Elektronische Gesundheitskarte und Telematikinfrastruktur

Spezifikation
TI-Messenger-Client

Version:	1.1.0~~.0~~
Revision:	~~408232~~482259
Stand:	~~01.10.2021~~29.07.2022
Status:	freigegeben
Klassifizierung:	öffentlich
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	29.07.2022		Überarbeitung folgender Features: – Erreichbarkeit einzelner Organisationseinheiten mittels Funktionsaccounts – Öffnung des TI-Messengers für Drittsysteme durch clientseitige Schnittstellen zur Integration z.B. ins Praxisverwaltungssystem – schnelles Finden von Kontaktdaten durch Zugriff auf FHIR-basiertes Adressbuch	gematik

Inhaltsverzeichnis

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~~Krankenversicherungsorganisationen 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 ~~Akzeptanzkriterium~~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 ~~Nutzers~~Akteurs installiert und ermöglicht eine sichere, ~~chatbasierte~~nachrichtenbasierte Kommunikation mit anderen ~~Teilnehmern~~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 ~~der~~des Messenger-Services eines TI-Messenger-~~Fachdienste~~Fachdienstes bereitgestellt werden.

Die Kommunikation zwischen ~~Teilnehmern~~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 ~~Schlüssel zur Entschlüsselung werden nur mit verifizierten Geräten innerhalb des jeweiligen Raumes geteilt. 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 ~~Nutzers durch zugelassene~~Akteurs mit zugelassenen TI-Messenger-Clients. Dies wird ermöglicht, indem während des Logins ~~ein~~die auf dem Client ~~hinterlegtes Zertifikat für~~ hinterlegte `client_id` durch den ~~Login verwendet~~ Messenger-Proxy überprüft wird. ~~Ein~~ Zusätzlich wird während des Anmeldevorgangs durch den TI-Messenger-Client ~~überprüft während des Logins~~am Auth-Service des VZD-FHIR-Directory geprüft, ob es sich um einen zugelassenen Matrix-Homeserver handelt.

~~Die folgende~~In der folgenden Abbildung ~~"*Systemüberblick (Vereinfachte Darstellung)*" zeigt einen Systemüberblick aller am~~sind alle beteiligten Komponenten der TI-Messenger ~~beteiligten Teilkomponenten~~-Architektur in vereinfachter Form~~.~~ dargestellt. Der in der Abbildung grün dargestellte TI-Messenger-Client zeigt die Komponente die in dieser Spezifikation beschrieben wird.

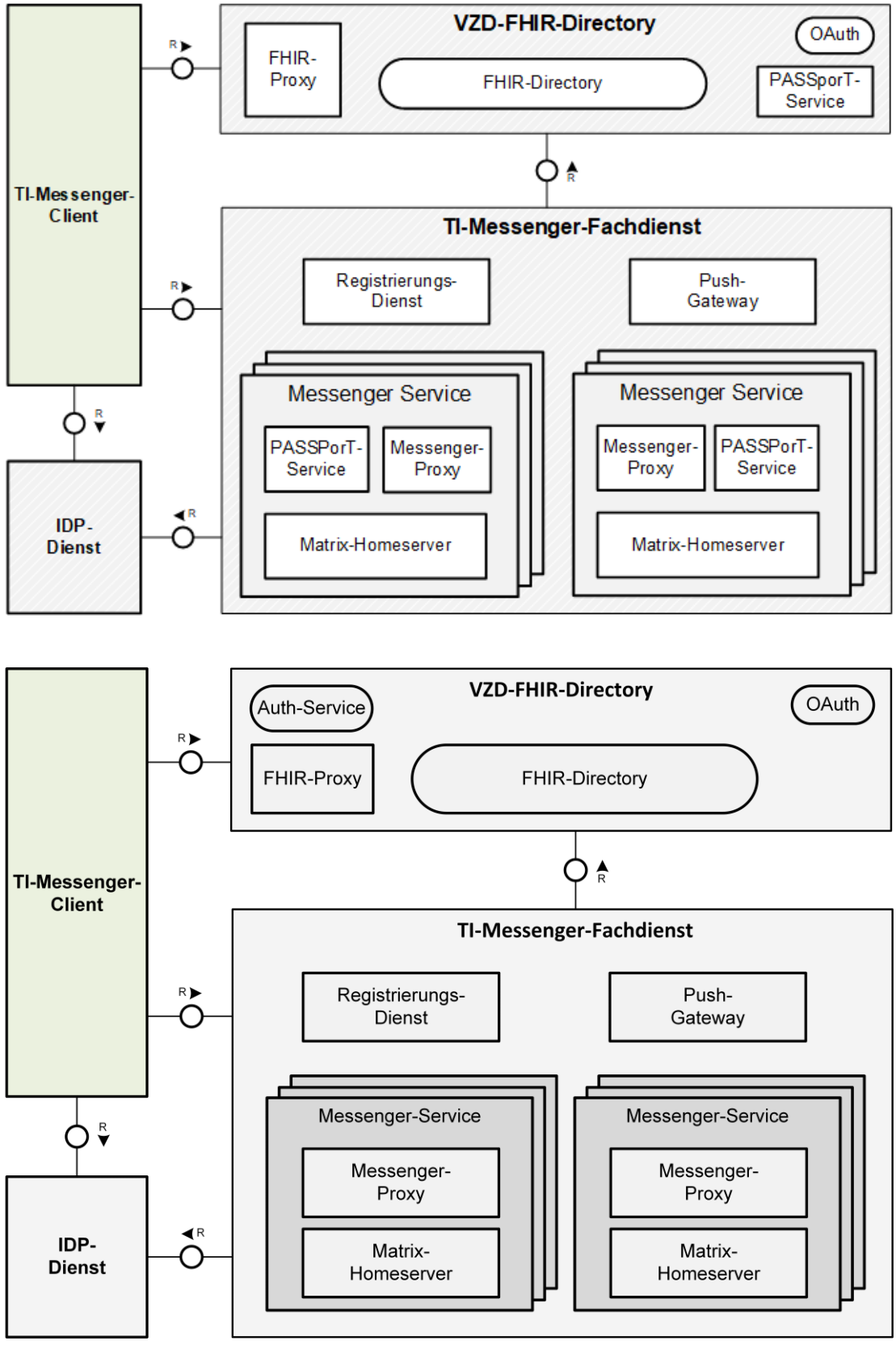


Abbildung 1: Systemüberblick (Vereinfachte Darstellung)

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:

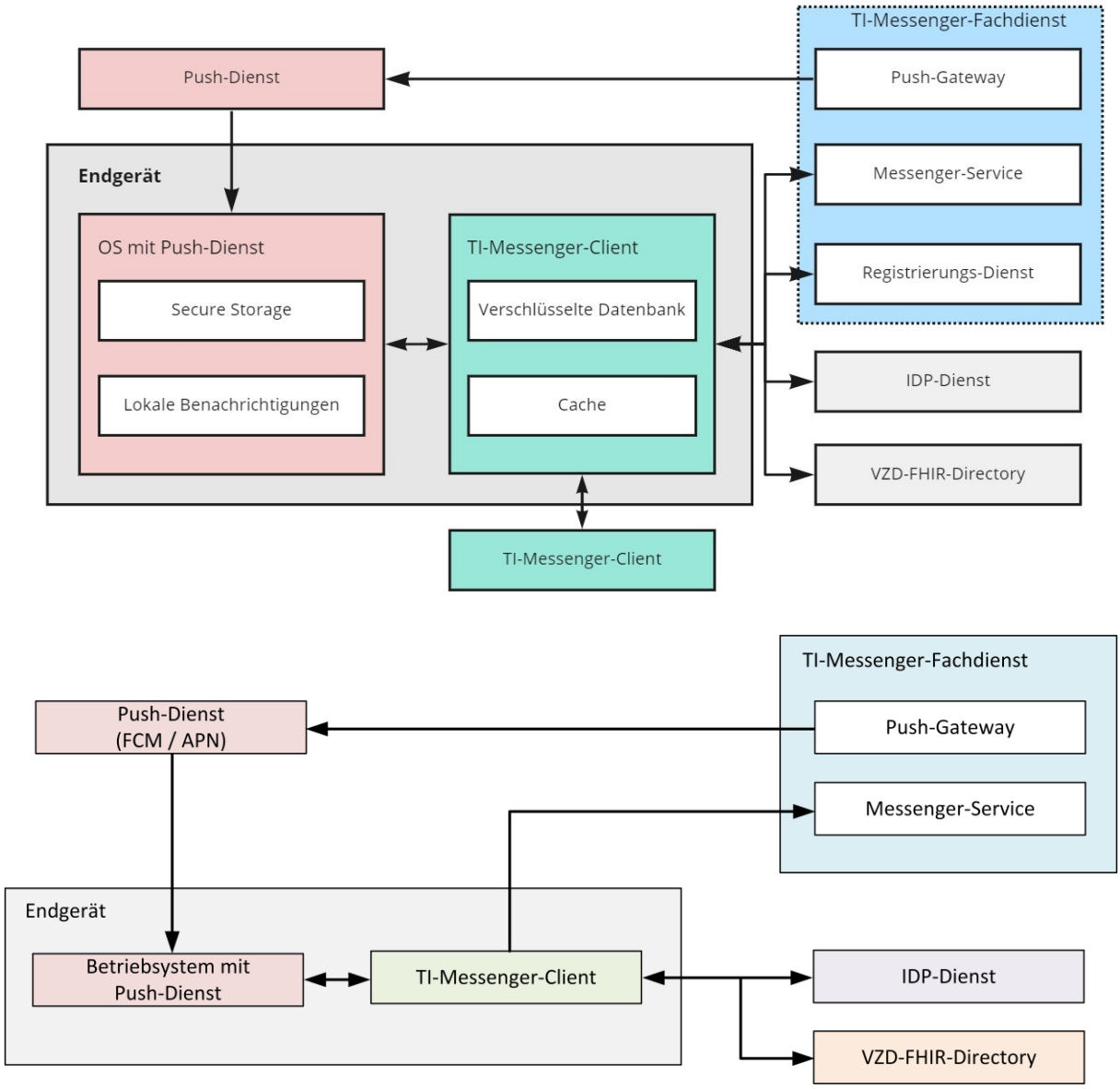


Abbildung 2: Benachbarte Komponenten des TI-Messenger-Clients

Die ~~im Folgenden~~in der Abbildung benannten Nachbarsysteme des TI-Messenger-Clients werden in der [gemSpec_TI-Messenger-Dienst] und [gemSpec_TI-Messenger-FD] hinreichend beschrieben. ~~Die in diesem Dokument zum jeweiligen Nachbarsystem genannten Punkte sollen an dieser Stelle~~Für die ~~für das Funktionieren~~Einordnung der Komponenten im Kontext des TI-Messenger-Clients ~~benötigten Funktionen benennen~~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
~~Messenger-Service~~	~~• Stellt für TI-Messenger-Clients Schnittstellen gemäß [Matrix Foundation#Client_Server] bereit~~ ~~• Liefert Matrix-OpenID-Token für Lesezugriff VZD-FHIR-Directory~~
~~Registrierungs~~Push-Dienst	~~Der TI-Messenger-Client benötigt für diverse Aktionen eine Verbindung zum Registrierungs-Dienst. Dazu gehören:~~ • ~~Bereitstellung einer Registrierungsmaske / Endpunkte für Erstellung von Messenger-Services~~ Push-Dienste (z. B. FCM / APN) sind Services von Push-Anbietern und werden für die native Unterstützung von Push-Benachrichtigungen auf mobilen Geräten benötigt.
~~IDP-Dienst~~	~~• OpenID-Connect für Schreibzugriff auf VZD-FHIR-Directory (mittels HBA/SMC-B)~~
~~VZD-FHIR-Directory~~	~~• Lesezugriff auf für einen Nutzer freigegebene, hinterlegte Attribute~~ ~~• Schreibzugriff zum Eintragen von FHIR-Ressourcen~~
~~TI-~~Messenger-~~Client~~Service	• ~~Für den Aufbau einer Kommunikation ohne das VZD-FHIR-Directory kann der TI-Messenger-Client eine direkte Verbindung zu einem anderen TI-Messenger-Client aufbauen. Ziel dieser Verbindung ist der Austausch der MXID und PASSporT, damit ein `Invite Request` durch die jeweiligen Messenger-Services validiert werden kann.~~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 eine Schnittstelle zur Pflege der persönlichen Freigabeliste bereit. • 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 authentisieren.
~~Push-Dienst~~ VZD-FHIR-Directory	• ~~Push-Dienste sind Services von Push-Anbietern und werden für die native Unterstützung von Push-~~

	~~Benachrichtigungen auf der Mehrzahl mobiler Geräte benötigt.~~ 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 ~~für unterschiedliche~~ 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 ~~Nutzer. Jeder Anbieter eines TI-Messenger-Fachdienstes MUSS für seine Nutzergruppen TI-Messenger-Clients in unterschiedlicher Ausprägung anbieten.~~ 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 ~~Client~~ wird im TI-Messenger-Kontext auch als Org-Admin-Client bezeichnet. Der Org-Admin-Client dient zur komfortablen Verwaltung der ~~jeweiligen~~ Messenger-Services bei einem TI-Messenger-Fachdienst ~~sowie der Organisationseinträge auf dem VZD-FHIR-Directory.~~. Mit dem Org-Admin-Client besteht die Möglichkeit ~~mittels SMC-B Schreibzugriffe auf das VZD-FHIR-Directory zu erhalten und~~, im Namen der Organisation FHIR-Ressourcen zur Verfügung zu stellen oder zu bearbeiten. Ebenfalls haben Administratoren einer Organisation ~~haben~~ die Möglichkeit ~~mittels~~mit Hilfe des ~~TI-Messenger~~Org-Admin-Clients ~~mit Administrationsfunktionen~~ Benutzer und Geräte auf dem jeweiligen Messenger-Service zu verwalten. ~~Es~~Darüber hinaus besteht ~~ebenfalls~~ die Möglichkeit, über den Org-Admin-Client Sessions von angemeldeten Geräten auf dem Messenger-Service zu verifizieren oder zu invalidieren ~~oder zu verifizieren.~~

. 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 ~~**Nutzer**~~die übergreifende Kommunikation innerhalb einer Organisationsstruktur des TI-Messenger-Fachdienstes administriert werden.

~~Der~~

TI-Messenger-Client für ~~Nutzer~~Akteure

Der TI-Messenger-Client für Akteure unterstützt die meisten aller, durch die Matrix-Spezifikation festgelegten Funktionalitäten eines Matrix-Messengers. ~~Nutzer~~Akteure können mit Hilfe ~~des TI-Messenger-~~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 ~~Nutzer~~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~~-Inhaber~~" haben zusätzlich die Möglichkeit, die eigene MXID als Kontaktadresse des bereits vorhandenen ~~Practitoner~~ *Practitioner*-Eintrages ~~zu setzen.~~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~~-Inhabern~~" und ermöglicht das Auffinden durch andere ~~HBA-Inhaber.~~ Akteure.

~~3.2.21.1.1 TI-Messenger-Clients für unterschiedliche~~ *Hinweis: Die beiden oben beschriebenen Ausprägungen KÖNNEN auch in einem*~~Plattformen~~

~~Anbieter eines TI-Messenger-Clients MÜSSEN einen mobilen- und einen desktopfähigen~~ *TI-Messenger-Client integriert sein. Die Art der Umsetzung obliegt dem jeweiligen TI-Messenger-Client-Hersteller.*

3.2.2 Plattformen

~~zur Verfügung stellen.~~ TI-Messenger-Clients haben je nach ~~Installationsort~~Plattform (Mobil/Stationär) unterschiedliche Anforderungen an Sicherheit, Datenschutz und ~~Funktionen.~~Funktionalität. Im Folgenden werden die zu unterstützenden Plattformen näher beschrieben~~:~~.

~~**Mobil**~~

TI-Messenger-Client für mobile Szenarien

Es handelt sich hierbei um ~~einen~~eine TI-Messenger-Client~~, der~~ Anwendung, die speziell für die Nutzung auf mobilen Geräten entwickelt wurde~~. Dabei handelt es sich um eine~~ (z. B. Android/IOS). Die Bereitstellung KANN als native mobile Anwendung erfolgen oder als eine Integration in ~~eine~~bereits bestehende ~~native Anwendung.~~Anwendungen. Die mobile Anwendung MUSS die betriebssystemseitigen Funktionen in Bezug auf Sicherheit nutzen~~ und~~. 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).

~~**Web**~~

~~Der~~

TI-Messenger-Client für stationäre Szenarien

Es handelt sich hierbei um eine 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-~~Frontend für den stationären Einsatz zur Verfügung gestellt werden. Es~~ Anwendung in einem Webbrowser ist ebenfalls möglich. Die Ver- und Entschlüsselung MUSS ~~sichergestellt werden, dass die Web-Applikation vor unerlaubten Zugriff durch andere Nutzer geschützt wird. Es~~lokal im Browser auf dem Endgerät erfolgen. Ebenfalls MUSS sichergestellt werden, dass bei

~~Aufruf des Web-Frontends~~Nutzung einer lokalen Web-Anwendung ein unerlaubter Zugriff durch Dritte aktiv verhindert wird (z. B. durch ~~Nutzer auf dem Mobilgerät ein entsprechender Nutzungshinweis angezeigt wird.~~ Invalidieren der Session oder durch eine aktive Abmeldung).

~~Desktop~~

~~Der TI-Messenger-Client KANN als native- oder Web-Applikation für Desktop-Geräte zur Verfügung gestellt werden.~~

~~Integriert~~

~~Für die Nutzung des TI-Messenger-Dienstes KANN die Integration eines TI-Messenger-Clients in existierende Primärsysteme erfolgen. Diese Primärsysteme können sowohl mobile als auch stationäre Anwendungen sein.~~

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

~~Für die~~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 ~~vom 29. April 2021 zum Thema "Technische Datenschutzanforderungen an Messenger-Dienste im Krankenhausbereich"~~gemäß [DSK2021] verwiesen. Die Inhalte der Stellungnahme werden ~~hier zusammenfassend und vereinfachend als Akzeptanzkriterium~~ an~~in~~ den ~~TI-Messenger-Client dargestellt.~~ Anforderungen~~, die durch andere Systemkomponenten sichergestellt werden, sind hier nicht dargestellt.~~ [A_22715] und [A_22955] vereinfacht zusammengefasst.

~~ML-124880 - Anforderungen aus der Konferenz der unabhängigen Datenschutzaufsichtsbehörden~~A_22715 - Anforderungen-Herstellererklärung aus der Konferenz der unabhängigen Datenschutzaufsichtsbehörden

- Der TI-Messenger-Client MUSS für den ~~Nutzer~~Akteur klar erkennbar Datenschutzinformationen bereitstellen.
- ~~—~~
- ~~Der mobile TI-Messenger-Client DARF KEINEN Zugriff (weder lesen noch schreibend) auf das Adressbuch des Endgerätes haben.~~
- Der TI-Messenger-Client MUSS eine allgemeine und selektive ~~Lösch-Funktion~~ 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 KANN eine Funktion zur Unkenntlichmachung von Ausschnitten von Bildaufnahmen implementieren.~~

- ~~Der TI-Messenger-Client MUSS bei der Nutzung von Fehleranalysetools datenschutzfreundliche Voreinstellungen (standardmäßig deaktiviert, bei opt-in klar erkennbar, etc.) treffen.~~
- ~~Der TI-Messenger-Client MUSS die Ende-zu-Ende-Verschlüsselung nach den Vorgaben unter 5.15. sowohl in Einzel- als auch Gruppenunterhaltungen fehlerfrei 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 Metadaten zu KEINEM anderen Zweck nutzen als zur Übermittlung der Kommunikation und Sicherstellung des Betriebs.~~
- Der TI-Messenger-Client MUSS sicherstellen, dass die Nutzersession bei Sperrung oder Abmeldung durch einen ~~Nutzer~~Akteur in der Rolle "Org-Admin" beendet wird.

~~Der TI-Messenger-Client DARF Standortdaten NICHT dauerhaft erheben.~~**[**<=**]**

A_23114 - App-Sperre TI-Messenger-Client
~~Der~~ TI-Messenger-~~Client MUSS über (teil-)automatisierte Updateprozesse verfügen.~~**~~[<=]~~**

~~ML-123584 - Authentisierung des Nutzers gegenüber dem TI-Messenger-Client~~Clients MÜSSEN~~Der TI-Messenger-Client MUSS über ein 2-Faktor-Authentisierungsverfahren verfügen, um sich zu authentisieren gibt der Nutzer~~ bei ~~jedem Start~~ der Entsperrung (der ~~Applikation~~ App oder des Geräts) mindestens eine ~~sechsstellige~~6-stellige PIN ~~ein, um die Applikation zu entsperren. Nach jeder Abmeldung, jedem Benutzerwechsel, jedem Schließen der Applikation, oder spätestens 12 Stunden nach letzter Entsperrung MUSS diese Authentisierung erneut vorgenommen werden~~verwenden. Alternativ ~~zum Authentisierungsmittel PIN~~ sind auch die Mittel Biometrie, starke Passphrase oder Fido-Token zulässig. Falls das ~~Merkmal Biomentrie~~Mittel Biometrie gewählt wird, MUSS es den Vorgaben ~~von~~aus [BSI-TR-03166] Kap. 2.3.1.5 oder 2.3.1.6 genügen. ~~Als zweiten Faktor MUSS der TI-Messenger-Client~~ Nach jeder Abmeldung, jedem Benutzerwechsel, jedem Schließen der Anwendung oder spätestens 12 Stunden nach letzter Entsperrung MUSS die erneute Entsperrung durch den Akteur vorgenommen werden.
Der TI-Messenger-Client MUSS prüfen, ob ~~er auf dem Gerät gestartet wurde, an welches er gebunden~~eine Gerätesperre aktiv ist. ~~Für Webclients entfällt diese Authentisierung. Diese Funktionen DÜRFEN NICHT abschaltbar sein und MÜSSEN unabhängig von den Entsperrfunktionen der Endgeräte sein.~~
~~Der Hersteller SOLL eine Sperre implementieren~~Ist eine konforme Gerätesperre aktiviert, dann muss keine zusätzlich App-Sperre vorgesehen werden. Ist keine konforme Gerätesperre aktiviert, dann ist eine konforme App-Sperre vorzusehen.
Für ein in ein Drittsystem (KIS, PVS, AVS, etc.) integriertes TI-Messenger-Clientmodul KANN eine vorhandene Sperre des übergeordneten Systems nachgenutzt werden.
App-Sperren für TI-Messenger-Clients und integrierte TI-Messenger-Clientmodule MÜSSEN vom Akteur deaktivierbar sein.
Für browserbasierte TI-Messenger-Clients ist keine App-Sperre erforderlich. Der browserbasierte Web-Client MUSS über eine Sperre verfügen, die nach längerer Inaktivität ~~an Webclients die weitere Nutzung verhindert, bis sich erneut wie zuvor beschrieben authentisiert wird.~~eine automatische Abmeldung durchführt. Die nötige Dauer der Inaktivität MUSS durch den ~~Nutzer~~Akteur konfigurierbar und per Default auf eine Stunde eingestellt sein.
[<=~~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 Fortschrittbalken dem Nutzer dargestellt werden. Dieser wird erst grün, sobald eine entsprechende Güte erreicht wurde. Der Hersteller KANN eine Funktion implementieren, die zufallsgenerierte Vorschläge für PIN oder Passphrase erstellt. Diese Vorschläge MÜSSEN auf sichere Erzeugung von Zufallszahlen gemäß [gemSpec_Krypt] basieren.~~
~~[<=~~]

~~ML-123585~~A_22717 - Verhinderung der Erstellung von Screenshots
~~Mobile~~ TI-Messenger-Clients für mobile Szenarien MÜSSEN Screenshots und Screencapturing verhindern, sofern das Betriebssystem dies zulässt, oder ~~Nutzer~~Akteure nach ~~Aufnahme~~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
~~ML-123589 - Mandantenfähigkeit von Clients~~TI-Messenger-Clients MÜSSEN verhindern~~Hersteller des TI-Messenger-Clients MÜSSEN sicherstellen, dass TI-Messenger-Clients eine geeignete Mandantentrennung unterstützen, die verhindert~~, dass bei geteilten Endgeräten ein ~~Nutzer~~Akteur des TI-Messenger-Clients auf Daten oder Funktionen der TI-Messenger-Client-Devices eines anderen ~~Nutzers~~Akteurs auf diesem Gerät zugreifen kann.
[<=]

~~ML-123610~~A_22719 - Datenschutzfreundliche MXIDs
Der TI-Messenger-Client ~~MUSS sicherstellen, dass~~ SOLL MXIDs so ~~generiert werden~~generieren, dass sie keine personenbezogenen Daten als Klarinformation beinhalten. ~~Nutzer~~Akteure des TI-Messenger~~ haben keinen~~-Clients DÜRFEN NICHT Einfluss auf die Bildung der MXID~~.~~ haben.
[<=]

~~ML-123583 - Informationspflicht bzgl. Gefahren unsicherer Endgeräte~~A_22720 - Informationspflicht bzgl. Gefahren unsicherer Endgeräte
~~Der~~Akteure eines TI-Messenger-~~Client MUSS den Nutzer~~Clients als Web-Anwendung MÜSSEN in einem Hinweistext auf die Gefahren ~~hinweisen~~hingewiesen werden, die bei ~~einem Betrieb des Clients~~ Nutzung auf Hardware, die nicht unter der Kontrolle des ~~Nutzern~~Akteurs steht, gegeben sind. Das betrifft neben geteilten Endgeräten ohne IT-Security-Überwachung insbesondere öffentlich zugängliche Endgeräte. Der ~~Nutzer~~Akteur MUSS die Empfehlung erhalten auf solchen Geräten den TI-Messenger-Client nicht zu nutzen.
Der TI-Messenger-Client MUSS den Akteur 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.
Es sind die Prüfvorschriften gemäß [BSI Frontend] zu berücksichtigen.
[<=]

~~ML-123586 - Key-Sharing zwischen Geräten eines Nutzers~~A_22721 - Key-Sharing zwischen Geräten eines Akteurs
~~Um~~TI-Messenger-Clients MÜSSEN die Matrix Vorgabe SHOULD "Key-Sharing nur für verifizierte Geräte" als MUST umsetzen.

Hinweis: Die Anforderung ist essentiell, um die Synchronisation von Nachrichteninhalten

zwischen mehreren ~~Devices~~Geräten eines ~~Nutzers zu ermöglichen, verfügt Matrix~~Akteurs über die von Matrix vorgesehene Key-Sharing-Funktionalität zu ermöglichen.
[<=~~. Der Hersteller MUSS die Matrix Vorgabe SHOULD "Key-Sharing nur für verifizierte Geräte" als MUST umsetzen.~~
~~[~~<=~~]~~**]**

~~ML-124004~~A_22722 - Key-Sharing zwischen Geräten innerhalb eines Chatraums
~~Hersteller des TI-Messenger-Clients MÜSSEN sicherstellen, dass~~ 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.
[<=**]**

~~ML-123587~~A_22723 - Versand von Dateien mittels Matrix
Für den Versand von Dateien gemäß der Matrix-Spezifikation über den TI-Messenger-Client gilt:

- ~~Der Hersteller MUSS sicherstellen, dass die~~TI-Messenger-Clients MÜSSEN Verschlüsselung für übertragene Inhalte ~~aktiviert ist~~verwenden.
- ~~Der Hersteller MUSS sicherstellen, dass~~TI-Messenger-Clients MÜSSEN in der Lage sein, mindestens Dateien mit einer Größe von ~~25MB versendet werden können~~100 MB zu versenden.
- ~~Der Hersteller SOLL~~TI-Messenger-Clients MÜSSEN über eine Größenbeschränkung zu versendender Inhalte verfügen.
- ~~—~~TI-Messenger-Clients für ~~versendete Dateien implementieren.~~
- ~~Der Hersteller MUSS sicherstellen, dass die Möglichkeit besteht,~~stationäre Szenarien KÖNNEN über eine Schnittstelle und Funktionen verfügen, mit denen empfangene und entschlüsselte Dateien an eine ~~Stelle~~Schnittstelle bekannter Virenscanner zur Schadsoftwareprüfung ~~zu übermitteln~~übermittelt und ~~prüfen zu lassen~~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 ~~Nutzer~~Akteur darüber ~~und~~sowie über den Grund informiert werden.
- ~~Nutzer~~TI-Messenger-Clients MÜSSEN Akteure bei ~~der Verwendung~~Fehlschlagen einer ~~nicht erfolgreich geprüften Datei~~Dateiprüfung auf ~~dessen~~deren Prüfstatus ~~– hingewiesen werden~~hinweisen.

Sofern ~~der Hersteller~~ TI-Messenger-Clients über eine Funktion ~~implementiert~~verfügen, Dokumente direkt über den TI-Messenger-Client ohne Nutzung von Third-party Software anzuzeigen, ~~MUSS~~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 ~~Nutzer~~TI-Messenger-Client MUSS den Akteur darüber ~~informiert werden~~informieren, dass Dokumente Schadsoftware enthalten können und welche Maßnahmen der ~~Nutzer~~Akteur zum Selbstschutz vornehmen kann.
Der TI-Messenger-Client MUSS, wenn er Dokumenteninhalte direkt anzeigt, Maßnahmen zum Schutz vor Schadsoftware in den Dokumenten umsetzen.**[**<=**]**

***Hinweis:* Maßnahmenvorschläge *zum Schutz vor Schadsoftware*:**

- Prüfen, ob ~~Dokumenten-Format~~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~~ersetzen.
- Die Anzeigesoftware des TI-Messenger-Clients in einer Sandbox betreiben.

A_23115 - Prüfung Device Integrität
TI-Messenger-Clients für mobile Szenarien MÜSSEN prüfen, ob ein Rooting des Gerätes vorliegt. Ist dies der Fall, MUSS dem Nutzer eine Warnung angezeigt werden und der Versand von Anhängen verhindert werden.
Bei der Verwendung von TI-Messenger-Clients, die auf dem Betriebssystem Android basieren, MUSS zur Integritätsprüfung Safetynet verwendet werden.
[<=]

~~ML-123588 - Abschottung der TI-Messengerinhalte~~A_22724 - Abschottung der Inhalte im TI-Messenger-Client
~~Mobile~~ TI-Messenger-Clients für mobile Szenarien MÜSSEN sicherstellen, dass Daten, die lokal gespeichert werden, ~~nicht im allgemeinen Speicher des Geräts abgelegt werden, sondern~~ in einem ~~TI-Messenger-Client spezifischen~~geschützten Speicherbereich auf dem Endgerät~~.~~
~~Mobile TI-Messenger-Clients MÜSSEN sicherstellen, dass andere Applikationen auf den Endgeräten nicht auf Inhalte des TI-Messengers zugreifen können.~~ abgelegt werden.
Hierzu ~~SOLL der Hersteller~~SOLLEN Clients eine Abschottung des Speichers, den der TI-Messenger-Client für Nutzerdaten belegt, ~~implementieren.~~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 ~~Applikationen~~Anwendungen ausgelesen werden können.
[<=]

A_23130 - Nutzung von Daten durch Drittsysteme
Um eine nahtlose Integration von TI-Messenger-Clients ~~MÜSSEN ein Öffnen von über den~~in z.B. Primär- (PVS, ZPVS, KIS, AVS etc.) oder Archivsysteme zu ermöglichen, KÖNNEN TI-Messenger~~-empfangenen Dateien durch Drittprogramme ermöglich. Hierbei MUSS er sicherstellen, dass eine solche Ausleitung von Daten nur ausgelöst~~-Clients eine Schnittstelle zum Zugriff auf ihre Daten durch ~~den TI-Messenger-Client erfolgt.~~ Drittsysteme anbieten.
Der TI-Messenger-Client ~~KANN eine Funktion enthalten, mittels derer empfangene Dateien außerhalb des dedizierten Speichers im Gerätespeicher abgelegt werden. Der TI-Messenger-Client MUSS sicherstellen , dass Nutzer~~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. Geeignet bedeutet dabei, dass darüber informiert wird, welche Daten in welches Drittsystem weitergeleitet werden.
[<=~~Messengers hinausbewegen.~~
~~[<=~~**]**

~~ML-123590~~A_22725 - Sicherheitskritische Updates
~~Anbieter des~~ TI-Messenger-~~Clients~~Client-Hersteller MÜSSEN sicherstellen, dass ~~Nutzer~~Akteure über die Veröffentlichung von Updates für ihre TI-Messenger-~~Clientsoftware~~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 ~~im Gegensatz zu einem Nachweis~~anstatt eines Nachweises gegenüber

dem Matrix-Homeserver. Die Möglichkeit weiter Updates einzuspielen MUSS in diesem Fall weiterhin gegeben sein. ~~Nutzer~~ 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.
[<=]

~~**ML-124867 - Resilienz von Clients**~~
~~Hersteller MÜSSEN sicherstellen, dass TI-Messenger-Clients resilient auf unerwartete Eingaben reagieren.~~
~~**[<=]**~~

~~**ML-123591 - 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.~~
~~Der Hersteller MUSS sicherstellen, dass alle Zusatzfunktionen des TI-Messenger-Clients von den Basisfunktionen unterscheidbar sind.~~
~~**[<=]**~~

~~Zusatzfunktionen sind Funktionen des TI-Messenger-Clients und verwenden den gleichen Speicherbereich, sofern es sich nicht um Drittprogramm konzipierte Zusatzfunktionen handelt.~~

~~ML-123629~~A_22792 - Device Verification, Cross-Signing und SSSS für TI-Messenger-Clients
~~Hersteller~~TI-Messenger-Clients MÜSSEN ~~sicherstellen, dass~~ die Funktionen Cross-Signing und Secure Secret Storage and Sharing (SSSS) zur Device Verification ~~unterstützt werden.~~unterstützen. Es MUSS der Spezifikation gemäß [Client-Server API#Sharing keys between devices] gefolgt werden.
~~**[<=die Spezifikation 12.11.2 (https://spec.matrix.org/unstable/client-server-api/#device-verification) und 12.11.3 (https://spec.matrix.org/unstable/client-server-api/#sharing-keys-between-devices) vollständig befolgt werden.**~~
~~**[<=**~~**]**

A_22793 - Ende-zu-Ende Verschlüsselung
~~ML-123861 - Ende-zu-Ende-Verschlüsselung~~TI-Messenger-Clients~~Hersteller~~ MÜSSEN ~~sicherstellen, dass~~ eine ~~vollständige~~ Ende-zu-Ende-Verschlüsselung auf Basis von OLM/MEGOLM ~~unterstützt wird.~~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.
~~**[<=12.11 (https://spec.matrix.org/unstable/client-server-api/#end-to-end-encryption) und 12.12 (https://spec.matrix.org/unstable/client-server-api/#secrets) gefolgt werden.**~~
~~**[<=**~~**]**

~~ML-124006~~A_22794 - Explizites Verbot von Profiling für TI-Messenger-Clients
TI-Messenger-Client-Hersteller und -Anbieter ~~von TI-Messenger-Komponenten~~ DÜRFEN NICHT Daten zu Profiling-Zwecken sammeln. Dies betrifft insbesondere eine Überwachung welche Akteure mit welchen anderen Akteuren kommunizieren.

Hinweis:

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.
[<=]

~~ML-123593~~A_22795 - Einbringung und Speicherung von Schlüsseln und Token
~~Hersteller von~~ TI-Messenger-~~Clients~~ Client-Hersteller MÜSSEN sicherstellen, dass Schlüssel und Token sicher in den TI-Messenger-Client eingebracht werden. ~~Hierzu genügt eine Prüfung des Prozesses.~~

TI-Messenger-Client-Hersteller ~~von TI-Messenger-Clients~~ 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 [Matrix-SSSS] des beteiligten Homeservers.
[<=]

~~ML-123596 - Verwendung von TLS zur Kommunikation mit Fachdienst und VZD-FHIR-Directory~~A_22796 - Verwendung von TLS zur Kommunikation mit dem Fachdienst und VZD-FHIR-Directory
~~Der Hersteller MUSS sicherstellen, dass der~~ TI-Messenger-~~Client~~Clients MÜSSEN in der Lage ~~ist~~sein, Verbindungen zu anderen ~~Bestandteilen~~Komponenten des TI-~~Messengers~~Messenger-Dienstes über TLS aufzubauen. Hierzu gelten die Festlegungen der [gemSpec_Krypt].
~~[<=Entsprechende Anforderungen werden dem Produkttypsteckbrief zugeordnet.~~
~~[<=~~]

~~ML-123597 - Löschfunktionen für TI-Messenger-Inhalte~~A_22797 - Automatische Löschfunktion
~~Der Hersteller von~~ TI-Messenger-Clients ~~MUSS~~MÜSSEN über eine ~~automatisierte~~automatische Löschfunktion für vom Nutzer im TI-Messenger-Client ~~Nachrichten implementieren. Diese MUSS eine zumutbare voreingestellte Löschfrist enthalten, welche für Nutzer konfigurierbar ist~~ erstellte Daten verfügen. Die Löschfrist MUSS ~~hierbei~~konfigurierbar und auf 6 Monate voreingestellt sein.
[<=]

A_23112 - Funktion zum Nachhalten von Löschungen und Änderung von TI-Messenger Inhalten
TI-Messenger-Clients MÜSSEN über eine ~~den minimal einstellbaren Wert initialisiert sein. Nach Verstreichen der eingestellten Löschfrist MÜSSEN Gesprächsinhalte aus dem TI-Messenger-Client sicher gelöscht werden. Der Hersteller MUSS zusätzlich eine~~ nachrichtenbasierte ~~Löschfunktion vorsehen~~Lösch- und Änderungsfunktion verfügen, die es ~~Nutzern~~Akteuren erlaubt ihre eigenen Nachrichten händisch nicht nur vom eigenen TI-Messenger-Client, sondern auch im Room State anzupassen. Wurde von einem anderen Client eine Löschung bzw. Änderung vorgenommen, so MUSS die Löschung/Änderung der Nachricht auch auf allen weiteren Clients, die an der Kommunikation beteiligt sind, durchgeführt und gekennzeichnet werden. Die Kennzeichnung MUSS den löschenden/ändernden Akteur, das Datum und die Uhrzeit der Löschung /Änderung enthalten.
~~[<=aus dem Room State zu löschen.~~
~~[<=~~]

~~ML-123607~~A_22798 - Privacy by Default
~~Der Hersteller eines TI-Messenger-Clients MUSS für die Standardeinstellungen des~~ TI-Messenger-Clients MÜSSEN stets die datenschutzfreundlichste Voreinstellung als Standardeinstellung verwenden.
[<=~~konfigurieren.~~
~~[<=~~**]**

~~ML-123608~~A_22799 - Verwendung von OWASP Mobile
~~Der~~ Hersteller eines~~ mobilen~~ TI-Messenger-~~Clients~~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 [~~OWASPMobileTop10~~OWASP MobileTop10] umsetzen. Hierbei SOLLEN die Vorgaben ~~der Prüfvorschrift für den Produktgutachter des „ePA~~ gemäß [BSI 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~~A_22795 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

[<=]

~~ML-123630~~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].
[<=]

~~ML-123606 - Ausführung nur von begutachtetem Code~~A_22801 - Sicheres Beziehen von fremden Programmbestandteilen
~~Der Hersteller des TI-Messenger-Clients MUSS technisch sicherstellen, dass nur im Rahmen eines Produktgutachtens begutachteter Code ausgeführt wird oder Code-Änderungen nach Vorgaben der gematik durch den Hersteller als nicht zulassungsrelevant bewertet wurden.~~
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.
[<=]

~~ML-123600~~A_22802 - Sichere Softwareverteilung
Der Hersteller eines TI-Messenger-Clients MUSS ~~Nutzer~~Akteure über die vertrauenswürdigen Quellen informieren, von denen ~~Nutzer~~Akteure den TI-Messenger-Client beziehen können und wie sie die Vertrauenswürdigkeit der Quelle erkennen können. Der Hersteller MUSS sicherstellen, dass der ~~Nutzer~~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.
[<=~~[<=~~]

~~ML-123602 - 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 Clients dies zulässt .~~
~~**[<=]**~~

~~ML-123605~~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 ~~gesammelten~~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 ~~Nutzers~~ 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 ~~Nutzers~~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 ~~Nutzers~~Akteurs nutzt, den ~~Nutzer~~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 ~~Nutzers~~Akteurs nutzt, für jede Clientnutzung neue Nutzungsidentifier zufällig generieren. Der ~~Nutzer~~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 ~~Nutzer~~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 ~~Nutzern~~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 ~~Nutzers~~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 ~~den Nutzer~~die Akteure erfolgt ist und MUSS jederzeit durch diese deaktivierbar sein.
Ein Verweis auf AGBs oder Nutzungsbedingungen des TI-~~Messengers~~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 ~~Hersteller~~Client DARF NICHT wiederholt beim ~~Nutzer~~Akteur anfragen um eine Einwilligung durch Belästigung zu erzwingen. Nach einmaliger Ablehnung durch den ~~Nutzer~~Akteur MUSS jede Anzeige des Dialogs explizit durch den ~~Nutzer~~Akteur initiiert werden.
[<=]

~~ML-123632 – CC-Evaluierung als Ersatz für Gutachten~~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-~~Client des Nutzers,~~ Clients,
- die in den zusätzlichen Funktionen verarbeiteten Daten,
- die Schnittstellen zwischen dem TI-Messenger-Client des ~~Nutzers~~Akteurs und den ggf. genutzten Backend-Diensten der zusätzlichen Funktionen inklusive ihrer Sicherheitsmaßnahmen und
- die Sicherheitsannahmen an ~~das~~den TI-Messenger-Client des ~~Nutzers~~Akteurs und die Ausführungsumgebung

[<=]

~~**ML-123631 – Sichere Produktentwicklung und Nachweise**~~

~~Der Hersteller MUSS innerhalb des Produktlebenszyklus (Entwicklung, Betrieb, Außerbetriebnahme) seines Produktes Sicherheitsaktivitäten integrieren und anwenden, d. h. in einschlägigen Fachkreisen anerkannte, erprobte und bewährte Regeln anwenden.~~
~~Der Hersteller MUSS die Sicherheits- und Datenschutzmaßnahmen für sein Produkt in einem Sicherheits- und Datenschutzkonzept dokumentieren und auf Verlangen der gematik zur Verfügung stellen.~~
~~Der Hersteller MUSS einen Testplan für Sicherheitstests erstellen und auf Verlangen der gematik zur Verfügung stellen. Dieser MUSS umgesetzt werden und der gematik bei jeder Veröffentlichung einer Produktversion als neuer Bericht vorgelegt werden.~~
~~Der Hersteller des TI-Messenger-Clients des Nutzers MUSS während der Entwicklung des Produktes implementierungsspezifische Sicherheitsanforderungen dokumentieren und umsetzen.~~
~~Der Hersteller MUSS ein sicherheitsrelevantes Softwarearchitektur-Review durchführen und identifizierte Architekturschwachstellen beheben. Dieses Review MUSS nach jeder Architekturänderung mit Sicherheitsrelevanz wiederholt werden.~~
~~Der Hersteller MUSS eine Bedrohungsanalyse durchführen und Maßnahmen gegen die identifizierten Bedrohungen implementieren.~~
~~Der Hersteller MUSS während der Entwicklung des Produktes sicherheitsrelevante Quellcode-Reviews oder automatisierte sicherheitsrelevante Quellcode-Scans durchführen.~~
~~Der Hersteller MUSS während der Entwicklung des Produktes automatisierte Sicherheitstests durchführen.~~
~~Der Hersteller MUSS einen Schulungsplan zur regelmäßigen Schulung von Entwicklern in sicherer Entwicklung und Secure-Coding-Techniken dokumentieren und umsetzen.~~
~~Der Hersteller MUSS alle Entwickler des Produktes in sicherer Entwicklung und Secure-Coding-Techniken schulen. Hierzu MUSS der Hersteller sicherstellen, dass alle Entwickler zu Beginn der Entwicklung geschult sind. Er SOLL für diese anschließend auch laufende Weiterbildung durchführen.~~
~~Der Hersteller MUSS den verwendeten sicheren Produktlebenszyklus und deren Teilprozesse dokumentieren und auf Nachfrage der gematik zur Verfügung stellen. Die Dokumentation soll mindestens die folgenden Sicherheitsaktivitäten beschreiben:~~

- ~~Erfassen und Umsetzen von implementierungsspezifischen Sicherheitsanforderungen für den Client und von Best-Practice-Sicherheitsanforderungen,~~
- ~~Durchführen von sicherheitsrelevanten Architektur- und Design-Reviews,~~

- ~~Durchführen von Bedrohungsanalyse,~~
- ~~Durchführen von sicherheitsrelevanten Quellcode-Reviews,~~
- ~~Durchführen von Sicherheitstests während der Qualitätssicherungsphase,~~
- ~~Etablieren von Quality Gates, die eine Veröffentlichung des Clients mit 'Mittel' oder 'Hoch' bewerteten Sicherheitsfehlern verhindert~~
- ~~Änderungs- und Konfigurationsmanagement,~~
- ~~Schwachstellen-Management~~

~~Der Hersteller MUSS während der Entwicklung des Produktes einen Änderungs- und Konfigurationsmanagementprozess verwenden. Das Änderungsmanagement umfasst mindestens den Entscheidungsprozess über vorgeschlagene Änderungen und die Autorisierung der Änderungen. Das Konfigurationsmanagement liefert mindestens zu jedem Zeitpunkt die eindeutige Zusammensetzung des Produktes bezüglich seiner eindeutigen Komponenten (Dritt-Software wie Bibliotheken und Frameworks) und den vorgenommenen Änderungen an eigenen Komponenten.~~
~~Der Hersteller MUSS bei Veröffentlichung einer neuen Produktversion des Produktes die Einhaltung der Herstellererklärung sicherheitstechnische Eignung durch seinen Datenschutzbeauftragten verifizieren.~~
~~**[<=]**~~

~~ML-124881 - Kein Schreibzugriff für Clients auf Room-States~~A_22806 - Kein Schreibzugriff für TI-Messenger-Clients auf Room-States
TI-Messenger-Clients MÜSSEN verhindern, dass ~~Nutzer mittels Nutzereingaben~~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 ~~bringen. Sobald durch die geplante~~ Matrix-~~Spec-Changes (MSCs) die Möglichkeit geschaffen wurde, vertrauliche Informationen sicher im Room-State zu speichern,~~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 MÜSSEN bei der Konfiguration des zu nutzenden Messenger-Service dem Akteur nur valide Messenger-Services, die zum gewählten Anbieter gehören, zur Auswahl anbieten.
[<=]

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 ~~direkt durch die~~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-~~Spezifikation abgedeckt. **[<=]**~~

OpenID-Token anfragen.

~~4.2~~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 ~~interoperablen~~interoperable Funktionen durch den Hersteller bereitgestellt werden, um ein Mindestmaß an ~~Nutzererfahrung~~Akzeptanz bei den Nutzern zu erreichen. Diese werden im Folgenden beschrieben.

Präsenzanzeige für andere Nutzer

Für eine Echtzeitnutzererfahrung, MÜSSEN TI-Messenger-Clients gemäß [~~Präsenzanzeige~~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 ~~ML-123607)~~gemäß [A_22798]) standardmäßig deaktiviert sein.

Erwähnungen von Nutzern im Chatraum

TI-Messenger-Clients MÜSSEN es ermöglichen, dass über das Eingabefeld andere Nutzer gemäß [~~Erwähnung~~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 ~~Geräte, oder Geräte mit Push-Funktionalität,~~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 ~~mobile~~ TI-Messenger-Clients die Matrix-Spezifikation gemäß [~~Lesebestätigungen] vollständig~~Client-Server API#Receipts] implementieren. TI-Messenger-Clients ~~für Nutzer~~ MÜSSEN ~~diese Funktion~~die Funktionen des Anzeigens und des Sendens von Lesebestätigungen ~~vollständig~~ 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 ~~ML-123607)~~gemäß [A_22798]) standardmäßig deaktiviert sein.

Eingabebenachrichtigungen

~~Mobile~~ TI-Messenger-Clients für mobile Szenarien MÜSSEN die Matrix-Spezifikation gemäß [~~Eingabebenachrichtigungen] vollständig~~Client-Server API#Typing Notifications] implementieren. TI-Messenger-Clients SOLLEN~~ Nutzern~~ 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 ~~ML-123607)~~gemäß [A_22798]) 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.
[<=]

~~4.34.4~~ Konfiguration~~ des TI-Messenger-Clients~~

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

Einstellung von Push-Benachrichtigungen

TI-Messenger-Clients MÜSSEN über eine Funktion verfügen, um Push-Benachrichtigungen auf einem ~~Gerät~~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 ~~zu~~ ignorieren zu können. Daher MÜSSEN ~~mobile~~ TI-Messenger-Clients die Matrix-Spezifikation gemäß [~~Nutzer ignorieren] vollständig~~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

~~Mobile~~ TI-Messenger-Clients MÜSSEN die Matrix-Spezifikation gemäß [~~Raum Historie] vollständig~~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-Proxy des VZD-FHIR-Directory das Attribut `status` des Endpoints einer Practitioner-Ressource auf den Wert `status == active` für das einschalten oder `status == off` für das ausschalten gesetzt werden. Wenn der Akteur den `status` von `active` nach `off` ändert, MUSS der TI-Messenger-Client über die REST-Schnittstelle `/search` am FHIR-Proxy des VZD-FHIR-Directory prüfen, ob diese MXID auch im Organisationsverzeichnis eingetragen ist. Wird die MXID ebenfalls im Organisationsverzeichnis gefunden und ist der hinterlegte `status` in diesem Verzeichnis `active`, dann MUSS der TI-Messenger-Client dem Akteur einen Hinweis anzeigen, dass eine Inkonsistenz in der hinterlegten Sichtbarkeit vorliegt. Aus dem Hinweis MUSS hervorgehen, dass ein Kontaktieren des Administrators seiner Organisation notwendig ist, um die gewünschte Sichtbarkeit ebenfalls im Organisationsverzeichnis zu hinterlegen.

~~4.4~~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 ~~sowie~~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 ~~früher~~zeitnaher IOP-Tests, die Synchronisierung von Meilensteinen und regelmäßige ~~industriepartnerübergreifenden~~industriepartnerübergreifende Test-Sessions. Die Test-Sessions umfassen gegenseitige IOP- und E2E-Tests.

Die gematik stellt eine TI-Messenger-~~Fachdienst~~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.
[<=]

~~Die gematik testet in den Zulassungsverfahren auf Basis von Anwendungsfällen. Dabei werden die Anwendungsfälle durchgespielt und es wird versucht viele Funktionsbereiche und Teile der Anwendung mit einzubeziehen. Anschließend wird mit den IOP Tests die Interoperabilität zwischen den verschiedenen Anbieter nachgewiesen. Für das Zulassungsverfahren des TI-Messenger-Dienst müssen die TI-Messenger-Clients und TI-Messenger FD~~

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 ~~beinhalten, welcher die Funktionalitäten der produktspezifischen Schnittstelle des TI-Messenger-Clients über eine standardisierte Schnittstelle von außen zugänglich macht und einen Fernzugriff ermöglicht~~intern oder extern zur Verfügung stellen. In den folgenden Abbildungen wird das interne sowie das externe Testtreiber-Modul dargestellt.

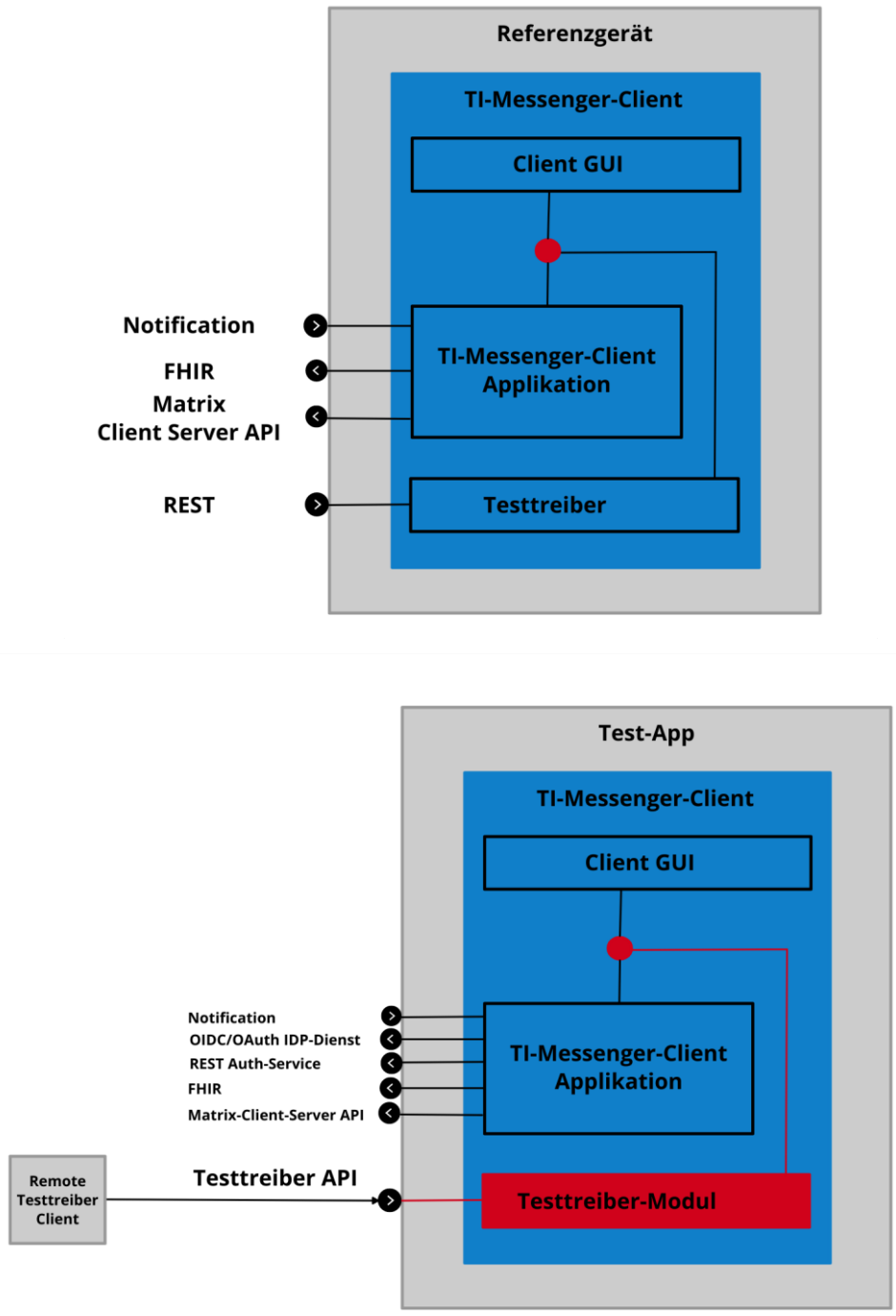


Abbildung 3: ~~Testtreiberschnittstelle~~interne Testtreiber-Modul

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

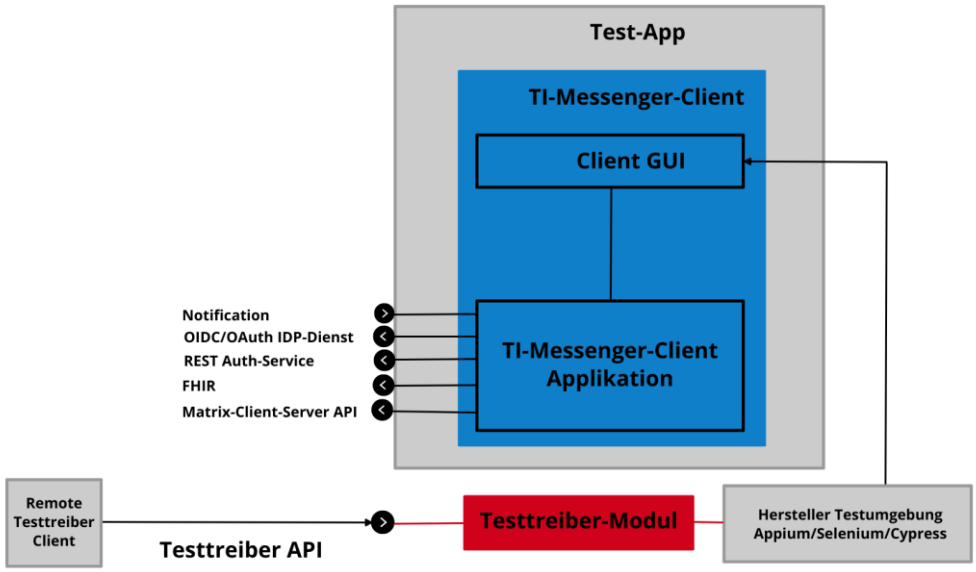


Abbildung 4: externes Testtreiber-Modul

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~~, welches eine Schnittstelle für automatisierte Tests anbietet. Diese Schnittstelle wird durch die gematik spezifiziert und bereitgestellt.~~ oder einen Zugang zum Test-Environment des Herstellers gewährleisten. 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 ~~nicht~~ verfälschen.

Hinweis: Die ~~konkrete Ausgestaltung der Schnittstellen~~Schnittstelle gemäß [Testtreiber

API] wird ~~im Fachportal der~~durch die gematik spezifiziert und bereitgestellt.
[<=]

~~in GitHub zur Verfügung gestellt.~~

ML-124878 - **~~Beschränkung Einsatz Testtreiber-Modul~~Beschränkung des Einsatzes des Testtreiber-Moduls**
Der produktive TI-Messenger-Client DARF NICHT ein Testtreiber-Modul ~~NICHT~~ 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 ~~fachliche Logik~~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.

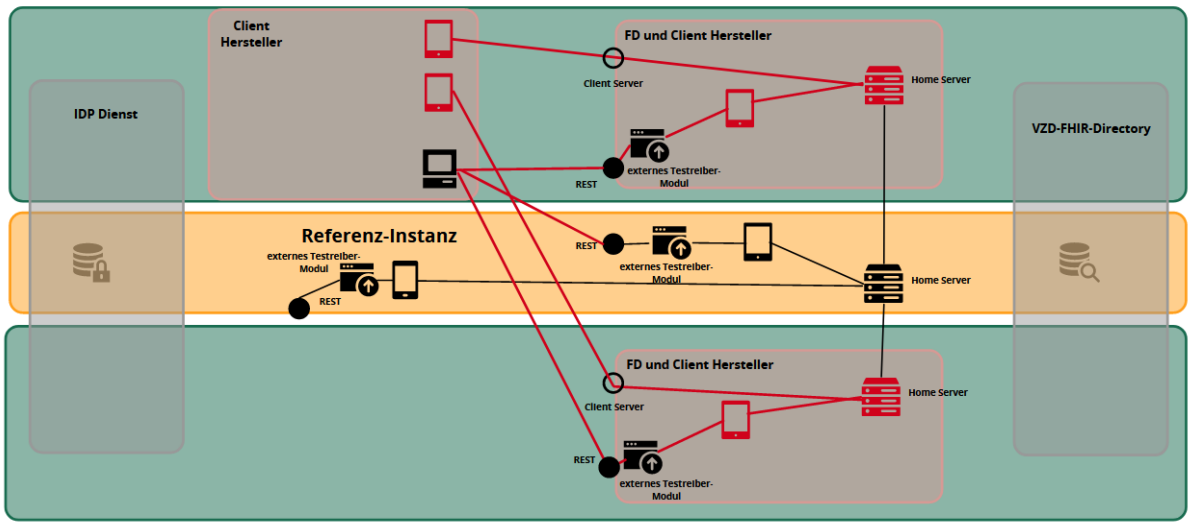


Abbildung 5: Testumgebung für Herstellertests

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.

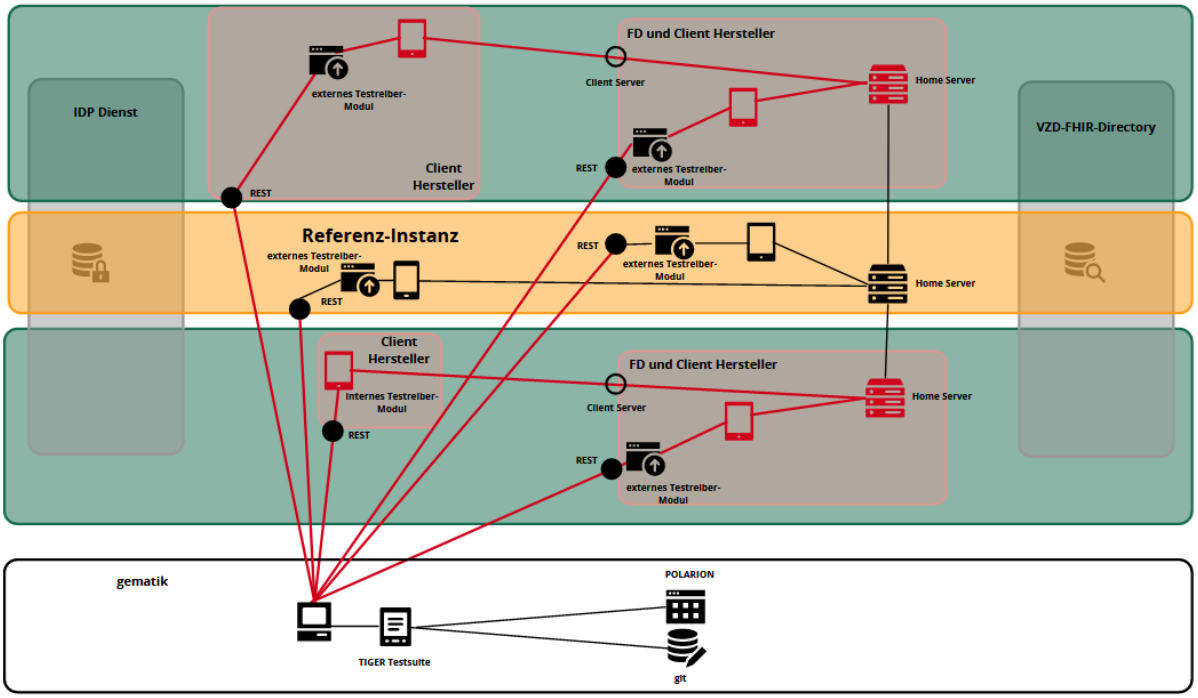


Abbildung 6: Testumgebung gematik

~~4.5~~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 ~~bei den Nutzern~~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 ~~Anbieter~~ TI-Messenger-Anbieter MUSS ~~sein~~das/die Produkt(e) TI-Messenger-Client mit einer vollumfänglich-funktionalen Verfügbarkeit von 98 % seinen Nutzern anbieten.

5 Funktionsmerkmale

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

~~5.1 Authentisierung~~

~~SSO Login~~

5.1 Authentifizierungsverfahren

TI-Messenger-Clients MÜSSEN ~~die Matrix-Spezifikation~~mindestens die folgenden Authentifizierungsverfahren unterstützen:

- **SSO Login** gemäß [Client-Server API#SSO ~~Login] vollständig implementieren.~~client login/authentication] und

~~OpenID~~

- **OpenID-Connect** gemäß [Client-Server API#OpenID]

Wird ein in der Organisation bereits genutztes Authentifizierungsverfahren verwendet, so MUSS der TI-Messenger-~~Clients MÜSSEN~~Client die ~~Matrix-Spezifikation gemäß [OpenID] vollständig implementieren.~~

~~Gäste Accounts~~

Eingabe der dafür benötigen Client Credentials unterstützen.

Zusätzlich MUSS der Hersteller eines TI-Messenger-~~Client MUSS~~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 [~~Matrix Foundation#~~Client~~ -~~Server API] in der Version v1.3 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] ~~vollständig~~ implementieren. TI-Messenger-Clients MÜSSEN mit ~~Raum~~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] ~~vollständig~~ implementieren~~ und umsetzen~~.

Geräteverwaltung

TI-Messenger-Clients MÜSSEN eine Geräteverwaltung für die eigenen Geräte eines Nutzers, ~~für die Geräte anderer Nutzer in einem Chatraum, sowie für die Geräte aller Nutzer eines Messenger-Services in der Rolle des *Org-Admin* ~~unterstützen. ~~Daher MÜSSEN ~~TI-Messenger-Clients MÜSSEN die Matrix-Spezifikation gemäß [Client-Server API#Device Management] ausschließlich für die eigene Geräteverwaltung~~] vollständig~~ 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 [~~Ende-zu-Ende-Verschlüsselung] vollständig~~Client-Server API#End-to-End Encryption] implementieren~~.~~ und unterstützen. Die TI-Messenger-Clients MÜSSEN ~~eine Ende-zu-End-Verschlüsselung entsprechend der Matrix-Spezifikation unterstützen. Der Hersteller von TI-Messenger-Clients MUSS ~~verhindern, dass nicht Ende-zu-Ende ~~verschlüsselten~~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

~~5.3~~ TI-Messenger-Clients MÜSSEN eine Funktion anbieten, um Sofortnachrichten gemäß [Client-Server API#Instant Messaging

~~Instant Messaging MUSS von~~] in einem ~~TI-Messenger-Client vollständig nach der Matrix-Spezifikation gemäß [Instant Messaging] implementiert werden~~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 ~~SOLLEN~~MÜSSEN die MXID eines ~~Nutzers~~Akteurs verstecken und ~~SOLLEN~~ den Displaynamen anzeigen. TI-Messenger-Clients MÜSSEN Nutzer informieren, falls ein Event nicht oder fehlerhaft versendet wurde.

~~Folgende~~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~~, ist~~ MUSS ein Fallback ~~im Plaintext~~ für beispielsweise Replies ~~spezifiziert:~~als Plaintext gemäß [Client-Server API#Fallbacks for rich replies] möglich sein.

~~https://spec.matrix.org/unstable/client-server-api/#fallbacks-for-rich-replies~~

Dabei MUSS der TI-Messenger-~~Clients MÜSSEN Fallbacks für~~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.

~~5.4 Direct Messaging~~

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 ~~Personen~~Akteuren erstellt wird. Dieser Chatraum kann nicht um weitere ~~Teilnehmer~~Akteure erweitert werden~~.~~, es sei denn, es handelt sich um ein technisches System zum Zweck der Archivierung. Soll ein Chatraum für mehr als zwei ~~Teilnehmer~~Akteure erstellt werden, ~~ist~~MUSS Group Messaging ~~zu~~(Gruppenunterhaltungen) verwenden ~~. Chaträume, die mit einer Organisation geführt~~ werden ~~sollen, unterliegen grundsätzlich dem Group Messaging. Die folgenden Möglichkeiten MÜSSEN dabei vom TI-Messenger-Client angeboten werden:~~.

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

Tabelle 3:Ablauf - Direktnachrichten

Direktnachrichten zwischen Akteuren innerhalb ~~eines Messenger-Services~~einer Organisation	
~~Userstory~~Userstory: Suchen eines Akteurs über das Nutzerverzeichnis des Matrix-Homeservers	1. ~~Nutzer~~Akteur möchte eine neue Unterhaltung starten 2. TI-Messenger-Client zeigt alle Akteure seiner Organisation im Nutzerverzeichnis des Matrix-Homeservers an 3. ~~Nutzer~~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 ~~verschiedenen Messenger-Services~~Akteuren außerhalb einer Organisation	
Userstory ~~mittels~~: Suche eines Akteurs über das Personenverzeichnis	1. ~~Nutzer~~Akteur A ~~(verifizierter~~ in der Rolle "User-HBA~~-Inhaber)~~" möchte eine neue Unterhaltung mit ~~Nutzer~~Akteur B ~~(verifizierten~~ in der Rolle "User-HBA~~-Inhaber)~~" starten

des VZD-FHIR-Directory	2. ~~Nutzer~~Akteur A durchsucht das Personenverzeichnis des VZD-FHIR-Directory nach ~~Nutzer~~Akteur B 3. TI-Messenger-Client zeigt Profil (z. B. Name, Organisationszugehörigkeit, Berufsgruppe~~)~~ etc.) von ~~Nutzer~~Akteur B an 4. ~~Nutzer~~Akteur A startet den Chat mit ~~Nutzer~~Akteur B Der TI-Messenger-Client zeigt an, dass es sich um einen Direktchat handelt. Eine Umwandlung in ~~Gruppe~~einen Gruppenchat ist nicht möglich.
Userstory: Austausch der Kontaktdaten mittels QR-Scan	1. ~~Nutzer~~Akteur A und ~~Nutzer~~Akteur B treffen sich in Person 2. ~~Nutzer~~Akteur A und ~~Nutzer~~Akteur B wählen jeweils im TI-Messenger-Client "neue Unterhaltung starten" aus 3. ~~Nutzer~~Akteur A wählt "QR-Code teilen" aus ~~1.~~ ~~Nutzer~~Akteur B wählt "QR-Code scannen" aus und scannt "QR-Code" von ~~Nutzer A~~ 4. ~~Nutzer~~Akteur A und ~~Nutzer~~erhält die MXID von Akteur A ~~4.~~5. Akteur A und Akteur B klicken "weiter" ~~5.~~6. ~~Nutzer~~Akteur B bekommt einen QR-Code angezeigt, ~~Nutzer~~Akteur A bekommt den QR-Code Scanner angezeigt ~~6.~~7. ~~Nutzer~~Akteur A scannt ~~Nutzer~~den QR-Code von Akteur B 8. ~~Nutzer~~Akteur B kann optional die Eintragung der MXID von Akteur A in seiner Freigabeliste durchführen ~~7.~~9. Akteur A bekommt einen Dialog angezeigt, dass der Chatraum ~~erstell~~erstellt wird, ~~Nutzer~~Akteur B kann den QR-Code schließen ~~Die in diesem Ablauf ausgetauschten Token haben eine Gültigkeit von 10 Minuten.~~Der TI-Messenger-Client zeigt an, dass es sich um einen Direktchat handelt. Eine Umwandlung in einen Gruppenchat ist nicht möglich.

~~5.5 Group Messaging~~

5.2.3 Gruppenunterhaltungen

TI-Messenger-Clients MÜSSEN eine Funktion anbieten, um Gruppenunterhaltungen zu starten und Nachrichten innerhalb einer Chatgruppe ~~mit unbegrenzt vielen Nutzern~~mitNutzern des TI-Messenger-Dienstes auszutauschen. TI-Messenger-Clients MÜSSEN alle Teilnehmer einer Chatgruppe anzeigen~~. Darüberhinaus~~ 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

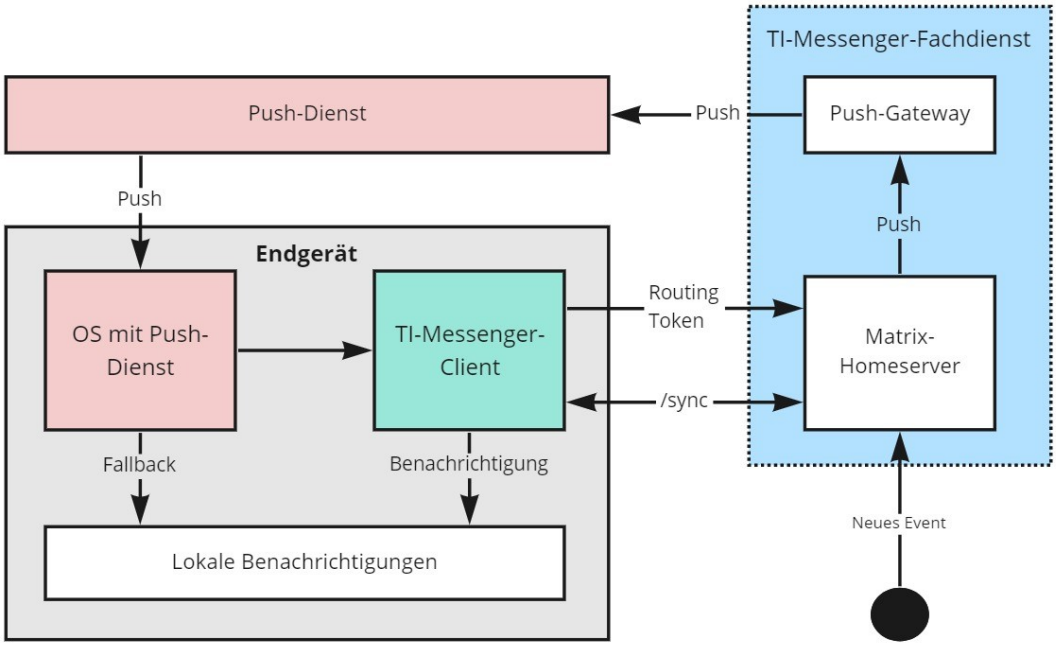
Gruppenunterhaltungen zwischen Akteuren innerhalb ~~eines Messenger-Services~~einer Organisation	
~~Neue Gruppenunterhaltung~~Userstory: Suchen eines Akteurs über das Nutzerverzeichnis des Matrix-Homeservers	1. ~~Nutzer~~Akteur möchte eine neue Gruppenunterhaltung starten. 2. TI-Messenger-Client zeigt alle Akteure seiner Organisation im Nutzerverzeichnis des Matrix-Homeservers an 3. ~~Nutzer~~Akteur wählt Gesprächspartner aus. 4. Gesprächspartner werden in die Gruppenunterhaltung eingeladen. 5. ~~Nutzer~~Akteur kann weitere Gesprächspartner hinzufügen.
Gruppenunterhaltungen zwischen ~~verschiedenen Messenger-Services~~Akteuren außerhalb einer Organisation	
~~Nachricht an Organisation~~ Userstory: Suche eines Akteurs über das Organisationsverzeichnis des VZD-FHIR-Directory	1. ~~Nutzer~~Akteur möchte eine Nachricht an eine andere Organisation senden und eine Gruppenunterhaltung starten 2. ~~Nutzer~~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. ~~Nutzer~~ Akteur selektiert die MXID eines Akteurs der Organisation und startet einen Chat mit ~~Organisation, hinterlegte MXID der~~

	~~Organisation wird in Chatgruppe eingeladen (Nutzer, Bot)~~diesem
~~Einladen weiterer Personen~~Userstory: Suche eines Akteurs über das Organisationsverzeichnis des VZD-FHIR-Directory um weitere Akteure in die Gruppenunterhaltung einzuladen	1. ~~Nutzer wollen~~Akteur möchte weitere ~~Personen~~Akteure anderer Organisationen in die bestehende Chatgruppe einladen 2. ~~Nutzer~~Akteur durchsucht ~~Nutzerverzeichnis oder~~das Organisationsverzeichnis des VZD-FHIR-Directory ~~(Wenn HBA-Inhaber)~~nach der Organisation ~~1. Nutzer wählt Person aus~~ 3. ~~Person wird~~TI-Messenger-Client zeigt das Profil der Organisation (z. B. Name, Typ, Kontaktmöglichkeiten) an ~~3.~~4. Akteur lädt den Akteur der Organisation in die bestehende ~~Chatgruppe eingeladen~~Gruppenunterhaltung ein
~~Einladen weiterer Organisationen~~Userstory: Suche eines Akteurs über das Nutzerverzeichnis des Matrix-Homeservers oder über das Personenverzeichnis des VZD-FHIR-Directory	1. ~~Nutzer wollen~~Akteur möchte weitere ~~Organisationen~~Akteure in ~~Chatgruppen~~die bestehende Chatgruppe einladen ~~1. Nutzer~~Akteur durchsucht entweder das Nutzerverzeichnis seiner Organisation oder das Personenverzeichnis des VZD-FHIR-Directory ~~nach Organisation~~ 2. ~~TI-Messenger-Client zeigt Profil der~~für die Einladung eines Akteurs außerhalb seiner Organisation ~~(Name, Typ, Kontaktmöglichkeiten)~~ 3. ~~Nutzer lädt Organisation~~Akteur wählt einen gefundenen Akteur aus ~~3.~~4. Akteur wird in bestehende ~~Gruppenunterhaltung ein~~Chatgruppe eingeladen

~~5.5.1~~5.2.4 Push-Benachrichtigungen

~~Mobile~~ TI-Messenger-Clients für mobile Szenarien MÜSSEN die Matrix-Spezifikation gemäß [Client-Server API#Push~~-Benachrichtigungen] vollständig~~ Notifications] implementieren.

~~5.5.2 Allgemein~~



Die folgende Abbildung ~~4: Push-Benachrichtigung für Mobilgeräte~~

~~Die Abbildung "*Push-Benachrichtigung für Mobilgeräte*"~~ zeigt den Fluss von Push-Benachrichtigungen, die an ein Mobiltelefon gesendet werden, bei dem die Push-Benachrichtigungen über den Anbieter des Mobiltelefons übermittelt werden~~. Dies geschieht wie folgt:~~.

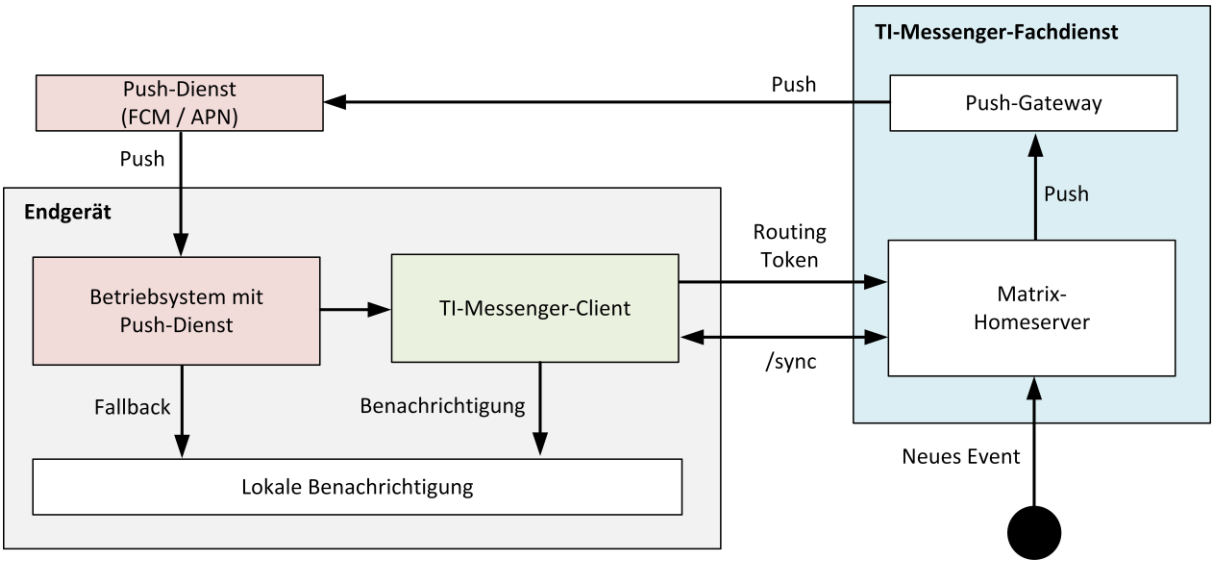


Abbildung 7: Push-Benachrichtigung für Endgeräte

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 ~~Gerät~~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 ~~Gerät~~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 ~~mobiler~~ 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 ~~werden soll~~ 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 ~~mobiler~~ 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-Ressource *HealthcareService* 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 Akteur in der Rolle "Org-Admin" MUSS der Displayname den Marker`Chatbot` enthalten, wenn der Funktionsaccount über einen Chatbot realisiert wird. Dabei ist folgende Bildungsregel für den Displaynamen zu verwenden: [Name des Funktionsaccounts] (Chatbot).

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

~~5.6~~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 ~~MUSS~~KANN bei der Erstellung des Localparts der MXID eines ~~Nutzers~~Akteurs sicherstellen, dass keine personenbezogenen Daten ~~entstehen.~~erkennbar sind. Dazu ~~MUSS~~KANN der TI-Messenger-Client den ~~local-Part~~Localpart der verwendeten MXID des ~~Nutzers~~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 ~~MUSS~~SOLL für die MXID einen Hash-Wert mittels Base32 SHA256 ~~zu~~ berechnen.
[<=]

Displayname

Der TI-Messenger-Client MUSS bei der initialen Vergabe des Displayname die folgende Bildungsregel anwenden: `[Name], [Vorname]`. Ebenfalls MUSS Der TI-Messenger-Client sicherstellen, dass ~~nur Nutzer in der Rolle *Org-Admin* den Displaynamen von Nutzern bearbeiten können. Es MUSS sichergestellt werden, dass Nutzer den~~ ein Akteur seinen eigenen Displaynamen nachträglich nicht ändern ~~können.~~ kann.

~~**Server-Administration**~~

~~Mobile TI-Messenger-Clients MÜSSEN die Matrix-Spezifikation gemäß [Server Administration] vollständig implementieren.~~

~~TI-Messenger-Clients MÜSSEN entsprechende Administrationsfunktionen für einen Messenger-Service zur Verfügung stellen. Dazu gehören:~~

- ~~Benutzerverwaltung (Liste aller Benutzer, Anlegen, Bearbeiten, Löschen)~~
- ~~Geräteverwaltung (Anzeigen, Abmelden, Löschen aller Geräte des Homeservers)~~
- ~~VZD-FHIR-Directory (Schreibzugriff mittels SMC-B)~~
- ~~Systemmeldungen an Nutzer eines Messenger-Services~~

~~Nutzerverzeichnis:~~

- ~~**Sichtbarkeit** zwischen Nutzern kann durch den Nutzer in der Rolle *Org-Admin* eingeschränkt werden~~

~~*Hinweis: Die Funktionen der Server-Administration können in einen separaten Administrations-Client ausgelagert werden. Sofern reguläre Nutzerfunktionen und Administrationsfunktionen in derselben Applikation angeboten werden, so sollte auf eine klar erkennbare Unterscheidung zwischen Nutzer- und Administrationsfunktionen geachtet werden. Es MUSS sichergestellt werden, dass nur Akteure in der Rolle Org-Admin die Administrationsfunktionen nutzen können.*~~

~~**Third-Party-Networks / Bridging**~~

~~Das Bridging zu Drittsystemen zur Zwecken der Kommunikation (Austausch von Matrix-Events) ist nicht erlaubt. 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.~~

~~**Nutzerverzeichnis eines Messenger-Services**~~

~~Der TI-Messenger-Client KANN eine Funktion bereitstellen, dass Nutzer auf dem jeweiligen Messenger-Service ein Verzeichnis von Nutzern aufrufen oder durchsuchen können.~~

~~**Suchabfragen VZD-FHIR-Directory**~~

~~Der TI-Messenger-Client MUSS eine Funktion bereitstellen, dass Nutzer 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 anzuzeigen.~~

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 User-Agent-Kennung in den TI-Messenger-Client implementiert werden. Die davon zulassungsrelevanten Anteile 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 User-Agent-Kennung MUSS bei jedem Aufruf im HTTP Header übertragen werden.

A_23104 - TI-M Client Useragent
Der TI-Messenger-Client für Akteure und der TI-Messenger-Client mit Administrationsfunktionen (Org-Admin-Client) MUSS folgende Useragent-Kennung bei jedem Verbindungsaufbau zum TI-Messenger-Fachdienst übermitteln:

```
"Useragent":
  {
    "Produkttypversion": $Produkttypversion,
    "Produktversion": $Produktversion,
    "Auspraegung": $Auspraegung,
    "Plattform": $Plattform,
    "OS": $OS,
    "OS-Version": $OS-Version,
    "client_id": $client_id,
  }
```

Zur Beschreibung der jeweiligen Datenfelder, siehe [gemSpec_TI-Messenger-FD#A_22940].
[<=]

Übersicht über verwendete Geräte/Devices

Der TI-Messenger-Client MUSS dem Akteur eine Übersicht der angemeldeten Geräte anzeigen können. Die Anzeige MUSS eine Unterteilung in verifizierte und nicht verifizierte Geräte vorsehen. Für jedes angezeigte Gerät MUSS der letzte Aktivitätsstatus angezeigt

werden und der Akteur MUSS einzelne Gerät abmelden und somit dessen Matrix-ACCESS_TOKEN invalidieren können.

~~Weitere Spezifikationen finden sich in [gemSpec_VZD_FHIR_Directory].~~

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 ~~Nutzer~~Akteur direkt ~~ausgeloggt~~abgemeldet werden.

Third Party Networks / Bridging

Ein Bridging zu anderen Messaging-Protokollen DARF NICHT stattfinden. Als Messaging-Protokoll MUSS ausschließlich die Matrix-Client-Server- und die Matrix-Server-Server-API verwendet werden. Ein clientseitiger bidirektionaler Austausch mit Drittsystemen KANN möglich sein, um zum Beispiel das Archivieren von Chatnachrichten oder Chatbots zu erlauben. Dazu KANN der TI-Messenger-Client als Modul in ein bestehendes System integriert werden.

Ende-zu-Ende Verschlüsselung

Der TI-Messenger-Client MUSS sicherstellen, dass sämtliche Nachrichteninhalte Ende-zu-Ende ~~[Ende-zu-Ende Verschlüsselung~~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 Messenger-Proxy seines Messenger-Service 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 ~~mittels Chatbot-Clients~~

~~Zur Archivierung von Gesprächsinhalten ist eine Lösung auf Basis automatisierter Matrix-Clients in der Leistungserbringerumgebung geplant. Die hier vorhandene Beschreibung ist für die Erstveröffentlichung der Spezifikation noch als informell zu betrachten und wird im ersten geplanten Hotfix konkretisiert und formalisiert.~~

~~Für eine echtzeitnahe und automatische Archivierung von Gesprächsinhalten zu Nachweiszwecken werden vom Anbieter des TI-Messenger-Homeservers sog. Archivbots bereitgestellt, bei welchen es sich um funktional eingeschränkte Matrix-Clients handelt. Diese können entweder von Leistungserbringern zu Gesprächen eingeladen werden oder sind für bestimmte Gesprächsraumtypen automatisch bei der Raumerstellung eingeladen (konfigurierbar durch LE-Organisation).~~

~~Der einzige Zweck des Archivbots besteht darin, eine Unterhaltung oder Teile dieser zu entschlüsseln und zu archivieren. Hierzu betritt der Archivbot den Gesprächsraum, in den er eingeladen wurde und kann somit darin versandte Nachrichten entschlüsseln und als FHIR-Ressource archivieren. Der Archivbot liegt in der Leistungserbringerumgebung und kommuniziert zum Ablegen archivierter Nachrichten mittels TLS mit einem Endpunkt, z.B. des PVS/KIS oder einem LE-Archivierungs-Backend.~~

~~Der Archivbot ist als Gesprächsteilnehmer für alle anderen Teilnehmer sichtbar und klar als rein funktionaler Archivbot benannt. Es wird empfohlen, dass der Archivbot bei Betreten eines Gesprächsraums ein kurzes Statement zu seiner Funktion abgibt, um Missverständnisse zu vermeiden.~~

~~Es ist vorgesehen, dass auch Gespräche ohne Archivbot geführt werden können, welche dementsprechend nicht archiviert werden. Bei Archivbots handelt es sich nicht um vollwertige TI-Messenger-Clients, weswegen sie bezüglich der Client-Anforderungen gesondert betrachtet werden müssen.~~

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

Die fallbezogene Kommunikation ermöglicht es den Nutzern strukturierte Daten zu einem medizinischen Fall auszutauschen und in ihrem Primärsystem weiter zu verarbeiten. Hierfür MUSS der TI-Messenger-Client FHIR-Ressourcen in den Room-State eines existierenden Chatraumes hinzufügen.

Art des Events: state event
`Event state_key: <vom Sender festgelegt>`
`Event type: "de.gematik.tim.casereference"`
Die FHIR-Ressourcen werden im Element content als json-Daten eingetragen und als FHIR-Bundle (type message) zusammengefasst.

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

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

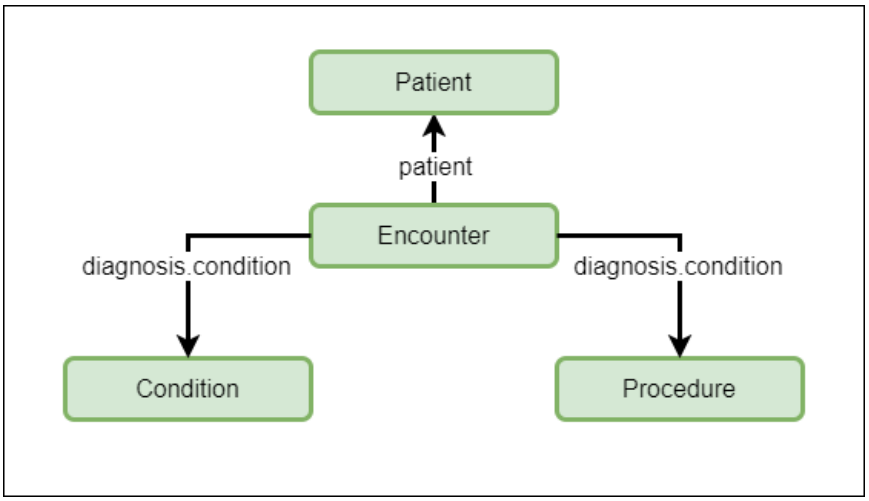


Abbildung 8: CaseReference Ressourcen

Hinweis: Voraussetzung für die produktive Nutzung ist die Umsetzung des MSC3414 Encrypted state events (https://github.com/matrix-org/matrix-spec-proposals/pull/3414).

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
~~OAuth~~OWASP	Open ~~Authorization~~Web Application Security Project
~~PASSporT~~PVS	~~Personal Assertion Token~~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

~~Das Glossar wird als eigenständiges Dokument (vgl. [gemGlossar]) zur Verfügung gestellt.~~

6.3 Abbildungsverzeichnis

6.4 Tabellenverzeichnis

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
[gemKPT_Betr]	gematik: Betriebskonzept Online-Produktivbetrieb
[gemSpec_Krypt]	gematik: Übergreifende Spezifikation - Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur
[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~~simplifier]	~~gematik: Betriebskonzept Online-Produktivbetrieb~~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
[BSI 2-Faktor]	BSI Bewertungstabellen IT-Sicherheit https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/2FA/it-sicherheit.pdf?__blob=publicationFile&v=3
[BSI Frontend]	BSI Prüfvorschrift für den Produktgutachter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/DigitaleGesellschaft/Pruefvorschrift_Produktgutachter_ePA-Frontend.pdf?__blob=publicationFile&v=3
[~~Matrix Foundation~~Client-Server API]	~~Matrix Foundation~~ ~~https://matrix.org/docs/spec/~~ Matrix Foundation: Matrix Specification - Client-Server API https://spec.matrix.org/v1.3/client-server-api/
[~~Instant Messaging~~DSK2021]	~~Matrix Foundation~~ ~~https://matrix.org/docs/spec/client_server/r0.6.1#id42~~ 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
[~~Direct Messaging~~ISO 9241]	~~Matrix Foundation~~ ~~https://matrix.org/docs/spec/client_server/r0.6.1#id140~~ Ergonomics of human-system interaction https://www.iso.org

~~[Erwähnung]~~	~~Matrix Foundation~~ ~~https://matrix.org/docs/spec/client_server/r0.6.1#user-room-and-group-mentions~~
~~[Präsenzanzeige]~~	~~Matrix Foundation~~ ~~https://matrix.org/docs/spec/client_server/r0.6.1#id62~~
~~[Push-Benachrichtigungen]~~	~~Matrix Foundation~~ ~~https://matrix.org/docs/spec/client_server/r0.6.1#id89~~
~~[Push-Rules]~~	~~Matrix Fundation~~ ~~https://matrix.org/docs/spec/client_server/r0.6.1#id89~~
~~[Lesebestätigungen]~~	~~Matrix Foundation~~ ~~https://matrix.org/docs/spec/client_server/r0.6.1#id53~~

~~[Eingabebenachrichtigungen]~~	~~Matrix Foundation https://matrix.org/docs/spec/client_server/r0.6.1#id49~~
~~[Nutzer ignorieren]~~	~~Matrix Foundation https://matrix.org/docs/spec/client_server/r0.6.1#id144~~
~~[Raum Historie]~~	~~Matrix Foundation https://matrix.org/docs/spec/client_server/r0.6.1#room-history-visibility~~
~~[Room Upgrades]~~	~~Matrix Foundation https://matrix.org/docs/spec/client_server/r0.6.1#id160~~
~~[Server Administration]~~[Matrix-SSSS]	~~Matrix Foundation https://matrix.org/docs/spec/client_server/r0.6.1#id129~~ Matrix Foundation: Secure Server Storage and Sharing https://matrix.org/docs/guides/implementing-more-advanced-e-2-ee-features-such-as-cross-signing
~~[Send-to-Device messaging]~~	~~Matrix Foundation https://matrix.org/docs/spec/client_server/r0.6.1#id70~~
~~[Geräteverwaltung]~~	~~Matrix Foundation https://matrix.org/docs/spec/client_server/r0.6.1#id73~~
~~[Reporting content]~~	~~Matrix Foundation https://matrix.org/docs/spec/client_server/r0.6.1#id150~~
~~[Ende-zu-Ende Verschlüsselung]~~	~~Matrix Foundation https://matrix.org/docs/spec/client_server/r0.6.1#id76~~
~~[SSO Login]~~	~~Matrix Foundation https://matrix.org/docs/spec/client_server/r0.6.1#sso-client-login~~
~~[OpenID]~~	~~Matrix Foundation https://matrix.org/docs/spec/client_server/r0.6.1#id154~~
[~~OWASPMobileTop10~~OWASP MobileTop10]	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/
[~~ISO 9241~~Testtreiber API]	~~Ergonomics of human-system interaction https://www.iso.org~~Testtreiber API https://github.com/gematik/api-ti-messenger/tree/master/src/openapi

[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-0316 6]	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