen enthalten neben der Fehlerbeschreibung und der Definition des erwünschten Verhaltens eine Bestätigung der Internet-Verfügbarkeit zum Zeitpunkt des Fehlerauftretens.

CompuGroup Medical Deutschland AG
Division Connectivity
Maria Trost 21 | 56070 Koblenz
T +49 (0) 261 8000-2323 | F +49 (0) 261 8000-2399

cgm.com/ti

STAND: April 2022