Elektronische Gesundheitskarte und Telematikinfrastruktur

Spezifikation
TI-Messenger-Client

Version:	1.1.0 CC
Revision:	469872
Stand:	13.06.2022
Status:	zur Abstimmung freigegeben
Klassifizierung:	öffentlich_Entwurf
Referenzierung:	gemSpec_TI-Messenger-Client

Dokumentinformationen

Änderungen zur Vorversion

Anpassungen des vorliegenden Dokumentes im Vergleich zur Vorversion können Sie der nachfolgenden Tabelle entnehmen.

Dokumentenhistorie

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
1.0.0	01.10.2021		Erstversion des Dokumentes	gematik
1.1.0 CC	13.06.2022		zur Abstimmung freigegeben	gematik

Inhaltsverzeichnis

1 Einordnung des Dokumentes 5
1.1 Zielsetzung 5
1.2 Zielgruppe 5
1.3 Geltungsbereich 5
1.4 Abgrenzungen 6
1.5 Methodik 6
2 Systemüberblick 8
3 Systemkontext 10
3.1 Nachbarsysteme 10
3.2 Ausprägungen der TI-Messenger-Clients 11
3.2.1 Nutzergruppen 11
3.2.2 Plattformen 12
3.2.3 Weitere Festlegungen 13
4 Übergreifende Festlegungen 14
4.1 Datenschutz und Sicherheit 14
4.2 Authentifizierung am VZD-FHIR-Directory 23
4.3 Benutzerführung 23
4.4 Konfiguration 24
4.5 Test 25
4.6 Betriebliche Aspekte 29
5 Funktionsmerkmale 30
5.1 Authentifizierungsverfahren 30
5.2 Matrix Client-Server API 30
5.2.1 Sofortnachrichten 31
5.2.2 Direktnachrichten 32
5.2.3 Gruppenunterhaltungen 33
5.2.4 Push-Benachrichtigungen 35
5.3 Administrationsfunktionen 36
5.4 Weitere Funktionen 37
6 Anhang A – Verzeichnisse 41
6.1 Abkürzungen 41
6.2 Glossar 41
6.3 Abbildungsverzeichnis 42
6.4 Tabellenverzeichnis 42

6.5 Referenzierte Dokumente 42
6.5.1 Dokumente der gematik 42
6.5.2 Weitere Dokumente 43

1 Einordnung des Dokumentes

1.1 Zielsetzung

Beim vorliegenden Dokument handelt es sich um die Festlegungen zur ersten Ausbaustufe des TI-Messengers. Diese Ausbaustufe ist definiert durch die Ad-hoc-Kommunikation zwischen Organisationen des Gesundheitswesens. Dabei wird insbesondere die Ad-hoc-Kommunikation zwischen Leistungserbringern bzw. zwischen Leistungserbringerinstitutionen betrachtet. Festlegungen zur Nutzergruppe der Versicherten und Anforderungen an Kassenorganisationen werden in der zweiten Ausbaustufe des TI-Messengers Berücksichtigung finden und daher im vorliegenden Dokument nicht weiter betrachtet.

Die vorliegende Spezifikation definiert die Anforderungen zu Herstellung, Test und Betrieb des Produkttyps TI-Messenger-Client. Der TI-Messenger-Client stellt dem Nutzer die benötigte Funktionalität zur sicheren Ad-hoc-Kommunikation mit anderen Teilnehmern bereit. Aus den Kommunikationsbeziehungen mit dem TI-Messenger-Fachdienst und dem VZD-FHIR-Directory resultieren vom TI-Messenger-Client zu nutzende Schnittstellen. In vorliegendem Dokument wird die Nutzung dieser Schnittstellen zur zur sicheren Ad-hoc-Kommunikation und die dafür benötigten Funktionalitäten beschrieben. Vom TI-Messenger-Client genutzte Schnittstellen werden in den entsprechenden Produkttypspezifikationen definiert.

1.2 Zielgruppe

Das Dokument richtet sich zwecks der Realisierung an Hersteller des Produkttypen TI-Messenger-Client sowie an Anbieter, welche diesen Produkttypen betreiben [gemKPT_Betr]. Alle Hersteller und Anbieter von TI-Anwendungen, die Schnittstellen der Komponente nutzen, oder Daten mit dem Produkttypen TI-Messenger-Client austauschen oder solche Daten verarbeiten, müssen dieses Dokument ebenso berücksichtigen.

1.3 Geltungsbereich

Dieses Dokument enthält normative Festlegungen zur Telematikinfrastruktur des deutschen Gesundheitswesens. Der Gültigkeitszeitraum der vorliegenden Version und deren Anwendung in Zulassungs- oder Abnahmeverfahren wird durch die gematik GmbH in gesonderten Dokumenten (z. B. gemPTV_ATV_Festlegungen, Produkttypsteckbrief, Anbietertypsteckbrief, u.a.) oder Webplattformen (z. B. gitHub, u.a.) festgelegt und bekanntgegeben.

Schutzrechts-/Patentrechtshinweis

Die nachfolgende Spezifikation ist von der gematik allein unter technischen Gesichtspunkten erstellt worden. Im Einzelfall kann nicht ausgeschlossen werden, dass die Implementierung der Spezifikation in technische Schutzrechte Dritter eingreift. Es ist allein Sache des Anbieters oder Herstellers, durch geeignete Maßnahmen dafür Sorge zu

tragen, dass von ihm aufgrund der Spezifikation angebotene Produkte und/oder Leistungen nicht gegen Schutzrechte Dritter verstoßen und sich ggf. die erforderlichen Erlaubnisse/Lizenzen von den betroffenen Schutzrechtsinhabern einzuholen. Die gematik GmbH übernimmt insofern keinerlei Gewährleistungen.

1.4 Abgrenzungen

Spezifiziert werden in dem Dokument die von dem Produkttyp bereitgestellten (angebotenen) Schnittstellen. Benutzte Schnittstellen werden hingegen in der Spezifikation desjenigen Produkttypen beschrieben, der diese Schnittstelle bereitstellt. Auf die entsprechenden Dokumente wird referenziert (siehe auch Anhang, Kap. 6.5-Referenzierte Dokumente).

Die vollständige Anforderungslage für den Produkttyp ergibt sich aus weiteren Konzept- und Spezifikationsdokumenten, diese sind in dem Produkttypsteckbrief des Produkttyps TI-Messenger verzeichnet.

1.5 Methodik

Die Spezifikation ist im Stil einer RFC-Spezifikation verfasst. Dies bedeutet:

- **Der gesamte Text in der Spezifikation ist sowohl für den Hersteller des Produktes TI-Messenger-Client als auch für den betreibenden Anbieter entsprechend [gemKPT_Betr] verbindlich zu betrachten und gilt sowohl als Zulassungskriterium beim Produkt und Anbieter.**
- Die Verbindlichkeit SOLL durch die dem RFC 2119 [RFC2119] entsprechenden, in Großbuchstaben geschriebenen deutschen Schlüsselworte MUSS, DARF NICHT, SOLL, SOLL NICHT, KANN gekennzeichnet werden.
- Da in dem Beispielsatz „Eine leere Liste DARF NICHT ein Element besitzen." die Phrase „DARF NICHT" semantisch irreführend wäre (wenn nicht ein, dann vielleicht zwei?), wird in diesem Dokument stattdessen „Eine leere Liste DARF KEIN Element besitzen." verwendet.
- Die Schlüsselworte KÖNNEN außerdem um Pronomen in Großbuchstaben ergänzt werden, wenn dies den Sprachfluss verbessert oder die Semantik verdeutlicht.

Anwendungsfälle und Akzeptanzkriterien als Ausdruck normativer Festlegungen werden als Grundlage für Erlangung der Zulassung durch Tests geprüft und nachgewiesen. Sie besitzen eine eindeutige, permanente ID, welche als Referenz verwendet werden SOLL. Die Tests werden gegen eine von der gematik gestellte Referenz-Implementierung durchgeführt.

Anwendungsfälle und Akzeptanzkriterien werden im Dokument wie folgt dargestellt:
<ID> - <Titel des Anwendungsfalles / Akzeptanzkriteriums>
Text / Beschreibung
[<=]

Die einzelnen Elemente beschreiben:

- **ID**: einen eindeutigen Identifier.
  - Bei einem Anwendungsfall besteht der Identifier aus der Zeichenfolge 'AF_' gefolgt von einer Zahl,

- Der Identifier eines Akzeptanzkriteriums wird von System vergeben, z.B. die Zeichenfolge 'ML_' gefolgt von einer Zahl

- **Titel des Anwendungsfalles / Akzeptanzkriteriums**: Ein Titel, welcher zusammenfassend den Inhalt beschreibt
- **Text / Beschreibung**: Ausführliche Beschreibung des Inhalts. Kann neben Text Tabellen, Abbildungen und Modelle enthalten

Dabei umfasst der Anwendungsfall bzw. das Akzeptanzkriterium sämtliche zwischen ID und Textmarke [<=] angeführten Inhalte.

Der für die Erlangung einer Zulassung notwendige Nachweis der Erfüllung des Anwendungsfalls wird in den jeweiligen Steckbriefen festgelegt, in denen jeweils der Anwendungsfall gelistet ist. Akzeptanzkriterien werden in der Regel nicht im Steckbrief gelistet.

Hinweis auf offene Punkte

Offener Punkt: Das Kapitel wird in einer späteren Version des Dokumentes ergänzt.

2 Systemüberblick

Der TI-Messenger-Client wird als eine Anwendung (oder eingebettet in bestehende Anwendungen) auf dem Endgerät eines Akteurs installiert und ermöglicht eine sichere, nachrichtenbasierte Kommunikation mit anderen Akteuren des TI-Messenger-Dienstes. Der TI-Messenger-Client folgt den offenen Standards des Kommunikationsprotokolls Matrix und synchronisiert, durch die Matrix Foundation festgelegte, JSON-Objekte mit Matrix-Homeservern, welche als Teil des Messenger-Services eines TI-Messenger-Fachdienstes bereitgestellt werden.

Die Kommunikation zwischen den Akteuren des TI-Messenger-Dienstes erfolgt Ende-zu-Ende verschlüsselt in Räumen. Die Nachrichten werden auf dem jeweiligen TI-Messenger-Client erstellt und Ende-zu-Ende verschlüsselt versendet. Die gesendeten Nachrichten werden verschlüsselt auf dem jeweiligen Matrix-Homeserver gespeichert. Der für die Entschlüsselung benötigte Schlüssel wird nur mit verifizierten Endgeräten innerhalb des jeweiligen Raumes geteilt. Die beteiligten Matrix-Homeserver können die Nachrichten nicht entschlüsseln.

Die Kommunikation zwischen einem TI-Messenger-Client und einem TI-Messenger-Fachdienst erfolgt über die Messenger-Proxies. Auf den Messenger-Proxies findet die TLS-Terminierung der Verbindungen von den TI-Messenger-Clients statt. Die TI-Messenger-Proxies erlauben nur das Anmelden eines Akteurs mit zugelassenen TI-Messenger-Clients. Dies wird ermöglicht, indem während des Logins die auf dem Client hinterlegte client_id durch den Messenger-Proxy überprüft wird. Zusätzlich wird während des Anmeldevorgangs durch den TI-Messenger-Client am Auth-Service des VZD-FHIR-Directory geprüft, ob es sich um einen zugelassenen Matrix-Homeserver handelt.

In der folgenden Abbildung sind alle beteiligten Komponenten der TI-Messenger-Architektur in vereinfachter Form dargestellt. Der in der Abbildung grün dargestellte TI-Messenger-Client zeigt die Komponente die in dieser Spezifikation beschrieben wird.

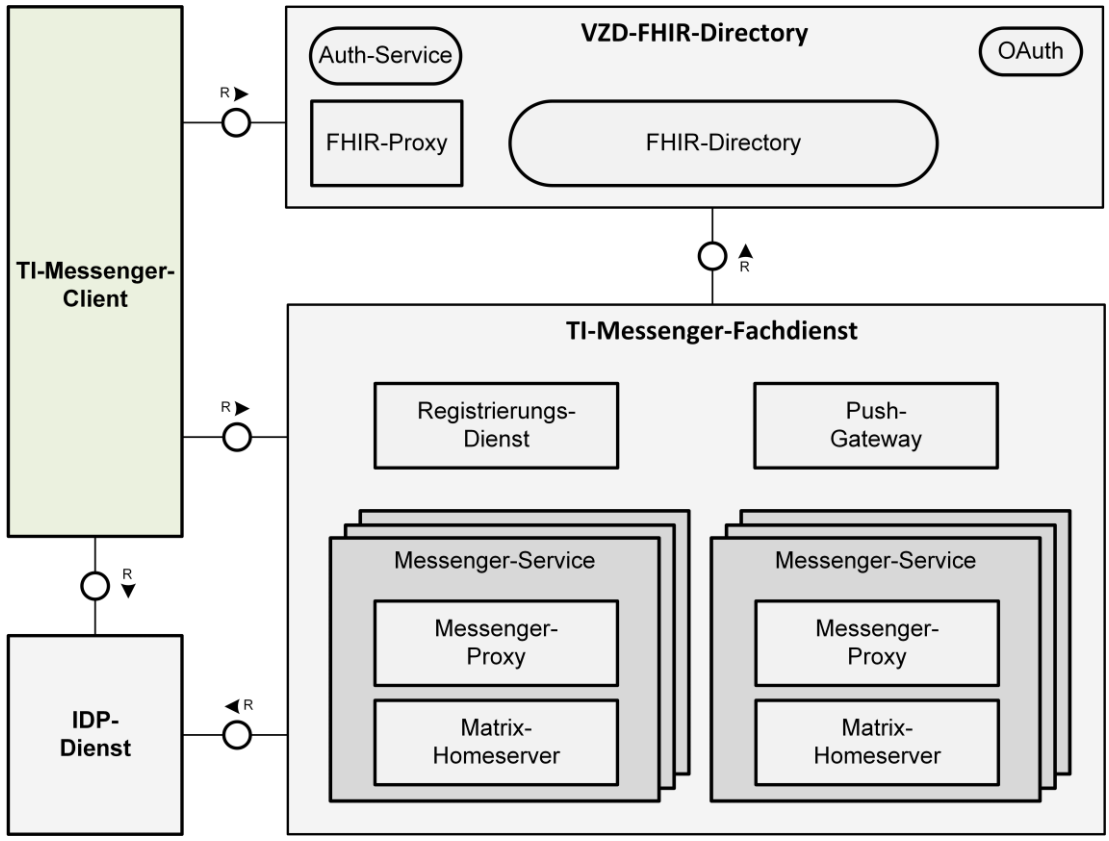

Abbildung 1: Systemüberblick (Vereinfachte Darstellung)

3 Systemkontext

Der folgende Abschnitt setzt den TI-Messenger-Client in den Systemkontext des TI-Messenger-Dienstes.

3.1 Nachbarsysteme

Der TI-Messenger-Client ermöglicht es den Akteuren mit dem TI-Messenger-Dienst zu interagieren. Für die Interaktion mit dem TI-Messenger-Dienst werden vom TI-Messenger-Client weitere Systeme benötigt. Die folgende Abbildung zeigt die benachbarten Komponenten des TI-Messenger-Clients:

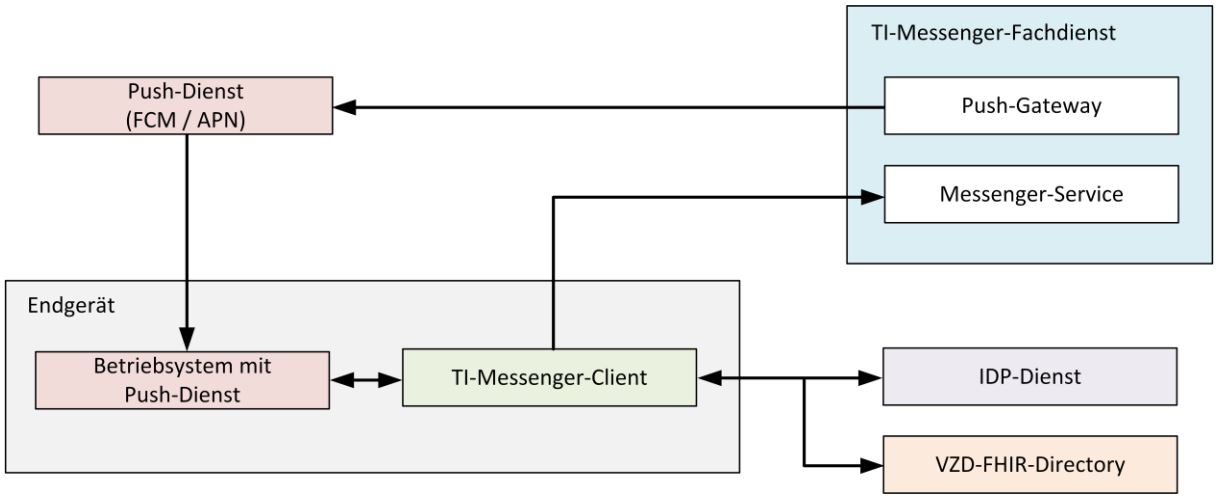

Abbildung 2: Benachbarte Komponenten des TI-Messenger-Clients

Die in der Abbildung benannten Nachbarsysteme des TI-Messenger-Clients werden in der [gemSpec_TI-Messenger-Dienst] und [gemSpec_TI-Messenger-FD] hinreichend beschrieben. Für die Einordnung der Komponenten im Kontext des TI-Messenger-Clients werden diese im Folgenden kurz erläutert.

Tabelle 1: Übersicht der Komponenten und deren Funktionen

Komponente	Funktion
Push-Gateway	• Weiterleitung von Push-Benachrichtigungen an Push-Dienste im Internet
Push-Dienst	• Push-Dienste (z. B. FCM / APN) sind Services von Push-Anbietern und werden für die native Unterstützung von Push-Benachrichtigungen auf mobilen Geräten benötigt.

Messenger-Service	• Stellt für die TI-Messenger-Client-Schnittstellen gemäß [Client-Server API] bereit. • Terminiert die TLS-Verbindung der TI-Messenger-Clients. • Prüft Anfragen der TI-Messenger-Clients. • Stellt für die TI-Messenger-Clients Matrix-OpenID-Token aus.
IDP-Dienst	• Stellt ID_TOKEN aus, um sich beispielweise an einem Matrix-Homeserver mittels OpenID-Connect zu authentifizieren.
VZD-FHIR-Directory	• Ausstellen von access-tokens (search-accesstoken und owner-accesstoken) • Lesen oder Schreiben von FHIR-Ressourcen

3.2 Ausprägungen der TI-Messenger-Clients

3.2.1 Nutzergruppen

Gemäß der Architektur des TI-Messenger-Dienstes wird zwischen zwei Arten von TI-Messenger-Clients unterschieden. Die Unterscheidung ergibt sich ausschließlich aus der Sicht der Akteure. Im Folgenden werden die beiden Ausprägungen beschrieben.

TI-Messenger-Client mit Administrationsfunktionen (Org-Admin-Client)

Der TI-Messenger-Client mit Administrationsfunktionen ist ein Client für Administratoren einer Organisation. Dieser wird im TI-Messenger-Kontext auch als Org-Admin-Client bezeichnet. Der Org-Admin-Client dient zur komfortablen Verwaltung der Messenger-Services bei einem TI-Messenger-Fachdienst. Mit dem Org-Admin-Client besteht die Möglichkeit, im Namen der Organisation FHIR-Ressourcen zur Verfügung zu stellen oder zu bearbeiten. Ebenfalls haben Administratoren einer Organisation die Möglichkeit mit Hilfe des Org-Admin-Clients Benutzer und Geräte auf dem jeweiligen Messenger-Service zu verwalten. Darüber hinaus besteht die Möglichkeit, über den Org-Admin-Client Sessions von angemeldeten Geräten auf dem Messenger-Service zu verifizieren oder zu invalidieren. Das bedeutet zum Beispiel, dass ein Akteur in der Rolle "Org-Admin" einen TI-Messenger-Client eines Akteurs bei Bedarf abmelden kann. Weiterhin können über den Org-Admin-Client Funktionsaccounts gemäß [gemSpec_TI-Messenger-Dienst#Funktionsaccounts] für die übergreifende Kommunikation innerhalb einer Organisationsstruktur des TI-Messenger-Fachdienstes administriert werden.

TI-Messenger-Client für Akteure

Der TI-Messenger-Client für Akteure unterstützt die meisten aller, durch die Matrix-Spezifikation festgelegten Funktionalitäten eines Matrix-Messengers. Akteure können mit Hilfe dieses Clients Ende-zu-Ende-verschlüsselte Chatnachrichten senden und empfangen. Innerhalb der Chaträume erfolgt der Zugriff auf Chatverläufe oder das Austauschen von Medien. Ebenfalls besteht für Akteure die Möglichkeit eigene Geräte und Geräte von Gesprächspartnern zu verifizieren und das VZD-FHIR-Directory nach Organisationen zu durchsuchen, um eine neue Chatkonversation mit einer Organisation zu starten. Es ist den Herstellern freigestellt wie die Oberfläche gestaltet wird. So besteht beispielsweise die Möglichkeit Chaträume nach unterschiedlichen Verwendungszwecken zu organisieren. Akteure in der Rolle "User-HBA" haben zusätzlich die Möglichkeit, die eigene MXID als Kontaktadresse des bereits vorhandenen*Practitioner*-Eintrages auf dem VZD-FHIR-Directory hinzuzufügen. Das Eintragen der MXID gewährt die Suche nach anderen, auf dem VZD-FHIR-Directory eingetragenen Akteuren in der Rolle "User-HBA" und ermöglicht das Auffinden durch andere Akteure in der Rolle "User-HBA".

Hinweis: Die beiden oben beschriebenen Ausprägungen KÖNNEN auch in einem TI-Messenger-Client integriert sein. Die Art der Umsetzung obliegt dem jeweiligen TI-Messenger-Client-Hersteller.

3.2.2 Plattformen

Anbieter eines TI-Messengers MÜSSEN eine mobile und eine stationäre TI-Messenger-Client Anwendung zur Verfügung stellen. TI-Messenger-Clients haben je nach Plattform (Mobil/Stationär) unterschiedliche Anforderungen an Sicherheit, Datenschutz und Funktionalität. Im Folgenden werden die zu unterstützenden Plattformen näher beschrieben.

TI-Messenger-Client für mobile Szenarien

Es handelt sich hierbei um eine TI-Messenger-Client Anwendung, die speziell für die Nutzung auf mobilen Geräten entwickelt wurde (z. B. Android/IOS). Die Bereitstellung KANN als native mobile Anwendung erfolgen oder als eine Integration in bereits bestehende Anwendungen. Die mobile Anwendung MUSS die betriebssystemseitigen Funktionen in Bezug auf Sicherheit nutzen. Die Anwendung MUSS sicherstellen, dass die Speicherung von Daten getrennt und verschlüsselt vom Dateisystem erfolgt. Ein unerlaubter Zugriff durch Dritte MUSS aktiv verhindert werden (z. B. durch PIN-Abfrage beim Öffnen der Anwendung).

TI-Messenger-Client für stationäre Szenarien

Es handelt sich hierbei um einen TI-Messenger-Client Anwendung, die speziell für die Nutzung auf stationären Endgeräten entwickelt wurde (z. B. Windows/MacOS). Die Bereitstellung KANN sowohl als eigenständige Lösung erfolgen oder als eine Integration in bereits bestehende Lösungen.

TI-Messenger-Client als Web-Anwendung

Die Ausführung des TI-Messenger-Client als lokale Web-Anwendung in einem Webbrowser ist ebenfalls möglich. Hierbei gelten die identischen Sicherheitsanforderungen wie bei einer nativen Anwendung. Die Ver- und Entschlüsselung MUSS lokal im Browser auf dem Endgerät erfolgen. Ebenfalls MUSS sichergestellt werden, dass bei Nutzung einer lokalen Web-Anwendung ein unerlaubter Zugriff durch Dritte aktiv verhindert wird (z. B. durch Invalidieren der Session oder durch eine aktive Abmeldung).

3.2.3 Weitere Festlegungen

Jeder Anbieter eines TI-Messengers MUSS für Organisationen, die einen Messenger-Service vom Anbieter erhalten, sowohl den TI-Messenger-Client für Akteure als auch den TI-Messenger-Client mit Administrationsfunktionen (Org-Admin-Client) anbieten.

4 Übergreifende Festlegungen

4.1 Datenschutz und Sicherheit

Zur Sicherstellung des Datenschutzes und der Sicherheit im Rahmen des TI-Messenger-Dienstes werden im Folgenden zu beachtende Anforderungen an den TI-Messenger-Client beschrieben. Anforderungen, die durch andere Systemkomponenten sichergestellt werden, sind hier nicht weiter aufgeführt.

Hinweis: Für datenschutzrechtlichen Anforderungen an den TI-Messenger-Dienst wird auf die Stellungnahme der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder gemäß [DSK2021] verwiesen. Die Inhalte der Stellungnahme werden in den Anforderungen [A_22715] [A_22955] vereinfacht zusammengefasst.

A_22715 - Anforderungen-Herstellererklärung aus der Konferenz der unabhängigen Datenschutzaufsichtsbehörden

- Der TI-Messenger-Client MUSS für den Akteur klar erkennbar Datenschutzinformationen bereitstellen.
- Der TI-Messenger-Client MUSS eine allgemeine und selektive Löschfunktion unterstützen.
- Der TI-Messenger-Client KANN eine Funktion zur Unkenntlichmachung von Ausschnitten von Bildaufnahmen implementieren.
- Der TI-Messenger-Client MUSS beim Versand von Nachrichten oder Dokumenten in Teilen sicherstellen, dass alle Teile gesendet werden.
- Der TI-Messenger-Client MUSS den Nutzer über Fehler beim Versand informieren.
- Der TI-Messenger-Client DARF Standortdaten NICHT dauerhaft erheben.

[<=]

A_22955 - Anforderungen-Gutachten aus der Konferenz der unabhängigen Datenschutzaufsichtsbehörden

- Der TI-Messenger-Client MUSS Inhalte verschlüsselt, separat vom allgemeinen Speicherbereich des Endgeräts speichern. Datenbanken MÜSSEN verschlüsselt sein und der jeweilige Schlüssel in den vom Betriebssystem bereitgestellten sicheren Speicherbereich abgespeichert werden. Medien und Dokumente MÜSSEN separat vom allgemeinen Speicherbereich gespeichert werden.
- Der TI-Messenger-Client MUSS sicherstellen, dass die Nutzersession bei Sperrung oder Abmeldung durch einen Akteur in der Rolle "Org-Admin" beendet wird.

[<=]

A_22716 - Authentisierung des Akteurs gegenüber dem TI-Messenger-Client

Der TI-Messenger-Client MUSS über ein 2-Faktor-Authentifizierungsverfahren verfügen, um sich zu authentisieren gibt der Akteur bei jedem Start der Applikation eine sechsstellige PIN ein, um die Anwendung zu entsperren. Nach jeder Abmeldung, jedem Benutzerwechsel, jedem Schließen der Anwendung, oder spätestens 12 Stunden nach letzter Entsperrung MUSS die Authentisierung des Akteurs erneut vorgenommen werden. Alternativ zum Authentisierungsmittel "PIN" sind auch die Mittel Biometrie, starke Passphrase oder Fido-Token zulässig. Falls das Merkmal "Biometrie" gewählt wird, MUSS

es den Vorgaben aus [BSI-TR-03166] Kap. 2.3.1.5 oder 2.3.1.6 genügen. Als zweiten Faktor MUSS der TI-Messenger-Client prüfen, ob er auf dem Gerät gestartet wurde, an welches er gebunden ist. Für Webclients entfällt diese Authentisierung. Diese Funktionen DÜRFEN NICHT abschaltbar sein und MÜSSEN unabhängig von den Entsperrfunktionen der Endgeräte sein.
Der TI-Messenger-Client SOLL über eine Sperre verfügen, die nach längerer Inaktivität an Webclients die weitere Nutzung verhindert, bis sich erneut, wie zuvor beschrieben, authentisiert wird. Die nötige Dauer der Inaktivität MUSS durch den Akteur konfigurierbar und auf eine Stunde voreingestellt sein.
Der TI-Messenger-Client MUSS den Nutzer bei Erstverwendung des TI-Messenger-Clients, falls das Merkmal PIN oder Passphrase gewählt wurde, dazu zwingen eine solche festzulegen. Dabei ist technisch zu prüfen, dass ein PIN oder Passphrase entsprechend sicher ist. Dies kann beispielsweise durch das Anzeigen von Fortschrittsbalken dem Akteur dargestellt werden. Dieser wird erst grün, sobald eine entsprechende Güte erreicht wurde. Der TI-Messenger-Client KANN eine Funktion verwenden, die zufallsgenerierte Vorschläge für PIN oder Passphrase erstellt. Diese Vorschläge MÜSSEN auf sichere Erzeugung von Zufallszahlen gemäß [gemSpec_Krypt] basieren.
[<=]

A_22717 - Verhinderung der Erstellung von Screenshots
TI-Messenger-Clients für mobile Szenarien MÜSSEN Screenshots und Screencapturing verhindern, sofern das Betriebssystem dies zulässt, oder Akteure nach Erstellen eines Screenshots klar darauf hinweisen, dass dieser nicht durch den TI-Messenger-Client geschützt werden kann. Diese Funktion MUSS durch Opt-Out der Akteure deaktivierbar sein. Wird die Funktion deaktiviert, MÜSSEN Akteure auf die Risiken von Screenshots sensibler Inhalte hingewiesen werden.
[<=]

A_22718 - Mandantenfähigkeit von TI-Messenger-Clients
TI-Messenger-Clients MÜSSEN eine Mandantentrennung unterstützen, die verhindert, dass bei geteilten Endgeräten ein Akteur des TI-Messenger-Clients auf Daten oder Funktionen der TI-Messenger-Client-Devices eines anderen Akteurs auf diesem Gerät zugreifen kann.
[<=]

A_22719 - Datenschutzfreundliche MXIDs
Der TI-Messenger-Client SOLL MXIDs so generieren, dass sie keine personenbezogenen Daten als Klarinformation beinhalten. Akteure des TI-Messenger-Clients DÜRFEN NICHT Einfluss auf die Bildung der MXID haben.
[<=]

A_22720 - Informationspflicht bzgl. Gefahren unsicherer Endgeräte
Der TI-Messenger-Client MUSS den Nutzer in einem Hinweistext auf die Gefahren hinweisen, die bei einem Betrieb des TI-Messenger-Clients auf Hardware, die nicht unter der Kontrolle des Akteurs steht, gegeben sind. Das betrifft neben geteilten Endgeräten ohne IT-Security-Überwachung insbesondere öffentlich zugängliche Endgeräte. Der Akteur MUSS die Empfehlung erhalten auf solchen Geräten den TI-Messenger-Client nicht zu nutzen.
Nutzer von Browserclients MÜSSEN darauf hingewiesen werden, dass diese keine sichere Plattformen darstellen.
[<=]

A_22721 - Key-Sharing zwischen Geräten eines Akteurs
Um Synchronisation von Nachrichteninhalten zwischen mehreren Geräten eines Akteurs zu ermöglichen, verfügt Matrix über eine vorgesehene Key-Sharing-Funktionalität. TI-Messenger-Clients MÜSSEN die Matrix Vorgabe SHOULD "Key-Sharing nur für verifizierte

Geräte" als MUST umsetzen.
[<=]

A_22722 - Key-Sharing zwischen Geräten innerhalb eines Chatraums
TI-Messenger-Clients MÜSSEN über eine Funktion verfügen, innerhalb eines Chatraums Key-Sharing Anfragen an andere Geräte zu stellen und Key-Sharing Anfragen von anderen Geräten anzunehmen oder abzulehnen.
[<=]

A_22723 - Versand von Dateien mittels Matrix
Für den Versand von Dateien gemäß der Matrix-Spezifikation über den TI-Messenger-Client gilt:

- TI-Messenger-Clients MÜSSEN Verschlüsselung für übertragene Inhalte verwenden.
- TI-Messenger-Clients MÜSSEN in der Lage sein, mindestens Dateien mit einer Größe von 25 MB zu versenden.
- TI-Messenger-Clients MÜSSEN über eine Größenbeschränkung zu versendender Inhalte verfügen.
- TI-Messenger-Clients MÜSSEN über eine Schnittstelle und Funktionen verfügen, mit denen empfangene und entschlüsselte Dateien an eine Stelle zur Schadsoftwareprüfung übermittelt und geprüft werden können, bevor diese verarbeitet werden. Dateien, die eine solche Prüfung nicht erfolgreich durchlaufen, SOLLEN verworfen werden. Falls eine Datei verworfen wird, MUSS der Akteur darüber sowie über den Grund informiert werden.
- TI-Messenger-Clients MÜSSEN Akteure bei Fehlschlagen einer Dateiprüfung auf deren Prüfstatus und mögliche Gefahren hinweisen.

Sofern TI-Messenger-Clients über eine Funktion verfügen, Dokumente direkt über den TI-Messenger-Client ohne Nutzung von Third-party Software anzuzeigen, MÜSSEN diese die Ausführung von aktiven Inhalten verhindern. Ebenfalls MUSS diese Funktion es ermöglichen, zugehörige Metadaten auch ohne Öffnen oder Herunterladen der Datei selbst einzusehen.
Der TI-Messenger-Client MUSS den Akteur darüber informieren, dass Dokumente Schadsoftware enthalten können und welche Maßnahmen der Akteur zum Selbstschutz vornehmen kann.
Der TI-Messenger-Client MUSS, wenn er Dokumenteninhalte direkt anzeigt, Maßnahmen zum Schutz vor Schadsoftware in den Dokumenten umsetzen.**[<=]**

Maßnahmenvorschläge zum Schutz vor Schadsoftware:

- Prüfen, ob das Dokumentenformat und dessen Inhalt mit dem angegebenen Dokumententyp in den Metadaten übereinstimmt.
- Vor der Anzeige eines Dokumentes im TI-Messenger-Client sind Sonder- und Meta-Zeichen im Dokument für die jeweilige Anzeigesoftware mit der richtigen Escape-Syntax zu entschärfen.
- Die Anzeigesoftware des TI-Messenger-Clients in einer Sandbox betreiben.

A_22724 - Abschottung der Inhalte im TI-Messenger-Client
TI-Messenger-Clients für mobile Szenarien MÜSSEN sicherstellen, dass Daten, die lokal gespeichert werden, in einem spezifischen Speicherbereich auf dem Endgerät abgelegt werden.

TI-Messenger-Clients für mobile Szenarien MÜSSEN sicherstellen, dass andere Anwendungen auf den Endgeräten nicht auf Inhalte des TI-Messenger-Clients zugreifen können. Hierzu SOLLEN Clients eine Abschottung des Speichers, den der TI-Messenger-Client für Nutzerdaten belegt, vornehmen. Hierzu genügen die vom Betriebssystem i.d.R. zur Verfügung gestellten Mittel.
Webclients MÜSSEN sicherstellen, dass sensible Daten im Browser (z. B. OLM-Keys, ACCESS_TOKEN) nicht durch andere Anwendungen ausgelesen werden können.
TI-Messenger-Clients MÜSSEN ein Öffnen von über den TI-Messenger-Fachdienst empfangenen Dateien durch Drittprogramme ermöglich. Hierbei MUSS er sicherstellen, dass eine solche Ausleitung von Dateien nur ausgelöst durch den TI-Messenger-Client erfolgt. Der TI-Messenger-Client KANN eine Funktion enthalten, mittels derer empfangene Dateien außerhalb des dedizierten Speichers im Gerät abgelegt werden. Der TI-Messenger-Client MUSS sicherstellen , dass Akteure bei Verwenden einer solchen Funktion geeignet darüber informiert werden, dass sie Daten aus dem geschützten Bereich des TI-Messenger-Clients hinausbewegen.
[<=]

A_22725 - Sicherheitskritische Updates
TI-Messenger-Client-Hersteller MÜSSEN sicherstellen, dass Akteure über die Veröffentlichung von Updates für ihre TI-Messenger-Clients informiert werden. Bei sicherheitskritischen Updates MÜSSEN sie sicherstellen, dass nach einer geeigneten Frist eine weitere Nutzung des TI-Messenger-Clients ohne vorheriges Sicherheitsupdate nicht möglich ist. Hierzu genügt eine clientseitige Sperre anstatt eines Nachweises gegenüber dem Matrix-Homeserver. Die Möglichkeit weiter Updates einzuspielen MUSS in diesem Fall weiterhin gegeben sein. Akteure MÜSSEN geeignet darüber informiert werden, dass sie sicherheitskritische Updates installieren müssen um den TI-Messenger-Client weiterhin zu nutzen.
Der Hersteller des TI-Messenger-Clients MUSS die gematik bei Veröffentlichung einer neuen Produktversion informieren und eine Erklärung zur sicherheitstechnischen Eignung liefern.
[<=]

A_22791 - Zusatzfunktionen für TI-Messenger-Clients
Hersteller des TI-Messenger-Clients MÜSSEN sicherstellen, dass alle implementierten Funktionen, die über den gewöhnlichen Funktionsumfang eines TI-Messenger-Clients hinausgehen die Sicherheit des Produkts nicht gefährden und die Interoperabilität mit anderen TI-Messenger-Produkten erhalten bleibt.
Der Hersteller MUSS sicherstellen, dass alle Zusatzfunktionen des TI-Messenger-Clients von den Basisfunktionen unterscheidbar sind.
[<=]

A_22792 - Device Verification, Cross-Signing und SSSS für TI-Messenger-Clients
TI-Messenger-Clients MÜSSEN die Funktionen Cross-Signing und Secure Secret Storage and Sharing (SSSS) zur Device Verification unterstützen. Es MUSS der Spezifikation gemäß [Client-Server API#Sharing keys between devices] gefolgt werden.
[<=]

A_22793 - Ende-zu-Ende Verschlüsselung
TI-Messenger-Clients MÜSSEN eine Ende-zu-Ende-Verschlüsselung auf Basis von OLM/MEGOLM unterstützen. Dazu MUSS der Spezifikation gemäß [Client-Server API#End-to-End Encryption] gefolgt werden.
TI-Messenger-Clients MÜSSEN für das Versenden von Nachrichten diese Verschlüsselung nutzen.
[<=]

A_22794 - Explizites Verbot von Profiling für TI-Messenger-Clients
TI-Messenger-Client-Hersteller und -Anbieter DÜRFEN NICHT Daten zu Profiling-Zwecken sammeln. Dies betrifft insbesondere eine Überwachung welche Akteure mit welchen anderen Akteuren kommunizieren.

Die gematik kann nach § 331 Abs. 2 SGB V Daten festlegen, die Anbieter von Komponenten und Dienste der gematik offenzulegen bzw. zu übermitteln haben, sofern diese erforderlich sind, um den gesetzlichen Auftrag der gematik zur Überwachung des Betriebs zur Gewährleistung der Sicherheit, Verfügbarkeit und Nutzbarkeit der Telematikinfrastruktur zu erfüllen. Nur die hierfür erforderlichen personenbezogenen Daten dürfen von den Anbietern und Herstellern als Ausnahme vom Profilingverbot erhoben und ausschließlich für den genannten Zweck verwendet werden.
[<=]

A_22795 - Einbringung und Speicherung von Schlüsseln und Token
TI-Messenger-Client-Hersteller MÜSSEN sicherstellen, dass Schlüssel und Token sicher in den TI-Messenger-Client eingebracht werden.
TI-Messenger-Client-Hersteller MÜSSEN technisch sicherstellen, dass Schlüssel und Token nicht in andere Speicher ausgelagert werden können , als die dafür vorgesehenen Speicher der TI-Messenger-Clients oder dem SSSS des beteiligten Homeservers.
[<=]

A_22796 - Verwendung von TLS zur Kommunikation mit dem Fachdienst und VZD-FHIR-Directory
TI-Messenger-Clients MÜSSEN in der Lage sein, Verbindungen zu anderen Komponenten des TI-Messenger-Dienstes über TLS aufzubauen. Hierzu gelten die Festlegungen der [gemSpec_Krypt].
[<=]

A_22797 - Löschfunktionen für TI-Messenger-Inhalte
TI-Messenger-Clients MÜSSEN über eine automatische Löschfunktion für Inhalte verfügen. Diese MUSS eine zumutbare voreingestellte Löschfrist enthalten, welche für Akteure konfigurierbar ist. Die Löschfrist MUSS hierbei auf den minimal einstellbaren Wert initialisiert sein. Nach Verstreichen der eingestellten Löschfrist MÜSSEN Gesprächsinhalte aus dem TI-Messenger-Client gelöscht werden. Zusätzlich MÜSSEN TI-Messenger-Clients über eine nachrichtenbasierte Löschfunktion verfügen, die es Akteuren erlaubt ihre eigenen Nachrichten händisch nicht nur vom eigenen TI-Messenger-Client, sondern auch aus dem Room State zu löschen.
[<=]

A_22798 - Privacy by Default
TI-Messenger-Clients MÜSSEN stets die datenschutzfreundlichste Voreinstellung als Standardeinstellung verwenden.
[<=]

A_22799 - Verwendung von OWASP Mobile
Hersteller eines TI-Messenger-Client für mobile Szenarien MUSS bei der Entwicklung von TI-Messenger-Clients die Maßnahmen und Vorgaben der aktuellen Version der OWASP-Top-10-Mobile-Risiken [OWASP MobileTop10] umsetzen. Hierbei SOLLEN die Vorgaben der Prüfvorschrift für den Produktgutachter des „ePA-Frontend des Versicherten" analog für den TI-Messenger-Client umgesetzt werden, mit Ausnahme folgender Punkte:

Punkt	Begründung

O.Arch_7	Der tatsächliche Sicherheitsgewinn steht in keinem Verhältnis zum Aufwand.
O.Auth_6	Diese Maßnahme wird im Zuge der Einführung des Zero-Trust-Modells in späteren TI-Messenger-Spezifikationsversionen ergänzt.
O.Auth_11	Diese Maßnahme wird bereits in ML-123584 behandelt.
O.Sess_1 bis _6	Das Session-Handling von Matrix weicht zu weit vom angenommenen Stand ab um diese Maßnahmen sinnvoll wie vorgesehen umzusetzen.
O.Tokn_10	Diese Funktion wird über das Matrix-Protokoll mittels Devices unterstützt.
O.Data_5 erster Satz	Für den TI-Messenger-Client wurde eine Funktion vorgesehen, die eine Standardlöschfrist für Inhalte setzt und Nutzern die Möglichkeit gibt selbst über die Aufbewahrungsdauer ihrer Gesprächsinhalte zu bestimmen.
O.Data_6	Diese Maßnahme steht den Sicherheitszielen des TI-Messengers diametral entgegen.
O.Data_12	Diese Maßnahme ist bereits in ML-123585 geregelt.
O.Data_19	Diese Maßnahme richtet sich nicht an den TI-Messenger-Client.
O.Ntwk_7	Integritätsschutz erfolgt bereits über das Matrix-Protokoll.
O.Ntwk_9	Diese Maßnahme ist datenschutzrechtlich nicht angemessen.
O.Ntwk_10	Diese Maßnahme ist datenschutzrechtlich nicht angemessen.
O.Resi_2	Diese Maßnahme erzeugt Nutzerprobleme, die dem schmalen Sicherheitsgewinn und dem eher geringen Risiko bei Zuwiderhandlung nicht gerecht überwiegen.
O.Resi_4 bis _5	Diese Maßnahme erzeugt Nutzerprobleme, die dem schmalen Sicherheitsgewinn und dem eher geringen Risiko bei Zuwiderhandlung nicht gerecht überwiegen.
O.Resi_7 bis _8	Diese Maßnahme erzeugt Nutzerprobleme, die dem schmalen Sicherheitsgewinn und dem eher geringen Risiko bei Zuwiderhandlung nicht gerecht überwiegen.

Darüber hinaus sind folgende Punkte der OWASP-Top-10-Mobile-Risiken nur für

eingeschränkte Clients relevant. Andere Client-Typen KÖNNEN auf die Umsetzung dieser Punkte verzichten:

Punkt	Relevant für
O.Arch_13	Nur mobil
O.Tokn_1	Nur mobil
O.Data_2	Nur mobil
O.Data_3	Nur mobil
O.Data_14	Nur mobil
O.Data_16	Nur mobil
O.Paid_1 bis _10	Nur mobil
O.Plat_1 bis _3	Nur mobil
O.Plat_5 bis _9	Nur mobil
O.Plat_11	Nur mobil
O.Resi_3	Nur mobil
O.Resi_9	Nur mobil

[<=]

A_22800 - Sicherheitsrisiken von Software Bibliotheken minimieren
Der TI-Messenger-Client MUSS Maßnahmen umsetzen, um die Auswirkung von unentdeckten Schwachstellen in benutzten Software-Bibliotheken zu minimieren.
Hinweis: Beispielmaßnahmen sind in [OWASP Proactive Control#C2] zu finden. Das gewählte Verfahren muss die gleiche Wirksamkeit aufweisen, wie die Kapselung gemäß [OWASP Proactive Control#C2 Punkt 4].
[<=]

A_22801 - Sicheres Beziehen von fremden Programmbestandteilen
Der Hersteller MUSS die Software-Komponenten des TI-Messenger-Clients, die nicht vom Hersteller selbst entwickelt oder zur Entwicklung beauftragt werden (z. B. TLS-Bibliotheken oder Matrix-Implementierungen), aus bekannten und vertrauenswürdigen Quellen beziehen.
[<=]

A_22802 - Sichere Softwareverteilung
Der Hersteller eines TI-Messenger-Clients MUSS Akteure über die vertrauenswürdigen Quellen informieren, von denen Akteure den TI-Messenger-Client beziehen können und wie sie die Vertrauenswürdigkeit der Quelle erkennen können. Der Hersteller MUSS sicherstellen, dass der Akteur bei Erstbezug eines TI-Messenger-Clients die Authentizität der vertrauenswürdigen Bezugsquelle verifizieren kann. Der TI-Messenger-Client MUSS sicherstellen, dass Updates nur von bekannten und vertrauenswürdigen Quellen bezogen

werden, nachdem die Authentizität der Quelle technisch erfolgreich verifiziert wurde. Der TI-Messenger-Client MUSS nach Installation und Update eine technische Prüfsumme generieren und anzeigen, anhand derer die Integrität der Installation überprüft werden kann.
[<=]

A_22803 - Lokale Ausführung des TI-Messenger-Clients
Der TI-Messenger-Client MUSS sicherstellen, dass alle TI-Messenger-Clientspezifischen Anteile lokal auf dem Gerät des Nutzers ausgeführt werden, sofern die Betriebsumgebung des TI-Messenger-Clients dies zulässt.
[<=]

A_22804 - Datenschutzkonformes Tracking
Der TI-Messenger-Client DARF NICHT Werbe-Tracking verwenden.
Im Folgenden wird unter Tracking auch Usability-Tracking sowie Crash-Reporting verstanden.
Der TI-Messenger-Client MUSS sicherstellen, falls er Tracking-Funktionen implementiert, dass in den übermittelten Tracking-Informationen keine Sicherheitsmerkmale, wie Device-ID oder Daten mit Sicherheitsbezug, enthalten sind.
Der Datenschutzrechtlich-Verantwortliche für den TI-Messenger-Clients MUSS die Verarbeitung und Auswertung etwaiger gesammelter Tracking-Daten des TI-Messenger-Clients selbst durchführen und nicht von einem Drittanbieter durchführen lassen.
Der TI-Messenger-Client MUSS sicherstellen, falls er Tracking-Funktionen nutzt, dass die Tracking-Daten keine Daten enthalten, die natürliche Personen direkt identifizieren.
Der TI-Messenger-Client MUSS, falls er Tracking-Funktionen ohne Einwilligung des Akteurs nutzt, sicherstellen, dass die Tracking-Daten

- sich nur auf eine Clientnutzung (von der ersten Interaktion des Nutzers mit dem Client bis zum Schließen des Clients bzw. bis zum Inaktivitätstimeout) beziehen und nicht mit anderen Clientnutzungen des Akteurs verknüpft werden,
- weder personenbezogene noch pseudonymisierte personenbezogene Daten enthalten,
- keine nutzerbezogenen IDs oder gerätespezifischen IDs der Nutzergeräte enthalten,
- keinen Rückschluss auf Versicherte, deren Vertreter, Leistungserbringer oder Kostenträger ermöglichen, insbesondere Rückschlüsse anhand des Nutzerverhaltens über die Zeit oder über Clientnutzungen hinweg,
- nicht durch die Verknüpfung mit personenbezogenen Daten aus anderen Quellen de-anonymisiert werden können.

Der TI-Messenger-Client MUSS, falls er Tracking-Funktionen ohne Einwilligung des Akteurs nutzt, den Akteur über das Tracking im TI-Messenger-Client in verständlicher und leicht zugänglicher Form sowie in einer klaren und einfachen Sprache informieren, bevor die Trackingdaten erhoben werden.
Der TI-Messenger-Client MUSS, falls er Tracking-Funktionen ohne Einwilligung des Akteurs nutzt, für jede Clientnutzung neue Nutzungsidentifier zufällig generieren. Der Akteur MUSS in der Lage sein jederzeit die Neugenerierung dieser Identifier zu erzwingen.
Der TI-Messenger-Client MUSS, falls er Tracking-Funktionen mit Verknüpfung der Tracking-Daten mehrerer Clientnutzungen implementiert, technisch sicherstellen, dass diese Tracking-Funktionen bei der Installation des TI-Messenger-Clients standardmäßig deaktiviert sind und nur nach expliziter Einwilligung durch den Akteur aktiviert werden (Opt-in). Die Ablehnung der Nutzung solcher Funktionen darf die Standardfunktionen des TI-Messenger-Clients nicht einschränken.

Falls solche Funktionen implementiert werden, MUSS den Akteuren vor der Einwilligung in die Aktivierung dieser Tracking-Funktionen in verständlicher und leicht zugänglicher Form sowie in einer klaren und einfachen Sprache folgende Einwilligungsinformationen angezeigt werden:

- welche Daten durch die Tracking-Funktionen erhoben werden,
- zu welchen Zwecken die Daten erhoben werden,
- welche Informationen durch die Auswertung der erhobenen Daten gewonnen werden und ob Rückschlüsse auf den Gesundheitszustand des Akteurs möglich wären,
- wer die Empfänger der Daten sind,
- wie lange die Daten gespeichert werden.

Diese Funktionen DÜRFEN NICHT aktiviert werden, bis eine explizite Einwilligung durch die Akteure erfolgt ist und MUSS jederzeit durch diese deaktivierbar sein.
Ein Verweis auf AGBs oder Nutzungsbedingungen des TI-Messenger-Clients ist hierzu NICHT ausreichend. Unter verständlicher und leicht zugänglicher Form wird explizit eine kurze Erklärung in einfacher und nicht juristischer Sprache verstanden, die direkt im TI-Messenger-Client angezeigt wird.
Der Client DARF NICHT wiederholt beim Akteur anfragen um eine Einwilligung durch Belästigung zu erzwingen. Nach einmaliger Ablehnung durch den Akteur MUSS jede Anzeige des Dialogs explizit durch den Akteur initiiert werden.
[<=]

A_22805 - CC-Evaluierung als Ersatz für das Gutachten
Falls der Hersteller entscheidet, eine CC-Zertifizierung statt eines Produktgutachtens durchzuführen, MUSS der Hersteller bei der Einreichung eines CC-Zertifizierungsantrags sein Security Target Dokument der gematik zur Verfügung stellen. In diesem müssen mindestens beschrieben sein:

- die zusätzlichen Funktionen des TI-Messenger-Clients,
- die in den zusätzlichen Funktionen verarbeiteten Daten,
- die Schnittstellen zwischen dem TI-Messenger-Client des Akteurs und den ggf. genutzten Backend-Diensten der zusätzlichen Funktionen inklusive ihrer Sicherheitsmaßnahmen und
- die Sicherheitsannahmen an den TI-Messenger-Client des Akteurs und die Ausführungsumgebung

[<=]

A_22806 - Kein Schreibzugriff für TI-Messenger-Clients auf Room-States
TI-Messenger-Clients MÜSSEN verhindern, dass Akteure die Möglichkeit erhalten zusätzliche Informationen in Room-States einzutragen.
[<=]

A_22937 - Einsatz nur von auditierter Verschlüsselung
TI-Messenger-Clients MÜSSEN für die Verschlüsselung von Nachrichten eine auditierte und ausreichend sichere Implementierung von OLM/MEGOLM verwenden. Sollte eine andere Implementierung genutzt werden, als die von der gematik vorgesehene, MUSS der Hersteller einen Sicherheitsnachweis, z. B. in Form eines beauftragten Audits, erbringen.**[<=]**

Hinweis: Die gematik hat in Kooperation mit der Matrix-Foundation ein Audit für die OLM/MEGOLM Rust-Implementierung Vodozemac der in Auftrag gegeben. Auf Basis dieses Audits wird Vodozemac als die von der gematik vorgesehene Implementierung benannt.

A_22938 - Nur Verbindung zu validen Messenger-Services
TI-Messenger-Clients DÜRFEN dem Akteur bei der Konfiguration genutzter Messenger-Services KEINE Messenger-Services zur Auswahl anzeigen, die nicht zum gewählten Anbieter gehören und valide TI-Messenger Messenger-Services sind.
[<=]

A_22964 - Zugriffsschutz auf Administrationsfunktionen
TI-Messenger-Clients, die eine Doppelrolle als gewöhnlicher Client und als Org-Admin-Client wahrnehmen, MÜSSEN für beide Funktionalitäten separate User-Interfaces bereitstellen. Um den Akteur auf Org-Admin-Client Funktionalitäten zugreifen zu lassen MUSS der TI-Messenger eine neue Authentisierung des Akteurs gegenüber dem TI-Messenger-Client erzwingen.**[<=]**

4.2 Authentifizierung am VZD-FHIR-Directory

Für den Zugriff auf den FHIR-Proxy des VZD-FHIR-Directory ist ein durch den Auth-Service ausgestelltes access-token notwendig. Hierfür MÜSSEN die am Auth-Service bereitgestellten REST-Schnittstellen vom TI-Messenger-Client aufgerufen werden.

Für den Schreibzugriff auf das FHIR-Directory MUSS der TI-Messenger-Client prüfen, ob ein gültiges owner-accesstoken lokal vorhanden ist. Wenn kein gültiges owner-accesstoken vorhanden ist MUSS der TI-Messenger-Client dies beim Auth-Service des VZD-FHIR-Directory mittels des Aufrufes `GET /owner-authenticate` unter Vorlage eines gültigen ID_TOKEN vom zuständigen IDP-Dienst anfragen. Für den Lesezugriff auf das VZD-FHIR-Directory MUSS der TI-Messenger-Client prüfen, ob ein gültiges search-accesstoken lokal vorliegt. Wenn kein gültiges search-accesstoken vorhanden ist MUSS der TI-Messenger-Client dies beim Auth-Service des VZD-FHIR-Directory mittels des Aufrufes `GET /tim-authenticate` unter Vorlage eines Matrix-OpenID-Token anfragen.

4.3 Benutzerführung

Mittels einer geeigneten Benutzerführung wird eine hohe Akzeptanz des Nutzers erreicht. Hierzu zählt eine einfache und selbsterklärende Bedienung der Oberfläche, die sich an gängige auf dem Markt zu findenden App-Design-Empfehlungen orientiert. Ebenfalls MÜSSEN alle infrage kommenden Zielgruppen betrachtet werden. Es MÜSSEN folgende interoperable Funktionen durch den Hersteller bereitgestellt werden, um ein Mindestmaß an Akzeptanz bei den Nutzern zu erreichen. Diese werden im Folgenden beschrieben.

Präsenzanzeige für andere Nutzer

Für eine Echtzeitnutzererfahrung, MÜSSEN TI-Messenger-Clients gemäß [Client-Server API#Presence] eine Präsenzanzeige für andere Gesprächspartner zur Verfügung stellen. Die Präsenzanzeige MUSS an- und abschaltbar sein und MUSS gemäß Privacy-by-

default (Art. 25 Abs. 2 DSGVO und nachgelagert gemäß [ML-123607]) standardmäßig deaktiviert sein.

Erwähnungen von Nutzern im Chatraum

TI-Messenger-Clients MÜSSEN es ermöglichen, dass über das Eingabefeld andere Nutzer gemäß [Client-Server API#User, room, and group mentions] im jeweiligen Chatraum erwähnt werden können. Dazu MUSS der TI-Messenger-Client eine entsprechende Nutzerliste anzeigen, sobald der Nutzer ein neues Wort mit "@" startet, oder einen entsprechenden "@" Knopf im Chatraum anbieten. TI-Messenger-Clients MÜSSEN Nutzererwähnungen entsprechend als "*Pile*" in dem Chatraum anzeigen. Handelt es sich um einen TI-Messenger-Client für mobile Szenarien MUSS der TI-Messenger-Client eine entsprechende Push-Benachrichtigung anzeigen, wenn der Nutzer die entsprechenden Push-Regeln eingestellt hat.

Lesebestätigungen

Lesebestätigungen dienen dem Ziel einen Aufschluss darüber zu geben, wann, ob und von wem eine Nachricht innerhalb eines Chatraums gelesen wurde. Aus diesem Grund MÜSSEN TI-Messenger-Clients die Matrix-Spezifikation gemäß [Client-Server API#Receipts] implementieren. TI-Messenger-Clients MÜSSEN die Funktionen des Anzeigens und des Sendens von Lesebestätigungen implementieren. Der TI-Messenger-Client MUSS *Fully-Readmarkers* unterstützen. Lesebestätigungen MÜSSEN an- und abschaltbar sein und MÜSSEN gemäß Privacy-by-default (Art. 25 Abs. 2 DSGVO und nachgelagert gemäß [ML-123607]) standardmäßig deaktiviert sein.

Eingabebenachrichtigungen

TI-Messenger-Clients für mobile Szenarien MÜSSEN die Matrix-Spezifikation gemäß [Client-Server API#Typing Notifications] implementieren. TI-Messenger-Clients SOLLEN anzeigen, wenn die Gegenseite eine Nachricht in einem Chatraum schreibt. Die Eingabebenachrichtigungen MÜSSEN an- und abschaltbar sein und MÜSSEN gemäß Privacy-by-default (Art. 25 Abs. 2 DSGVO und nachgelagert gemäß [ML-123607]) standardmäßig deaktiviert sein.

Barrierefreiheit

ML-123582 - Standards zur Barrierefreiheit
Hersteller eines TI-Messenger-Clients SOLLEN die in [ISO 9241] aufgeführten Qualitätsrichtlinien zur Sicherstellung der Ergonomie interaktiver Systeme und Anforderungen aus der Verordnung zur Schaffung barrierefreier Informationstechnik nach dem Behindertengleichstellungsgesetz (Barrierefreie-Informationstechnik-Verordnung – [BITV 2.0]) beachten.
[<=]

4.4 Konfiguration

Im folgenden Kapitel werden alle zu konfigurierenden Funktionen beschrieben, die im TI-Messenger-Client durch den Akteur konfigurierbar sein MÜSSEN.

Einstellung von Push-Benachrichtigungen

TI-Messenger-Clients MÜSSEN über eine Funktion verfügen, um Push-Benachrichtigungen auf einem Endgerät konfigurieren zu können. Dazu MÜSSEN neben Push-Rules gemäß [Client-Server API#Push Rules] auch geräteseitige Einstellungsmöglichkeiten den Nutzern zur Verfügung gestellt werden.

Nutzer ignorieren

TI-Messenger-Clients MÜSSEN über eine Funktion verfügen, um Nachrichten anderer Nutzer ignorieren zu können. Daher MÜSSEN TI-Messenger-Clients die Matrix-Spezifikation gemäß [Client-Server API#Ignoring Users] implementieren. TI-Messenger-Clients MÜSSEN eine Liste aller ignorierten Nutzer anzeigen und die Möglichkeit bieten das Ignorieren von Nutzern rückgängig zu machen.

Raum-Historie

TI-Messenger-Clients MÜSSEN die Matrix-Spezifikation gemäß [Client-Server API#Room History Visibility] implementieren. TI-Messenger-Clients MÜSSEN Einstellungen zur Verfügung stellen, um die Sichtbarkeit der Raum-Historie festlegen zu können. Als Standard SOLLTE die Raum-Historie ab dem Zeitpunkt des Beitritts zu einem Chatraum sichtbar sein.

Sichtbarkeit

TI-Messenger-Clients MÜSSEN über eine Funktion verfügen die die Sichtbarkeit eines Akteurs in der Rolle "User-HBA" für den TI-Messenger-Dienst im Personenverzeichnis des VZD-FHIR-Directory ein bzw. ausschalten kann. Hierfür MUSS über die REST-Schnittstelle`/owner` am FHIR-Directory des VZD-FHIR-Directory das Attribut `status` des Endpoints einer Practitioner-Ressourceauf den Wert `status == active` für das einschalten oder `status == off` für das ausschalten gesetzt werden.

4.5 Test

Produkttests zur Sicherstellung der Konformität mit der Spezifikation sind vollständig in der Verantwortung der Anbieter/Hersteller des TI-Messenger-Clients. Die gematik konzentriert sich bei der Zulassung auf das Zusammenspiel der Produkte durch E2E- und IOP Tests.

Die eigenverantwortlichen Produkttests bei den Industriepartnern umfassen:

- Testumgebung entwickeln,
- Testfallkatalog erstellen (für eigene Produkttests) und
- Produkttest durchführen und dokumentieren.

Die Hersteller der TI-Messenger-Fachdienste MÜSSEN zusichern, dass die gematik die Produkttests der Industriepartner in Form von Reviews der Testkonzepte, der Testspezifikationen, der Testfälle und mit dem Review der Testprotokolle (Log- und Trace-Daten) überprüfen kann.

Die gematik fördert eine enge Zusammenarbeit und unterstützt Industriepartner dabei, die Qualität der Produkte zu verbessern. Dies erfolgt durch die Organisation zeitnaher IOP-Tests, die Synchronisierung von Meilensteinen und regelmäßige industriepartnerübergreifende Test-Sessions. Die Test-Sessions umfassen gegenseitige IOP- und E2E-Tests.

Die gematik stellt eine TI-Messenger-Dienst Referenzimplementierung zur Verfügung. Zur Sicherstellung der Interoperabilität zwischen verschiedenen TI-Messenger-Fachdiensten innerhalb des TI-Messenger-Dienstes MUSS der TI-Messenger-Fachdienst eines TI-Messenger-Anbieters gegen die Referenzimplementierung (TI-Messenger-Client und TI-Messenger Fachdienst) getestet werden.

ML-124204 - Test des TI-Messenger-Clients gegen die Referenzimplementierung
Der TI-Messenger-Client MUSS gegen die Referenzimplementierung erfolgreich getestet werden. Die Testergebnisse sind der gematik vorzulegen.
[<=]

Für die Anbieter-Zulassung MÜSSEN die TI-Messenger-Fachdienste und TI-Messenger-Clients vom TI-Messenger-Anbieter bereitgestellt werden. Um einen automatisierten Test für den TI-Messenger-Dienst zu ermöglichen, MUSS die Test-App des TI-Messenger-Clients zusätzlich ein Testtreiber-Modul intern oder extern zur Verfügung stellen. In den folgenden Abbildungen wird das interne sowie das externe Testtreiber-Modul dargestellt.

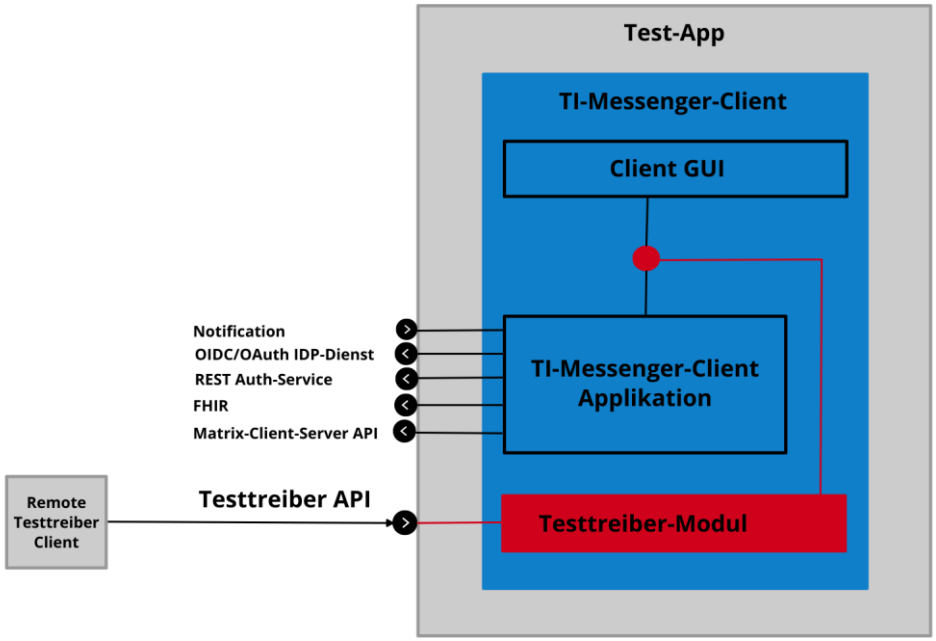

Abbildung 3: internes Testtreiber-Modul

Das externe Testtreiber-Modul erlaubt den Zugriff auf die Testumgebung des Herstellers und steuert so die Test-App.

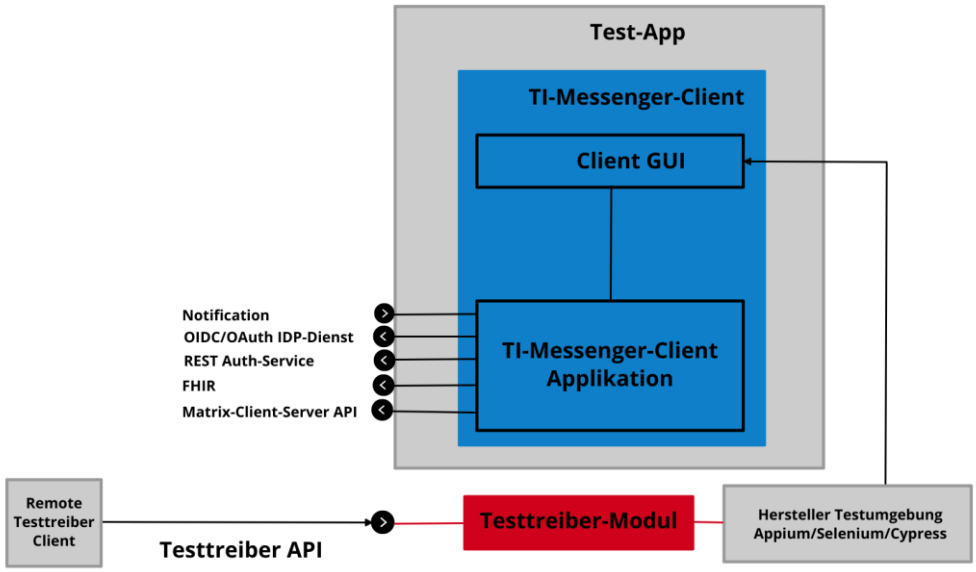

Abbildung 4: externes Testtreiber-Modul

Das Testtreiber-Modul MUSS die Funktionalitäten der produktspezifischen Schnittstellen des TI-Messenger-Clients über eine standardisierte Schnittstelle von außen zugänglich machen und einen Fernzugriff ermöglichen. Dieses Testtreiber-Module MUSS Bestandteil der Test-APP sein (internes Testtreiber-Modul) oder ein Zugang zum Test-Environment des Herstellers gewährleisten (externes Testtreiber-Modul). Die Schnittstelle wird gemäß [Testtreiber API] durch die gematik spezifiziert und bereitgestellt. Das Testtreiber-Modul MUSS die durch den TI-Messenger-Client über eine produktspezifische Schnittstelle angebotene Funktionalität nutzen, um die Operationen des TI-Messenger-Clients umzusetzen. Bei einem internen Testtreiber-Modul wird die REST-Schnittstelle in die Test-App integriert (der Zugriff erfolgt hierbei direkt über das Endgerät). Der Test von Web-Clients (TI-Messenger-Client als Web-Anwendung) findet ausschließlich über externe Treiber-Module statt. Für die Ausführung der Tests werden Organisationen und Messenger-Services benötigt. Diese Organisationen und Messenger-Services MÜSSEN von den Herstellern vor Beginn der Testphase eingerichtet und die Daten (Organisationsnamen usw.) MÜSSEN an die gematik übermittelt werden.

ML-124877 - Test-App des TI-Messenger-Clients und Testtreiber-Modul
Die Test-App des TI-Messenger-Clients MUSS ein Testtreiber-Modul beinhalten oder einen Zugang zum Test-Environment des Herstellers gewährleisten. Die Schnittstelle gemäß [Testtreiber API] wird durch die gematik spezifiziert und bereitgestellt. Das Testtreiber-Modul MUSS die durch den TI-Messenger-Client (dem Zulassungsgegenstand) über eine produktspezifische Schnittstelle angebotene Funktionalität nutzen, um die Operationen der Schnittstellen umzusetzen. Das Testtreiber-Modul DARF die Ausgaben des TI-Messenger-Clients gemäß der technischen Schnittstelle aufarbeiten, aber DARF NICHT die Inhalte verfälschen.
[<=]

ML-124878 - Beschränkung des Einsatzes des Testtreiber-Moduls

Der produktive TI-Messenger-Client DARF NICHT ein Testtreiber-Modul enthalten. Der Einsatz des Testtreiber-Moduls ist auf das Zulassungsverfahren in Test-Apps beschränkt und DARF NICHT in Wirkbetriebs-Apps genutzt werden.
[<=]

ML-124879 - Keine Fachlogik in Testtreiber-Modul
Das Testtreiber-Modul DARF NICHT die Fachlogik des TI-Messenger-Clients umsetzen.
[<=]

Die gematik testet im Rahmen der Zulassungsverfahren auf Basis von Anwendungsfällen. Dabei wird sich auf die Anwendungsfälle aus der [gemSpec_TI-Messenger-Dienst] bezogen. Hierbei wird versucht, möglichst viele Funktionsbereiche der Komponenten des TI-Messenger-Dienstes einzubeziehen. Die Tests werden zunächst gegen die Referenzimplementierung der gematik durchgeführt. In diesem Schritt wird die Funktionalität des Zulassungsobjektes "TI-Messenger-Dienst" geprüft. Anschließend wird mit den IOP- und E2E-Tests die Interoperabilität zwischen den verschiedenen TI-Messenger-Anbietern nachgewiesen. Hierfür werden dann alle bereits zur Verfügung stehenden TI-Messenger-Dienste (die Test-Instanzen der einzelnen Hersteller) zusammengeschlossen und anschließen gegeneinander getestet. Alle Anbieter MÜSSEN bereits im Vorfeld diesen IOP- und E2E-Tests selbständig und eigenverantwortlich durchführen. Bei Problemen im Rahmen der Zulassung MÜSSEN die Anbieter bei der Analyse unterstützen. In der folgenden Abbildung ist eine Systemumgebung für Herstellertests dargestellt.

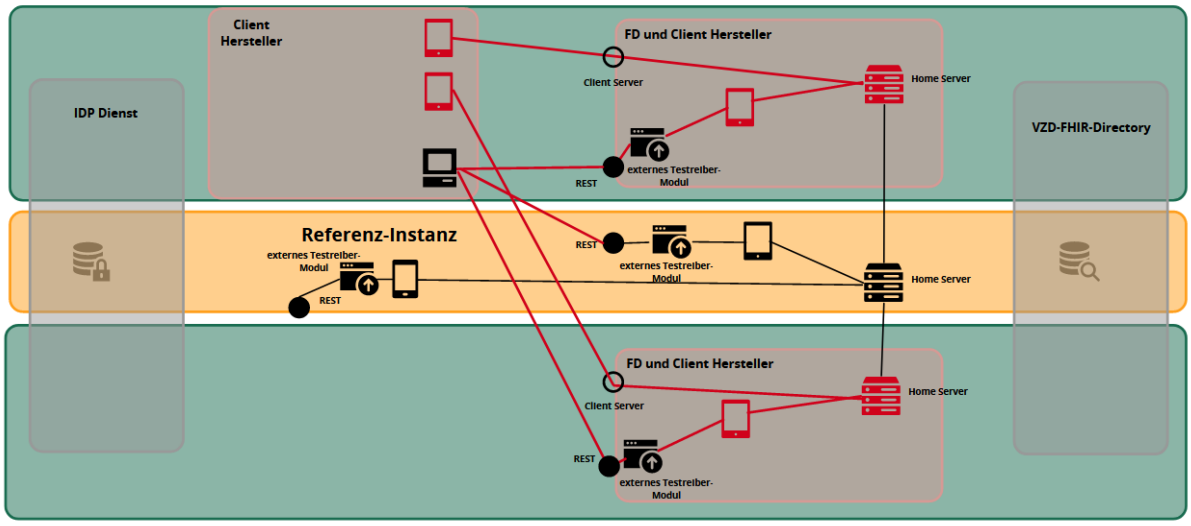

Abbildung 5: Testumgebung für Herstellertests

Zusätzlich zu den bereits durchgeführten IOP- und E2E-Tests werden weitere Interoperabilitätstests von verschiedenen TI-Messenger-Lösungen vor und nach der Zulassung durch die gematik durchgeführt. Die folgende Abbildung zeigt die Nutzung der existierenden Testumgebung durch die gematik während der Zulassungs- und Interoperabilitätstests.

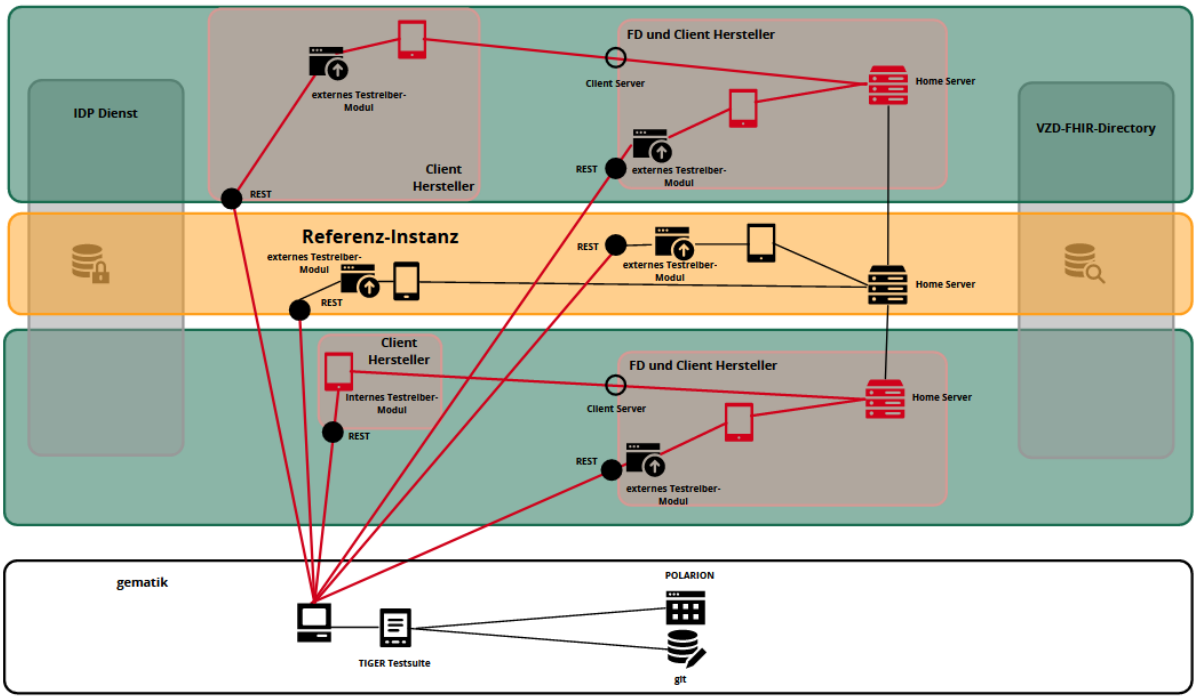

Abbildung 6: Testumgebung gematik

4.6 Betriebliche Aspekte

Die Betriebsbereitschaft des bzw. der Clients vom TI-Messenger-Anbieter bezieht sich in diesem Kapitel auf serverseitige Systeme welche notwendig sind, damit der Client vom Nutzer sicher-funktional betrieben werden kann. Der sichere Betrieb im Sinne der Nutzung auf ihren Endgeräten des TI-Messenger-Clients liegt letztendlich in der Verantwortung der Nutzer bzw. Akteure des TI-Messengers.

Der TI-Messenger-Anbieter MUSS seine Nutzer bzw. die Akteure dabei unterstützen, einen sicheren und funktionalen Betrieb der TI-Messenger-Clients zu ermöglichen.

Der TI-Messenger-Client MUSS mit einer vollumfänglich-funktionalen Verfügbarkeit von 98 % betreibbar sein.

Der TI-Messenger-Anbieter MUSS das/die Produkt(e) TI-Messenger-Client mit einer vollumfänglich-funktionalen Verfügbarkeit von 98 % seinen Nutzern anbieten.

5 Funktionsmerkmale

Der Funktionsumfang des TI-Messenger-Clients ergibt sich aus der Matrix-Spezifikation und MUSS durch den jeweiligen TI-Messenger-Client unterstützt werden. Funktionalitäten, welche durch die Matrix Foundation beschrieben wurden, aber nicht Teil dieser Spezifikation sind und keine Fallbacks bieten, DÜRFEN NICHT implementiert werden, um die Interoperabilität nicht zu gefährden.

5.1 Authentifizierungsverfahren

TI-Messenger-Clients MÜSSEN mindestens die folgenden Authentifizierungsverfahren unterstützten:

- **SSO Login** gemäß [Client-Server API#SSO client login/authentication] und
- **OpenID-Connect** gemäß [Client-Server API#OpenID]

Wird ein in der Organisation bereits genutztes Authentifizierungsverfahren verwendet, so MUSS der TI-Messenger-Client die Eingabe der dafür benötigen Client Credentials unterstützen.

Zusätzlich MUSS der Hersteller eines TI-Messenger-Clients sicherstellen, dass eine Erstellung von Gäste-Accounts verhindert wird.

5.2 Matrix Client-Server API

Die Kernbestandteile des TI-Messenger-Clients basieren auf der Matrix Client-Server API. Diese umfasst neben dem eigentlichen Funktionsumfang für einen Ad-hoc-Nachrichtendienst auch die Verwaltung der Sessions, Benachrichtigungen etc., worauf in dieser Spezifikation nicht weiter eingegangen wird. TI-Messenger-Clients MÜSSEN die Matrix Client-Server API gemäß [Client-Server API] umsetzen. Bei der Umsetzung der Matrix Client-Server API ist folgendes zu beachten:

Room Upgrades

TI-Messenger-Clients MÜSSEN die Matrix-Spezifikation gemäß [Client-Server API#Room Upgrades] implementieren. TI-Messenger-Clients MÜSSEN mit Room Upgrades umgehen können. Der Nutzer SOLLTE NICHT bemerken, dass eine neue Raumversion vorliegt.

Send-to-Device messaging

TI-Messenger-Clients MÜSSEN die Matrix-Spezifikation gemäß [Client-Server API#Send-to-Device messaging] implementieren.

Geräteverwaltung

TI-Messenger-Clients MÜSSEN eine Geräteverwaltung für die eigenen Geräte eines Nutzers, unterstützen. TI-Messenger-Clients MÜSSEN die Matrix-Spezifikation gemäß [Client-Server API#Device Management] ausschließlich für die eigene Geräteverwaltung implementieren. Bei der Implementierung DARF NICHT die Geräteverwaltung für die Geräte anderer Nutzer in einem Chatraum sowie für die Geräte aller Nutzer eines Messenger-Services unterstützt werden.

Ende-zu-Ende-Verschlüsselung

TI-Messenger-Clients MÜSSEN die Matrix-Spezifikation gemäß [Client-Server API#End-to-End Encryption] implementieren und unterstützen. Der TI-Messenger-Clients MÜSSEN verhindern, dass nicht Ende-zu-Ende verschlüsselte Nachrichten versendet werden.

Reporting von Inhalten

TI-Messenger-Clients MÜSSEN die Matrix-Spezifikation gemäß [Client-Server API#Reporting Content] implementieren und den Nutzern die Möglichkeit geben, unerwünschten Inhalt an Nutzer in der Rolle "Org-Admin" zu melden.

5.2.1 Sofortnachrichten

TI-Messenger-Clients MÜSSEN eine Funktion anbieten, um Sofortnachrichten gemäß [Client-Server API#Instant Messaging] in einem Chatraum austauschen zu können. Ein TI-Messenger-Client MUSS sicherstellen, dass alle eingehenden und ausgehenden Events in der richtigen chronologischen Reihenfolge dem Nutzer angezeigt werden. Ein TI-Messenger-Client MUSS eine Wiederholungslogik für das Senden von Nachrichten unterstützen. TI-Messenger-Clients MÜSSEN die MXID eines Akteurs verstecken und den Displaynamen anzeigen. TI-Messenger-Clients MÜSSEN Nutzer informieren, falls ein Event nicht oder fehlerhaft versendet wurde.

Die folgenden `Events` und `Msgtypes` MÜSSEN vom TI-Messenger-Client unterstützt werden:

Tabelle 2: Events und Msgtypes

Events	Msgtypes
`m.room.message`	`m.text`
`m.room.name`	`m.emote`
`m.room.topic`	`m.notice`
`m.room.avatar`	`m.image`
	`m.file`
	`m.audio`
	`m.location`

	`m.video`

Nachrichten in Matrix können sowohl im Plaintext als auch in HTML-formatierter Form versendet werden. Für den Fall, dass ein TI-Messenger-Client keine formatierten Nachrichten unterstützt MUSS ein Fallback für beispielsweise Replies als Plaintext gemäß [Client-Server API#Fallbacks for rich replies] möglich sein.

Dabei MUSS der TI-Messenger-Client folgende Fallback Events unterstützen:

- Fallback für Antworten/Zitieren und
- Fallback für `m.text`, `m.notice`

Hinweis: Unter einem Fallback versteht man, dass der TI-Messenger-Client neben dem formatierten Body auch einen unformatierten Body sendet, welcher von TI-Messenger-Clients ohne die jeweilige Formatierung genutzt werden kann.

5.2.2 Direktnachrichten

TI-Messenger-Clients MÜSSEN eine Funktion anbieten, um Direktnachrichten gemäß [Client-Server API#Direct Messaging] mit anderen Nutzern des TI-Messenger-Dienstes auszutauschen. Direktnachrichten bedeutet, dass ein Chatraum nur zwischen zwei Akteuren erstellt wird. Dieser Chatraum kann nicht um weitere Akteure erweitert werden. Soll ein Chatraum für mehr als zwei Akteure erstellt werden, MUSS Group Messaging (Gruppenunterhaltungen) verwenden werden.

Die folgenden Möglichkeiten MÜSSEN dabei vom TI-Messenger-Client angeboten werden:

Tabelle 3:Ablauf - Direktnachrichten

Direktnachrichten zwischen Akteuren innerhalb einer Organisation	
Userstory: Suchen eines Akteurs über das Nutzerverzeichnis des Matrix-Homeservers	1. Akteur möchte eine neue Unterhaltung starten 2. TI-Messenger-Client zeigt alle Akteure seiner Organisation im Nutzerverzeichnis des Matrix-Homeservers an 3. Akteur wählt einen Gesprächspartner aus und startet den Chat Der TI-Messenger-Client zeigt an, dass es sich um einen Direktchat handelt. Eine Umwandlung in einen Gruppenchat ist nicht möglich.
Direktnachrichten zwischen Akteuren außerhalb einer Organisation	
Userstory: Suche eines Akteurs über das Personenverzeichnis des VZD-FHIR-Directory	1. Akteur A in der Rolle "User-HBA" möchte eine neue Unterhaltung mit Akteur B in der Rolle "User-HBA" starten 2. Akteur A durchsucht das Personenverzeichnis des VZD-FHIR-Directory nach Akteur B

	3. TI-Messenger-Client zeigt Profil (z. B. Name, Organisationszugehörigkeit, Berufsgruppe etc.) von Akteur B an 4. Akteur A startet den Chat mit Akteur B Der TI-Messenger-Client zeigt an, dass es sich um einen Direktchat handelt. Eine Umwandlung in einen Gruppenchat ist nicht möglich.
Userstory: Austausch der Kontaktdaten mittels QR-Scan	1. Akteur A und Akteur B treffen sich in Person 2. Akteur A und Akteur B wählen jeweils im TI-Messenger-Client "neue Unterhaltung starten" aus 3. Akteur A wählt "QR-Code teilen" aus 4. Akteur B wählt "QR-Code scannen" aus und scannt "QR-Code" von Akteur A und erhält die MXID von Akteur A 5. Akteur A und Akteur B klicken "weiter" 6. Akteur B bekommt einen QR-Code angezeigt, Akteur A bekommt den QR-Code Scanner angezeigt 7. Akteur A scannt den QR-Code von Akteur B 8. Akteur B kann optional die Eintragung der MXID von Akteur A in seiner Freigabeliste durchführen 9. Akteur A bekommt einen Dialog angezeigt, dass der Chatraum erstell wird, Akteur B kann den QR-Code schließen Der TI-Messenger-Client zeigt an, dass es sich um einen Direktchat handelt. Eine Umwandlung in einen Gruppenchat ist nicht möglich.

5.2.3 Gruppenunterhaltungen

TI-Messenger-Clients MÜSSEN eine Funktion anbieten, um Gruppenunterhaltungen zu starten und Nachrichten innerhalb einer Chatgruppe mit unbegrenzt vielen Nutzern des TI-Messenger-Dienstes auszutauschen. TI-Messenger-Clients MÜSSEN alle Teilnehmer einer Chatgruppe anzeigen können. Darüber hinaus MÜSSEN TI-Messenger-Clients alle Teilnehmer einer Gruppe benachrichtigen, wenn ein weiterer Teilnehmer in die Chatgruppe hinzugefügt wurde. Teilnehmer dürfen nur mittels Einladung in eine Chatgruppe hinzugefügt werden. Chaträume, die mit einer Organisation geführt werden sollen, MÜSSEN grundsätzlich Group Messaging verwenden.

Die folgenden Möglichkeiten MÜSSEN dabei vom TI-Messenger-Client angeboten werden:

Tabelle 4: Ablauf - Gruppenunterhaltungen

Gruppenunterhaltungen zwischen Akteuren innerhalb einer Organisation

Userstory: Suchen eines Akteurs über das Nutzerverzeichnis des Matrix-Homeservers	1. Akteur möchte eine neue Gruppenunterhaltung starten. 2. TI-Messenger-Client zeigt alle Akteure seiner Organisation im Nutzerverzeichnis des Matrix-Homeservers an 3. Akteur wählt Gesprächspartner aus. 4. Gesprächspartner werden in die Gruppenunterhaltung eingeladen. 5. Akteur kann weitere Gesprächspartner hinzufügen.
Gruppenunterhaltungen zwischen Akteuren außerhalb einer Organisation	
Userstory: Suche eines Akteurs über das Organisationsverzeichnis des VZD-FHIR-Directory	1. Akteur möchte eine Nachricht an eine andere Organisation senden und eine Gruppenunterhaltung starten 2. Akteur durchsucht das Organisationsverzeichnis des VZD-FHIR-Directory nach der Organisation 3. Der TI-Messenger-Client zeigt das Profil der Organisation (z. B. Name, Typ, Kontaktmöglichkeiten etc.) an 4. Akteur selektiert die MXID eines Akteurs der Organisation und startet einen Chat mit diesem
Userstory: Suche eines Akteurs über das Organisationsverzeichnis des VZD-FHIR-Directory um weitere Akteure in die Gruppenunterhaltung einzuladen	1. Akteur möchte weitere Akteure anderer Organisationen in die bestehende Chatgruppe einladen 2. Akteur durchsucht das Organisationsverzeichnis des VZD-FHIR-Directory nach der Organisation 3. TI-Messenger-Client zeigt das Profil der Organisation (z. B. Name, Typ, Kontaktmöglichkeiten) an 4. Akteur lädt den Akteur der Organisation in die bestehende Gruppenunterhaltung ein
Userstory: Suche eines Akteurs über das Nutzerverzeichnis des Matrix-Homeservers oder über das Personenverzeichnis des VZD-FHIR-Directory	1. Akteur möchte weitere Akteure in die bestehende Chatgruppe einladen 2. Akteur durchsucht entweder das Nutzerverzeichnis seiner Organisation oder das Personenverzeichnis des VZD-FHIR-Directory für die Einladung eines Akteurs außerhalb seiner Organisation 3. Akteur wählt einen gefundenen Akteur aus 4. Akteur wird in bestehende Chatgruppe eingeladen

998

5.2.4 Push-Benachrichtigungen

TI-Messenger-Clients für mobiles Szenarien MÜSSEN die Matrix-Spezifikation gemäß [Client-Server API#Push Notifications] implementieren. Die folgende Abbildung zeigt den Fluss von Push-Benachrichtigungen, die an ein Mobiltelefon gesendet werden, bei dem die Push-Benachrichtigungen über den Anbieter des Mobiltelefons übermittelt werden.

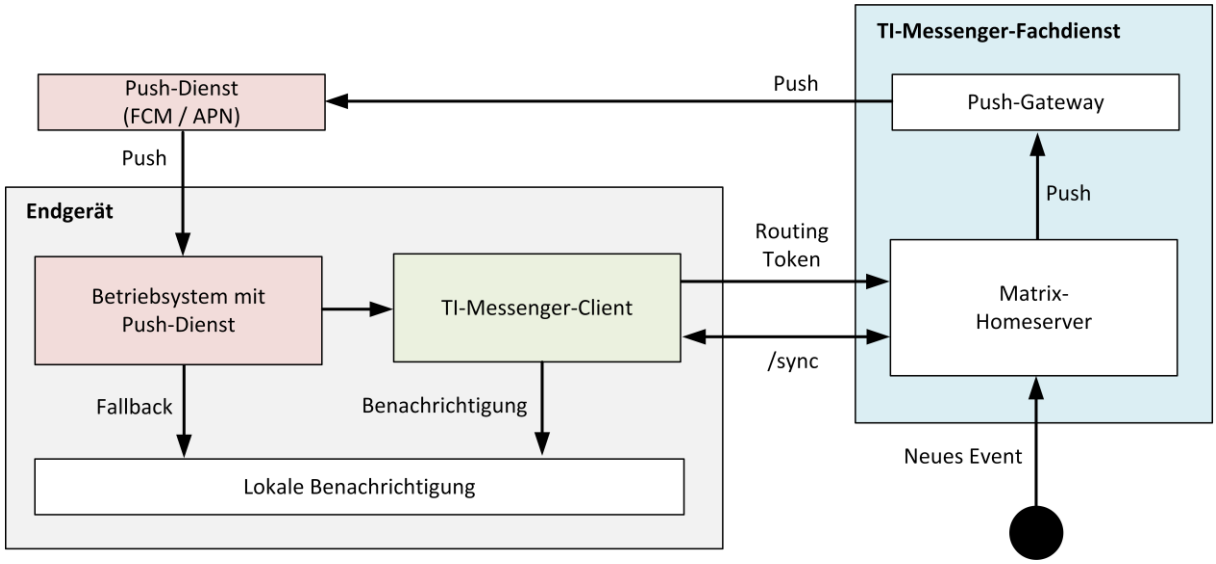

Abbildung 7: Push-Benachrichtigung für Endgeräte

Hinweis: In der Abbildung wurde der Messenger-Proxy aus Gründen der Übersichtlichkeit nicht dargestellt.

Fluss:

1. Der TI-Messenger-Client meldet sich bei einem Matrix-Homeserver an.
2. Der TI-Messenger-Client meldet sich beim Push-Anbieter an und erhält ein Routing-Token.
3. Der TI-Messenger-Client verwendet die Matrix-Client/Server-API, um einen "Pusher" hinzuzufügen, indem die URL des Push-Gateways angegeben wird, das für den TI-Messenger-Client konfiguriert ist und gibt das Routing-Token weiter.
4. Der Matrix-Homeserver leitet Push-Benachrichtigungen an das unter der URL angegebene Push-Gateway. Das Push-Gateway leitet diese Benachrichtigung an den Push-Anbieter weiter und übergibt dabei das Routing-Token zusammen mit allen erforderlichen privaten Anmeldeinformationen, die der Anbieter zum Senden von Push-Benachrichtigungen benötigt.
5. Der Push-Anbieter sendet die Benachrichtigung an das Endgerät.
6. Das Betriebssystem des Endgeräts reicht die Benachrichtigung an den TI-Messenger-Client weiter.
7. Der TI-Messenger-Client entschlüsselt die Benachrichtigung.
8. Der TI-Messenger-Client synchronisiert sich mit dem Matrix-Homeserver und zeigt die Benachrichtigung lokal an.

Push-Anbieter

Ein Push-Anbieter ist ein vom Gerätehersteller verwalteter Dienst, der Benachrichtigungen direkt an das Endgerät senden kann. Ein mobiler TI-Messenger-Client MUSS den jeweiligen Push-Anbieter des Systems unterstützen.

Push-Gateway

Ein Push-Gateway wird vom TI-Messenger-Anbieter zur Verfügung gestellt und ist ein Server, der Ereignisbenachrichtigungen von Matrix-Homeservern empfängt und diese an andere Dienste weiterleitet . Die TI-Messenger-Clients erhalten organisatorisch ein Routing-Token durch den TI-Messenger-Anbieter und teilen dem Matrix-Homeserver mit, an welches Push-Gateway die Benachrichtigungen gesendet werden sollen. Ein TI-Messenger-Client für mobile Szenarien MUSS organisatorisch mit dem Push-Gateway des TI-Messenger-Anbieters verknüpft sein. Der TI-Messenger-Client MUSS sicherstellen, dass das Routing-Token sicher auf dem Endgerät verwahrt wird und nicht missbräuchlich verwendet werden kann.

Push-Regel

Eine Push-Regel ist eine einzelne Regel, die festlegt, unter welchen Bedingungen ein Ereignis an ein Push-Gateway weitergeleitet und wie die Benachrichtigung präsentiert werden soll. Diese Regeln werden auf dem Matrix-Homeserver des Benutzers gespeichert. Der TI-Messenger-Client MUSS Nutzern die Möglichkeit geben, Push-Regeln für jeden Raum zu erstellen und anzuzeigen.

Push-Regelsatz

Ein Push-Regelsatz deckt einen Satz von Regeln nach bestimmten Kriterien ab. Beispielsweise können einige Regeln nur für Nachrichten von einem bestimmten Absender, einem bestimmten Raum oder standardmäßig angewendet werden. Der Push-Regelsatz enthält den gesamten Satz an Geltungsbereichen und Regeln. Ein TI-Messenger-Client für mobile Szenarien MUSS dem Nutzer Möglichkeiten anbieten Push-Regelsätze zu verwalten.

Opt-In

Der Hersteller eines TI-Messenger-Clients MUSS ein Opt-In Verfahren für Push-Benachrichtigungen durch Nutzer bereitstellen. Das Opt-In Verfahren MUSS jeweils pro Endgerät bereitgestellt werden.

5.3 Administrationsfunktionen

Der TI-Messenger-Client mit Administrationsfunktionen ist ein Client für Akteure einer Organisation in der Rolle "Org-Admin". Dieser wird im Kontext des TI-Messenger-Dienstes auch als Org-Admin-Client bezeichnet. Der Org-Admin-Client dient der komfortablen Verwaltung der Messenger-Services bei einem TI-Messenger-Fachdienst. Die Bereitstellung des Org-Admin-Clients KANN als eigenständiger Client erfolgen oder

als eine Integration in einen TI-Messenger-Client für Akteure. Sofern reguläre Nutzerfunktionen und Administrationsfunktionen in dem selben Client angeboten werden, MUSS auf eine klar erkennbare Unterscheidung zwischen Nutzer- und Administrationsfunktionen geachtet werden. TI-Messenger-Clients mit Administrationsfunktionen MÜSSEN die Matrix-Spezifikation gemäß [Client-Server API#Server Administration] implementieren. Im Folgenden werden die durch den Org-Admin-Client bereitzustellenden Administrationsfunktionen genauer beschrieben.

Der Org-Admin-Client MUSS die Administration von Akteuren und Geräten auf den seiner Organisation zugeordneten Messenger-Services ermöglichen. Ebenfalls MUSS der Org-Admin-Client Sessions von angemeldeten Geräten auf dem Messenger-Service verifizieren und invalidieren können. Das bedeutet zum Beispiel, dass ein Akteur in der Rolle "Org-Admin" einen TI-Messenger-Client eines Akteurs abmelden kann. Darüber hinaus MUSS der Org-Admin-Client das Senden von Informationen/Systemmeldungen an die an einem Messenger-Service angemeldeten TI-Messenger-Clients ermöglichen.

Mit dem Org-Admin-Client besteht die Möglichkeit im Namen der Organisation FHIR-Ressourcen im VZD-FHIR-Directory zu verwalten. Hierfür MUSS der Org-Admin-Client die FHIR-Ressourcen *HealthcareService* sowie *PractitionerRole* über die Schnittstelle `/owner` im VZD-FHIR-Directory administrieren können. Ebenfalls MUSS der Org-Admin-Client über die Schnittstelle `/search` Einträge im VZD-FHIR-Directory lesen können. Für das Administrieren von Datensätze auf dem VZD-FHIR-Directory MUSS der Org-Admin-Client zunächst dem Akteur in der Rolle "Org-Admin" die betreffenden Einträge anzeigen bevor dieser die Daten durch Aufruf der`/owner` Schnittstelle im VZD-FHIR-Directory ändert.

Über den Org-Admin-Client MUSS es möglich sein Funktionsaccounts in das VZD-FHIR-Directory als `Endpoint` einer *HealthcareService* Ressource einer Organisation einzutragen. Bei der Konfiguration des Endpoints durch den Org-Admin MUSS der Displayname einen Marker enthalten, der ihn als Chatbot ausweist.

Zusammenfassung

- Benutzerverwaltung (Liste aller Akteure, Anlegen, Bearbeiten, Löschen)
- Geräteverwaltung (Anzeigen, Abmelden, Löschen aller Geräte eines Messenger-Service seiner Organisation)
- die Verwaltung von Einträgen im VZD-FHIR-Directory
- Systemmeldungen an Akteure eines Messenger-Services senden (z. B. Wartungsfenster bekannt machen)
- Einrichtung von Funktionsaccounts

5.4 Weitere Funktionen

Im folgenden Kapitel werden weitere Funktionalitäten beschrieben, die der TI-Messenger-Client implementieren MUSS.

Anmeldung an einem Messenger-Service

Der TI-Messenger-Client KANN beim Anmeldevorgang dem Akteur eine Liste aller vom TI-Messenger-Anbieter unterstützten Messenger-Services anzeigen. Wird dies vom

Anbieter nicht unterstützt so MUSS dem Akteur eine Möglichkeit angeboten werden, den gewünschten Messenger-Service konfigurieren zu können.

Hinweis: Die Bereitstellung der vom Akteur zu verwendenden Parameter (z. B. Matrix-Domain des Messenger-Service) bleibt dem jeweiligen Anbieter überlassen.

Authentifizierungsmaske

Der TI-Messenger-Client MUSS dem Akteur beim Anmeldevorgang eine Authentifizierungsmaske mit den vom Messenger-Service unterstützten Authentifizierungsverfahren anzeigen.

Erstellung des Localparts

Der TI-Messenger-Client KANN bei der Erstellung des Localparts der MXID eines Akteurs sicherstellen, dass keine personenbezogenen Daten erkennbar sind. Dazu KANN der TI-Messenger-Client den Localpart der verwendeten MXID des Akteurs als Base32 SHA256 Hash berechnen. Wird diese Variante zur Erstellung des Localparts der MXID nicht gewünscht, kann dies ein Akteur deaktivieren.

Beispiel einer MXID:

```
@74c1fecc710ce4c8a8bbe310fbc5954c2a5e1e9ef5f70d651da1bfc4c9abe43f:<domain>.de
```

ML-124045 - Base32 SHA256 Hash
Der TI-Messenger-Client SOLL für die MXID einen Hash-Wert mittels Base32 SHA256 berechnen.
[<=]

Displayname

Der TI-Messenger-Client MUSS sicherstellen, dass ein Akteur seinen eigenen Displaynamen nicht ändern kann.

ML-132303 - Editierbarkeit von Displaynamen
Das Editieren des Displayname eines Akteurs in der Rolle "User / User-HBA" ist durch den Akteur selbst nicht möglich.
[<=]

Identifikationsmerkmale

Zur Sicherstellung, dass nur zugelassenen TI-Messenger-Clients verwendet werden, MUSS durch den TI-Messenger-Client-Hersteller eine client_id in den TI-Messenger-Client implementiert werden. Diese MUSS der TI-Messenger-Client-Hersteller dem TI-Messenger-Anbieter nach jeder Änderung zur Verfügung stellen, damit diese bei der Prüfung am Messenger-Proxy eines Messenger-Services verwendet werden können. Die client_id MUSS bei jedem Aufruf im HTTP Header übertragen werden.

Dabei ist folgendes zu verwenden:

```
client_id: <sample_id>.<version>
```

Verbindung nur mit in der Föderation vorhandenen Messenger-Services

Der TI-Messenger-Client MUSS sicherstellen, dass eine Nutzung nur mit Matrix-Homeservern möglich ist die Teil der Föderation sind. Verbindet sich der TI-Messenger-Client mit einem Matrix-Homeserver, welcher nicht Teil der Föderation ist, MUSS der Akteur direkt abgemeldet werden.

Third Party Networks / Bridging

Das Bridging zu Drittsystemen zu Zwecken der Kommunikation (Austausch von Matrix-Events) DARF NICHT stattfinden. Das Bridging zu Drittsystemen ist nur zum Archivieren von Chatinhalten erlaubt. Es MUSS sichergestellt werden, dass eine Ende-zu-Ende Verschlüsselung mittels OLM/MEGOLM zu jeder Zeit erfolgt.

Ende-zu-Ende Verschlüsselung

Der TI-Messenger-Client MUSS sicherstellen, dass sämtliche Nachrichteninhalte Ende-zu-Ende gemäß [Client-Server API#End-to-End Encryption] verschlüsselt werden. Das Senden von Nachrichten ohne Ende-zu-Ende Verschlüsselung MUSS technisch unterbunden werden.

Nutzerverzeichnis eines Messenger-Services

Der TI-Messenger-Client MUSS eine Funktion bereitstellen, dass Akteure auf dem jeweiligen Matrix-Homeserver eines Messenger-Services ein Verzeichnis von anderen Akteuren innerhalb ihrer Organisation aufrufen und durchsuchen können.

Suchabfragen VZD-FHIR-Directory

Der TI-Messenger-Client MUSS eine Funktion bereitstellen, dass Akteure das VZD-FHIR-Directory nach Ressourcen durchsuchen können. Der TI-Messenger-Client MUSS eine Funktion bereitstellen, um Detailinformationen, der auf dem VZD-FHIR-Directory gespeicherten Ressourcen, anzeigen zu können. Weitere Spezifikationen finden sich in [gemSpec_VZD_FHIR_Directory].

Administration der Freigabeliste

Der TI-Messenger-Client MUSS eine Funktion bereitstellen, mit der ein Akteur eine Freigabe für Einladungen in einen Chatraum für andere Akteure ermöglicht. Hierfür MUSS der TI-Messenger-Client die Operationen des RESTful Webservice `/tim-contact-mgmt/v1.0` gemäß [api-messenger#TiMessengerContactManagement.yaml] in der Version 1.0 am Registrierungs-Dienst aufrufen. Der TI-Messenger-Client MUSS es ermöglichen, dem Akteur eine Liste anzuzeigen, in der alle Akteure die eine Freigabe erhalten haben gezeigt werden. Ebenfalls MUSS der TI-Messenger-Client es ermöglichen, Freigaben zu erstellen und diese zu bearbeiten.

Hinweis: Die Freigabeliste wird benötigt, wenn eine Kontaktaufnahme der Akteure in Person mittels eines QR-Scan erfolgte. Es ist empfehlenswert die Freigabe des Einladenden Akteurs in diesem Zusammenhang auf der Seite des Einzuladenden im TI-Messenger-Client zu ermöglichen.

Archivierung von Gesprächsinhalten

Um den Dokumentationspflichten von Ärzten nachzukommen, ist es notwendig, dass Chatverläufe mit Fallbezug auch über Löschung der Gesprächsdaten hinaus aufbewahrt werden können. Daher MUSS der TI-Messenger-Client sicherstellen, dass Chatverläufe aus dem TI-Messenger-Client extrahiert werden können, damit diese beispielweise in Archivsysteme überführt werden können. Die gematik macht keine Vorgaben wie die Archivierung zu gestalten ist, da sowohl die Art der Archivierung als auch die anzubindenden Systeme stark variieren.

Fallbezogene Kommunikation

Unter einer fallbezogenen Kommunikation versteht man die Möglichkeit der Klassifizierung eines Chatverlaufes. Dabei KANN dieser beispielweise einen Personenbezug oder einen Fachbezug zu einem Chatraum haben. Um dies zu ermöglichen MUSS der TI-Messenger-Client eine fallbezogene Kommunikation unterstützen. Hierfür MUSS der TI-Messenger-Client FHIR-Ressourcen in den Room-State eines existierenden Chatraumes hinzufügen.

Die Profile der FHIR-Ressourcen befinden sich im Simplifier Projekt [simplifier].

Die Canonical URLs der Ressourcen enthalten immer:
`http://gematik.de/fhir/TIM/CaseReference`

6 Anhang A – Verzeichnisse

6.1 Abkürzungen

Kürzel	Erläuterung
APN	Apple Push Notification Service
CC	Common Criteria
FCM	Firebase Cloud Messaging
FHIR	Fast Healthcare Interoperable Resources
IDP	Identity Provider
JSON	JavaScript Object Notation
MXID	Matrix-ID
OLM/MEGOLM	Verschlüsselungsprotokoll für Nachrichteninhalte, spezifiziert durch die Matrix Foundation
OWASP	Open Web Application Security Project
PVS	Praxisverwaltungssystem
SMC-B	Institutionenkarte (Security Module Card Typ B)
SSO	Single Sign-on
SSSS	Secure Secret Storage and Sharing
TI	Telematikinfrastruktur
TLS	Transport Layer Security
VZD	Verzeichnisdienst

6.2 Glossar

Begriff	Erläuterung

MXID	Eindeutige Identifikation eines TI-Messenger-Nutzers

6.3 Abbildungsverzeichnis

Abbildung 1: Systemüberblick (Vereinfachte Darstellung) 9
Abbildung 2: Benachbarte Komponenten des TI-Messenger-Clients.....10
Abbildung 3: internes Testtreiber-Modul 26
Abbildung 4: externes Testtreiber-Modul 27
Abbildung 5: Testumgebung für Herstellertests 28
Abbildung 6: Testumgebung gematik 29
Abbildung 7: Push-Benachrichtigung für Endgeräte.....35

6.4 Tabellenverzeichnis

Tabelle 1: Übersicht der Komponenten und deren Funktionen 10
Tabelle 2: Events und Msgtypes 31
Tabelle 3:Ablauf - Direktnachrichten 32
Tabelle 4: Ablauf - Gruppenunterhaltungen.....33

6.5 Referenzierte Dokumente

6.5.1 Dokumente der gematik

Die nachfolgende Tabelle enthält die Bezeichnung der in dem vorliegenden Dokument referenzierten Dokumente der gematik zur Telematikinfrastruktur. Der mit der vorliegenden Version korrelierende Entwicklungsstand dieser Konzepte und Spezifikationen wird pro Release in einer Dokumentenlandkarte definiert; Version und Stand der referenzierten Dokumente sind daher in der nachfolgenden Tabelle nicht aufgeführt. Deren zu diesem Dokument jeweils gültige Versionsnummern sind in der aktuellen, von der gematik veröffentlichten Dokumentenlandkarte enthalten, in der die vorliegende Version aufgeführt wird.

[Quelle]	Herausgeber: Titel

[api-messenger]	gematik: api-ti-messenger https://github.com/gematik/api-ti-messenger/
[gemGlossar]	gematik: Einführung der Gesundheitskarte – Glossar
[gemSpec_TI-Messenger-Dienst]	gematik: Spezifikation TI-Messenger-Dienst
[gemSpec_TI-Messenger-FD]	gematik: Spezifikation TI-Messenger-Fachdienst
[gemSpec_Krypt]	gematik: Übergreifende Spezifikation - Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur
[gemSpec_VZD_FHIR_Directory]	gematik: Spezifikation Verzeichnisdienst FHIR-Directory
[gemKPT_Betr]	gematik: Betriebskonzept Online-Produktivbetrieb
[simplifier]	gematik: TI-Messenger https://simplifier.net/tim

6.5.2 Weitere Dokumente

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[BITV 2.0]	Verordnung zur Schaffung barrierefreier Informationstechnik nach dem Behindertengleichstellungsgesetz (Barrierefreie-Informationstechnik-Verordnung - BITV 2.0) https://www.gesetze-im-internet.de/bitv_2_0/BJNR184300011.html
[BSI-TR-03166]	BSI TR-03166 - Technical Guideline for Biometric Authentication Components in Devices for Authentication https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TR03166/BSI-TR-03166.pdf
[Client-Server API]	Matrix Foundation: Matrix Specification - Client-Server API https://spec.matrix.org/v1.2/client-server-api/
[DSK2021]	Datenschutzkonferenz (DSK): Stellungnahme der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 29. April 2021 https://www.datenschutzkonferenz-online.de/media/st/20210429_DSK_Stellungnahme_Messengerdienste_Krankenhausbereich.pdf

[ISO 9241]	Ergonomics of human-system interaction https://www.iso.org
[OWASP MobileTop 10]	OWASP Mobile Top 10 https://owasp.org/www-project-mobile-top-10/
[OWASP Proactive Control]	OWASP Proactive Controls https://owasp.org/www-project-proactive-controls/
[Testtreiber API]	Testtreiber API https://github.com/gematik/api-ti-messenger/tree/master/src/openapi

1261