

Elektronische Gesundheitskarte und Telematikinfrastruktur

Feature: TI-Messenger Pro Headless Client

Version: 1.0.0 CC
Revision: 1495670
Stand: 27.01.2026
Status: zur Abstimmung
freigegeben
Klassifizierung: öffentlich_Entwurf
Referenzierung: gemF_TI-M_Headless_Client

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 CC	27.01.202 6		Zur Abstimmung freigegeben	gematik

Inhaltsverzeichnis

1 Einordnung des Dokuments.....	4
1.1 Zielsetzung.....	4
1.2 Zielgruppe.....	5
1.3 Abgrenzungen.....	5
1.4 Methodik.....	5
2 Neue Funktionalitäten.....	6
3 Technisches Konzept.....	7
3.1 Sicherheit.....	8
3.1.1 Betriebliche Sicherheitsaspekte.....	8
3.1.2 Absicherung der Headless-Client API.....	9
3.1.3 Kryptografische Sicherheit.....	9
3.1.4 Logging, Audit und Nachvollziehbarkeit.....	10
3.1.5 Sicherheitsvorfälle und Incident Handling.....	10
3.2 Test.....	10
3.2.1 Testvorgehen.....	10
3.2.2 Testtreiber.....	12
3.3 Betrieb.....	12
3.3.1 Anbieter.....	12
3.3.2 Client.....	14
4 Produkt und Anbieterkonstellationen.....	15
5 Anhang A - Verzeichnisse.....	17
5.1 Abkürzungen.....	17
5.2 Abbildungsverzeichnis.....	18
5.3 Referenzierte Dokumente.....	18
5.3.1 Dokumente der gematik.....	18

1 Einordnung des Dokuments

Dieses Dokument "TI-Messenger Pro - Headless Client" beschreibt die Erweiterungen an der TI-Messenger Spezifikation, die benötigt werden, um eine verbesserte Integration und Nutzbarkeit von TI-Messenger Pro Clients in medizinische Informationssysteme zu ermöglichen.

1.1 Zielsetzung

Im Gesundheitswesen ist die effiziente und sichere Kommunikation zwischen Akteuren ein zentraler Bestandteil, um die Versorgungsqualität sicherzustellen und Arbeitsabläufe zu optimieren. Dabei spielt die Integration von Kommunikationslösungen in bestehende medizinische Informationssysteme wie Praxisverwaltungssysteme (PVS) oder Krankenhausinformationssysteme (KIS) eine entscheidende Rolle. Der Austausch von Informationen über separate Anwendungen oder Systeme führt häufig zu Medienbrüchen, erhöhtem Arbeitsaufwand und potenziellen Fehlerquellen, die die Effizienz und Sicherheit der Versorgung beeinträchtigen können.

Neben der Integration in klassische Primärsysteme (z. B. PVS, KIS) adressiert der TI-M Pro Headless Client auch Szenarien, in denen zentrale Serverkomponenten oder Contact Center Systeme von Kostenträgern die TI-M Funktionalitäten bündeln und über eigene Oberflächen oder Webschnittstellen an Arbeitsplatzsystemen der Sachbearbeitenden bereitstellen.

Ein typisches Szenario verdeutlicht die Herausforderung: Ein Arzt erhält wichtige Informationen über einen TI-Messenger-Chat, die für die Behandlung eines Patienten relevant sind. Um diese Informationen weiterzuverarbeiten, müssen sie manuell in das PVS übertragen werden – ein zeitaufwendiger Prozess, der nicht nur Ressourcen bindet, sondern auch die Gefahr von Fehlern birgt. Zudem wird die Kommunikation häufig außerhalb des direkten Kontextes der Fallakte geführt, was die Übersichtlichkeit und Nachvollziehbarkeit erschwert.

Mit der Einführung des TI-M Pro Headless Clients wird dieses Problem grundlegend adressiert. Ziel ist es, die Kommunikation innerhalb der Telematikinfrastruktur direkt in die medizinischen Informationssysteme zu integrieren, um eine nahtlose Nutzung sicherzustellen. Der Headless Client wird als Modul oder Bibliothek in die bestehenden Systeme eingebettet und bietet eine direkte Schnittstelle für die Kommunikation, ohne dass eine separate Anwendung oder grafische Benutzeroberfläche notwendig ist. Durch die direkte Integration des Headless Clients können Chats und Nachrichten automatisch passend zu einem angezeigten Patienten oder einer Fallakte angezeigt und verarbeitet werden. Informationen, die in einem Chat ausgetauscht werden, lassen sich ohne manuellen Aufwand direkt mit der Fallakte verknüpfen oder aus dieser heraus teilen. Dies ermöglicht eine erhebliche Zeitersparnis und reduziert die Fehleranfälligkeit, da die Daten direkt im Kontext der Versorgung verarbeitet werden können.

Ein weiterer Vorteil des TI-M Pro Headless Clients liegt in der verbesserten Übersichtlichkeit und Nachvollziehbarkeit der Kommunikation. Leistungserbringer können sicherstellen, dass alle relevanten Informationen in einem zentralen System verfügbar sind und nicht über verschiedene Anwendungen fragmentiert werden. Die direkte Einbindung des Headless Clients in die Arbeitsabläufe ermöglicht eine optimierte Nutzung der TI-Messenger-Funktionalitäten, die sich nahtlos in die täglichen Prozesse integrieren lassen. Der Headless Client stärkt damit die Zusammenarbeit zwischen Ärztinnen und

Ärzten, Praxisteams, Kliniken und anderen Akteuren und bringt die Versorgung durch integrierte Prozesse spürbar voran.

1.2 Zielgruppe

Das Dokument richtet sich an Hersteller und Anbieter von TI-M Headless Clients, welche den beschriebenen Produkttyp betreiben und diesen Institutionen des Gesundheitswesens und ihren Akteuren (z. B. Sachbearbeitern bei Kostenträgern, Pflegern in Krankenhäusern, etc.) zur Verfügung stellen.

1.3 Abgrenzungen

Der TI-M Pro Headless Client erfordert eine neue Herangehensweise an den Zulassungsprozess. Im Gegensatz zum bestehenden TI-M Pro Client wird nicht das gesamte Produkt geprüft und zugelassen, sondern ausschließlich der Headless Client selbst. Dieses Vorgehen trägt den praktischen Gegebenheiten Rechnung, da die gematik die komplexen Systemlandschaften der integrierenden Anwendungen nicht vollständig bereitstellen oder prüfen kann. Stattdessen konzentriert sich die gematik auf die Prüfung der Sicherheitsmechanismen wie der Ende-zu-Ende-Verschlüsselung (E2EE) sowie auf das korrekte technische Funktionieren des Clients.

Die Ausgestaltung der Headless-Client-API ist herstellerspezifisch und bietet die Freiheit, die Schnittstelle individuell auf die Anforderungen des jeweiligen, bestehenden medizinischen Informationssystems zuzuschneiden. Die Verantwortung für die Implementierung und den Einsatz des Headless Clients liegt bei den Herstellern dieser Systeme. Für den Betrieb definiert die gematik klare Vorgaben im Anbietersteckbrief und überwacht deren Einhaltung, um sicherzustellen, dass der Headless Client ausschließlich im vorgesehenen Rahmen genutzt wird und die Sicherheit sowie die Konformität der Telematikinfrastruktur gewährleistet sind.

1.4 Methodik

Dieses Dokument ist ein Konzept und bereitet die spätere Spezifikation vor. Es beschreibt den aktuellen Diskussions- und Entscheidungsstand zum Feature „Headless Client“ im TI-Messenger Pro und veranschaulicht dessen fachliche wie technische Ausprägung. Ziel ist es, frühzeitig ein gemeinsames Verständnis herzustellen, zentrale Annahmen transparent zu machen und strukturiertes Feedback aus der Praxis einzuholen. Im Mittelpunkt steht die frühe Abstimmung mit den Gesellschaftern sowie die Einbindung weiterer relevanter Stakeholder. Auf diese Weise werden fachliche Anforderungen, technische Lösungsansätze und Abgrenzungen so konkretisiert, dass sie als belastbare Grundlage für die anschließende Normierung dienen. Durch das frühzeitige Einbeziehen der Perspektiven – insbesondere zu Datenschutz und Informationssicherheit – wird die spätere Kommentierung der Spezifikation vereinfacht und beschleunigt. Das konsolidierte Feature-Konzept wird von den Gesellschaftern beschlossen und – im Benehmen mit dem BfDI und dem BSI – als verbindliche Basis für die Spezifikation herangezogen. Die Spezifikation wird anschließend aus dem beschlossenen Konzept abgeleitet und normativ ausgeformt. Auf diese Weise basieren die späteren Festlegungen auf einem abgestimmten, tragfähigen Fundament.

2 Neue Funktionalitäten

In diesem Dokument werden keine neuen Funktionalitäten für Nutzer festgelegt. Das Feature "Headless Client" stellt eine technische Neuausrichtung dar, bei der die Grundlage des TI-M Pro Clients geändert wird. Dabei handelt es sich um ein Refactoring, das ausschließlich die technische Struktur betrifft und keine neuen Funktionen für Nutzer einführt, vorhandene Funktionen verändert oder entfernt. Ziel des Refactorings ist es, die technische Basis zu schaffen, um den Client effizienter in bestehende medizinische Informationssysteme zu integrieren. Dies verbessert die Nutzbarkeit des Clients innerhalb der Systeme, ohne die grundlegenden Funktionen oder direkten Interaktionen für Nutzer zu verändern.

3 Technisches Konzept

Es wird ein neuer TI-M Client, der sogenannte *TI-Messenger Pro Headless Client*, eingeführt. Dieser Client basiert auf den Spezifikationen TI-M Basis und TI-M Pro mit angepasster Zuordnung der Anforderungen. Genau wie der bereits existierende TI-M Pro Client kommuniziert auch der Headless Client mit seinem Fachdienst über die Matrix Client-Server-API unter Nutzung von Ende-zu-Ende-Verschlüsselung (E2EE) und Transportverschlüsselung (TLS). Im Unterschied zum TI-M Pro Client kann der Headless Client allerdings nicht direkt über eine grafische Oberfläche bedient werden. Anforderungen aus TI-M Basis und TI-M Pro, die sich gegen das UI richten werden dem Headless Client daher nicht zugeordnet.

A_28650 -Keine grafische Oberfläche

Der TI-M Pro Headless Client DARF Endanwendern KEINE grafische Benutzeroberfläche anbieten.【<=】

Stattdessen verfügt der Headless Client über eine Schnittstelle, die sogenannte *Headless-Client-API*, die von anderen Systemen angesprochen werden kann. Diese API ist zur direkten Integration in das verwendende System im Sinne eines Moduls bzw. einer Bibliothek gedacht. Sie darf daher nicht als Netzwerkschnittstelle ausgestaltet werden.

A_28653 -Headless-Client-API

Der TI-M Pro Headless Client MUSS eine Schnittstelle zur Verwendung durch integrierende Systeme anbieten.【<=】

A_28651 -Keine Webschnittstelle

Die Schnittstelle am TI-M Pro Headless Client DARF KEINE Netzwerkschnittstelle sein.【<=】

Unabhängig von dieser Vorgabe darf das integrierende System selbst Netzwerkschnittstellen bereitstellen, über welche die Headless-Client-API direkt oder indirekt angesprochen wird.

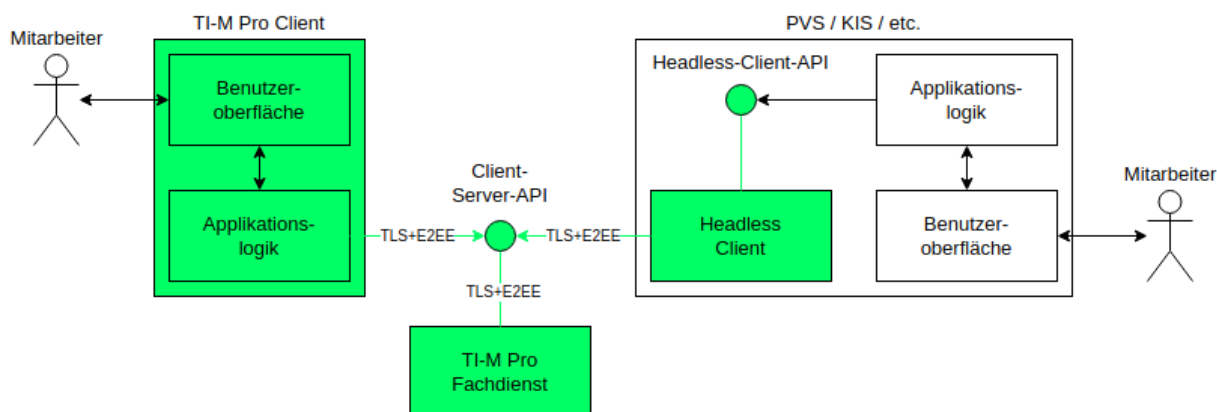


Abbildung 1: Übersicht Headless Client Architektur (farbig: von der gematik regulierte Teile)

Nachrichtenschlüssel müssen sicher im Headless Client verwahrt werden und dürfen nicht über die Headless-Client-API ausgeleitet werden. Das bedeutet der Headless Client bildet den Endpunkt der Ende-zu-Ende-Verschlüsselung (E2EE) im Sinne des Matrix-Protokolls. Nähere Details zu diesem Punkt finden sich im nachfolgenden Kapitel 3.1- Sicherheit.

Weitere Einzelheiten der Headless-Client-API (wie z. B. konkrete Technologien, Interfaces oder Methoden) werden von der gematik nicht vorgegeben. Diese Aspekte liegen

stattdessen in der Hoheit der Hersteller. Des Weiteren ergibt sich aus der Verwendung der Headless-Client-API keine Zulassungspflicht für das integrierende System.

Für die Authentifizierung des Headless Clients am Fachdienst werden die Mechanismen aus TI-M Pro wiederverwendet. Dabei kann das integrierende System die Anmeldung am Fachdienst über die Headless-Client-API steuern. Da der Headless Client direkt in das verwendende System integriert wird, gibt es am Headless Client selbst jedoch keine Anmelde-mechanismen. Diese Mechanismen werden stattdessen im integrierenden System umgesetzt. Anbieter können dadurch bei Bedarf auch eine Trennung zwischen den vom Headless Client verwendeten Accounts am Fachdienst und den von Mitarbeitern verwendeten Accounts am integrierenden System realisieren. So wäre es z. B. denkbar, dass jeder Mitarbeiter einen eigenen Account am integrierenden System hat, der Headless Client aber nur einen einzigen Matrix-Account am Fachdienst benutzt. Nach außen könnten alle Mitarbeiter dadurch unter derselben Matrix-ID kommunizieren. Alternativ könnte der Headless Client aber auch so integriert sein, dass sich Mitarbeiter direkt mit ihren personalisierten Matrix-Accounts anmelden.

3.1 Sicherheit

Dieses Kapitel legt die sicherheitstechnischen Ziele, Grundannahmen und Abgrenzungen für den Headless Client fest. Es beschreibt Maßnahmen zum Schutz sicherheitsrelevanter Funktionen, Daten und Zustände. Die Sicherheitsanforderungen adressieren ausschließlich den Betrieb des Headless Client als Bestandteil eines Systems (zum Beispiel PVS). Andere Betriebsformen oder Ausführungsumgebungen des Headless Clients sind nicht Gegenstand dieser Spezifikation und werden durch die gematik nicht abgesichert.

Ziel der Sicherheitsanforderungen ist es, den Headless Client so auszugestalten, das sicherheitskritische Funktionen ausschließlich innerhalb eines definierten und kontrollierten Sicherheitskontextes ausgeführt werden. Dabei sollen insbesondere Risiken aus Fehlbedienung, fehlerhafter Integration, unzureichend abgesicherten Schnittstellen sowie aus unbeabsichtigten Implementierungsfehlern systematisch begrenzt werden.

3.1.1 Betriebliche Sicherheitsaspekte

Ziel ist es, sicherzustellen, dass der Headless Client ausschließlich innerhalb einer definierten, kontrollierten und vertrauenswürdigen Betriebsumgebung eingesetzt wird und das sicherheitsrelevante Funktionen nur unter klar geregelten betrieblichen Voraussetzungen ausgeführt werden. Ein wesentliches Element des sicheren Betriebs ist zudem die Kontrolle der eingesetzten Softwareversionen.

A_28703 -Ausführungsumgebung

Der TI-M Pro Headless Client MUSS innerhalb einer geschützten Ausführungsumgebung betrieben werden, die eine wirksame Trennung gegenüber anderen Komponenten, Modulen und Erweiterungen gewährleistet. [≤]

A_28704 -Ansteuerung

Der TI-M Pro Headless Client MUSS als eigenständiges Modul implementiert sein und DARF im produktiven Betrieb ausschließlich über vorgesehene lokale Funktionsaufrufe angesteuert werden. [≤]

A_28727 -Hinweis des Anbieters

Der Anbieter MUSS in der technischen Dokumentation explizit und nachvollziehbar darauf hinweisen, dass der TI-M Pro Headless Client in der Produktivversion ausschließlich über vorgesehene lokale Funktionsaufrufe angesteuert werden darf. [≤]

A_28707 -Freigegebene Version ausführen

Der Anbieter des TI-M Pro Headless Clients MUSS sicherstellen, dass die Verwendung des Headless Clients auf signierte, geprüfte und freigegebene Versionen beschränkt ist. [≤]

3.1.2 Absicherung der Headless-Client API

Die Schnittstellen des Headless Clients stellen sicherheitskritische Einstiegspunkte dar, über die Funktionen mit Auswirkungen auf Vertraulichkeit, Integrität und korrekte Nutzung sensibler Daten ausgelöst werden können. Daher müssen diese Schnittstellen so gestaltet und abgesichert sein, dass missbräuchliche, fehlerhafte oder unvollständige Aufrufe erkannt und vor Ausführung unterbunden werden. Ziel ist es, sicherzustellen, dass sämtliche über die Schnittstellen ausgelöste Funktionsaufrufe ausschließlich in zulässiger, kontrollierter und sicherheitskonformer Weise erfolgen.

A_28699 -Prüfung von Funktionsaufrufen

Der TI-M Pro Headless Client MUSS sicherstellen, dass Funktionsaufrufe nur ausgeführt werden, wenn die angegebenen Parameter konsistent und für die angeforderte Funktion technisch zulässig sind. [≤]

A_28709 -Fehlerhafte oder missbräuchliche Nutzung

Der TI-M Pro Headless Client MUSS technische Maßnahmen implementieren, um missbräuchliche oder fehlerhafte Nutzung seiner Schnittstellen zu erkennen und zu unterbinden. [≤]

3.1.3 Kryptografische Sicherheit

Dieses Unterkapitel beschreibt die Sicherheitsziele zum Schutz kryptografischer Schlüssel, Ende-zu-Ende Verschlüsselung (E2EE) sowie temporärer kryptischer Sitzungszustände. Ziel ist es, sicherzustellen, dass kryptografisches Material ausschließlich innerhalb des Sicherheitskontextes des Headless Clients verarbeitet wird.

A_28710 -Verschlüsselte Kommunikation

Der TI-M Pro Headless Client MUSS der alleinige kryptografische Endpunkt für die Ende-zu-Ende verschlüsselte Kommunikation sein. [≤]

A_28713 -Schutzmechanismen

Der Anbieter des TI-M Pro Headless Clients MUSS sicherstellen, dass sicherheitsrelevante Prüf- und Schutzmechanismen des Headless Clients im Produktivbetrieb nicht modifiziert, umgangen oder außer Kraft gesetzt werden. [≤]

A_28715 -Kryptografische Isolation

Das TI-M Pro Headless Client MUSS sicherstellen, dass kryptografisches Schlüsselmaterial, interne E2EE-Zustände und andere sicherheitsrelevante Laufzeitinformationen weder ausgelesen, manipuliert oder rekonstruiert werden können. Im Produktbetrieb dürfen keine detaillierten Exception-Dumps erzeugt oder persistiert werden, die Rückschlüsse auf kryptografische Schlüssel oder E2EE-Zustände des Headless Clients zulassen. [≤]

A_28734 -Absicherung integrierender Netzwerkschnittstellen

Der Anbieter TI-Messenger Pro MUSS in den bereitgestellten Komponenten, Referenzarchitekturen und Integrationsvorgaben sicherstellen, dass Daten, die über seine Funktionsaufrufe zur Weiterverarbeitung bereitgestellt werden, ausschließlich über TLS-gesicherte Netzwerkschnittstellen des integrierenden Systems übertragen werden. Der Anbieter MUSS in seiner technischen Dokumentation und im Betriebshandbuch explizit und nachvollziehbar darauf hinweisen. [≤]

3.1.4 Logging, Audit und Nachvollziehbarkeit

Ziel ist es, sicherheitsrelevante Entscheidungen, Zustandsänderungen und erkannte Fehl- und Missbrauchssituationen nachvollziehbar zu erfassen, ohne dabei selbst neue Sicherheitsrisiken zu erzeugen.

A_28720 -Protokolle

Der TI-M Pro Headless Client MUSS sicherstellen, dass sicherheitsrelevante Protokolle und Ereignisdaten unverändert und zeitlich korrekt erzeugt werden. Zu den sicherheitsrelevanten Ereignissen zählen insbesondere: Entscheidungen über die Ablehnung von Funktionsaufrufen, erkannte Fehl- oder Missbrauchssituation sowie sicherheitsrelevante Zustands- oder Konfigurationsänderungen. [\leq]

A_28728 -Integrität von Audit-Logs

Der Anbieter MUSS in der technischen Dokumentation explizit und nachvollziehbar darauf hinweisen, dass die Erzeugung und Weitergabe von Audit-Logs durch den Headless Client nicht durch externe Konfigurationen oder von externen Komponenten, Modulen und Erweiterungen deaktiviert, unterdrückt oder manipuliert werden dürfen. [\leq]

3.1.5 Sicherheitsvorfälle und Incident Handling

Das Incident Handling umfasst nicht nur die Erkennung, sondern auch die Unterstützung angemessener Reaktionsmaßnahmen, wie etwa die temporäre Einschränkung von Funktionen, die kontrollierte Deaktivierung des Headless Clients oder die Übergabe relevanter Informationen an übergeordnete Sicherheits- und Betriebsprozesse.

A_28721 -Erkannter Vorfall und Risikominimierung

Der TI-M Pro Headless Client MUSS bei erkannter Manipulation, fehlender und unvollständiger Nutzungskontext oder sonstigen sicherheitsrelevanten Abweichungen geeignete Maßnahmen zur Risikominimierung ergreifen und Funktionen einschränken oder den Betrieb mit einer aussagekräftigen Rückmeldung kontrolliert beenden. [\leq]

3.2 Test

3.2.1 Testvorgehen

Für die Erlangung einer Produkt-/Anbieterzulassung müssen folgende Teststufen durchlaufen werden:

- Vorbereitung der Zulassung
 - allg. Festlegungen siehe [gemKPT_Test] (Testdokumentation, eigenverantwortliche Tests usw.)
 - Tests der Hersteller gegen eine weitere eigene Instanzen
 - Tests der Hersteller gegen eine Referenzimplementierungs-Instanz
- Zulassung der gematik
 - automatisierte Tests gegen die gematik Referenzimplementierungs-Instanz
 - automatisierte Tests mit anderen Herstellern (Headless Client/Fachdienst gegen einen anderen Client oder Headless Client/Fachdienst) zur Prüfung der Interoperabilität

Für die Tests der Hersteller und die automatisierten Tests der gematik gegen die Referenzimplementierung wird eine Testsuite [gematik Testsuite] bereitgestellt. Mit dieser Testsuite und der dazugehörigen Testtreiberschnittstelle [api-testtreiber] werden

dann auch die Zulassungstests durchgeführt. Um einen automatisierten Test für den TI-Messenger zu ermöglichen, muss die Test-App des TI-M Clients zusätzlich ein Testtreiber-Modul bereitstellen, welches über eine definierte API [api-testtreiber] die Remotesteuerung des Clients erlaubt. Die Verbindung zum Client ist durch Mutual TLS (mTLS) abgesichert. Die Testtreiber API ist eine zusätzliche Schnittstelle, die nur für die Tests benötigt wird. Aus diesem Grund wurde die Testtreiberschnittstelle auch nicht in der Übersicht "Headless Client Architektur" dargestellt. Das Testtreiber-Module kann für die Zulassung isoliert von der späteren Lösung betrieben werden. Die Zulassung beschränkt sich ausschließlich auf den TI-Messenger Client, das dahinter liegendem System wird nicht betrachtet. Durch den Wegfall der grafische Benutzeroberfläche werden bei der Zulassung des TI-M Headless Clients keine "Look and Feel" Workshops durchgeführt.

A_25619 -TI-Messenger Instanzen

Der TI-Messenger-Anbieter MUSS eine Referenzinstanz und mindestens eine Testinstanz des TI-M FD und TI-M Clients bereitstellen und betreiben.【<=】

A_28687 -TI-Messenger Instanzen für IOP Tests

Der TI-Messenger-Anbieter MUSS die Referenzinstanz des TI-M FD und TI-M Clients auch nach erfolgreicher Zulassung für weitere IOP Tests dauerhaft bereitstellen und betreiben. 【<=】

Die Referenzinstanz hat die gleiche Version wie die Produktionsumgebung. Weiterhin wird die Referenzinstanz für die Reproduktion aktueller Fehler/Probleme aus der Produktionsumgebung genutzt. Der Zugriff auf die Referenzinstanz muss für die gematik zur Fehleranalyse und für weiterführende IOP Tests gewährleistet sein. Die Testinstanz wird von den Herstellern als Entwicklungsumgebung für neuer TI-Messenger Clients und TI-Messenger Fachdienste und für die IOP-Tests zwischen den verschiedenen TI-Messenger-Anbietern genutzt. Die Zulassungstests werden ebenfalls auf der Testinstanz der Hersteller und auf der gematik Referenzimplementierungs-Instanz durchgeführt.

A_28678 -Tests des TI-M Pro Headless Clients gegen die Referenzimplementierung

Der TI-M Client MUSS erfolgreich mit einem Fachdienst (eigener Fachdienst, ein Partner Fachdienst oder ein zusätzlichen Fachdienst einer Referenzimplementierungs-Instanz) gegen eine eigene Instanz und gegen eine Referenzimplementierungs-Instanz getestet werden. Das Ergebnis dieser Tests wird als Eingangskriterium für die Zulassung herangezogen. Die Eingangskriterien für die Zulassung sind in der Verfahrensbeschreibung festgelegt. Die Testergebnisse (Serenity Report) MÜSSEN der gematik vorgelegt werden.【<=】

A_25620 -Nutzung der Referenz- und Testinstanzen

Der TI-Messenger-Anbieter MUSS die verschiedenen Benutzer der Referenzinstanz und der Testinstanz koordinieren (z. B. Verwaltung eines Test-/Nutzungsplans).【<=】

A_25621 -Weitere Testinstanzen

Bei Bedarf (Entwicklung verschiedener Versionen, hoher Auslastung durch andere Hersteller oder durch die gematik) MUSS der TI-Messenger-Anbieter auch mehrere Testinstanzen mit der gleichen oder mit verschiedene Versionen bereitstellen und betreiben.【<=】

Eine detaillierte Beschreibung des Testvorgehens, der Testumgebung befindet sich im Testkonzept [gematik Testkonzept], in der Testtreiberschnittstelle [api-testtreiber] und der Testsuite Dokumentation [gematik TestsuiteUserGuide].

A_25622 -Umsetzung des Testkonzepts

Die TI-Messenger Hersteller MÜSSEN sicherstellen, dass das Testkonzept [gematik Testkonzept] vollständig umgesetzt wird.【<=】

3.2.2 Testtreiber

Die gematik konzentriert sich bei der Zulassung auf das Zusammenspiel der Produkte durch E2E- und IOP-Tests und testet übergreifend die in dieser Spezifikation definierten Anwendungsfälle. Um einen automatisierten Test für den TI-Messenger zu ermöglichen, muss die Test-App des TI-M Clients zusätzlich ein Testtreiber-Modul bereitstellen, welches über eine definierte API die Remotesteuerung des Clients erlaubt. Details zum Testkonzept können unter [gematik Testkonzept] nachgelesen werden.

A_25363 -Testtreiber-Modul

Für jeden TI-M Client MUSS für die Zulassung ein Testtreiber Modul bereitgestellt werden, welches die von der gematik vorgegebene Schnittstelle [api-Testtreiber] anbietet.【<=】

A_25360 -Kein Testtreiber in der produktiven Anwendung

Der Einsatz des Testtreiber-Moduls ist auf das Zulassungsverfahren in Test-Apps beschränkt und DARF NICHT in produktiven Wirkbetriebs-Apps genutzt werden.【<=】

A_25361-01 -Keine Modifikation der Inhalte

Das Testtreiber-Modul DARF die ausgegebenen Inhalte des TI-M Clients NICHT verfälschen und keine Fachlogik des Clients umsetzen.【<=】

Hinweis: Das Testtreiber-Modul kann die Ausgaben des TI-M Clients gemäß der technischen Schnittstelle aufarbeiten.

3.3 Betrieb

Durch die Einführung eines neuen Produkttypen, dem TI-Messenger Pro Headless Client braucht es eine klare Verantwortung im Betrieb. Die Verantwortung wird dem Anbieter TI-Messenger Pro zugeordnet und erweitert damit sein Portfolio an möglichen Produkten welche dieser anbieten kann.

3.3.1 Anbieter

A_28679 -Betriebliche Verantwortung Anbieter TI-M Pro Headless Client

Der Anbieter TI-Messenger Pro MUSS die betriebliche Verantwortung für das Produkt TI-Messenger Headless Client übernehmen, sofern er dieses Produkt anbietet.【<=】

Ein On-Premise-Betrieb ist weiterhin möglich, vorausgesetzt, dass dieser mit dem Anbieter abgestimmt wird. Dabei ist sicherzustellen, dass alle Anforderungen – sowohl unmittelbar als auch mittelbar – durch geeignete Maßnahmen erfüllt werden können.

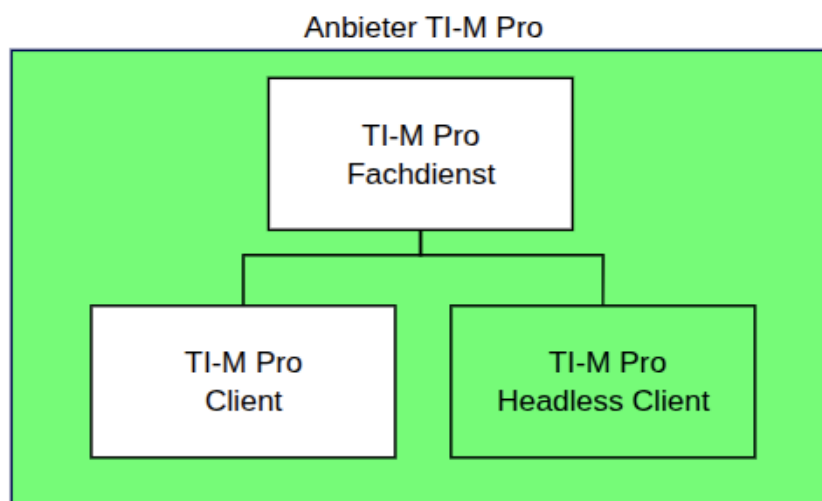


Abbildung 2: Verantwortung im Betrieb für den Anbieter TI-Messenger Pro (farbig: neue/angepasste Anteile)

Damit die gematik in der Rolle des Gesamtverantwortlichen für die TI (GTI) ihrer Pflicht nachkommt, braucht es definierte Governance-Prozesse zur Integration von neuen Komponenten in der TI. Dies erstreckt sich auf den laufenden Betrieb als auch die Außerbetriebnahme.

A_28683 -TI-M Pro Headless Client (un-)mittelbares Bridging-Verbot

Der Anbieter TI-Messenger Pro DARF NICHT den TI-M Pro Headless Client un- oder mittelbar dafür nutzen um ein Bridging in andere Messenger-Systeme durchzuführen. [\leq]

A_28681 -TI-M Pro Headless Client Integrationsbeschreibung Betriebshandbuch

Der Anbieter TI-Messenger Pro MUSS die Integration in jedes verschiedene System in seinem Betriebshandbuch grob in der Architektur beschreiben. Dabei MUSS jedes System in welches der Headless Client integriert wurde, einzeln benannt und mit dem jeweils verantwortlichen Hersteller verknüpft werden.

Hinweis: Die Benennung eines solchen Systems in welches der Headless Client integriert wurde, kann z.B. so aussehen (das folgende Beispiel ist fiktiv):

- 1) E-Rezept-App, verantwortlicher Hersteller: gematik GmbH
- 2) Titus, verantwortlicher Hersteller: gematik GmbH
- 3) ... [\leq]

A_28682 -TI-M Pro Headless Client Integrationsbeschreibung Aktualisierung Betriebshandbuch

Der Anbieter TI-Messenger Pro MUSS spätestens halbjährlich beginnend ab Zulassungserteilung die Systeme in welche der TI-M Pro Headless Client integriert wurde auf Aktualität prüfen und das Betriebshandbuch dahingehend aktualisieren. [\leq]

A_28685 -TI-M Pro Headless Client kontrollierte Inbetriebnahme

Der Anbieter TI-Messenger Pro MUSS für die initiale Inbetriebnahme des TI-M Pro Headless Client eine Inbetriebnahme entsprechend der Vorgaben von [gemKPT_Inbetriebnahme_TI-Messenger_Pro] durchführen. [\leq]

A_28733 -TI-M Pro Headless Client Einsatzkontext

Der Anbieter TI-Messenger Pro MUSS sicherstellen, dass der TI-M Pro Headless Client ausschließlich im Verantwortungsbereich von Organisationen des Gesundheitswesens betrieben wird, die berechtigt sind, einen TI-Messenger zu bestellen und zu nutzen. Der Anbieter MUSS sicherstellen, dass die über den TI-M Pro Headless Client verarbeiteten medizinischen Daten ausschließlich zur Gesundheitsversorgung genutzt werden. [\leq]

3.3.2 Client

Um auch während des dezentralen Betriebs bei den jeweiligen Anbietern aussagefähig zur aktuellen Betriebslage zu sein braucht die gematik zuverlässige Daten aus dem Produktivbetrieb.

A_28725 -TI-M Pro Headless Client Integrationsbeschränkung

Der Anbieter TI-Messenger Pro MUSS sicherstellen, dass der TI-M Pro Headless Client ausschließlich im Verantwortungsbereich von Organisationen des Gesundheitswesens betrieben wird, die berechtigt sind, einen TI-Messenger zu bestellen und zu nutzen. Der Anbieter MUSS sicherstellen, dass die über den TI-M Pro Headless Client verarbeiteten medizinischen Daten ausschließlich zur Gesundheitsversorgung genutzt werden.【<=】

A_28693 -TI-M Pro Headless Client Ereignisdaten

Der TI-M Pro Headless Client MUSS auf Produkttyp- und Produktversionsebene gegenüber dem TI-M Pro Fachdienst eindeutig identifizierbar sein.【<=】

A_28684 -TI-M Pro Headless Client Selbstauskunft

Der TI-M Pro Headless Client MUSS Selbstauskunftsdaten inkl. Informationen zum integrierenden System senden.【<=】

Wie beim TI-M Pro Client werden die Informationen am jeweiligen Fachdienst gesammelt und konsolidiert an die gematik weitergeleitet. Die Verpflichtung beim Anbieter TI-M Pro zum bereits für TI-M Pro bestehenden Monitoring wird analog auf das neue Produkt TI-M Pro Headless Client ausgeweitet.

4 Produkt und Anbieterkonstellationen

Dieses Kapitel beschreibt drei exemplarische Ansätze zur Entwicklung, Zulassung und Integration des TI-M Pro Headless Clients. Die Beispiele zeigen unterschiedliche Verantwortlichkeiten und Konstellationen zwischen Herstellern und Anbietern, die sich aus den spezifischen Anforderungen der Telematikinfrastruktur ergeben. Sie verdeutlichen, wie der Headless Client entweder als eigenständige Komponente in bestehende Primärsysteme integriert wird oder im Rahmen einer vollständig durch den Hersteller kontrollierten Lösung bereitgestellt werden kann.

Beispiel: Integration des Headless Clients in ein Primärsystem durch Dritte

1. Hersteller A entwickelt entsprechend dem Produkttypsteckbrief TI-M Pro Headless Client einen TI-M Pro Headless Client, reicht diesen zur Zulassung ein und erlangt eine Produktzulassung.
2. Hersteller A überreicht das zugelassene Produkt an einen PS-Hersteller B, und der PS-Hersteller integriert das Produkt in sein Primärsystem (z. B. PVS, KIS, AVS oder KTR-System).
3. Anbieter A möchte eine Anbieterzulassung für TI-M Pro erlangen und weist nach, dass er alle Anforderungen aus dem Anbietertypsteckbrief TI-M Pro erfüllt. Anbieter A verantwortet dabei im Produktivbetrieb die Produkte von Hersteller A und B (TI-M Pro Headless Client und PS-System, wobei letzteres nicht der Anbietersteuerung der gematik unterliegt).

Dieses Szenario zeigt, wie ein spezialisierter Hersteller durch die Entwicklung und Zulassung eines TI-M Pro Headless Clients die Grundlage für die Integration in ein Primärsystem durch einen Dritten schafft. Der Anbieter übernimmt die Verantwortung für die Konformität und den Betrieb der Gesamtlösung innerhalb der Telematikinfrastruktur. Dieses Modell verdeutlicht die Flexibilität des Headless Clients, der sich nahtlos in unterschiedliche Systeme wie PVS, KIS, AVS oder KTR-Systeme einfügen lässt.

Beispiel: Einheitlicher Hersteller für Headless Client, TI-M Fachdienst und PS-System

1. Hersteller A entwickelt gemäß den Vorgaben der Produkttypsteckbriefe sowohl den TI-M Pro Headless Client als auch den TI-M Pro Fachdienst und reicht beide Produkte gemeinsam zur Zulassung ein. Nach erfolgreicher Prüfung erlangt er die Produktzulassungen für beide Komponenten.
2. Hersteller A integriert den zugelassenen TI-M Pro Headless Client in sein eigenes Praxisverwaltungssystem (PS-System).
3. Hersteller A, in der Rolle des Anbieters, weist nach, dass er alle Anforderungen aus dem Anbietertypsteckbrief TI-M Pro inkl. dem TI-M Headless Client erfüllt und erlangt die Zulassung für TI-M Pro. Er übernimmt die Verantwortung für den Betrieb seiner eigenen Produkte (TI-M Pro Headless Client, TI-M Pro Fachdienst und PS-System, wobei letzteres nicht der Anbietersteuerung der gematik unterliegt). Der Hersteller stellt das System den Nutzern im Gesundheitswesen in der Anbieterrolle bereit.

Dieses Szenario zeigt, wie ein Hersteller durch die vollständige Kontrolle über Entwicklung, Zulassung und Integration eine konsistente und aufeinander abgestimmte Lösung für seine Nutzer bereitstellen kann.

Beispiel: Zentrale Contact Center Integration bei einem Kostenträger

1. Hersteller A entwickelt entsprechend dem Produkttypsteckbrief TI-M Pro Headless Client einen TI-M Pro Headless Client, reicht diesen zur Zulassung ein und erlangt eine Produktzulassung.
2. Hersteller B entwickelt ein Contact Center System für Kostenträger und integriert den zugelassenen TI-M Pro Headless Client als Modul in eine zentrale Serverkomponente im Rechenzentrum des Kostenträgers.
3. Sachbearbeitende des Kostenträgers nutzen Arbeitsplatz- oder Web Clients, die über transportverschlüsselte Netzwerkschnittstellen mit der zentralen Serverkomponente kommunizieren.
4. Der TI-M Pro Headless Client wird ausschließlich lokal durch die Serverkomponente angesteuert. Nachrichteninhalte, Anhänge, Nutzerdaten und Metadaten zu Chats werden innerhalb der IT Landschaft des Kostenträgers verarbeitet und nur in Informationssystemen genutzt, die die Bedingungen aus A_28725 erfüllen.
5. Der Anbieter TI-Messenger Pro beschreibt diese Integration im Betriebshandbuch (inkl. Systembenennung, verantwortlichem Hersteller, Nutzungsformen und Maßnahmen) und stellt sicher, dass die Nutzung nur im Rahmen der von der gematik veröffentlichten Rahmenbedingungen erfolgt. Bei Verstößen unterstützt der Anbieter die von der gematik initiierten Sperrprozesse.

Dieses Szenario zeigt, wie der TI-M Pro Headless Client in einer zentralen Serverkomponente eines Kostenträgers eingesetzt werden kann, um TI-Messenger Funktionalitäten in ein bestehendes Contact Center System zu integrieren. Die fachliche Kommunikation mit Versicherten erfolgt dabei über die Arbeitsoberflächen der Sachbearbeitenden im Contact Center, während der TI-M Pro Headless Client im Hintergrund die Anbindung an den TI-M Pro Fachdienst übernimmt. Durch die zentrale Integration des TI-M Pro Headless Clients in das Contact Center Backend können eingehende TI Chats anhand von Metadaten und Gesprächsinhalten im Rahmen der Gesundheitsversorgung automatisiert disponiert, geroutet und den jeweils zuständigen Sachbearbeitenden zugewiesen werden. Die Sachbearbeitenden arbeiten ausschließlich in der gewohnten Contact Center Oberfläche, ohne einen separaten TI-M Pro Client bedienen zu müssen. Die Verantwortung für den sicheren und konformen Betrieb des TI-M Pro Headless Clients liegt beim Anbieter TI-Messenger Pro.

5 Anhang A - Verzeichnisse

5.1 Abkürzungen

Kürzel	Erläuterung
BfDI	Bundesbeauftragter für den Datenschutz und die Informationsfreiheit
BSI	Bundesamt für Sicherheit in der Informationstechnik
E2EE	Ende-zu-Ende-Verschlüsselung (Ein Kommunikationssystem, bei dem Nachrichten nur von den Kommunikationspartnern und nicht von Dritten gelesen werden können)
HC	Headless Client (Ein TI-Messenger Client ohne eigene Benutzeroberfläche, die über Schnittstellen in andere Systeme eingebettet wird)
KIM	Kommunikation im Medizinwesen
KIS	Krankenhausinformationssystem (Ein IT-System zur Unterstützung der administrativen, organisatorischen und medizinischen Prozesse in Krankenhäusern)
PS	Primärsystem (Ein IT-System, das bei einem Leistungserbringer eingesetzt wird – z. B. eine Praxisverwaltungssoftware (PVS), ein Zahnarztpraxisverwaltungssystem (ZVS), ein Krankenhausinformationssystem (KIS), ein Laborinformationssystem (LIS) oder eine Apothekensoftware (AVS) – und sich unter dessen administrativer Hoheit befindet. Das Primärsystem ist kein Bestandteil der TI-Plattform.)
PVS	Praxisverwaltungssystem
TI	Telematikinfrastruktur
TI-M	TI-Messenger (Kommunikationslösung der Telematikinfrastruktur für das Gesundheitswesen)
TI-M Pro	TI-Messenger Professional (Spezialisierte Version des TI-Messengers für berufliche Anwender im Gesundheitswesen)
TLS	Transport Layer Security (Protokoll zur sicheren Datenübertragung im Internet)

5.2 Abbildungsverzeichnis

Abbildung 1: Übersicht Headless Client Architektur (farbig: von der gematik regulierte Teile).....	7
Abbildung 2: Verantwortung im Betrieb für den Anbieter TI-Messenger Pro (farbig: neue/angepasste Anteile).....	13

5.3 Referenzierte Dokumente

5.3.1 Dokumente der gematik

Die nachfolgende Tabelle enthält die Bezeichnung der in dem vorliegenden Dokument referenzierten Dokumente der gematik zur Telematikinfrastruktur.

[Quelle]	Herausgeber: Titel
[api-testtreiber]	gematik: Testtreiber-Schnittstelle https://github.com/gematik/TI-Messenger-Testsuite/blob/main/src/main/resources/api/TiMessengerTestTreiber.yaml
[gematik Testkonzept]	gematik: Test und Zertifizierung TI-Messenger https://github.com/gematik/api-ti-messenger/blob/main/docs/Test/Test.adoc
[gematik Testsuite]	gematik: TI-Messenger Testsuite https://github.com/gematik/TI-Messenger-Testsuite
[gematik TestsuiteUserGuide]	gematik: TI-Messenger TestsuiteUserGuide https://github.com/gematik/TI-Messenger-Testsuite/tree/main/doc/userguide
[gemGlossar]	gematik: Glossar der Telematikinfrastruktur
[gemKPT_Test]	gematik: Testkonzept der TI