Elektronische Gesundheitskarte und Telematikinfrastruktur

Konzeptpapier
TI-Messenger

Version:	1.0.0
Revision:	385013
Stand:	21.07.2021
Status:	freigegeben
Klassifizierung:	öffentlich
Referenzierung:	gemKPT_TI_Messenger

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	21.07.2021		Erstversion des Dokumentes	gematik

Inhaltsverzeichnis

1 Einleitung

Mit dem Digitale-Versorgung-und-Pflege-Modernisierungs-Gesetz (DVPMG), welches am 09.06.21 in Kraft getreten ist, erhält die gematik den gesetzlichen Auftrag, die sicheren Übermittlungsverfahren im Gesundheitswesen um einen Sofortnachrichtendienst zu erweitern. Die gematik schafft mit der Spezifikation die Voraussetzungen für den Standard einer anbieter- und sektorenübergreifenden, sicheren Ad-hoc-Kommunikation im gesamten deutschen Gesundheitswesen.

1.1 Einordnung des Dokuments

Das vorliegende Dokument stellt die Zusammenfassung der aktuellen Konzeption eines solchen Kommunikationsstandards durch die gematik dar. Die Veröffentlichung erfolgt nach Freigabe des Dokuments durch die Gesellschafter der gematik.

1.1.1 Zielsetzung

Im vorliegenden Dokument soll auf Basis der aktuellen Überlegungen der gematik die Entscheidung für eine sinnvolle Lösungsarchitektur des TI-Messengers nachvollziehbar argumentiert und erörtert werden. Dabei wird ein Ausblick auf die technischen Details und mögliche Anforderungen an den TI-Messenger gegeben.

1.1.2 Zielgruppe

Das Konzeptpapier richtet sich dabei an alle Stakeholdergruppen der gematik, insbesondere an Vertreter aus der Industrie, Angehörige zukünftiger Nutzerkreise und an die interessierte Öffentlichkeit.

1.1.3 Abgrenzungen

Das vorliegende Dokument widerspiegelt den aktuellen Stand der konzeptionellen Arbeiten und stellt somit noch keine abschließende Betrachtung dar. Vielmehr ist das Konzeptpapier als Grundlage für Diskussionen mit der Industrie und Nutzern sowie als Basis für die nachfolgende Spezifikation zu verstehen.

---

[1] https://www.gematik.de/fileadmin/user_upload/gematik/files/Presseinformationen/gematik_Whitepaper_Arena_digitale_Medizin_TI_2.0_Web.pdf

1.2 Ausgangslage

Der heutige Versorgungsalltag verlangt einen umfassenden und schnellen Austausch von Informationen zwischen Akteuren im Gesundheitswesen. Nur durch eine erschöpfende Verfügbarkeit von Informationen zu einem Patientenfall können medizinische

Entscheidungen richtig und schnell getroffen werden. Aber auch der Austausch zu organisatorischen Themen und zur interdisziplinären Abstimmung in medizinisch tätigen Teams macht eine schnelle und unkomplizierte Kommunikation erforderlich. Dieser Bedarf spiegelt sich jüngst vor allem in der Intensivierung einer digitalen, asynchronen Ad-hoc-Kommunikation. Im Positionspapier der Bundesärztekammer vom 20.05.2020 wurde im Zuge der Herausforderungen der Covid19-Pandemie der Bedarf für einen interoperablen Messaging-Dienst nochmals verdeutlicht und folgende Maßnahme abgeleitet [1]:

„Flächendeckende Einführung einer einheitlichen und sicheren Messenger-App/Anwendung für eine schnelle asynchrone, unproblematische Kommunikation im gesamten medizinischen Bereich." [2]

Ebenso beobachtet das PraxisBarometer der Kassenärztlichen Bundesvereinigung vom 18.11.2020 [3] einen deutlichen Anstieg bei der Nutzung von Messenger-Diensten und SMS sowohl bei der Kommunikation zwischen Ärzten als auch zwischen Ärzten und Patienten, obwohl diese keinen sicheren Standard für den Schutz von Gesundheitsdaten bieten. [4]

*„Deutlich zugenommen hat im Vergleich zu den Vorjahren der Anteil der Praxen, der mit anderen Praxen bzw. ambulanten Einrichtungen mittels Video-konferenzen kommuniziert: Während in den Jahren 2018 und 2019 lediglich 1 Prozent Videokonferenzen als Kommunikationsmedium angegeben hat, liegt der Anteil im Jahr 2020 bei rund 12 Prozent (Abbildung 47). Auch der Anteil der Praxen, der Messenger-Dienste/SMS nutzt, hat sich im Jahr 2020 im Vergleich zum Jahr 2018 verdoppe*lt." [5]

Auch der Deutsche Apotheker Verband erkennt diesen Bedarf und erarbeitet eine eigene sichere Instant-Messaging-Lösung für die Apothekerschaft.

Für den schnellen (ad-hoc) Austausch von Informationen mit Patientenbezug zwischen Leistungserbringern existieren derzeit verschiedene Wege. Diese sind oft datenschutzrechtlich bedenklich (z. B. Fax, WhatsApp) oder unpraktikabel durch zu ermittelnde Kontaktdaten (z. B. Telefon) und Fragmentierung der Systeme (bestehende Messenger-Nischenlösungen). Für die digitale Ad-hoc-Kommunikation haben sich sogenannte Sofortnachrichtendienste bzw. Instant-Messaging-Lösungen (im Folgenden IM) im Alltag bewährt. IM-Dienste (wie z.B. WhatsApp, Threema, Signal etc.) ermöglichen eine schnelle Informationsweitergabe und bilden den Kommunikationsverlauf übersichtlich ab. IM-Dienste werden vorrangig im mobilen Umfeld mit marktüblichen Endgeräten (Smartphones mit Android oder iOS) und Identitäten auf Basis der Telefonnummer verwendet. Die konventionellen, am Markt verfügbaren IM-Dienste erfüllen aktuell nicht den im Gesundheitswesen angestrebten Anspruch an Interoperabilität, Sicherheit, Nutzung offener Standards oder Datenschutzkonformität. In dieser Bedarfssituation haben sich diverse Anbieter etabliert, die für das deutsche Gesundheitswesen angepasste datenschutzkonforme IM-Anwendungen anbieten. Diese Messengerlösungen basieren jedoch auf unterschiedlichen Protokollen und sind untereinander nicht oder nur sehr selten interoperabel. Auch eine einheitliche Ende-zu-Ende Prüfung und Zertifizierung der Einhaltung von Datenschutz-Standards ist aktuell nur eingeschränkt möglich. Darüber hinaus kann die Authentizität der Nutzer und eine anbieterübergreifende Suche nach Kontakten aktuell nicht durchgeführt werden. An dieser Versorgungslücke setzt die Konzeption zum TI-Messenger an. Die Zielsetzung besteht darin, einen einheitlichen Standard für sichere, leistungsfähige und vielseitig einsetzbare Messenger-Dienste zu erarbeiten, die die verschiedenen Akteure im Gesundheitswesen anbieter- und sektorenübergreifend verbinden können.

---

[1] Vgl. Digitale Transformation in der Medizin in Pandemiezeiten (2020), S. 3 ff
[2] Vgl. Digitale Transformation in der Medizin in Pandemiezeiten (2020), S. 3

[3] Vgl. PraxisBarometer Digitalisierung 2020 (2020)
[4] Vgl. PraxisBarometer Digitalisierung 2020 (2020), S.70 ff.
[5] Vgl. PraxisBarometer Digitalisierung 2020 (2020), S.70

1.3 Gesetzliche Rahmenbedingungen

Die gesetzliche Grundlage zur Entwicklung des TI-Messengers ergibt sich aus dem DVPMG, welches zum 09.06.2021 in Kraft getreten ist. Mit dem DVPMG werden die bestehenden Bestimmungen des Fünften Buch Sozialgesetzbuch (SGB V) angepasst und ergänzt. Der Bedarf für eine Instant-Messaging-Lösung wird in § 312 Absatz 1 Satz 1 Nr. 4, 9 und 15 ausgeführt [1]:

§ 312 Aufträge an die Gesellschaft für Telematik

(1) Die Gesellschaft für Telematik hat im Rahmen ihrer Aufgaben nach § 312 Absatz 1 Nummer 1 [...]

4. bis zum 1. Oktober 2021 die Maßnahmen durchzuführen, die erforderlich sind, damit sichere Übermittlungsverfahren nach § 311 Absatz 6 einen Sofortnachrichtendienst zur Kommunikation zwischen Leistungserbringern umfassen, [...]

9. bis zum 1. April 2022 die Maßnahmen durchzuführen, die erforderlich sind, damit der in Nummer 4 definierte Dienst auch zur Kommunikation zwischen Versicherten und Leistungserbringern bzw. Versicherten und Krankenkassen genutzt werden kann, [...]

15. bis zum 1. Oktober 2023 die Maßnahmen durchzuführen, die erforderlich sind, damit die sicheren Übermittlungsverfahren nach § 311 Absatz 6 auch den Austausch von medizinischen Daten in Form von Text, Dateien, Ton und Bild, auch als Konferenz mit mehr als zwei Beteiligten, ermöglichen [...]

„Mit Nummer 16 wird sichergestellt, dass die sicheren Übermittlungsverfahren um zusätzliche Funktionen erweitert werden, um den Kommunikationsbedürfnissen in der Versorgung der gesetzlichen Krankenversicherung umfassend gerecht werden zu können. Die sicheren Übermittlungsverfahren werden durch die vorgesehenen Regelungen daher zum zentralen sicheren Kommunikationsdienst aufgewertet. Die neuen Funktionalitäten umfassen dabei die Möglichkeit der Übertragung von Text, Dateien, Bild und Ton sowie die Schaffung der Möglichkeit von Videokommunikation.

Dabei sollen die sicheren Übermittlungsverfahren die Kommunikation zwischen

Versicherten (oder deren Vertretern) und den Leistungserbringern oder Leistungserbringerinstitutionen,

Leistungserbringern untereinander,

Versicherten (oder deren Vertretern) und den Krankenkassen oder Unternehmen der privaten Krankenversicherung, sowie

Versicherten (oder deren Vertretern) untereinander ausschließlich zum Austausch von Informationen nach § 360 Absatz 12 unterstützen.

Mit der vorgesehenen Aufwertung der sicheren Übermittlungsverfahren wird auch der Forderung nach der Einführung von Diensten zum „Instant-Messaging" in der Versorgung der gesetzlichen Krankenversicherung Rechnung getragen, die den Schutz der Gesundheitsdaten zuverlässig ermöglichen. Insbesondere der Austausch von Sofortnachrichten, sowohl zwischen Beschäftigten im Gesundheitswesen untereinander als auch zwischen Beschäftigten im Gesundheitswesen und Versicherten bzw. Patientinnen und Patienten, ist von großem Vorteil, da er ortsunabhängige (mobile)

Kommunikation ermöglicht. Darüber hinaus ermöglicht der Austausch von Kurznachrichten zwischen Leistungserbringern die direkte, gleichwohl asynchrone Ansprache eines Kommunikationspartners (z.B. von Ärztinnen und Ärzten untereinander oder von Pflegekräften), die auf anderen Wegen nur mit hohem Aufwand etabliert werden kann und aus diesem Grund oft gänzlich unterbleibt. Die Nutzung entsprechender Verfahren ermöglicht eine erhebliche Verbesserung der Kommunikation zur Abstimmung patienten- und versorgungsbezogener Belange sowohl zwischen Leistungserbringern als auch zwischen Leistungserbringern und Versicherten. Dabei gilt es, aus Gründen der Datensicherheit und des Datenschutzes einen einheitlichen und sicheren Standard für Nachrichtensofortversanddienste für das Gesundheitswesen zu etablieren. Zugleich werden die großen Vorteile von „Instant Messaging" als moderne Kommunikationslösung durch die sicheren Übermittlungsverfahren für das Gesundheitswesen erschlossen. Soweit den Leistungserbringern für die Nutzung des Dienstes zusätzliche Aufwände entstehen, obliegt es den jeweiligen Vertragspartnern, eine angemessene Vergütung zu gewährleisten." [2]

§ 342 Angebot und Nutzung der elektronischen Patientenakte

(2) Die elektronische Patientenakte muss technisch insbesondere gewährleisten, dass

4. zusätzlich spätestens ab dem 1. Januar 2023
d) die Versicherten den Sofortnachrichtendienst mit Leistungserbringern und mit Krankenkassen als sicheres
Übermittlungsverfahren nach § 311 Absatz 6 über die Benutzeroberfläche nach Nummer 1 Buchstabe b nutzen können;
[...] [1]

"Die Neuregelung in Nummer 4 sieht vor, dass die Gesellschaft für Telematik mit der Spezifikation der Schnittstelle eines Messaging-Dienstes für die Kommunikation zwischen Leistungserbringern beauftragt wird. [...]

Die Neuregelung in Nummer 8 sieht vor, dass die Kommunikation über den Messaging-Dienst auch für die Kommunikation zwischen Versicherten und Leistungserbringern bzw. Versicherten und Krankenkassen genutzt werden kann. Für die Nutzung des Messaging-Dienstes der Versicherten darf kein neues Verzeichnis der Versicherten aufgebaut werden. Stattdessen kann beispielsweise ein Pseudonym der Krankenversichertennummer verwendet werden. Die Schnittstelle muss insbesondere das ePA-Frontend des Versicherten, das heißt die ePA-App, und die Komponenten zur Wahrnehmung der Versichertenrechte an stationären Endgeräten, unterstützen. [...]

Bei der Nutzung des Messaging-Dienstes zwischen Leistungserbringern und Versicherten kann der Leistungserbringer festlegen, dass eine Kommunikation mit Versicherten immer vom ihm selbst initiiert werden muss. Es besteht keine Rechtspflicht zur Nutzung für den Leistungserbringer. [...]" [3]

§ 366 Vereinbarung über technische Verfahren zur Videosprechstunde in der vertragszahnärztlichen Versorgung

(1) Die Kassenzahnärztliche Bundesvereinigung vereinbart mit dem Spitzenverband Bund der Krankenkassen im Benehmen mit der Gesellschaft für Telematik die Anforderungen an die technischen Verfahren zu Videosprechstunden, insbesondere Einzelheiten hinsichtlich der Qualität und der Sicherheit, und die Anforderungen an die technische Umsetzung. Die Kassenzahnärztliche Bundesvereinigung und der Spitzenverband Bund der Krankenkassen berücksichtigen in der Vereinbarung nach Satz 1 die sich ändernden Kommunikationsbedürfnisse der Versicherten, insbesondere hinsichtlich der Nutzung digitaler Kommunikationsanwendungen auf mobilen Endgeräten. Bei der Fortschreibung

der Vereinbarung ist vorzusehen, dass für die Durchführung von Videosprechstunden Dienste der Telematikinfrastruktur genutzt werden können, sobald diese zur Verfügung stehen. § 630e des Bürgerlichen Gesetzbuchs ist zu beachten.

Geltungsbereich des Telekommunikationsgesetzes (TKG) und des Telemediengesetz (TMG)

TK- und TM-rechtliche Vorschriften stehen dem Technologiesprung zur TI 2.0 nicht entgegen. In Umsetzung des Art. 2 Nr. 4 Richtlinie (EU) 2018/1972 wurde der Begriff des Telekommunikationsdienstes grundlegend überarbeitet. Die Definition des Telekommunikationsdienstes in dem ab 01. Dezember 2021 geltenden TKG umfasst drei Kategorien von Diensten, die sich inhaltlich überschneiden können, den Internetzugangsdienst, den interpersonellen Telekommunikationsdienst und Dienste, die ganz oder überwiegend in der Übertragung von Signalen bestehen.

Die Anwendung TI-Messenger ist als interpersoneller Telekommunikationsdienst im Sinne des TKG n.F. zu qualifizieren. Sobald dieser Dienst auch gegenüber den Versicherten erbracht wird, handelt es sich zudem um einen öffentlich zugänglichen Telekommunikationsdienst, der zusätzlichen Verpflichtungen nach dem TKG unterliegt.

Der Anbieter einer TI-Messenger-Anwendung ist Adressat der telekommunikationsrechtlichen Pflichten nach dem TKG. Der Umfang der telekommunikationsrechtlichen Verpflichtungen richtet sich einerseits danach, ob die Anwendungen als nummerngebundene oder nummernunabhängige Dienste ausgestaltet werden, andererseits danach, ob die Dienste als öffentlich zugänglich einzustufen sind oder nicht. Die derzeit vorgesehene Anwendung ist als nummernunabhängiger Dienst anzusehen und nach unserer Einschätzung dann öffentlich zugänglich, wenn die Dienste auch gegenüber den Versicherten erbracht werden. Bis dahin ist von einem nicht öffentlich zugänglichen Telekommunikationsdienst auszugehen.

Der Anbieter einer TI-Messenger-Anwendung hat im Fall der Einstufung als öffentlich zugänglicher Telekommunikationsdienst die Vorschriften zum Kundenschutz in Teil 3 des TKG n.F. und der öffentlichen Sicherheit in Teil 10 Abschnitt 1 des TKG n.F. zu beachten. Dazu gehören etwa die Erfüllung besonderer Transparenzpflichten, die Erstellung eines Sicherheitskonzepts und die Bestellung eines Sicherheitsbeauftragten. Umfang und Art der einzelnen telekommunikationsrechtlichen Pflichten hängen von der konkreten Ausgestaltung und Art des Dienstes ab.

Ferner sind die datenschutzrechtlichen Bestimmungen sowie das Fernmeldegeheimnis zu beachten, die künftig im neuen Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG) geregelt sind. Das Fernmeldegeheimnis gilt für den jeweiligen Anbieter eines TI-Messenger-Dienstes sowie die Betreiber der dafür genutzten Netze, nicht jedoch für die Nutzer des Dienstes. Diese sind stattdessen ggfs. als Leistungsträger (auch) hinsichtlich der von ihnen übermittelten Sozialdaten an das Sozialgeheimnis gebunden. Das Fernmeldegeheimnis erstreckt sich auf den Inhalt der Telekommunikation, ihre näheren Umstände, insbesondere die Tatsache, ob jemand an einem Telekommunikationsvorgang beteiligt ist oder war und auf die näheren Umstände erfolgloser Verbindungsversuche (§ 88 Abs. 1 TKG a.F. bzw. § 3 Abs. 1 TTDSG). Zum Schutz des Fernmeldegeheimnisses hat der Anbieter des Dienstes geeignete technische und organisatorische Maßnahmen zu implementieren.

Im Fall der Einstufung als nicht öffentlich zugängliche Telekommunikationsdienste gelten zwar nach derzeitigem Stand die Regelungen des TTDSG, im Bereich des TKG aber nicht die Regelungen zum Kundenschutz und lediglich ein geringerer Pflichtenumfang im

Bereich der Öffentlichen Sicherheit.

[1] SGB V

[2] DVPMG (2021), S. 118

[3] DVPMG (2021), S. 117

1.4 Abgrenzung KIM und TI-Messenger

Das sich im Rollout befindliche sichere Übermittlungsverfahren KIM (Kommunikation im Medizinwesen) ist ein auf E-Mail-Technologie basierender Kommunikations-Dienst. Dieser Dienst unterstützt Leistungserbringer in der Standard- oder Regelkommunikation mit anderen Teilnehmern in der Telematikinfrastruktur (TI). Standard- und Regelkommunikation sei dabei definiert als jene Kommunikation, die eine im Gesundheitswesen tätige Person im verwaltungstechnischen und organisatorischen Rahmen dieser Tätigkeit zu bewerkstelligen hat. Zur Standard- oder Regel-Kommunikation gehört demnach u. a. der Versand von Dokumenten mit medizinischem, teilweise auch administrativem Inhalt, wie z. B. der eArztbrief, die elektronische Arbeitsunfähigkeits-bescheinigung (eAU) und Labordaten. Die Kommunikation mittels KIM erfolgt ortsfest (durch den notwendigen Konnektor bzw. Basis-Consumer) und wird durch Clientsoftware auf dem Primärsystem oder als E-Mail-Client unterstützt.

Der Fokus bei IM-Diensten liegt auf einer unmittelbaren und asynchronen Kommunikation, die eher mit einem Telefonat als einer E-Mail zu vergleichen ist. Darüber hinaus werden IM-Dienste, wie in Kapitel 1.2 beschrieben, im Gegensatz zur konnektorgebundenen E-Mail-Technologie bei KIM vorrangig im mobilen Umfeld mit marktüblichen Endgeräten verwendet. Da die Use Cases beim TI-Messenger sowohl eine stationäre als auch mobile Anwendung erfordern, muss sich die anzustrebende Technologie zur Übermittlung der Kommunikation grundlegend von der bei KIM verwendeten E-Mail-Technologie unterscheiden. Der TI-Messenger wird dabei neben mobilen Anwendungsszenarien auch als Desktop-Version mit gängigen Betriebssystemen nutzbar und in Primärsysteme integrierbar sein können. Anders als bei KIM werden auch Versicherte und deren Vertreter zu den Nutzern des TI-Messengers zählen. Besonders vor dem Hintergrund der Erweiterung um diese Nutzergruppe wird eine konnektorlose Architektur erforderlich.

Der TI-Messenger wird die erste TI 2.0-fähige Anwendung der gematik. Es wird via Internet auf die serverseitigen Komponenten des TI-Messengers zugegriffen. Zur Nutzung des TI-Messengers durch Leistungserbringer aus einem PS muss eine Integration in dieses erfolgen. Im Marktmodell ist dafür der PS-Anbieter verantwortlich. Wie in Kapitel 3.1.1 (A3) beschrieben, muss ein TI-Messenger-Anbieter auch desktopfähige Clients anbieten. Für die Nutzung via Desktop-PC ist dann lediglich ein Internetzugang des Desktop-PCs erforderlich. Für Organisationen ohne direkten Internetzugang kann über den Konnektor der sichere Internet-Service des VPN-Zugangsdienstes genutzt werden. Im zeitlichen Verlauf des Roll-Outs des TI-Messengers wird dieser, wie in Kapitel 1.3 beschrieben, auch Versicherten die Möglichkeit zur sicheren Ad-hoc-Kommunikation im medizinischen Kontext bieten. Dabei sind die Krankenkassen oder Unternehmen der privaten Krankenversicherung verpflichtet, einen TI-Messenger-Client für die Versicherten in das jeweilige ePA-Frontend-des-Versicherten (mobil und stationär nutzbar) zu integrieren.

1.5 Zeitplan und Ausblick

Der TI-Messenger wird in drei Ausbaustufen spezifiziert werden. Im Fokus der ersten Ausbaustufe (TI-Messenger 1.0) steht zunächst die Kommunikation zwischen Leistungserbringern. Verkammerte Leistungserbringerberufen, die über einen Heilberufsausweis (HBA) verfügen, werden direkt am TI-Messenger teilnehmen können. Darüber hinaus wird auch für Institutionen, die über eine Institutionenkarte (SMC-B) verfügen, die Option eröffnet, allen ihren Mitarbeitern unabhängig von der Verfügbarkeit eines HBAs die Nutzung eines TI-Messengers zu ermöglichen. Eine Erweiterung der Nutzergruppen wird fortlaufend stattfinden und vor allem in der zweiten Ausbaustufe (TI-Messenger 2.0) durch die Versicherten erfolgen. In der dritten Ausbaustufe (TI-Messenger 3.0) wird der Funktionsumfang um eine Möglichkeit zur Videotelefonie erweitert werden. Abbildung 1 zeigt den Zeitplan der Entwicklung gemäß DVPMG zur Fertigstellung des TI-Messengers in der Version 1.0 durch die gematik. Zudem wird bereits ein Ausblick auf die folgenden Meilensteine der Ausbaustufen 2.0 und 3.0 des TI-Messengers aus dem DVPMG gegeben.

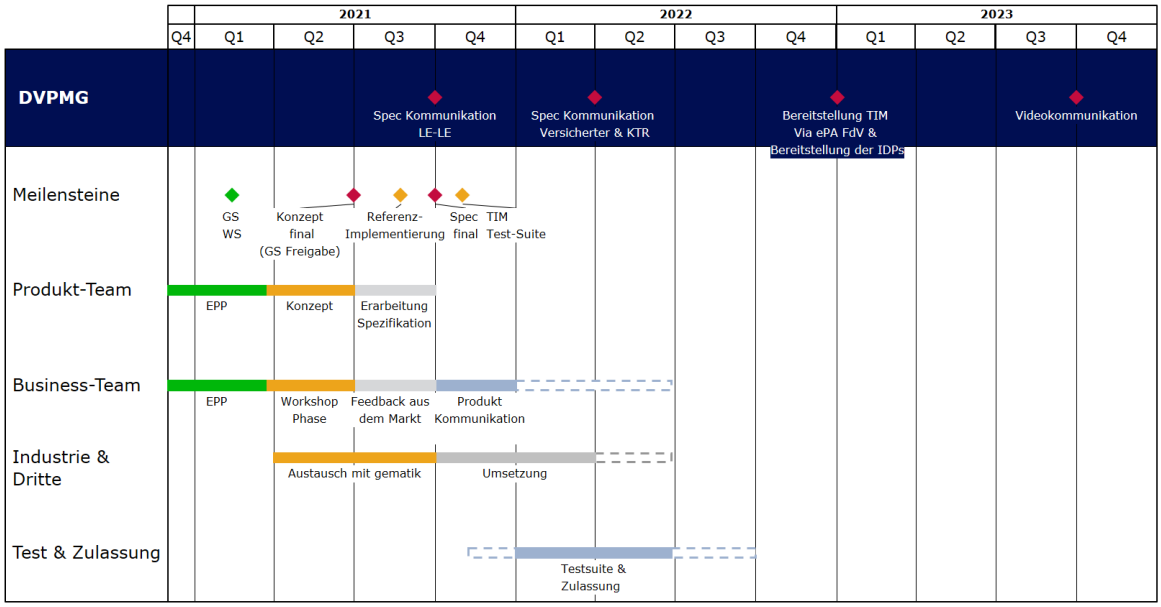

Abbildung 1: Zeitplan TI-Messenger

Um dem im DVPMG gesetzten Zeitplan gerecht werden zu können, hat die gematik zum 09.04.21 bereits ein Eckpunktepapier [gemEP_TIM] mit den Gesellschaftern der gematik abgestimmt, welches die Rahmenbedingungen des TI-Messengers skizziert. Diese Eckpunkte sind in Kapitel 2 zu finden. Das Konzeptpapier stellt die nächste Stufe in der Erarbeitung des TI-Messengers dar und wurde ebenfalls auf Basis des Gesetzentwurfes zum DVPMG und parallel zu dessen Verabschiedung erstellt. Im weiteren zeitlichen Verlauf folgt dem vorliegenden Konzeptpapier die Erarbeitung der Spezifikation des TI-Messengers in der Version 1.0 (Kommunikation zwischen Leistungserbringern (§ 312 Absatz 1 Nr. 4 SGB V). Die von den Gesellschaftern der gematik freigegebene Spezifikation wird zum 01.10.2021 veröffentlicht. Die Umsetzung der Spezifikation durch die Industrie-Partner kann entsprechend nach der Veröffentlichung ab dem 01.10.2021 beginnen. Die Test- und Zulassungsverfahren können parallel zur Umsetzungsphase beginnen und werden fortlaufend weitergeführt.

Die Kommunikation zwischen Leistungserbringern und Versicherten beziehungsweise Versicherten und Kostenträgern (§ 312 Absatz 1 Nr. 9 SGB V) wird zum 01.04.22 in der

Spezifikation der Version 2.0 des TI-Messengers durch die gematik festgelegt werden. Ab dem 01.10.2023 wird die Funktionalität des TI-Messengers in einer dritten Phase um eine Möglichkeit erweitert, Videokonferenzen mit mehr als zwei Personen durchzuführen (§ 312 Absatz 1 Nr. 15 SGB V). Grundlegende technische Voraussetzungen für den TI-Messenger in den Versionen 2.0 und 3.0 werden bereits im vorliegenden Konzept sowie der zu erstellenden Spezifikation für den TI-Messenger 1.0 berücksichtigt.

1.6 Nutzergruppen des TI-Messengers

Die Nutzergruppen und Akteure des TI-Messengers sind in Tabelle 1 aufgelistet.

Tabelle 1: Nutzergruppen und Akteure

Version	Nutzergruppen	Akteure
TI-Messenger 1.0	Leistungserbringer	niedergelassene Ärzte in einer Klinik tätige Ärzte Ärzte im mobilen Einsatz (Notärzte, Ärzte bei Hausbesuchen) Zahnärzte Apotheker psychologische Psychotherapeuten Mitarbeiter in einer Organisation im Gesundheitswesen mit SMC-B: Rettungsdienst Pflegepersonal Berufsmäßige Gehilfen nach § 352 SGB V Hebammen Weitere Mitarbeiter
	Leistungserbringer Institutionen	Praxen Apotheken Zahnarztpraxen Krankenhäuser Pflege-Einrichtungen und Rehakliniken (mit SMC-B) kassenärztliche und kassenzahnärztliche Vereinigungen sowie Ärztekammern
TI-Messenger 2.0	Leistungserbringer	Mitarbeiter einer Organisation im Gesundheitswesen ohne SMC-B: Rettungsdienst Pflegepersonal Hebammen medizinische Fachangestellte weitere Mitarbeiter

	weitere Institution	weitere Institutionen der Leistungserbringer (ohne SMC-B) Robert-Koch-Institut (RKI) Gesundheitsämter BfArM (Rote Hand Brief / Warnbrief)
	Kostenträger	gesetzliche Krankenversicherungen Unternehmen der privaten Krankenversicherung
	Versicherte	Versicherte (gesetzliche) Betreuer / Bevollmächtigte / Vormund sonstige Vertreter (z. B. Eltern)
TI-Messenger 3.0	Die Nutzergruppen und Akteure in der Ausbaustufe TI-Messenger 3.0 ergeben sich aus der Gesamtheit der Nutzergruppen aus den Ausbaustufen 1.0 und 2.0.	

2 Eckpunkte

Im Eckpunktepapier der gematik [gemEP_TIM] vom 21.02.2021 wurden die Eckpunkte zum TI-Messenger als Rahmenbedingungen für die Konzeption erstmals bei den Gesellschaftern vorgestellt. Gemäß den Kommentierungen der Gesellschafter und Diskussion dieser am Gesellschafter-Workshop am 12.02.2021 werden die Eckpunkte entsprechend angepasst und am 09.04.2021 finalisiert. Die mit den Gesellschaftern geteilten, finalen Eckpunkte sind in Tabelle 2 zusammengefasst.

Tabelle 2: Eckpunkte TI-Messenger

ID	Eckpunkt
01	**Nutzer** Die Nutzung des TI-Messengers muss die Kommunikation (1) zwischen Leistungserbringern untereinander sowie (2) zwischen Leistungserbringer und Versicherten ermöglichen. Dabei ist sowohl eine 1:1 Kommunikation, als auch eine Kommunikation in einem Gruppenchat möglich. Die Kommunikation zwischen (3) Versicherten untereinander soll jedoch ausschließlich zur Übermittlung von E-Rezept-Token im Sinne einer Vertreterregelung möglich sein. Die Nutzung des TI-Messengers soll neben personenbezogener Kommunikation auch eine einrichtungsbezogene Kommunikation mit Leistungserbringerinstitutionen (4) ermöglichen. Dementsprechend müssen sowohl personenbezogene als auch institutionsbezogene Accounts möglich sein.
02	**Offene Standards** Bei der Konzeptionierung des TI-Messengers wird darauf geachtet, dass auf bereits etablierte Lösungsmodelle (z.B. Open Source) zurückgegriffen wird. Auf eine proprietäre Lösung / Eigenentwicklung soll verzichtet werden. Die Entwicklung erfolgt in Stufen, dabei soll bereits die Erstumsetzung als Minimallösung für die LE-LE-Kommunikation eine Architektur wählen, die sich ohne grundlegende Änderungen auf die nachfolgenden Stufen erweitern lässt
03	**Marktmodell, Interoperabilität und Innovationsfreiheit** Der TI-Messenger soll von verschiedenen Marktteilnehmern angeboten werden können. Durch den Wettbewerb können Nutzerbedarfe unterschiedlicher Professionen durch Lösungen mit z. B. unterschiedlichen Features entstehen und die Clients in ihrem Zulassungsumfang nicht auf die Unterstützung bestimmter Ziel-OS festgeschrieben werden. Daher sollen für Client- und Fachdienstanteile getrennte Zulassungsverfahren angeboten werden. Dabei wird die Sicherheit und Betriebsfähigkeit durch einheitliche von der gematik vorgegebene Standards gewährleistet. Die Interoperabilität der einzelnen Messenger-Clients wird durch eine Föderation der Homeserver gewährleistet. Diese Interoperabilität gewährleistet, dass eine Kommunikation über Anbietergrenzen hinaus möglich ist.

04	**Identitäten und Authentisierung** Die Nutzer des TI-Messenger werden sicher über bestehende Identitäten (föderierter Identity Provider (IDP) und Authentifizierungs-Mechanismen authentifiziert. Die Nutzung von Institutions-Accounts (z. B. ein Client für eine Krankenkasse) ist bereits in der Konzeptionsphase zu berücksichtigen. Der TI-Messenger muss darüber hinaus die von den Krankenkassen und Mitgliedsunternehmen bereitgestellten Identitäten von Versicherten berücksichtigen. Die jeweiligen Rollen (z. B. Arzt, Apotheker etc.) des Kommunikationsteilnehmers wird für andere TI-Messenger-Nutzer kenntlich gemacht.
05	**Sicherheit und Datenschutz** Die Kommunikation ist für alle Beteiligten Ende-zu-Ende-verschlüsselt. Darüber hinaus muss der TI-Messenger die sicherheits- und datenschutztechnischen Anforderungen erfüllen, welche für die Verarbeitung von Gesundheitsdaten eingehalten werden müssen. Dieser Zweck muss mit einer einfachen und den Nutzer entlastenden Bedienung in Einklang gebracht werden. Die gematik führt eine Sicherheitsanalyse unter Einbeziehung der zuständigen Behörden durch, in der auch Bedienbarkeit und Transparenz der Lösung für den Endnutzer einbezogen werden, und stellt die Ergebnisse transparent dar.
06	**Steuerung der Kommunikation** Grundsätzlich müssen der Leistungserbringer und Organisationen die Möglichkeit haben, festzulegen, dass die initiale Kommunikation immer von ihnen ausgehen muss. Es sollte jedoch die Möglichkeit einer anlass- und teilnehmerbezogenen Konfigurierbarkeit geprüft werden, die es dem LE ermöglicht, für bestimmte Anlässe bzw. Versicherte die Initiierung der Kommunikation durch die Versicherten zuzulassen (z. B. für Terminanfragen oder Fragen bekannter Patienten).
07	**Test und Zulassung** Vor Markteintritt, aber auch im Laufe der Nutzung einzelner TI-Messengerlösungen der Anbieter führt die gematik Funktions- und Interoperabilitätstests durch. Die noch festzulegenden Zulassungs-, Bestätigungs- und Prüfverfahren müssen auf die Dynamik im Markt mobiler Endgeräte und Anwendungen ausgerichtet sein. Anbieter und Hersteller bringen im Rahmen der Zulassungsverfahren Sicherheitsnachweise bei.
08	**Mobile und stationäre Verwendung** Der TI-Messenger kann sowohl im mobilen als auch stationären Umfeld verwendet werden. Somit soll die Nutzung des TI-Messengers im Browser, in Apps als auch im Primärsystem gewährleistet werden. Eine Synchronisierung zwischen mehreren verwendeten Clients pro User muss gewährleistet werden.
09	**Attraktivität der Lösung** Anbieter und Hersteller des TI-Messengers achten bei der Umsetzung auf marktübliche ergonomische Standards im Messenger-Bereich. Der Einsatz des TI-Messengers soll auf marktüblichen Endgeräten (bring your own device) erfolgen. Der TI-Messenger muss unter dem Gesichtspunkt der Wirtschaftlichkeit konzeptioniert werden, mit der Zielsetzung, bereits am Markt bewährte (Standard-) Lösungen/Komponenten zu verwenden.

10	**Koexistenz KIM und TI-Messenger** Der TI-Messenger wird parallel zum bestehenden sicheren Übermittlungsverfahren KIM betrieben und weiterentwickelt. Es besteht somit eine Koexistenz zweier technisch unterschiedlicher sicherer Übermittlungsverfahren mit unterschiedlichen Anwendungsschwerpunkten, welche sich in ihrer Funktionalität aber nicht gegenseitig ausschließen.
11	**Integrierbarkeit** Der TI-Messenger bietet offene Schnittstellen, welche für Anwendungen der TI, Hersteller von Primärsystemen und weiteren Systemen (z.B. Rechenzentren bei Krankenhäusern) nutzbar bzw. integrierbar sind. Auch versichertenseitig werden offene Schnittstellen unterstützt, um die Nachnutzung des TI-Messengers für Chatbots (z.B. für Terminvergabe), Digitale Gesundheitsanwendungen (DIGA) und anderen Gesundheitsanwendungen zu gewährleisten. Beispiel 1: Arzt-Versicherten-Kommunikation via ePA-Frontend Beispiel 2: Vertretungsregelung beim E-Rezept Beispiel 3: Integration in Primärsysteme Chatverläufe müssen dabei für Leistungserbringer fallbezogen zuweisbar und zu Dokumentationszwecken (Dokumentationspflicht des Arztes) nahtlos in ein Primärsystem (bspw. als PDF) übernehmbar sein
12	**Abschottung der Lösung** Die Datenhaltung erfolgt dezentral auf einem gekapselten und verschlüsselten Speicher der Messenger-Umgebung. Die Verarbeitung von Daten findet innerhalb der Messenger-Lösung und somit ausnahmslos getrennt von den Bestandsdaten des Endgerätes statt. Eine Kommunikation mit umliegenden Systemen, Datenexporte zu Nachweiszwecken, etc. laufen über die Nutzung von spezifizierten Schnittstellen ab. Diese Schnittstellen werden z.B. vom Primärsystem angesprochen, in welches TI-Messenger-Clients integriert sind.
13	**Referenzimplementierung** Die gematik kann eine Referenzimplementierung mit Mindestanforderungen des TI-Messengers als Guideline für die Hersteller und Anbieter veröffentlichen.
14	**Betrieb** Der reibungslose Betrieb inkl. Support der Messenger-App und dazugehöriger Fachdienste wird durch die Anbieter sichergestellt. Dabei wird die betriebliche Koordination der Anwendungen durch geeignete Monitoring- und Steuerungsinstrumente unterstützt.

3 Anforderungen

Da das Konzeptpapier als Grundlage für die Abstimmung und Diskussion zum TI-Messenger dienen soll (siehe Kapitel 1), sind auch die nachfolgenden Anforderungen zunächst als Sammlung ohne normativen Charakter zu verstehen. Eine normative Aufarbeitung der Anforderungen erfolgt im Rahmen der Spezifikation.

3.1 Anforderungen TI-Messenger 1.0

3.1.1 Funktionsumfang

Tabelle 3: Anforderungen – Funktionsumfang TI-Messenger 1.0

ID	Titel	Beschreibung	Priorität
A1	Versenden und Empfangen von Textnachrichten, Dokumente (z. B. PDF), Foto und Sprachnachrichten	Über den TI-Messenger sollen Texte, Dokumente (PDF), Fotos und Sprachnachrichten versendet und empfangen werden können. Eine Größenbeschränkung ist nicht vorgesehen.	hoch
A2	Sehr gute User-Experience	Der TI-Messenger wird im professionellen Umfeld eingesetzt. TI-Messenger-Clients müssen daher übersichtlich und intuitiv in der Handhabung sein.	hoch
A3	Geräteunabhängige Nutzung	Der TI-Messenger muss sowohl auf privaten, mobilen Endgeräten wie Handy und Tablet (bring your own device - BYOD) als auch via PC nutzbar sein. Die zur mobilen Version gleichwertige Desktop-Version erleichtert die Zusammenarbeit zwischen dem stationären Arbeitsplatz und den mobilen Szenarien. Eine Synchronisation von Clients der gleichen User-ID muss stattfinden können.	hoch
A4	Verwendung eines Nutzerverzeichnisses	Über ein anbieterübergreifendes Nutzerverzeichnis (VZD-FHIR-Server) soll die einfache Suche anderer Nutzer gewährleistet werden. Der VZD-FHIR-Server ist eine Weiterentwicklung des bisherigen LDAP-basierten VZD der TI und kann auch als VZD 2.0 bezeichnet werden. Durch das FHIR-Protokoll und Format wird es einfacher, den VZD um die erforderlichen Funktionen wie z. B. die Speicherung von mehreren Adressen pro Eintrag zu erweitern. Die bisher von den Kartenherausgebern gepflegten Einträge im LDAP-VZD werden in den VZD-FHIR-Server synchronisiert. Die folgenden Kriterien können angegeben werden: 1. Personen Name Vorname	hoch

		Straße Postleitzahl Stadt Bereich (Hausarzt, Facharzt XYZ, etc.) weitere Merkmale (z. B. Spezialisierungen oder Stations- / Organisationsstruktur) 2. Institutionen Name der Institution Straße Postleitzahl Stadt Art der Institution (Krankenhaus, Praxis XY, etc.) weitere Merkmale (z. B. Spezialisierungen) Lokale Adressbücher im Sinne einer Favoritenliste sollen innerhalb der Clients möglich sein. Versicherte werden nicht in den Verzeichnisdienst aufgenommen werden. Eine Möglichkeit zur Umsetzung einer Wildcard-Search muss gegeben sein, um eine hohe Nutzbarkeit der Suchfunktion zu erreichen.	
A5	Klassifizierung der Nutzer	LEI können unterschiedliche Berechtigungsumfänge für ihre Mitarbeitenden festlegen. Eine eindeutige Kennzeichnung des Berechtigungsumfangs eines jeweiligen Nutzers des TI-Messenger (z. B. Arzt vs. Pflegekraft) ist für eine hohe Usability der Nutzersuche sinnvoll. Ein bestimmter Berechtigungsumfang (z.B. der eines Arztes) soll graphisch verdeutlicht werden. Es ist denkbar, eine grobe Einteilung der Nutzer vorzunehmen und die Berufsgruppe mit noch zu definierenden Grafiken zu kennzeichnen, welches beim Eintrag im VZD-FHIR-Server vergeben wird.	hoch
A6	Erstellen von Chatgruppen	Es ist möglich, Chatgruppen für den Austausch zw. Institution/LE, LE/LE, Dienstgruppen in einer Leistungserbringerinstitution zu erstellen. Hier kann der Fokus auf organisatorischen Themen liegen oder um z. B. Fälle zu besprechen.	hoch
A7	Kennzeichnung von Chats als Fall	Chats können als Patienten-Fall deklariert werden, indem interdisziplinär und institutionsübergreifend zu diesem Fall kommuniziert werden kann. Medien und relevante Kommentare zu einem Fall sollen separat vom restlichen Chatverlauf in Form von FHIR-Datenstrukturen schnell und einfach zusammenfassen und exportieren zu können.	hoch

A8	Nachnutzung als Push-Dienst	Der TI-Messenger soll von vornherein so aufgebaut werden, dass eine Nachnutzung durch andere Dienste als Übermittler von automatisierten Benachrichtigungen an Nutzer möglich ist. Es wird einen Opt-in für Push-Notfications geben.	hoch
A9	Verfügbarkeit der Chatverläufe und Anhänge	Chatverläufe und Anhänge werden zeitlich begrenzt auf den Servern vorgehalten. Eine konkrete Frist wird noch mit den Nutzern diskutiert und erarbeitet. Der User muss vor einem automatischen Löschen älterer Nachrichten und Anhänge benachrichtigt werden, um die betrachteten Inhalte vor dem Löschvorgang in der ePA oder lokal persistieren zu können.	hoch
A10	Vergabe von Statusmeldungen	User können Statusmeldungen veröffentlichen (Emoji und Text, z. B. Haken für aktiv). Beispielhafte Standardmeldung: aktiv abwesend nicht stören Urlaub bis [DATUM], Vertretung ist [VERTRETER]	mittel
A12	Barrierefreiheit der Anwendung	Bei der Entwicklung von Messeger-Clients müssen Möglichkeiten zur Schaffung von Barrierefreiheit berücksichtigt werden (wie z.B. eine Anpassung der Schriftgrößte, Transformation Sprache in Text oder eine Vorlesefunktion)	hoch

3.1.2 Sicherheit

Tabelle 4: Anforderungen – Sicherheit TI-Messenger 1.0

ID	Titel	Beschreibung	Priorität
A13	Sichere komfortable Authentifizierung	Um einen hohen Sicherheitsanspruch mit einer komfortablen Authentifizierung zu kombinieren, soll eine Zwei-Faktor-Authentifizierung verwendet werden. Hierbei soll einerseits auf schwache Authentifizierungsfaktoren verzichtet werden, jedoch andererseits sichergestellt werden, dass die verwendeten Authentisierungsmethoden die Nutzerakzeptanz nicht wesentlich einschränken.	hoch
A14	Transportverschlüsselung	Es muss eine Ende-zu-Ende-Verschlüsselung und zusätzlicher Transportverschlüsselung der Nachrichten zwischen Endgeräten gewährleistet sein. Letztere soll tatsächlich über Anbietergrenzen hinaus gehen. Hierzu sind State-of-the-art-Protokolle zu verwenden.	hoch

A15	Entkopplung von Mobilgerät-Kontaktliste	Die Suche nach Kontakten erfolgt über den VZD-FHIR-Server und darf nicht über das Adressbuch des Geräts bzw. des Betriebssystems abgebildet werden.	hoch
A16	Medienspeicher entkoppelt von Mobilgerätmedien	Mittels der App versandte Medien dürfen nicht automatisiert im Speicher des Mobilgeräts abgelegt werden. Stattdessen sind die Medien in einem gekapselten und verschlüsselten Speicher der Applikation zu hinterlegen, auf den ein Zugriff nur mittels der Applikation möglich ist. Eine Speicherung von Medien auf dem Gerät soll möglich sein, aber jeweils einzeln pro Vorgang die explizite Zustimmung des Nutzers erfordern.	hoch
A17	Grundsätze sicherer Softwareentwicklung	Schon in Entwurfs- und Implementierungsphase sind Grundsätze sicherer Softwareentwicklung einzuhalten wie z.B.: Secure Software Development Lifecycle Security und Privacy by Design und by Default Economy of Mechanisms Least Psychological Acceptability Least Privilege Complete Mediation	hoch
A18	Verwendung aktueller Best Practices in Security	z.B.: OWASP Application/Mobile security	hoch
A19	Sichere komfortable Einbindung neuer Geräte	Es müssen sichere, aber dennoch einfache Wege gefunden werden, neue Geräte durch bereits bestehende Benutzer zu ermächtigen, an Konversationen teilzunehmen. Ein Beispiel hierzu wäre das Scannen eines zeitlich begrenzt gültigen QR-Codes zusammen mit einem zweiten Faktor, wie z.B. einer PIN-Eingabe.	hoch
A20	Schutz von Metadaten	Nachrichten, die mittels TI-Messenger versandt werden, erzeugen Metadaten, die z.B. verwendet werden können, um Nachrichtenverhalten zu analysieren. Um die Nutzung des TI-Messengers möglichst weit zu anonymisieren, sind gängige Praktiken zum Schutz von Metadaten zu verwenden.	hoch

3.1.3 Betrieb TI-Messenger

Tabelle 5: Anforderungen – Betrieb TI-Messenger

ID	Titel	Beschreibung	Priorität
A21	Betrieb by Design	Es müssen grundlegende betriebliche Aspekte bei der Entwicklung der Apps/Dienste beachtet und adressiert werden. Nicht abschließend: definierte Rollen definierte Prozesse definierte Use Cases verknüpfende Darstellung zwischen Rollen, Use Cases und Technologie flexible Technologie inkl. Schnittstellen und Komponenten Inbetriebnahme muss beschrieben sein Transition muss beschrieben sein Betriebsmodell muss beschrieben sein Realistische Steuerungsmöglichkeiten müssen definiert sein (Kennzahlen, Service Level Agreements (SLA), Durchsetzbarkeit der kontinuierlichen Verbesserung)	hoch
A22	Kennzahlenlieferungen	Es müssen Kennzahlen zum sicheren Betrieb geliefert werden, damit man verlässliche Aussagen zu folgenden Punkten machen kann: Nutzerakzeptanz bzw. -verhalten/Hochlaufkurve Fehler bzw. verdächtiges Verhalten (Angriff, Spam etc.) sicherheitstechnische Kennzahlen im Betrieb, um z.B. OWASP Application/Mobile Security Lücken zu identifizieren und dediziert zu adressieren Integration ins Security Monitoring	hoch
A23	Support	Es muss einen Support für alle Nutzergruppen geben.	hoch

3.2 Ausblick Anforderungen TI-Messenger 2.0

3.2.1 Zielgruppe und Reichweite des Messengers

Tabelle 6: Anforderungen – Zielgruppe TI-Messenger 2.0

ID	Titel	Beschreibung	Priorität
A24	Nutzergruppe Versicherter	Mit der TI-Messenger-Version 2.0 sollen die Versicherten einen Zugang zum TI-Messenger erhalten. Sie besitzen zu diesem Zeitpunkt die Voraussetzung, um den TI-Messenger zu nutzen. Hinweise: Neben der Übermittlung von E-Rezept-Token via TI-Messenger, dürfen Versicherte untereinander nicht direkt in einem Chat kommunizieren! Aus Gründen der Akzeptanz muss vorgesehen werden, dass Versicherte nicht von sich aus einen Kommunikationskanal via TI-Messenger zu beliebigen Leistungserbringern eröffnen können. Die Eröffnung eines Kanals muss durch den Leistungserbringer initiiert werden bzw. erfolgen können. (Leistungserbringer zu Versicherter und Leistungserbringer zu vielen Versicherten) Versicherte müssen die Möglichkeit erhalten die Kommunikation mit einem Leistungserbringer ablehnen zu können. Darüber hinaus muss ein Chatraum inaktiviert werden, sobald der letzte Leistungserbringer diesen verlässt.	hoch

3.3 Ausblick Anforderungen TI-Messenger 3.0

3.3.1 Funktionsumfang

Tabelle 7: Anforderungen – Funktionsumfang TI-Messenger 3.0

ID	**Titel**	**Beschreibung**	**Priorität**
A25	Sprach- und Videoanrufe	Über den TI-Messenger sind Sprach- und Videoanrufe möglich.	hoch
A26	Broadcast-Nachrichten (nur eine Richtung)	Mit dem TI-Messenger soll es möglich sein, eine Nachricht an Kontakte einer definierten Benutzergruppe (z.B. Arzt, Zahnarzt) zu senden, ohne dass die Empfänger darauf antworten können (Antwortunterbindung). Die Beteiligung an einem Broadcast-Raum ist optional erfolgt via Opt-in für die LE oder LEI. Broadcasträume dürfen nur von	mittel

		Institutionen mit entsprechender Berechtigung eröffnet werden. Beispiel: Das RKI kann eine Nachricht an alle Ärzte mit einer Anpassung der aktuellen Empfehlung zur Behandlung von Covid-19 versenden.	
A27	Schnittstellen zu medizinischen Geräten/Software	Mit dem TI-Messenger soll durch die Implementierung von Schnittstellen zu den Primärsystemen ein Versand von Daten aus medizinischen Geräten/Software sichergestellt werden. Die flexible Ausgestaltung der Schnittstellen für LEI soll möglich sein. Für Versicherte sollen die Festlegungen aus § 354 Abs. 2 Nr. 6 SGB V synchronisiert werden.	hoch

4 Lösungsalternativen

Zur Umsetzung des gesetzlichen Auftrags aus dem DVPMG ergeben sich für die gematik verschiedene Lösungsalternativen zur Umsetzung eines sicheren Messaging-Verfahrens. Neben den in Kapitel 3 dargestellten Anforderungen zukünftiger Nutzer erscheint es vor allem wichtig eine Lösung zu finden, die schnell umgesetzt und dem fortschreitenden Bedarf an Innovation gerecht werden kann. Der nachfolgend dargestellten Argumentationslinie zur Entscheidungsfindung ist eine umfangreiche Marktanalyse der gematik sowie Diskussionen mit Herstellern und zukünftigen Nutzern vorausgegangen. Als Kriterien für die Entscheidung zum Vorgehen werden insbesondere das Erreichen von Interoperabilität, die Sicherheit der Lösung (i.S.d. der Ende-zu-Ende-Verschlüsselung), die Nutzerzentriertheit der Lösung und die kurzfristige Umsetzbarkeit der Lösung angesetzt. Im Folgenden werden die möglichen Lösungsalternativen dargestellt und diskutiert.

4.1 Proprietäre Messenger-Lösung der gematik

Die gematik legt die Technologie, den Funktionsumfang und die Sicherheitsmechanismen für TI-Messenger fest und entwickelt einen proprietären Messenger für alle in Kapitel 1.6 beschriebenen Nutzergruppen. Alternativ könnte die gematik eine der am Markt bestehende Lösungen einkaufen. Die gematik betreibt den Messenger selbst und steht somit in Konkurrenz zu den bereits etablierten Messenger-Providern.

Vorteile:

Hohes Sicherheitsniveau und hohes Grundvertrauen in die gematik-eigene Technologie (analog zur E-Rezept-App)

Nachteile:

Voraussichtlich 2,5 Jahre von der Spezifikation bis zur Verfügbarkeit im Feld (Rückstand zu den bereits verfügbaren Gesundheits-Messengern)

Kaum Nutzerzentriert: gematik-Messenger mit einem festen Funktionsumfang für alle Nutzergruppen

Kaum Innovation: Weiterentwicklung des TI-Messengers ist an die Spezifikation der gematik geknüpft

Fehlende Interoperabilität: bereits bestehende Messenger-Lösungen bleiben im Markt weiterhin nicht interoperabel bestehen

Marketing-Aufwand: TI-Messenger muss bekannt gemacht werden (Freiwilligkeit für Leistungserbringer = Hindernis bei der Markteinführung)

Fazit:

Eine proprietäre Messenger-Lösung der gematik erscheint vor dem Hintergrund der aktuellen Marktsituation für Gesundheits-Messenger wie in Kapitel 1.2 beschrieben wenig sinnvoll. Neben der sehr langen und aufwändigen Entwicklungsphase und der hohen Betriebskosten, die für das Gesundheitssystem anfallen würden, stünde der TI-Messenger in direkter Konkurrenz zu bereits bestehenden IM-Anwendungen im Markt, welche dedizierte Usergruppen nutzerzentriert ansprechen können und durch diese Spezialisierung einen klaren Vorteil bezüglich User-Experience gegenüber einem allgemeinen TI-Messenger der gematik bieten würden. Darüber hinaus würde eine proprietäre TI-Messenger-Lösung das Problem fehlender Interoperabilität zwischen

bestehenden Anbietern nicht adressieren. Somit würde bestehende Dilemma der fehlenden Interoperabilität zwischen einzelnen Messenger-Anbietern nicht gelöst, sondern potentiell verstärkt werden. Folglich sieht die gematik von diesem Lösungsansatz ab.

4.2 Bestehende Messenger-Lösungen in die TI integrieren

Wie zuvor beschrieben, gibt es Messenger-Lösungen mit stark unterschiedlichem Funktionsumfang und Kosten im Gesundheitswesen. Einige richten sich an die Prozesse im Krankenhaus mit hoher Integration in die Krankenhausinformationssysteme. Andere haben nur wenige Sonderfunktionen für Leistungserbringer, können aber im Vergleich zu WhatsApp zumindest mit einer besseren Sicherheitsleistung aufwarten. Die Anbindung an die TI könnte diesen Messengern bessere Authentisierungslösungen und ggf. eine deutschlandweite Nutzersuche mittels zentralem VZD-FHIR-Server

bieten. Dennoch würde das bestehende Marktmodell erhalten bleiben.

Vorteile:

Wahlfreiheit: Leistungserbringer können die für sie passende Lösung wählen

Verfügbarkeit: bestehende Messenger sind nach Zulassung sofort verfügbar

Innovation: Messenger werden im freien Markt für die Nutzer weiterentwickelt (Differenzierung und Wettbewerb)

Authentizität: Funktionen der TI können zur Erreichung von Authentizität und Sicherheit nachgenutzt werden

Nachteile:

keine Interoperabilität zwischen den Messengern

kein einheitliches Sicherheitsniveau

Test- und Zulassungsverfahren und somit die Kontrollfunktion durch die gematik nur mit sehr hohem Aufwand möglich

Fazit:

Die bestehende Marktvielfalt von Messenger-Herstellern im deutschen Gesundheitswesen erlaubt es, Nutzergruppen zielgerichtet anzusprechen und deren dedizierte Bedürfnisse zu befriedigen. Darüber hinaus ist das Marktmodell durch stetigen Wettbewerb charakterisiert, wodurch eine fortlaufende Innovation und Weiterentwicklung einzelner Angebote gewährleistet ist. Diese Vorteile überwiegen jedoch nicht die Tatsache, dass einzelne Messenger im Markt aufgrund der Freiheit zur Auswahl unterschiedlicher Messenger-Protokolle nicht interoperabel sind. Eine anbieter- und sektorenübergreifende Ad-hoc-Kommunikation wird somit ausgeschlossen. Dieser Nachteil wird auch durch eine Anbindung der Messenger an die TI nicht überwunden. Vielmehr stellt die Anbindung bestehender Gesundheits-Messenger an die TI ein großes Risiko für die gematik dar, da die Ende-zu-Ende-Sicherheit wie auch Qualität der Datenübertragung nicht durch die gematik überprüft werden kann. Folglich sieht die gematik auch von diesem Lösungsansatz ab.

4.3 Interoperable Messenger-Lösung als Kommunikationsstandard

Das in Kapitel 4.2 beschriebene Dilemma stellt den Ansatzpunkt für die Überlegungen der gematik bei der Entwicklung einer für das deutsche Gesundheitswesen sinnvollen Lösungen im IM-Bereich dar. Die Herausforderung besteht darin, die Vorteile eines Marktmodells mit der Interoperabilität der einzelnen Anbieter zu kombinieren und darüber hinaus eine Anbindung an die TI und somit eine mögliche Nachnutzung von sinnvollen Komponenten wie einem zentralen VZD-FHIR-Server und einheitlichen Authentifizierungsmechanismen zu operationalisieren. Als Lösung sieht die gematik die Festlegung des Protokolls, welches den Gesundheits-Messengern zugrunde liegt, sowie Anforderungen an den Funktionsumfang und die Sicherheit der einzelnen Messenger. Durch diese einheitlichen Festlegungen wird nicht nur die Interoperabilität gewährleistet, sondern auch die Sicherheit und der Datenschutz der Anwendungen Ende-zu-Ende sinnvoll durch die gematik überprüfbar.

Vorteile:

Interoperabilität zwischen teilnehmenden Messenger-Anwendungen im Markt

Überprüfbares, einheitlich hohes Sicherheitsniveau

Wahlfreiheit: Leistungserbringer können die für sie passende Lösung wählen

Verfügbarkeit: Messenger sind sofort verfügbar

Innovation: Messenger werden im freien Markt für die Nutzer weiterentwickelt (Differenzierung und Wettbewerb)

Authentizität: Funktionen der TI können zur Erreichung von Authentizität und Sicherheit nachgenutzt werden

Nachteile:

Voraussichtlich 6 bis 9 Monate von der Spezifikation bis zur Verfügbarkeit erster zertifizierter Anwendungen im Markt

Innovation wird teilweise durch Spezifikation der gematik eingeschränkt

Abhängigkeit vom Interesse der Anbieter und Hersteller an diesem Lösungsansatz

Zusätzliche Entwicklungsaufwände für Anbieter (Anpassung bestehender IM-Anwendungen)

Fazit:

Um den vielseitigen Anforderungen an einen interoperablen Messenger-Dienst im Gesundheitswesen erschöpfend gerecht werden zu können, sieht die gematik ein Marktmodell vor. Dabei sollen unterschiedlichen Messenger-Clients, welche in Summe den verschiedenen Anforderungen der diversen Nutzergruppen im Gesundheitswesen gerecht werden können, miteinander im Wettbewerb stehen. Gleichzeitig ist es die Aufgabe der gematik, ihrem gesetzlichen Auftrag und dem angesetzten Maßstab an Sicherheit und Datenschutz im Rahmen des Zulassungsprozesses umfassend nachzukommen. Die Festlegung der gematik auf ein einheitliches Messenger-Protokoll, welches in einem Marktmodell umgesetzt wird, kann diese Anforderung befriedigen, ohne dabei die notwendigen Zulassungsprozesse der gematik einzuschränken. Darüber hinaus wird eine Differenzierung von bestehenden unsicheren Verfahren (wie z. B. WhatsApp) durch die übergreifenden Komponenten der TI, wie einheitliche Authentifizierungsmechanismen und einen VZD-FHIR-Server erreicht.

4.3.1 Entscheidung für das Matrix-Messenger-Protokoll

Um den Aufwand bei der Umsetzung eines einheitlichen Messenger-Protokolls beim TI-Messenger möglichst gering zu halten, ist es der Anspruch der gematik, auf ein bestehendes Open-Source-Protokoll zu setzen. Bei der Entscheidung für ein bestimmtes Protokoll wurden vor allem die Kriterien Nutzerzentriertheit, Erreichung der in Kapitel 3 definierten Anforderungen, Erreichen des von der gematik angestrebten überprüfbaren Sicherheitsniveaus und Erfahrungen mit Open-Source-Protokollen im Markt angesetzt. Unter Berücksichtigung dieser Kriterien erscheint das Messenger-Protokoll der Matrix Foundation als Best Fit für das Vorhaben der gematik. Diese Entscheidung wird im Folgenden weiter erläutert.

Dezentraler Lösungsansatz

Matrix = REST-basiertes Open-Source-Protokoll = frei verfügbar und einfach umzusetzen

Das Matrix-Protokoll wird durch eine breite Community fortlaufend weiterentwickeln

Die Gesprächsdaten sind durch die Ende-zu-Ende-Verschlüsselung für Anbieter nicht lesbar. Prinzip der Datenminimierung wird für Gesprächsdaten gewahrt (zeitliche Begrenzung der Datenspeicherung auf den Servern, siehe Kapitel 3.1.3, A9)

Vertraulichkeit der Daten ist ein integraler Bestandteil des Matrix-Protokolls

Matrix-Messaging-Server lassen sich hochverfügbar betreiben

Matrix-Open-Source Server-Implementierung (Synapse) sind mit großen Nutzerzahlen erprobt und TI-Messenger-Architektur kann auf bereits bestehende Matrix-Client-Server- und Server-Server-Protokolle aufsetzen.

Sicherheit

Das Matrix-Protokoll nutzt E2E Encryption mittels Double-Ratchet-Verschlüsselung (OLM- und MEGOLM)

Der Verschlüsselungsmechanismus MEGOLM mitigiert die Hürden von OLM bei Gruppenchats

OLM und MEGOLM wurden auditiert und gelten allgemein als sicher

MEGOLM skaliert bei größeren Nutzerzahlen gut

Forward- und Backward-Secrecy ist durch die Änderung der Schlüssel gewährleistet

Innovationspotential

Matrix verfügt mit Synapse über stabile Server-Implementierung mit weltweit über 28 Mio. Nutzern

Das Matrix-Protokoll wird durch eine breite Community stetig weiterentwickelt

Innovation im Anwendungsfall Gesundheitswesen durch die Spezifikation der gematik

Erweiterung der Clients um innovative Funktionen (unter Berücksichtigung der Sicherheit und Interoperabilität) möglich

Nutzerzentrierte Entwicklung durch eine Vielzahl unterschiedlicher Anbieter im Marktmodell

Die gematik hat Hoheit über Spezifikation des TI-Messengers - die Spezifikation ist Grundvoraussetzung für Test- und Zulassungsverfahren.

User Experience (UX)

Das Entwicklungspotential der Clients wird durch die Wahl des Protokolls kaum eingeschränkt

Wettbewerb fördert die stetige Verbesserung der UX der Clients

Mittels Trust-Management können Institutionen wie Kliniken oder Praxen eine eigene Rechteverwaltung für Angestellte implementieren.

Mit dem Matrix-Protokoll wird die Nutzung mehrerer Clients auf einer ID möglich

Die UX wird durch gematik-Spezifikation nicht eingeschränkt

Über die zuvor genannten Punkte hinaus wird die Entscheidung der gematik für das Messenger-Protokoll der Matrix-Foundation als Basis für den Kommunikationsstandard TI-Messenger durch folgende Aspekte begründet:

International und national gibt es gute Erfahrungen mit dem Matrix-Messaging als Basis für kommerzielle und öffentliche Anwendungen

das hohe Abstraktionsmaß erlaubt einen flexiblen und zugleich sicheren Umgang mit fachlichen Anforderungen wie z. B. Institutionsaccounts, ein strukturiertes Verzeichnis, Gruppenchats sowie Rollen und Berechtigungen.

das dezentrale Server-Modell entspricht der bestehenden Kommunikationsstruktur und ist so besonders datensparsam: z. B. krankenhaus-interne Chats können auf Krankenhaus-Server verbleiben.

4.3.2 Marktmodell

Wie im vorherigen Kapitel 4.3 erörtert, sieht die gematik bei der Umsetzung des TI-Messengers ein Marktmodell vor, um den vielseitigen Anforderungen an einen Messenger-Dienst im Gesundheitswesen erschöpfend gerecht werden zu können.

Backendseitig wird durch den Betrieb von Matrix-Homeservern ein föderiertes System aufgebaut, welches eine Kommunikation über Sektorengrenzen hinweg interoperabel ermöglichen kann. Im Rahmen der Spezifikation durch die gematik wird größtenteils das bestehende Server-Server- und Client-Server-Protokoll der Matrix Foundation nachgenutzt. [MA-SPEC] Für den Einsatz im Gesundheitswesen relevante Komponenten der Architektur des TI-Messengers, die aktuell nicht in den bestehenden Spezifikationen der Matrix-Foundation berücksichtigt sind, werden von der gematik spezifiziert. Die Industriepartner können zentrale Server-Instanzen (User-IDs mit Authentifizierung via HBA) und Institutions-Server (für Institutionen mit dedizierten Homeservern und eigenem Rechtemanagement, betrieben on premise oder in der Cloud) bei der gematik zur Zulassung bringen. Anbieter von Matrix-Homeservern sind verpflichtet, mindestens einen TI-Messenger-Client zur Verfügung zu stellen, können ihre Serverleistung darüber hinaus aber auch für Anbieter von Clients ohne eigene Matrix-Homeserver (z. B. für gesetzliche Krankenkassen und Unternehmen der privaten Krankenversicherung) anbieten.

Leistungserbringer können in diesem Markt die für sie passende Anwendung wählen, ohne auf die Interoperabilität mit allen weiteren am TI-Messenger teilnehmenden Clients verzichten zu müssen. Die so erreichte Innovationsfreiheit soll verschieden ausgeprägte professionelle Clients hervorbringen, die die unterschiedlichen Bedürfnisse der unterschiedlichen Leistungserbringergruppen befriedigen können. So wird eine effiziente Nutzung des Messengers im Praxis- oder Klinik-Kontext sowie eine flexible Synchronisation mit der bestehenden Primärsystem-Infrastruktur ermöglicht. Eine

Absicherung hinsichtlich der Authentizität der Nutzerkreise erfolgt durch Authentifizierungsmechanismen an zentralen TI-Komponenten (IDP). Auch die sektorenübergreifende Kommunikation mit dem TI-Messenger wird durch zentrale TI-Komponenten (VZD-FHIR-Server) sichergestellt.

Für die Versicherten soll das ePA-Frontend des Versicherten (ePA-FdV) zum 01.01.2023 die TI-Messenger-Funktion unterstützen und von gesetzlichen Krankenkassen sowie von Unternehmen der privaten Krankenversicherung zur Verfügung gestellt werden.Da diese Kostenträger als aktive Kommunikationspartner für Versicherte vorgesehen sind, ist auch kostenträgerseitig eine Verfügbarkeit von TI-Messenger-Clients notwendig. Für die Kommunikationsbeziehungen Versicherte - Kostenträgern und Versicherte - Leistungserbringer sind dedizierte Matrix-Homeserver von den Kostenträgern vorzuhalten, welche ebenfalls von der gematik zugelassen werden. Zur Authentifizierung der Versicherten sind bestehende Verfahren nachzunutzen. Darüber hinaus wird kein eigener Versicherten-Verzeichnisdienst aufgebaut werden, da Versicherte eineindeutig über ihre gehashte KVNR als der ihrer Matrix-ID in der Matrix-Föderation auffindbar sind.

5 Systemüberblick

Im folgenden Kapitel wird ein Überblick über die angestrebte Architektur des TI-Messengers gegeben. Basis der beschriebenen Architektur ist das Matrix-Messenger-Protokoll. Die Gründe der Entscheidung für das Open-Source verfügbare Matrix-Messenger-Protokoll können in Kapitel 4 nachvollzogen werden.

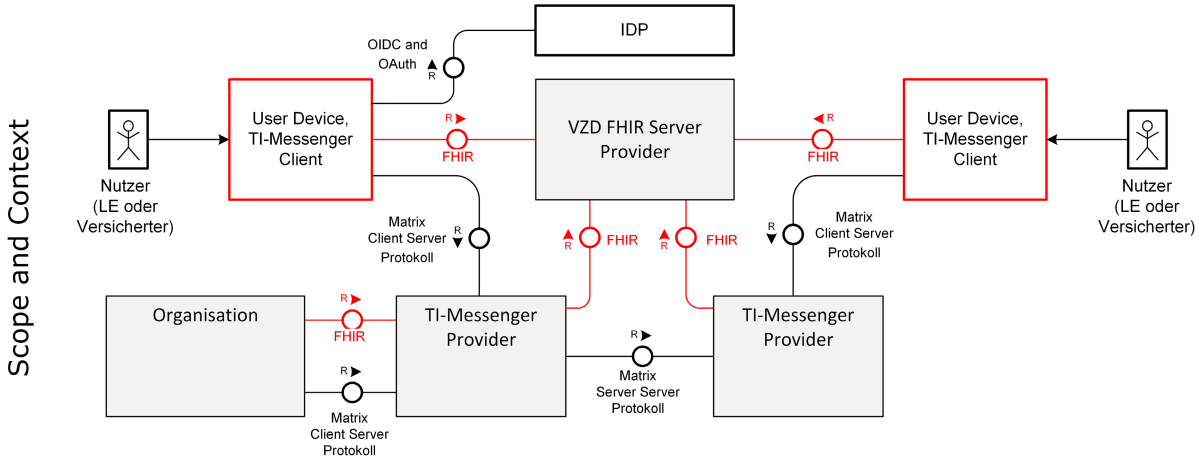

Abbildung 2: TI-Messenger_Architecture_Scope_and_Context

Die Abbildung 2 zeigt eine grobe Übersicht der TI-Messenger-Architektur. Grau dargestellt sind Blackbox-Ansichten von Systemen, die nachfolgend detailliert betrachtet werden. Die schwarz dargestellten Schnittstellen (schwarze Linien) sind bereits durch die Matrix Foundation spezifiziert. Die rot dargestellten Schnittstellen (rote Linien) werden durch die gematik spezifiziert. Es kommen Matrix-Homeserver und Matrix Clients zum Einsatz. Das Client-Server-Protokoll und das Server-Server-Protokoll der Matrix-Spezifikation werden unverändert übernommen. Die Matrix-Clients erhalten zusätzlich eine FHIR-Schnittstelle zur Suche nach Personen und Organisationen auf dem VZD-FHIR-Server und werden so zu TI-Messenger-Clients. Der VZD-FHIR-Server ist eine Weiterentwicklung des bisherigen LDAP basierten VZD der TI und kann auch als VZD 2.0 bezeichnet werden. Durch das FHIR-Protokoll und -Format wird es einfacher, den VZD um die erforderlichen Funktionen wie z. B. die Speicherung von mehreren Adressen pro Eintrag zu erweitern. Die bisher von den Kartenherausgebern gepflegten Einträge im LDAP-VZD werden in den VZD-FHIR-Server synchronisiert.

Die Authentisierung der Nutzer erfolgt für Leistungserbringer und Versicherte mit OpenID Connect und OAuth2. Organisationen benötigen spezielle TI-Messenger-Homeserver, die ihnen exklusiv zur Verfügung stehen. Dort können die Mitarbeiter die zu ihrer Organisation passende Authentisierung nutzen. Für die Suche nach Personen und Organisationen erhalten die Organisationen Zugang zu einem FHIR-Proxy des TI-Messenger-Anbieters, der die Anfragen an den VZD-FHIR-Server weiterleitet. Über den FHIR-Proxy kann der Admin der Organisation auch den Eintrag der Organisation im VZD-FHIR-Server verändern.

Die Kommunikation mittels TI-Messenger zwischen den Nutzern ist Ende zu Ende verschlüsselt mit der Matrix eigenen Verschlüsselung Olm (für Chats mit zwei Personen) und Megolm (für Gruppenchats). Für eine geräteunabhängige Verschlüsselung kann ein Key Backup genutzt werden. Neue Geräte des Nutzers erhalten die Schlüssel aus dem Key Backup.

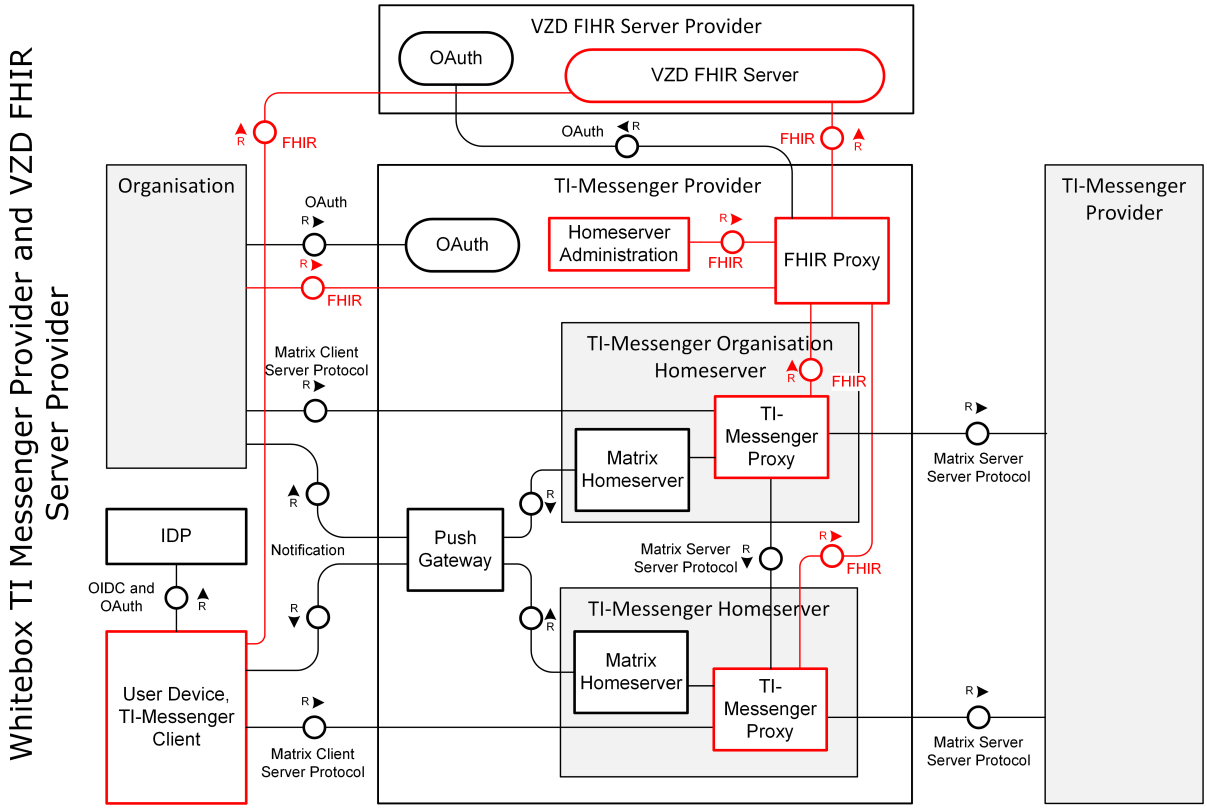

Abbildung 3: TI-Messenger_Architecture_Whitebox_TI-Messenger_Provider

Die Abbildung 3 zeigt die Whitebox-Ansicht des TI-Messenger-Providers.

Um den föderierten Betrieb der Homeserver verschiedener TI-Messenger-Provider zu ermöglichen und um nicht zum TI-Messenger gehörende Matrix-Homeserver auszuschließen, werden die Matrix-Homeserver um TI-Messenger-Proxies ergänzt, die sicherstellen, dass nur Homeserver von zugelassenen TI-Messenger-Providern an der Föderation teilnehmen (grundsätzlich kann der TI-Messenger-Proxy auch im Homeserver integriert sein). Mit dem TI-Messenger Proxy kann ein Load Balancing mit mehreren Matrix-Homeservern für eine Matrix-Domain implementiert werden. Zusätzlich kann so den Clients die TLS-Verbindung zum Matrix-Homeserver auf dem well known TLS TCP-Port 443 angeboten werden. Der TI-Messenger-Proxy ermöglicht auch ein rollenbasiertes Messaging. Die Kombination aus Matrix-Homeserver und TI-Messenger-Proxy wird im Folgenden als TI-Messenger-Homeserver bezeichnet. TI-Messenger Anbieter können auch exklusiv für Organisationen (wie z. B. Krankenhäuser) TI-Messenger-Homeserver bereitstellen, die gleichberechtigt an der TI-Messenger-Föderation teilnehmen. Die TI-Messenger-Organisations-Homeserver können ihre eigene DNS Domain in den Matrix-Adressen (MXID) verwenden und zusätzliche Authentifizierungsverfahren unterstützen, damit z. B. Krankenhäuser ihre eigene Benutzerverwaltung wie z. B. Active Directory nutzen können. Für kleinere Organisationen können die Benutzer auch mit Username und Passwort registriert und authentisiert werden. Die TI-Messenger Organisations-Homeserver verbleiben in der betrieblichen Hoheit der Organisation selbst, welche einen TI-Messenger-Anbieter beauftragen kann (z. B. Betrieb im Rechenzentrum des TI-Messenger-Anbieters). Die TI-Messenger-Proxies fragen bei eingehenden Events über den FHIR-Proxy den VZD-FHIR-Server ab, um zu prüfen, ob die Domain des Senders und des Empfängers Teil der TI-Messenger-Föderation sind. Der FHIR-Proxy authentisiert sich

beim VZD-FHIR-Server mit OAuth2 Client Credentials Flow. Die TI-Messenger-Proxies prüfen auch, ob ein Nutzer berechtigt ist eine Kommunikation mit anderen Nutzern aufzubauen. Dazu lassen sich LE und Mitarbeiter von Organisationen vom VZD-FHIR-Server PASSporT-Token ausstellen, die die Berechtigung zum Kommunikationsaufbau ausweisen und die Rolle des Nutzers beinhalten (LE oder Mitarbeiter einer Organisation). Zusätzlich können Organisationen und LE im VZD-FHIR-Server Policies eintragen, die ihre Erreichbarkeit durch andere Nutzer verändern. So kann z. B. ein Krankenhaus den Empfang (als Sub-Struktur der Organisation) für Versicherte erreichbar machen. Die PASSporT-Token und die Policies der Empfänger werden von den TI-Messenger-Proxies beim Aufbau einer Verbindung geprüft.

Die Komponente Homeserver-Administration soll die automatisierte Erzeugung und Inbetriebnahme von TI-Messenger-Organisations-Homeservern ermöglichen. Dazu muss die Matrix-Domain der Organisation im VZD-FHIR-Server eingetragen werden. Zusätzlich wird eine Kennung des TI-Messenger-Providers zur Matrix-Domain eingetragen. Diese Domain ist dadurch für andere gesperrt und kann von keinem anderen TI-Messenger-Provider im VZD-FHIR-Server verwaltet werden. Die TI-Messenger-Clients der Nutzer sowie der Admin Client müssen Credentials für die Authentisierung nach dem OAuth Client Credential Flow erhalten, um den Zugriff auf den FHIR-Proxy zu ermöglichen. Alternativ kann die Organisation auch einen TLS-Proxy einsetzen, der die Authentisierung zum Zugriff auf den FHIR-Proxy für alle TI-Messenger-Clients stellvertretend übernimmt. Der FHIR Proxy des TI-Messenger-Providers prüft bei schreibenden Zugriffen anhand des AccessTokens und dem Inhalt des Requests, ob es sich um den zur Organisation gehörenden Eintrag im VZD-FHIR-Server handelt und lehnt unberechtigte Schreibzugriffe ab. Der VZD-FHIR-Server prüft zusätzlich, ob der TI-Messenger-Provider berechtigt ist, den Eintrag der Organisation zu ändern.

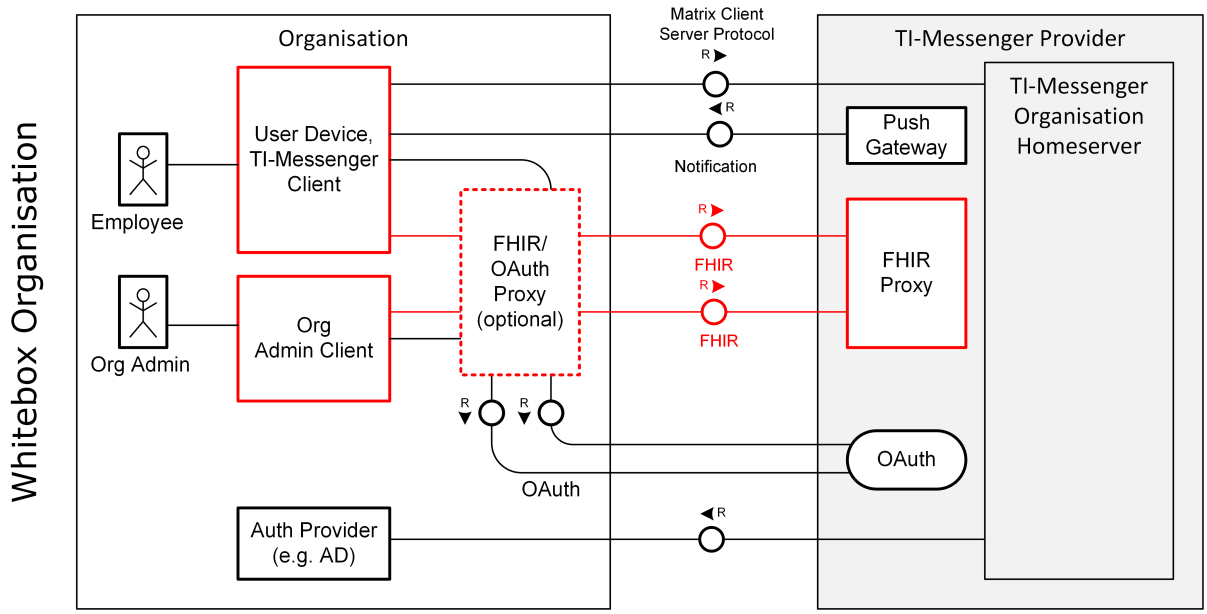

Abbildung 4: TI-Messenger_Architecture_Whitebox_Organisation

Die Matrix-Adressen der LE und Organisationen werden im neu eingeführten VZD-FHIR-Server der TI eingetragen und sind aus dem TI-Messenger-Client suchbar. Die Einträge für Personen (nur LE) und Organisationen werden durch die sektoralen Landesvereinigungen der Personen und Organisationen gepflegt. Die Organisationen können mit dem Org-Admin-Client selbst verwaltete Sub-Strukturen im VZD-FHIR-Server

anlegen und die Matrix-Adressen ihrer Nutzer dort zuweisen sowie erweiterte Kommunikations-Policies konfigurieren.

Im VZD-FHIR-Server werden durch die Komponente Home Administration die Matrix-Domains der TI-Messenger-Homeserver eingetragen. Die Matrix-Domains sind Organisationen zugeordnet. Daher haben auch TI-Messenger Anbieter einen Organisations-Eintrag im VZD-FHIR-Server, wenn sie einen TI-Messenger-Homeserver für Personen betreiben. Pro Organisation können mehrere Matrix-Domains genutzt werden, wenn für die Domains auch TI-Messenger-Homeserver oder Organisations-Homeserver betrieben werden.

Für Versicherte ist vorgesehen, dass die Matrix-Adressen (MXID) aus der Krankenversicherungsnummer (KVNR) abgeleitet werden. Dadurch ist es möglich, dass Ärzte Versicherte adressieren können ohne in einem Verzeichnis für Versicherte die Adresse abfragen zu müssen. Der TI-Messenger-Client des Versicherten muss dafür die aus der KVNR abgeleitete MXID bei der Registrierung am Homeserver der Krankenkasse verwenden. Die Krankenkassen stellen für ihre Versicherten TI-Messenger Organisation Homeserver bereit, die die Authentifizierung mit OIDC und OAuth2 unterstützen.

Die Versicherten können im TI-Messenger-Client in einem Opt-in-Verfahren feingranular festlegen, mit welchen LE sie kommunizieren möchten und mit welchen LE nicht.

6 Use Cases

Alle Messenger Use Cases, die gemäß Matrix Client Server Protokoll umgesetzt werden können, werden in diesem Konzept nicht aufgeführt. Statt dessen wird auf die Matrix Client Server API verwiesen (https://matrix.org/docs/guides/client-server-api). Die nachfolgend beschriebenen Use Cases sind spezifisch für den TI-Messenger und weichen daher teilweise von der Matrix Client Server API ab. Die genaue Zuordnung der Use Cases wird nachfolgend mit den Gesellschaftern der gematik abgestimmt.

Für alle Use Cases gelten die folgenden Randbedingungen:

Der TI-Messenger Anbieter hat die Zulassung für den TI-Messenger-Homeserver erlangt.

Der TI-Messenger Anbieter hat die Teilnahmebedingungen für den föderierten Betrieb von TI-Messengern akzeptiert.

6.1 Nutzerverwaltung

Für die Nutzung des TI-Messengers sind folgende Rollen vorgesehen:

Leistungserbringer (z. B. LE)

Org-Admin

Mitarbeiter einer Organisation (z. B. Pflege oder Mitarbeiter einer Krankenkasse)

Versicherte

Abhängig von der Rolle des Nutzers gibt es verschiedene Abläufe für die Registrierung an einem TI-Messenger-Homeserver.

AF_10003 - LE registrieren (persönlicher Account)

Mit diesem Anwendungsfall registriert sich der LE als Person an einem TI-Messenger-Homeserver seines TI-Messenger-Anbieters.

Anwendungsfall 1: Nutzer registrieren

Attribute	Bemerkung
Beschreibung	Die Registrierung von LE an einem TI-Messenger-Homeserver erfolgt gemäß Matrix-Client-Server-Protokoll durch den Nutzer mit seinem TI-Messenger-Client. Nach erfolgreicher Registrierung erhält der Client ein AccessToken, dass für folgende Autorisierungen genutzt wird. Das AccessToken ist mit dem TI-Messenger-Client des Nutzers über die device_id verknüpft. Akteure: LE Komponenten: TI-Messenger-Client, Identity Provider, TI-Messenger-Homeserver, VZD-FHIR-Server

Vorbedingung	Der Nutzer verfügt über ein Gerät, das einen Browser oder einen TI-Messenger-Client seines TI-Messenger-Anbieters installiert hat sowie über eine Möglichkeit zur Authentisierung an seinem Identity Provider (in der Regel Authenticator App seines IDP). Der Nutzer kennt die URL des Homeservers oder die URL ist bereits in seinem TI-Messenger-Client konfiguriert. Der Nutzer ist bereits an einem Identity Provider der TI registriert.
Ablauf	Der Nutzer startet seinen TI-Messenger-Client. Optional kann der gewünschte TI-Messenger-Homeserver ausgewählt werden. Nach der Wahl des Homeservers werden dem Nutzer die möglichen OIDC-Registrierungsverfahren dieses Homeservers angeboten. Der Nutzer wählt eines der angebotenen Registrierungsverfahren. Der Nutzer wird vom Identity Provider (IDP) des gewählten Registrierungsverfahrens aufgefordert einen bestehenden Account (Benutzerkonto) zu wählen oder einen neuen Account anzulegen. Nach der Wahl des IDP-Accounts folgt die Authentisierung des Nutzers. Dem Nutzer werden dabei vom IDP zu diesem Account bereitgestellte Daten angezeigt und es wird vorgeschlagen, diese für die TI-Messenger-Anwendung zu verwenden. Vom Client wird ein Benutzername generiert, der keine Rückschlüsse auf die Person ermöglicht. Der Nutzer wird aufgefordert den Nutzungsbedingungen des TI-Messenger-Clients zuzustimmen. Nach erneuter Zustimmung wird ein TI-Messenger-Account erzeugt und der TI-Messenger-Client hat das Zugriffsrecht auf diesen Account. Der Nutzer hat einen Eintrag im VZD-FHIR-Server. Der TI-Messenger-Client trägt auf Wunsch des Nutzers die MXID in seinem Eintrag ein (Beispiel für eine MXID einer Praxis: @skdakdhwiudncoeiru4lskjd8:praxis-mueller.de). Die Authentisierung am VZD-FHIR-Server erfolgt per OIDC. Single Sign On (SSO) wird unterstützt. Die MXID kann auch nachträglich im VZD-FHIR-Server eingetragen oder entfernt werden. Die Registrierung ist damit abgeschlossen.
Nachbedingung	Der Nutzer ist im Homeserver registriert und hat eine eindeutige TI-Messenger-Adresse (die MXID) zugewiesen bekommen. Als Ergebnis der Registrierung hat der Nutzer einen für sein Gerät spezifisches Access-Token erhalten, mit dem er sich für zukünftige Verbindungen gegenüber dem TI-Messenger Homeserver authentisieren kann. Optional ist die MXID im zugehörigen VZD-FHIR-Server Eintrag gespeichert.
Alternativen	keine
Test-Prüfpunkte	Authentisierung Eintrag im VZD-FHIR-Server
Betriebsaspekte	keine
Sicherheitsaspekte	keine

AF_10010 - Nutzer einer Organisation registrieren

Mit diesem Anwendungsfall wird ein Mitarbeiter einer Organisation an einem exklusiven TI-Messenger-Organisations-Homeserver registriert.

Anwendungsfall 2: Nutzer einer Organisation registrieren

Attribute	Bemerkung
Beschreibung	Die zu einer Organisation gehörenden Nutzer werden an einem exklusiv dieser Organisation zugeordneten TI-Messenger Organisation Homeserver registriert. Der TI-Messenger Anbieter kann dafür mit den IT-Administratoren der Organisation eine Integration in die bestehende Nutzerverwaltung der Organisation abstimmen und den Homeserver entsprechend konfigurieren. Die Authentisierung des Nutzers kann anschließend mit der vereinbarten Authentifizierungsmethode (z. B. Active Directory oder Basic Authentication) erfolgen. *Dieser Authentisierungsmechanismus wird im Rahmen der Spezifikation noch mit dem BSI und dem BfDI geklärt.* Die Pflege der MXIDs im Eintrag der Organisation im VZD-FHIR-Server erfolgt durch den von der Organisation beauftragten Administrator. Der Eintrag im VZD-FHIR-Server ist in diesem Fall optional. Die Nutzer einer Organisation können zusätzlich auch die Rolle LE und/oder Versicherter einnehmen. In diesen Rollen können sie zusätzlich an anderen TI-Messenger-Homeservern registriert sein. Anstatt eines personenbezogenen Accounts, kann auch ein Funktions-Account verwendet werden, der von mehreren Mitarbeitern der Organisation genutzt wird.
Vorbedingung	Es wird ein TI-Messenger Organisation Homeserver verwendet. Der Homeserver steht ausschließlich einer Organisation zur Verfügung. Der TI-Messenger-Client und der TI-Messenger Organisation Homeserver unterstützen die gewählte Authentifizierungsmethode.
Ablauf	Wird nicht durch die gematik festgelegt.
Nachbedingung	Der Nutzer ist im Homeserver registriert und hat eine eindeutige TI-Messenger-Adresse (die MXID) zugewiesen bekommen.
Alternativen	keine
Test-Prüfpunkte	keine
Betriebsaspekte	keine
Sicherheitsaspekte	keine

AF_10011 - Registrierung eines Versicherten

Attribute	Bemerkung
Beschreibung	Versicherte können einen beliebigen zugelassenen TI-Messenger-Client verwenden, der die Authentisierung mit OIDC und OAuth unterstützt. Die

	Registrierung erfolgt am TI-Messenger Organisation Homeserver der Krankenkasse.
Vorbedingung	Der Nutzer verfügt über ein Gerät, das einen Browser oder einen TI-Messenger-Client installiert hat sowie über eine Möglichkeit zur Authentisierung am Identity Provider (in der Regel Authenticator App seines IDP). Der Nutzer kennt die URL des Homeservers oder die URL ist bereits in seinem TI-Messenger-Client konfiguriert. Der Nutzer ist bereits an einem Identity Provider der TI registriert.
Ablauf	Der Nutzer startet seinen TI-Messenger-Client. Optional kann der gewünschte TI-Messenger-Homeserver ausgewählt werden. Der Versicherte muss der TI-Messenger Organisation Homeserver seiner Krankenkasse auswählen. Nach der Wahl des Homeservers werden dem Nutzer die möglichen OIDC-Registrierungsverfahren dieses Homeservers angeboten. Der Nutzer wählt eines der angebotenen Registrierungsverfahren. Der Nutzer wird vom Identity Provider (IDP) des gewählten Registrierungsverfahrens aufgefordert einen bestehenden Account (Benutzerkonto) zu wählen oder einen neuen Account anzulegen. Nach der Wahl des IDP-Accounts folgt die Authentisierung des Nutzers. Dem Nutzer werden dabei vom IDP zu diesem Account bereitgestellte Daten angezeigt und es wird vorgeschlagen, diese für die TI-Messenger-Anwendungg zu verwenden. Versicherte erhalten eine vordefinierte Matrix-Adresse (MXID). Die MXID wird aus der KVNR und der Matrix-Domain der Krankenkasse nach folgender Bildungsregel abgeleitet: [@<Hash der KVNR>:<Matrix-Domain der Krankenkasse>] Der Nutzer wird aufgefordert den Nutzungsbedingungen des TI-Messenger-Clients zuzustimmen. Nach erneuter Zustimmung wird ein TI-Messenger-Account erzeugt und der TI-Messenger-Client hat das Zugriffsrecht auf diesen Account. Die Registrierung ist damit abgeschlossen.
Nachbedingung	keine
Alternativen	keine
Test-Prüfpunkte	keine
Betriebsaspekte	keine
Sicherheitsaspekte	Eine Profilbildung muss ausgeschlossen werden (inhaltlich als auch durch eine Auswertung des Nutzungsverhaltens der Versicherten).

6.2 Kommunikation mit Nutzern

Leistungserbringer und Mitarbeiter von Organisationen können im VZD-FHIR-Server gesucht werden.

AF_10012 - Nutzer im VZD-FHIR-Server suchen

Anwendungsfall 3 Nutzer im VZD-FHIR-Server suchen

Attribute	Bemerkung
Beschreibung	Der VZD-FHIR-Server ist ein Verzeichnis von Organisationen und Leistungserbringern. Das Verzeichnis kann von allen TI-Messenger Nutzern abgefragt werden, um die MXIDs von anderen Nutzern zu finden. Versicherte haben keine Einträge im VZD-FHIR-Server.
Vorbedingung	Der Nutzer hat einen TI-Messenger-Client und ist an einem Homeserver registriert. Der Nutzer hat einen Zugang zum VZD-FHIR-Server (Authentisierung mittels OIDC).
Ablauf	In seinem TI-Messenger-Client kann der Nutzer auswählen, ob er nach einer Organisation (FHIR Ressource Organization) oder nach einem Leistungserbringer (FHIR Ressource Practitioner) suchen möchte. Die Suchergebnisse können eingeschränkt werden, indem zur FHIR Ressource gehörende Attribute als Suchbedingung angegeben werden. Als Ergebnis der Suche werden vom TI-Messenger-Client die gefundenen Einträge angezeigt, wenn mindestens eine MXID im Eintrag vorhanden ist. Durch Auswahl eines gefundenen Eintrags kann die Kommunikation mit dem Nutzer begonnen werden.
Nachbedingung	keine
Alternativen	TI-Messenger-Clients, die für die Nutzung mit Primärsystemen entwickelt wurden, können zusätzlich die Suche nach den im Primärsystem gespeicherten Patienten bzw. Versicherten implementieren.
Test-Prüfpunkte	keine
Betriebsaspekte	keine
Sicherheitsaspekt	keine

Das Matrix Protokoll sieht vor, dass unbekannte Geräte und Nutzer verifiziert werden müssen, bevor ihnen vertraut werden kann. Zukünftig soll die Verifikation automatisch (ohne Nutzer-Aktion) durch ein hierarchisches Trust-Modell erfolgen können (den Nutzern wird vertraut, die wiederum ihren Geräten vertrauen wodurch eine Vertrauenskette zu Stande kommt), um zu erreichen, dass die Nutzer nicht mit unnötig aufwändigen Vertrauenszuordnungen und Authentizitätsnachweisen konfrontiert werden. Vorerst ist jedoch eine manuelle Verifikation erforderlich.

AF_10013 - Gerät oder Person manuell verifizieren

Anwendungsfall 4: Gerät oder Person manuell verifizieren

Attribute	Bemerkung
Beschreibung	Eine manuelle Verifikation muss erfolgen, wenn der User den Client auf einem neuen/zusätzlichen Gerät nutzen möchte oder sich vom Client abmeldet. Die

	manuelle Verifikation von unbekannten Geräten oder Nutzern ist im Matrix Protokoll spezifiziert und erfolgt indem sich beide Geräte Verifikations-Nachrichten senden und eine gemeinsam unterstützte Verifikations-Methode durchführen.
Vorbedingung	Der Nutzer ist bereits mit einem anderen Gerät an einem TI-Messenger Homeserver registriert. Der Nutzer verfügt über ein Gerät, das einen Browser oder einen TI-Messenger-Client installiert hat sowie über eine Möglichkeit zur Authentisierung am Identity Provider (in der Regel Authenticator App seines IDP). Der Nutzer kennt die URL des Homeservers oder die URL ist bereits in seinem TI-Messenger-Client konfiguriert. Der Nutzer ist bereits an einem Identity Provider der TI registriert.
Ablauf	Nutzer A sendet Nutzer B einen Verifikations-Request, der auch die unterstützten Methoden enthält. Nutzer B empfängt den Request und sein TI-Messenger-Client fragt nach, ob B der Verifikation mit A zustimmt. B akzeptiert und sendet A eine Nachricht, dass B bereit zur Verifikation ist. Auch in dieser Nachricht sind die unterstützten Methoden enthalten. A empfängt Bs Methoden, wählt eine gemeinsam unterstützte Methode und sendet eine Nachricht an B zum Start der Verifikation. Nach Abschluss der Verifikation senden sich A und B Nachrichten, die die erfolgte Verifikation bestätigen.
Nachbedingung	keine
Alternativen	keine
Test-Prüfpunkte	keine
Betriebsaspekte	keine
Sicherheitsaspekt	keine

6.3 TI-Messenger-Föderation

Die TI-Messenger-Anwendung unterstützt die Föderationsmechanismen des Matrix-Protokolls um Homeserver und Domains verschiedener TI-Messenger Anbieter nutzen zu können. Die Föderation ist jedoch auf Homeserver der TI-Messenger Anbieter beschränkt. Homeserver anderer Matrix Messenger Anbieter sind ausgeschlossen.

AF_10014 - TI-Messenger Organisation Homeserver bereitstellen

Anwendungsfall 5: TI-Messenger Organisation Homeserver bereitstellen

Attribute	Bemerkung
Beschreibung	Für Organisationen können TI-Messenger Anbieter exklusive TI-Messenger-Homeserver bereitstellen und in die Föderation aufnehmen. Die exklusiv einer Organisation zugeordneten TI-Messenger-Homeserver können z. B. eine zentrale Administration der TI-Messenger-Accounts und spezifische Authentisierungsverfahren für Organisationen anbieten. Die exklusiven TI-Messenger Organisation Homeserver (OrgHS) werden optional von den TI-Messenger Anbietern angeboten.
Vorbedingung	Die Organisation für die der TI-Messenger Homeserver bereitgestellt wird, ist eine Organisation des Gesundheitswesens.
Ablauf	Eine Organisation des Gesundheitswesens möchte an der TI-Messenger-Kommunikation teilnehmen und schließt einen Vertrag mit einem TI-Messenger-Provider. Die Organisation weist gegenüber dem TI-Messenger-Provider nach, dass sie zur Nutzung der TI-Messenger-Anwendung berechtigt ist (z. B. durch Nachweis, dass der Eintrag im FHIR-VZD-Server der Organisation gehört). Der Organisations-Administrator und der TI-Messenger-Provider vereinbaren eine Konfiguration für den OrgHS. Die Konfiguration beinhaltet die Matrix-Domain sowie Details zum Authentifizierungsverfahren des OrgHS. Der TI-Messenger-Provider installiert und konfiguriert den OrgHS. Über die Komponente Homeserver-Administration registriert der TI-Messenger-Provider die Matrix-Domain der Organisation im VZD-FHIR-Server um den OrgHS in die TI-Messenger-Föderation zu integrieren. Der TI-Messenger-Provider stellt der Organisation einen Administrations-Client und zugehörige Credentials für den FHIR-Proxy zur Verfügung. Wenn nicht vorhanden, stellt der TI-Messenger-Provider TI-Messenger-Clients für die Organisation bereit. Auch für die TI-Messenger-Clients der Mitarbeiter stellt der TI-Messenger-Provider-Credentials für den FHIR-Proxy zur Verfügung. Der OrgHS kann nun genutzt werden.
Nachbedingung	keine
Alternativen	Die TI-Messenger-Clients der Mitarbeiter können für den Zugriff auf den FHIR-Proxy des TI-Messenger-Providers alternativ auch einen eigenen FHIR-Proxy nutzen, sodass die Organisation nur an einer Stelle Credentials benötigt.
Test-Prüfpunkte	keine
Betriebsaspekte	keine
Sicherheitsaspekt	keine

AF_10007 - TI-Messenger-Homeserver in die Föderation aufnehmen

Mit diesem Anwendungsfall wird ein TI-Messenger-Homeserver in die TI-Messenger Matrix Föderation aufgenommen.

Anwendungsfall 6: TI-Messenger-Homeserver in die Föderation aufnehmen

Attribute	Bemerkung
Beschreibung	Ein TI-Messenger-Homeserver kann erst dann mit anderen TI-Messenger-Homeservern und den dort registrierten Nutzern kommunizieren, wenn er in die TI-Messenger-Föderation aufgenommen wurde. Dazu wird ein Eintrag in den VZD-FHIR-Server erzeugt. Andere TI-Messenger-Homeserver, mit denen dieser Homeserver kommunizieren möchte, erlauben die Kommunikation nur wenn der Homeserver einen Eintrag im VZD-FHIR-Server hat.
Vorbedingung	keine
Ablauf	Der TI-Messenger Anbieter erzeugt einen neuen Homeserver für eine bestehende oder neue Matrix-Domain. Über die Komponente "Homeserver-Administration" erzeugt der TI-Messenger Anbieter im VZD-FHIR-Server ein Eintrag für den neuen Homeserver als Teil der FHIR Organization Ressource. Dazu authentisiert sich die Komponente "Homeserver-Administration" beim VZD-FHIR-Server mittels OAuth2 Client Credentials Flow. Der Eintrag der Organisation (oder der Organisations-Unterstruktur) im VZD-FHIR-Server wird um folgende Daten ergänzt. Dazu muss der Organization.identifier bekannt sein. TI-Messenger-Domain, # Die Matrix-Domain des TI-Messenger-Homeservers FQDN, # Der FQDN des Homeservers TI_Messenger_provider # Der TI-Messenger-Provider, der den Homeserver verwaltet. Der Homeserver wird im DNS registriert.
Nachbedingung	Der Eintrag im VZD-FHIR-Server wurde für den Homeserver erzeugt.
Alternativen	Falls im Organisations-Eintrag die TI-Messenger-Domain und der TI_Messenger_provider schon existieren, wird nur der FQDN des Homeservers zu diesem Eintrag hinzugefügt. Falls im Organisations-Eintrag der TI_Messenger_provider aber nicht die TI-Messenger-Domain existiert, werden die TI-Messenger-Domain und der FQDN des Homeservers zu diesem Eintrag hinzugefügt. Falls die Domain einem Kunden gehört, erfolgt der DNS-Eintrag durch den Kunden.
Test-Prüfpunkte	Authentisierung mit OAuth2 Client credentials flow. Prüfung, ob die Domain oder der FQDN nicht schon in anderen Organisations-Einträgen vergeben sind. Die Domain darf nicht im Internet für Matrix verwendet werden. Ein TI-Messenger-Provider darf nicht Einträge für einen anderen TI-Messenger-Provider vornehmen können.
Betriebsaspekte	Reporting der TI-Messenger Anbieter, Organisationen, deren Matrix-Domains und Homeserver FQDNs
Sicherheitsaspekt	keine

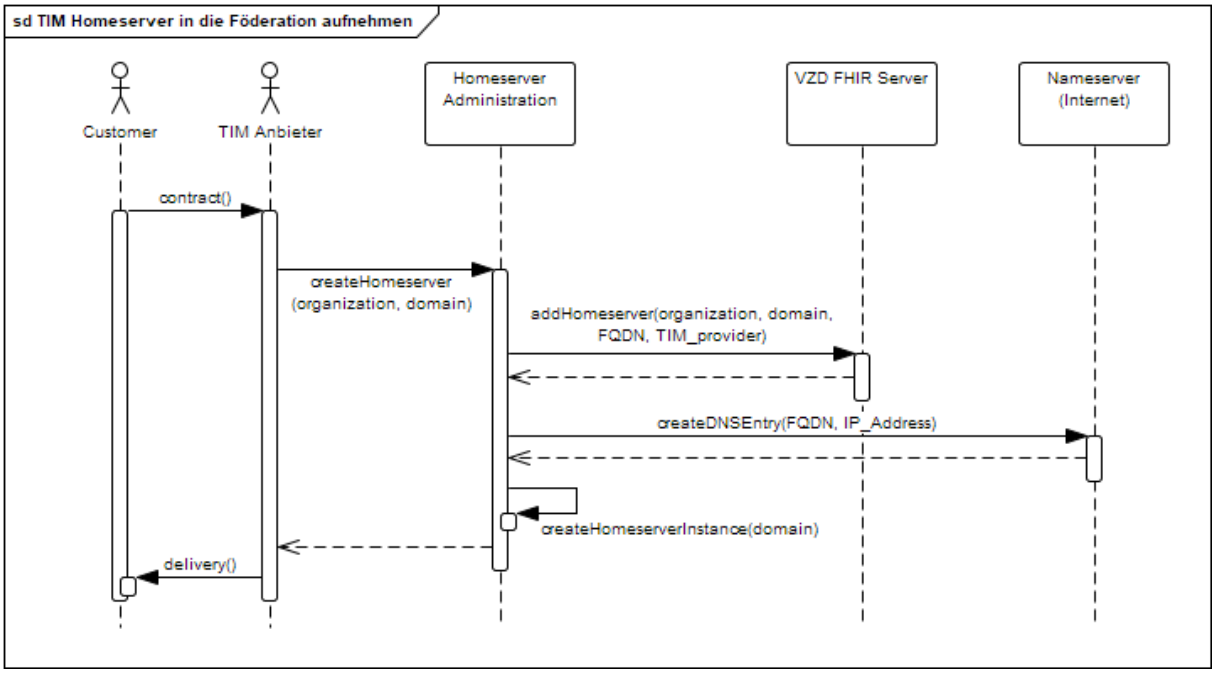

Abbildung 5: TI-Messenger-Homeserver in die Föderation aufnehmen

AF_10008 - Invite Event senden

Ein TI-Messenger Nutzer möchte einen anderen TI-Messenger Nutzer in einen Raum einladen.

Anwendungsfall 7: Invite Event senden

Attribute	Bemerkung
Beschreibung	Am TI-Messenger dürfen nur berechtigte Nutzer teilnehmen. Daher werden durch die TI-Messenger-Homeserver die Invite Events geprüft, ob: - die Homeserver des Senders und des Empfängers zur TI-Messenger-Föderation gehören, - der Sender berechtigt ist eine Invite Event zum TI-Messenger-Homeservers des Empfängers zu senden - der Empfänger diese Kommunikation wünscht
Vorbedingung	Der Nutzer ist bereits auf einem TI-Messenger-Homeserver registriert.
Ablauf	Der Nutzer sucht den Teilnehmer mit dem er kommunizieren möchte. Der Client bietet dem Nutzer dafür verschiedene Möglichkeiten, die sich je nach Einsatzzweck des Clients oder Rolle des Nutzers unterscheiden können (z. B. Suche auf dem eigenen Homeserver, Suche im TI Verzeichnisdienst nach Personen und Organisationen, für LE: Suche nach Versicherten im Primärsystem). Als Ergebnis der Suche ist die MXID des Empfängers bekannt. Der Client erzeugt ein Invite Event. Wenn der Sender ein LE (als Person) oder ein Mitarbeiter einer Organisation ist, dann lässt sich der Client vom VZD-FHIR-Server ein PASSporT-Token ausstellen, das bestätigt, dass es sich um einen Nutzer der Rolle LE oder einen Nutzer aus einer bestimmten Organisation handelt und fügt es in das Invite Event ein (invite_room_state). Der Client sendet das Event an seinen Homeserver. Der Homeserver verarbeitet das Event gemäß Matrix Protokoll und leitet es

	weiter an den TI-Messenger-Proxy. Der TI-Messenger-Proxy prüft, ob die TI-Messenger-Domain des Empfängers in der TI-Messenger-Föderation registriert ist und leitet es an den TI-Messenger-Homeserver des Empfängers weiter. Der TI-Messenger-Proxy des Empfängers prüft das Invite Event, ob der sendende Nutzer berechtigt ist den Empfänger einzuladen. Dazu werden folgende Prüfungen durchgeführt: - Die Domain des Senders ist in der TI-Messenger-Föderation registriert. - Das PASSportT-Token ist vorhanden, gültig und wurde für einen LE oder eine Organisation ausgestellt. - Es wurden vom Empfänger keine Einschränkungen im VZD-FHIR-Server eingetragen, die die Einladung verhindern. Wenn alle Prüfungen ergeben, dass das Invite Event zulässig ist, dann leitet der TI-Messenger-Proxy das Event an den Matrix-Homeserver weiter. Der Matrix-Homeserver verarbeitet das Event und leitet es weiter an die Clients des Empfängers.
Nachbedingung	keine
Alternativen	keine
Test-Prüfpunkte	keine
Betriebsaspekte	keine
Sicherheitsaspekte	keine

7 Sicherheit

Wie in Kapitel 4.3.1 beschrieben, wird der TI-Messenger auf dem Matrix-Protokoll fußen, welches auditiert und mehrfach erfolgreich in sicheren Instant-Messaging-Anwendungen verwendet wurde. Um die Schutzziele sicherer Kommunikation zu erreichen, insbesondere natürlich der Vertraulichkeit von Nachrichteninhalten, kommt hier die Bibliothek libolm mit den Protokollen OLM und MEGOLM zum Einsatz. Diese stellt eine Variante des Double-Ratchet-Protokolls dar, welche auch für Gruppenchats mit vielen Beteiligten geeignet ist. Mittels OLM und MEGOLM wird die Ende-zu-Ende-Verschlüsselung anbieterübergreifend gewährleistet.

Hierbei werden Nachrichten mit AES-256-CBC symmetrisch Ende-zu-Ende verschlüsselt und die verwendeten Schlüssel für jede Nachricht frisch erzeugt. Die verwendeten Schlüsselerzeugungsparameter werden ebenfalls abhängig von gewählten Parametern i.d.R. zwischen 1 und 100 Nachrichten neu ausgehandelt. Dadurch ergibt sich neben forward-secrecy auch eine "selbstheilende" Eigenschaft, für die Double Ratchet bekannt wurde. Somit ist es Angreifern, wie auch beteiligten Servern nicht möglich, Nachrichten zu entschlüsseln, sofern keine Decryption Keys erbeutet werden. Selbst in einem solchen Angriffsszenario ist die Nützlichkeit des erbeuteten Keys stark begrenzt, da mit ihm nur wenige Nachrichten entschlüsselt werden können.

Die Integrität von Nachrichten ist durch die Verwendung von HMAC-SHA-256 sichergestellt.

Libolm weist sowohl Abstreitbarkeit, als auch begrenzte Nichtverkettbarkeit von Nachrichten als Merkmal auf. Die Authentizität von Nachrichten ist jedoch gewährleistet und fußt auf einem Cross-Signing-Verfahren, bei welchem ein User seinen Gesprächspartnern vertraut, die wiederum ihren Geräten vertrauen, was eine Chain-of-Trust zwischen Geräten erzeugt. Wie bei vielen modernen Instant-Messengern auch unterstützt Matrix die Absicherung der Authentizität von Gesprächsteilnehmern und den Man-in-the-Middle-Schutz über den Vergleich eines Authentication Strings. Hierzu bringt Matrix das nutzerfreundliche Emoji-Vergleichsverfahren mit sich.

MEGOLM bietet nativ keine Replay-Schutz, jedoch ist eine Implementationsempfehlung gegeben, die dieses Problem mitigiert.

MEGOLM bietet keine perfekte Forward- und Post-Compromise-Security, da Nachrichtenschlüssel für begrenzte Zeit aufbewahrt werden müssen, z.B. falls Nachrichten in falscher Reihenfolge ankommen. Unter dieser Einschränkung sind Forward- und Post-Compromise-Security jedoch gegeben.

Matrix bietet keine Gewähr für die Konsistenz eines Gesprächs zwischen allen Teilnehmern, da u.a. nicht für alle Nachrichten eine für alle Teilnehmer gültige absolute Reihenfolge der gesendeten Nachrichten besteht.

Die Sicherheitseigenschaften von Matrix sind auf den TI-Messenger übertragbar und anwendbar. Der TI-Messenger gewährt darüber hinaus noch zusätzliche Sicherheitsmerkmale, wie eine Einschränkung der Kommunikation auf berechtigte Teilnehmer, welche mittels der in Kapitel 5 beschriebenen, proxygeschützten Föderation erreicht wird. Sämtliche Nachrichtenkommunikation erfolgt zudem innerhalb TLS-verschlüsselter Verbindungen und ist somit zusätzlich nach außen geschützt.

8 Betrieb

Der Betrieb für den TI-Messenger wird grundsätzlich analog der definierten Rollen der Hersteller und Anbieter und der gematik als Gesamtverantwortliche für die TI (GTI) realisiert.

Die neuen Produkte des VZD-FHIR, des TI-Messenger-Fachdienstes (FD) und des TI-Messenger-Clients können von Herstellern zur Zulassung gebracht werden.

Diese Produkte können dann von entsprechenden, zugelassenen Anbietern in Betrieb genommen werden. Somit sind die jeweiligen Anbieter für den Betrieb ihrer Produkte entsprechend der Vorgaben der GTI verantwortlich.

Damit entstehen folgende neuen betrieblichen Rollen:

1) Anbieter VZD-FHIR
2) Anbieter TI-Messenger (Fachdienst und Client(s))

Der Anbieter TI-Messenger-Fachdienst muss auch mindestens einen TI-Messenger-Client anbieten. Damit können die Rollen zum Anbieter TI-Messenger zusammengefasst werden.

Es werden in der konkreten Ausgestaltung ähnliche Marktkonstellationen mit Unterauftragnehmern erwartet wie sie in [gemKPT_Betr#3.2.3.1] abgebildet sind. Beim Anbieter TI-Messenger ist es möglich, dass der Anbieter z.B. für verschiedene Nutzergruppen mehrere Clients anbietet.

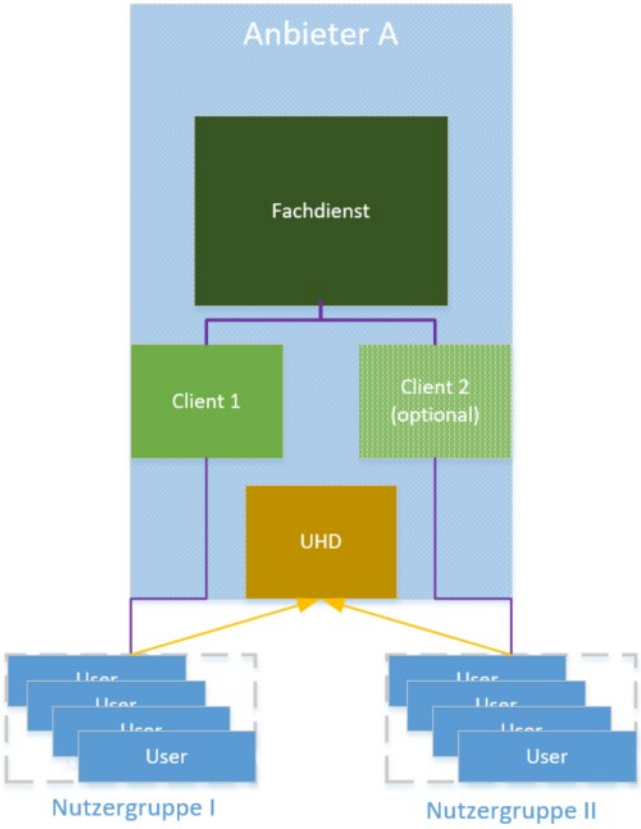

Abbildung 6: TI-Messenger-Anbieter-Modell

8.1 Betriebs- und Support-Modell

Im Folgenden wird das Betriebs- und Support-Modell für den TI-Messenger im Zusammenspiel mit den bisherigen Produkten und Rollen in der TI beschrieben.

Weil der Zugriff vom TI-Messenger-Client nicht über die TI zum TI-Messenger-Fachdienst erfolgt, sondern abgesichert über das Internet, entfällt damit die Nachnutzung des VPN-Zugangsdienst-Anbieters als Eingangskanal für den Support aus Leistungserbringersicht. Das gute Nutzererlebnis mit einem Single Point of Contact (SPOC) steht dabei jedoch weiter im Vordergrund und soll soweit möglich auch beim TI-Messenger realisiert werden. Diese Sicht wird nach dem Support zwischen den Anbietern beleuchtet.

Der gegenseitige Support richtet sich damit an den beteiligten und jeweils von den Anbietern verantworteten Komponenten aus und wird die folgt aufgegliedert:

Tabelle 8: Komponenten und deren Support

benötigte Komponente für TI-Messenger	Supportverantwortung aus Nutzersicht	Anmerkung
LE(I) Identität (HBA, SMC-B)	entsprechender Identitätsherausgeber (z.B. TSP) bei welchem der LE den HBA bzw. SMC-B bestellt hat	Für die Befüllung des VZD im zentralen Netz der TI (nicht der VZD-FHIR) sind unabhängig davon weiterhin die Organisationen nach § 313 SGB V Abs. 5 Satz 1 verantwortlich.
IDP	Muss entsprechend aussagekräftige Fehlerlogs an Clients ausgeben.	Die Fehlerlogs müssen direkt an den Nutzer über den TI-Messenger-Client ausgegeben werden.
Versichertenidentitäten (eGK)	UHD des Anbieters TI-Messenger	Der Versicherte wendet sich an den von seiner Krankenkasse/-versicherung bereitgestellten Supportkanal.
TI-Messenger-Client	UHD des Anbieters TI-Messenger	Wenn der Client vom TI-Messenger-Fachdienst bereitstellt wird, fällt damit auch die nachgelagerte Verantwortung zusammen. Sollte der Client von einem anderen Anbieter als den Fachdienst-Anbieter bereitgestellt werden und der UHD nicht an den Fachdienst-Anbieter ausgelagert sein, übernimmt der Client-Anbieter die Koordination mit seinem UHD.

TI-Messenger-Fachdienst	UHD des Anbieters TI-Messenger	Nimmt Anfragen nach Konstellation entweder direkt vom Nutzer über den UHD entgegen oder erhält sie über andere UHD eines anderen Client-Anbieters.
VZD-FHIR-Server	UHD des Anbieters TI-Messenger	Die Kommunikation zum Anbieter VZD-FHIR läuft über den UHD des Anbieters TI-Messenger.

Die Aufgliederung richtet sich dabei an den verschiedenen Anbieterkonstellationen aus wie sie schon bereits bei anderen Produkten im Betrieb sind (gemKPT_Betr#Anbieterkonstellationen) und der Support aus Nutzersicht nutzt soweit möglich bestehende Kanäle nach.

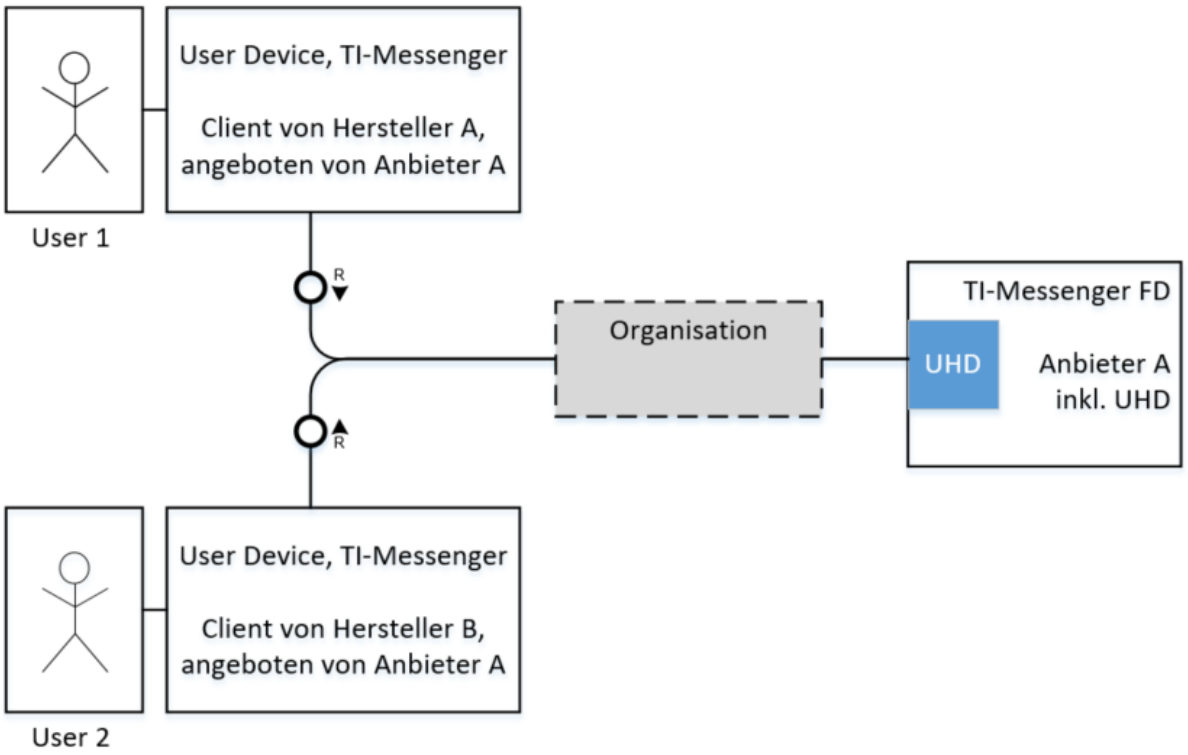

Abbildung 7: TI-Messenger-Support-Modell

Aus Nutzersicht gibt es genau einen User Help Desk (UHD) für die Anwendung TI-Messenger. Dieser koordiniert den TI-Messenger-Client-, den TI-Messenger-Fachdienst- als auch den VZD-FHIR-Server-Support. Nutzer können hierbei sowohl Versicherte als auch Leistungserbringer und Leistungserbringerorganisationen sein, je nachdem in welchem Szenario und welcher Rolle der TI-Messenger angeboten wird.

Für unterstützende Komponenten wie eGK, HBA und SMC-B sind weiterhin die jeweiligen Kartenherausgeber die primären Ansprechpartner.

Sollte es den Bedarf im Markt geben, dass ein Client-Anbieter B den UHD für seine Kunden bereitstellt und damit die Rechte und Pflichten zur Fehlerkoordination im nachgelagerten Support mit anderen Anbietern im IT-Service-Management der TI (TI-ITSM) übernimmt, so wird es dafür eine entsprechende Anbieterzulassungsmöglichkeit geben. Dafür ist die Kooperationsbeziehung zwischen Client-Anbieter B und Fachdienst-Anbieter A aus der oberen Abbildung der gematik im Rahmen der Zulassung von Client-Anbieter B nachzuweisen.

Somit übernimmt der UHD die folgenden Koordinationsaufgaben:

a) zum TI-Messenger Anbieter (Fachdienst, Client und ggf. Clients von "Unter-Anbietern"),

b) zum VZD-FHIR-Server-Anbieter,

c) zum IDP.

Zusätzlich zum Support aus Nutzersicht stehen alle Anbieter gegenseitig in der Verpflichtung, entsprechende Meldungen anderer, mit ihrem Dienst beteiligter Anbieter, entgegenzunehmen und qualifiziert zu beantworten.

8.2 Anbieterverantwortung

In diesem Abschnitt werden übergreifend die Anforderungen an die jeweiligen Anbieter aufgeführt. Die konkreten Ausprägungen der Anforderungen werden im Rahmen der Spezifikation erhoben und in den jeweiligen Steckbriefen gestellt.

Alle Anbieter nehmen am TI-ITSM teil und erhalten entsprechend ihrer Rolle zugehörige Rechte und Pflichten. Die konkrete Ausgestaltung erfolgt im Rahmen der Spezifikation in den jeweiligen Konzepten und Spezifikationen.

Alle Anbieter sind für die durch sie angebotenen Produkte im Betrieb verantwortlich. Dazu zählt unter anderem der sichere und unterbrechungsfreie Betrieb gemäß den Vorgaben des GTI in den nachfolgenden Spezifikationen. Besonders die Funktionalität, die Sicherheit und die Interoperabilität der Produkte nach ihrer Zulassung ist durch den Anbieter im Betrieb stets aufrecht zu erhalten.

Bezogen auf die Basis-Funktionalitäten müssen die TI-Messenger-Clients mit allen Fachdiensten interoperabel sein. D.h. dass bei Ausfall eines TI-Messenger-Fachdienstes der Nutzer theoretisch den gleichen Fachdienst mit einem anderen Client verwenden kann. Eine vollständige Migration (z.B. Account, Verlauf) ist für TI-Messenger 1.0 nicht vorgesehen.

Verfügbarkeit/Erreichbarkeit

Alle Anbieter müssen für ihre jeweiligen Dienste und Komponenten eine sehr hohe Verfügbarkeit sicherstellen.

Last

Zentrale Dienste wie der VZD-FHIR-Server als auch der IDP müssen mit wachsenden Nutzerzahlen eine entsprechend hohe Last an Anfragen bedienen.

Die Last an verteilten Systemen wie dem TI-Messenger-Client und -Fachdienst ist von den Kundenzahlen der jeweiligen Anbieter abhängig und damit ihm entsprechend sicherzustellen.

Durchsatz

Die Mindestvorgaben zum Durchsatz entsprechender Datenmengen der jeweiligen Use Cases aus den nachfolgenden Spezifikationen müssen auch bei hoher Last eingehalten werden. Leistungen darüber hinaus sind durch Angebot und Nachfrage vom Markt zu finden.

Bearbeitungszeiten

Die Mindestvorgaben zu Bearbeitungszeiten der jeweiligen Use Cases aus den nachfolgenden Spezifikationen müssen auch bei hoher Last eingehalten werden. Leistungen darüber hinaus sind durch Angebot und Nachfrage vom Markt zu finden.

8.3 Technischer Betrieb

Monitoring und Reporting (technisch)

Zur Gewährleistung eines sicheren Betriebs ist ein Monitoring und Reporting der jeweiligen Komponente, Dienste und Anbieter erforderlich. Dieses gliedert sich in folgende Aspekte auf:

a) Lieferung von Betriebs- und Rohdaten an GTI von den Produkten VZD-FHIR-Server und TI-Messenger Fachdienst

b) Datenübermittlung zur Fehleranalyse von TI-Messenger-Client an TI-Messenger-Fachdienst inkl. Rückkanal zum Nutzer (z.B. für Kartenherausgeber)

c) automatisches Monitoring am TI-Messenger Fachdienst zur Sperre nicht zugelassener Clients

Synchronisation der Dienste

Der VZD-FHIR-Server muss sich regelmäßig mit dem VZD der TI synchronisieren, sowohl SMC-B Einträge für Organisationen als auch HBA-Einträge für persönliche Accounts. Der VZD dient dabei als führendes Verzeichnis.

Die Schnittstelle und Synchronisation wird analog zum Apothekenverzeichnis (APOVZD) erfolgen. Das bedeutet, dass die SMC-B Einträge im VZD für Organisationen die Basis einer Organisation abbilden, auf welcher sich Unterstrukturen im VZD-FHIR-Server aufbauen lassen.

---

[1] gemäß den Änderungen des DVPMG (2021)
[2] gemäß den Änderungen des DVPMG (2021)
[3] gemäß den Änderungen des DVPMG (2021)

9 Anhang – Verzeichnisse

9.1 Abkürzungen

Kürzel	Erläuterung
APOVZD	Apothekenverzeichnis
AVS	Apothekenverwaltungssystem
BYOD	bring your own device
BfARM	Bundesinstitut für Arzneimittel und Medizinprodukte
DVPMG	Digitale Versorgung und Pflege – Modernisierungs-Gesetz
ePA	elektronische Patientenakte
E-Rezept	elektronisches Rezept
FHIR	Fast Healthcare Interoperable Resources
GTI	Gesamtverantwortlicher TI
IDP	Identity Provider
KIM	Kommunikation im Medizinwesen
KVNR	Krankenversicherungsnummer
PVS	Praxisverwaltungssystem
OIDC	OpenID Connect
OWASP	Open Web Application Security Project
QR-Code	Quick Response (zweidimensionaler Code)
RKI	Robert-Koch-Institut
SGB V	Sozialgesetzbuch Fünftes Buch
SMS	Short Message Service (Kurznachrichtendienst)
SMC-B	Institutionenkarte (Security Module Card Typ B)
TI	Telematikinfrastruktur

TI-ITSM	IT-Service-Management der TI
TKG	Telekommunikationsgesetz
TMG	Telemediengesetz
TSP	Trust Service Provider
TTDSG	Telekommunikation-Telemedien-Datenschutz-Gesetz
UHD	User Help Desk
VZD	Verzeichnisdienst

9.2 Glossar

Das Projektglossar wird als eigenständiges Dokument zur Verfügung gestellt.

9.3 Abbildungsverzeichnis

9.4 Tabellenverzeichnis

9.5 Referenzierte Dokumente

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

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[gemEP_TIM]	gematik: Eckpunkte TI-Messenger
[gemKPT_Betr]	gematik: Betriebskonzept Online-Produktivbetrieb

Weitere Referenzierungen:

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[OLM]	Matrix OLM GitLab: https://gitlab.matrix.org/matrix-org/olm
[MA-SPEC]	Matrix Spezifikation: https://matrix.org/docs/spec/
[SGB V]	Das Fünfte Buch Sozialgesetzbuch – Gesetzliche Krankenversicherung – (Artikel 1 des Gesetzes vom 20. Dezember 1988, BGBl. I S. 2477, 2482), das zuletzt durch Artikel 3 des Gesetzes vom 3. Juni 2021 (BGBl. I S. 1444) geändert worden ist: https://www.gesetze-im-internet.de/sgb_5/