Elektronische Gesundheitskarte und Telematikinfrastruktur

Spezifikation
TI-Messenger-Client

Version:	1.0.0
Revision:	408232
Stand:	01.10.2021
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

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 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 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 installiert und ermöglicht eine sichere, chatbasierte Kommunikation mit anderen Teilnehmern 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 TI-Messenger-Fachdienste bereitgestellt werden.

Die Kommunikation zwischen Teilnehmern 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 Nachrichten werden verschlüsselt auf dem jeweiligen Matrix-Homeserver gespeichert. Die beteiligten 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 TI-Messenger-Clients. Dies wird ermöglicht, indem während des Logins ein auf dem Client hinterlegtes Zertifikat für den Login verwendet wird. Ein TI-Messenger-Client überprüft während des Logins, ob es sich um einen zugelassenen Matrix-Homeserver handelt.

Die folgende Abbildung "*Systemüberblick (Vereinfachte Darstellung)*" zeigt einen Systemüberblick aller am TI-Messenger beteiligten Teilkomponenten in vereinfachter Form.

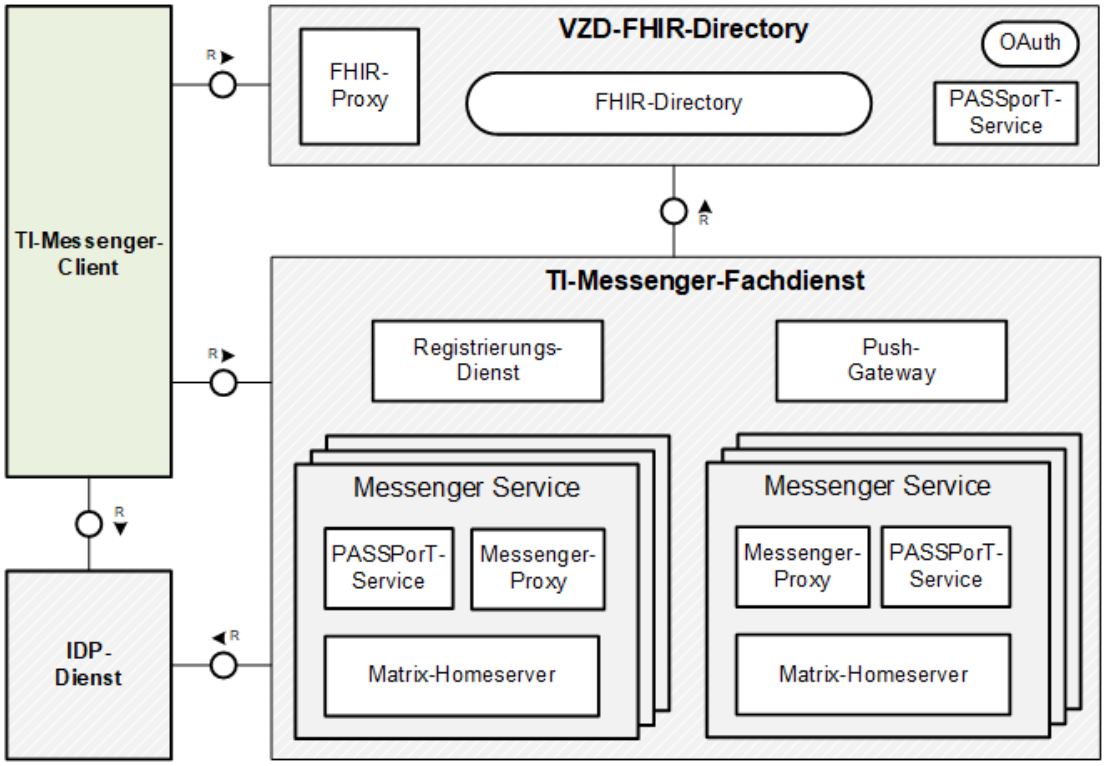

Abbildung 1: Systemüberblick (Vereinfachte Darstellung)

3 Systemkontext

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

3.1 Nachbarsysteme

Die folgende Abbildung zeigt die benachbarten Komponenten des TI-Messenger-Clients:

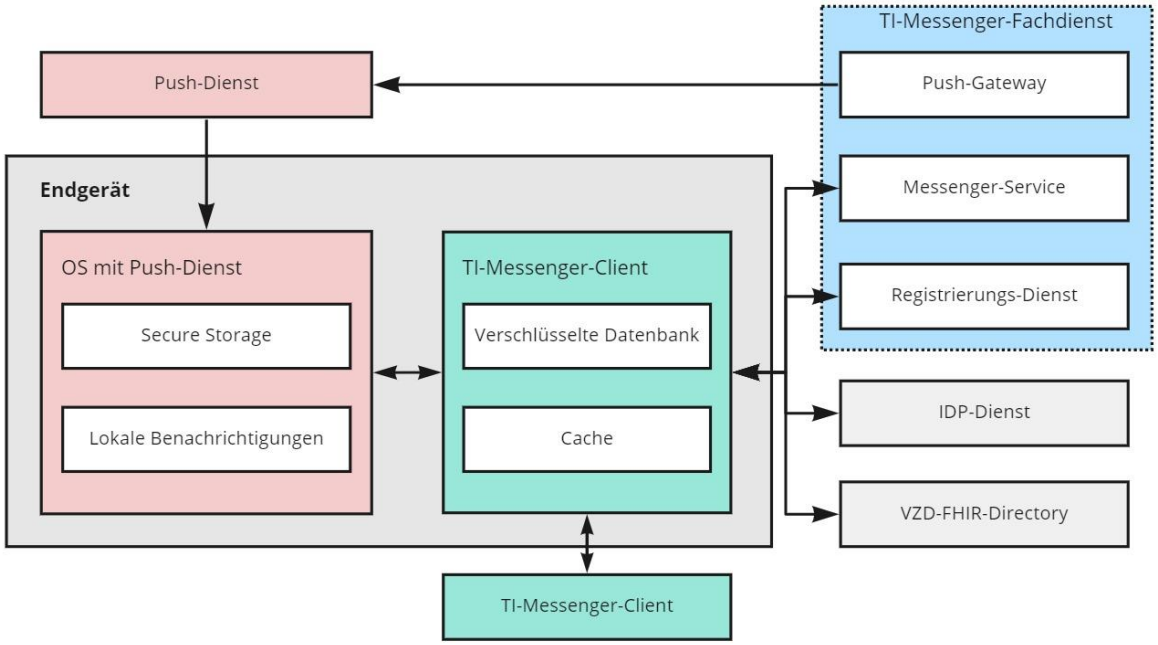

Abbildung 2: Benachbarte Komponenten des TI-Messenger-Clients

Die im Folgenden 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 die für das Funktionieren des TI-Messenger-Clients benötigten Funktionen benennen.

Tabelle 1: Übersicht der Komponenten und deren Funktionen

Komponente	Funktion
Push-Gateway	• Weiterleitung von Push-Benachrichtigungen

Messenger-Service	• Stellt für TI-Messenger-Clients Schnittstellen gemäß [Matrix Foundation#Client_Server] bereit • Liefert Matrix-OpenID-Token für Lesezugriff VZD-FHIR-Directory
Registrierungs-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
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	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.
Push-Dienst	Push-Dienste sind Services von Push-Anbietern und werden für die native Unterstützung von Push-Benachrichtigungen auf der Mehrzahl mobiler Geräte benötigt.

3.2 TI-Messenger-Clients 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. Im Folgenden werden die beiden Ausprägungen beschrieben:

TI-Messenger-Client mit Administrationsfunktionen

Der TI-Messenger-Client mit Administrationsfunktionen ist ein Client für Administratoren einer Organisation. Dieser 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. Administratoren einer Organisation haben die Möglichkeit mittels des TI-Messenger-Clients mit Administrationsfunktionen Benutzer und Geräte auf dem jeweiligen

Messenger-Service zu verwalten. Es besteht ebenfalls die Möglichkeit über den Org-Admin-Client Sessions von angemeldeten Geräten auf dem Messenger-Service zu invalidieren oder zu verifizieren.

TI-Messenger-Client für Nutzer

Der TI-Messenger-Client für Nutzer unterstützt die meisten aller, durch die Matrix-Spezifikation festgelegten Funktionalitäten eines Matrix-Messengers. Nutzer können mit Hilfe des TI-Messenger-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 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. HBA-Inhaber haben zusätzlich die Möglichkeit, die eigene MXID als Kontaktadresse des bereits vorhandenen Practitoner-Eintrages zu setzen. Das Eintragen der MXID gewährt die Suche nach anderen, auf dem VZD-FHIR-Directory eingetragenen HBA-Inhabern und ermöglicht das Auffinden durch andere HBA-Inhaber.

3.3 TI-Messenger-Clients für unterschiedliche Plattformen

Anbieter eines TI-Messenger-Clients MÜSSEN einen mobilen- und einen desktopfähigen TI-Messenger-Client zur Verfügung stellen. TI-Messenger-Clients haben je nach Installationsort (Mobil/Stationär) unterschiedliche Anforderungen an Sicherheit, Datenschutz und Funktionen. Im Folgenden werden die zu unterstützenden Plattformen beschrieben:

Mobil

Es handelt sich hierbei um einen TI-Messenger-Client, der speziell für die Nutzung auf mobilen Geräten entwickelt wurde. Dabei handelt es sich um eine native mobile Anwendung oder eine Integration in eine bestehende native Anwendung. Die mobile Anwendung MUSS die betriebssystemseitigen Funktionen in Bezug auf Sicherheit nutzen und sicherstellen, dass die Speicherung von Daten getrennt und verschlüsselt vom Dateisystem erfolgt. Ein unerlaubter Zugriff durch Dritte MUSS aktiv verhindert werden.

Web

Der TI-Messenger-Client KANN als Web-Frontend für den stationären Einsatz zur Verfügung gestellt werden. Es MUSS sichergestellt werden, dass die Web-Applikation vor unerlaubten Zugriff durch andere Nutzer geschützt wird. Es MUSS sichergestellt werden, dass bei Aufruf des Web-Frontends durch Nutzer auf dem Mobilgerät ein entsprechender Nutzungshinweis angezeigt wird.

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.

4 Übergreifende Festlegungen

4.1 Datenschutz und Sicherheit

Für die datenschutzrechtlichen Anforderungen an den TI-Messenger 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" verwiesen. Die Inhalte der Stellungnahme werden hier zusammenfassend und vereinfachend als Akzeptanzkriterium an den TI-Messenger-Client dargestellt. Anforderungen, die durch andere Systemkomponenten sichergestellt werden, sind hier nicht dargestellt.

ML-124880 - Anforderungen aus der Konferenz der unabhängigen Datenschutzaufsichtsbehörden

- Der TI-Messenger-Client MUSS für den Nutzer 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 unterstützen.
-
- 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 in der Rolle *Org-Admin* beendet wird.

- Der TI-Messenger-Client DARF Standortdaten NICHT dauerhaft erheben.
- Der TI-Messenger-Client MUSS über (teil-)automatisierte Updateprozesse verfügen.

[<=]

ML-123584 - Authentisierung des Nutzers gegenüber dem TI-Messenger-Client
Der TI-Messenger-Client MUSS über ein 2-Faktor-Authentisierungsverfahren verfügen, um sich zu authentisieren gibt der Nutzer bei jedem Start der Applikation eine sechsstellige 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. Alternativ zum Authentisierungsmittel PIN sind auch die Mittel Biometrie, starke Passphrase oder Fido-Token zulässig. Falls das Merkmal Biomentrie gewählt wird, MUSS es den Vorgaben von [BSI-TR-03166] Kap. 2.3.1.5 oder 2.3.1.6 genügen. Als zweiten Faktor MUSS der TI-Messenger-Client prüfen, ob er auf dem Gerät gestartet wurde, an welches er gebunden ist. Für Webclients entfällt diese Authentisierung. Diese Funktionen DÜRFEN NICHT abschaltbar sein und MÜSSEN unabhängig von den Entsperrfunktionen der Endgeräte sein.
Der Hersteller SOLL eine Sperre implementieren, die nach längerer Inaktivität an Webclients die weitere Nutzung verhindert, bis sich erneut wie zuvor beschrieben authentisiert wird. Die nötige Dauer der Inaktivität MUSS durch den Nutzer konfigurierbar und auf eine Stunde voreingestellt sein.
Der TI-Messenger-Client MUSS den Nutzer bei Erstverwendung des TI-Messenger-Clients, falls das Merkmal PIN oder Passphrase gewählt wurde, dazu zwingen eine solche festzulegen. Dabei ist technisch zu prüfen, dass ein PIN oder Passphrase entsprechend sicher ist. Dies kann beispielsweise durch das Anzeigen von 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 - Verhinderung der Erstellung von Screenshots
Mobile TI-Messenger-Clients MÜSSEN Screenshots und Screencapturing verhindern, sofern das Betriebssystem dies zulässt, oder Nutzer nach Aufnahme eines Screenshots klar darauf hinweisen, dass dieser nicht durch den TI-Messenger geschützt werden kann.
[<=]

ML-123589 - Mandantenfähigkeit von Clients
Hersteller des TI-Messenger-Clients MÜSSEN sicherstellen, dass TI-Messenger-Clients eine geeignete Mandantentrennung unterstützen, die verhindert, dass bei geteilten Endgeräten ein Nutzer des TI-Messenger-Clients auf Daten oder Funktionen der TI-Messenger-Client-Devices eines anderen Nutzers auf diesem Gerät zugreifen kann.
[<=]

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

ML-123583 - Informationspflicht bzgl. Gefahren unsicherer Endgeräte
Der TI-Messenger-Client MUSS den Nutzer in einem Hinweistext auf die Gefahren hinweisen, die bei einem Betrieb des Clients auf Hardware, die nicht unter der Kontrolle

des Nutzern steht, gegeben sind. Das betrifft neben geteilten Endgeräten ohne IT-Security-Überwachung insbesondere öffentlich zugängliche Endgeräte. Der Nutzer MUSS die Empfehlung erhalten auf solchen Geräten den TI-Messenger-Client nicht zu nutzen.
[<=]

ML-123586 - Key-Sharing zwischen Geräten eines Nutzers
Um Synchronisation von Nachrichteninhalten zwischen mehreren Devices eines Nutzers zu ermöglichen, verfügt Matrix über vorgesehene Key-Sharing-Funktionalität. Der Hersteller MUSS die Matrix Vorgabe SHOULD "Key-Sharing nur für verifizierte Geräte" als MUST umsetzen.
[<=]

ML-124004 - Key-Sharing zwischen Geräten innerhalb eines Chatraums
Hersteller des TI-Messenger-Clients MÜSSEN sicherstellen, dass TI-Messenger-Clients 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 - Versand von Dateien mittels Matrix
Für den Versand von Dateien gemäß der Matrix-Spezifikation über den TI-Messenger gilt:

- Der Hersteller MUSS sicherstellen, dass die Verschlüsselung für übertragene Inhalte aktiviert ist.
- Der Hersteller MUSS sicherstellen, dass mindestens Dateien mit einer Größe von 25MB versendet werden können.
- Der Hersteller SOLL eine Größenbeschränkung für versendete Dateien implementieren.
- Der Hersteller MUSS sicherstellen, dass die Möglichkeit besteht, empfangene und entschlüsselte Dateien an eine Stelle zur Schadsoftwareprüfung zu übermitteln und prüfen zu lassen, bevor diese verarbeitet werden. Dateien, die eine solche Prüfung nicht erfolgreich durchlaufen, SOLLEN verworfen werden. Falls eine Datei verworfen wird MUSS der Nutzer darüber und über den Grund informiert werden.
- Nutzer MÜSSEN bei der Verwendung einer nicht erfolgreich geprüften Datei auf dessen Prüfstatus - und mögliche Gefahren - hingewiesen werden.

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

Maßnahmenvorschläge:

- Prüfen, ob Dokumenten-Format und Inhalt mit dem angegebenen Dokumententyp in den Metadaten übereinstimmt
- Vor der Anzeige eines Dokumentes sind Sonder- und Meta-Zeichen im Dokument für die jeweilige Anzeigesoftware mit der richtigen Escape-Syntax zu entschärfen.
- Die Anzeigesoftware in einer Sandbox betreiben.

ML-123588 - Abschottung der TI-Messengerinhalte
Mobile TI-Messenger-Clients MÜSSEN sicherstellen, dass Daten, die lokal gespeichert werden, nicht im allgemeinen Speicher des Geräts abgelegt werden, sondern in einem TI-Messenger-Client spezifischen Speicherbereich auf dem Endgerät.
Mobile TI-Messenger-Clients MÜSSEN sicherstellen, dass andere Applikationen auf den Endgeräten nicht auf Inhalte des TI-Messengers zugreifen können. Hierzu SOLL der Hersteller eine Abschottung des Speichers, den der TI-Messenger für Nutzerdaten belegt, implementieren. 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 ausgelesen werden können.
TI-Messenger-Clients MÜSSEN ein Öffnen von über den TI-Messenger empfangenen Dateien durch Drittprogramme ermöglich. Hierbei MUSS er sicherstellen, dass eine solche Ausleitung von Daten nur ausgelöst durch den TI-Messenger-Client erfolgt. Der TI-Messenger-Client KANN eine Funktion enthalten, mittels derer empfangene Dateien außerhalb des dedizierten Speichers im Gerätespeicher abgelegt werden. Der TI-Messenger-Client MUSS sicherstellen , dass Nutzer bei Verwenden einer solchen Funktion geeignet darüber informiert werden, dass sie Daten aus dem geschützten Bereich des TI-Messengers hinausbewegen.
[<=]

ML-123590 - Sicherheitskritische Updates
Anbieter des TI-Messenger-Clients MÜSSEN sicherstellen, dass Nutzer über die Veröffentlichung von Updates für ihre TI-Messenger-Clientsoftware 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 gegenüber dem Homeserver. Die Möglichkeit weiter Updates einzuspielen MUSS in diesem Fall weiterhin gegeben sein. Nutzer 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 - Device Verification, Cross-Signing und SSSS für TI-Messenger-Clients
Hersteller MÜSSEN sicherstellen, dass die Funktionen Cross-Signing und Secure Secret Storage and Sharing (SSSS) zur Device Verification unterstützt werden. Es MUSS 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.
[<=]

ML-123861 - Ende-zu-Ende-Verschlüsselung
Hersteller MÜSSEN sicherstellen, dass eine vollständige Ende-zu-Ende-Verschlüsselung auf Basis von OLM/MEGOLM unterstützt wird. Dazu MUSS der Spezifikation 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 - Explizites Verbot von Profiling für TI-Messenger-Clients
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.

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 - Einbringung und Speicherung von Schlüsseln und Token
Hersteller von TI-Messenger-Clients MÜSSEN sicherstellen, dass Schlüssel und Token sicher in den Client eingebracht werden. Hierzu genügt eine Prüfung des Prozesses. 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 des beteiligten Homeservers.
[<=]

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

ML-123597 - Löschfunktionen für TI-Messenger-Inhalte
Der Hersteller von TI-Messenger-Clients MUSS eine automatisierte Löschfunktion für TI-Messenger-Client-Nachrichten implementieren. Diese MUSS eine zumutbare voreingestellte Löschfrist enthalten, welche für Nutzer konfigurierbar ist. Die Löschfrist MUSS hierbei auf den minimal einstellbaren Wert initialisiert sein. Nach Verstreichen der eingestellten Löschfrist MÜSSEN Gesprächsinhalte aus dem TI-Messenger-Client sicher gelöscht werden. Der Hersteller MUSS zusätzlich eine nachrichtenbasierte Löschfunktion vorsehen, die es Nutzern erlaubt ihre eigenen Nachrichten händisch nicht nur vom

eigenen TI-Messenger-Client, sondern auch aus dem Room State zu löschen.
[<=]

ML-123607 - Privacy by Default
Der Hersteller eines TI-Messenger-Clients MUSS für die Standardeinstellungen des TI-Messenger-Clients stets die datenschutzfreundlichste Voreinstellung konfigurieren.
[<=]

ML-123608 - Verwendung von OWASP Mobile
Der Hersteller eines mobilen TI-Messenger-Clients MUSS bei der Entwicklung von TI-Messenger-Clients die Maßnahmen und Vorgaben der aktuellen Version der OWASP-Top-10-Mobile-Risiken [OWASPMobileTop10] umsetzen. Hierbei SOLLEN die Vorgaben der Prüfvorschrift für den Produktgutachter des „ePA-Frontend des Versicherten" analog für den TI-Messenger-Client umgesetzt werden, mit Ausnahme folgender Punkte:

Punkt	Begründung
O.Arch_7	Der tatsächliche Sicherheitsgewinn steht in keinem Verhältnis zum Aufwand.
O.Auth_6	Diese Maßnahme wird im Zuge der Einführung des Zero-Trust-Modells in späteren TI-Messenger-Spezifikationsversionen ergänzt.
O.Auth_11	Diese Maßnahme wird bereits in ML-123584 behandelt.
O.Sess_1 bis _6	Das Session-Handling von Matrix weicht zu weit vom angenommenen Stand ab um diese Maßnahmen sinnvoll wie vorgesehen umzusetzen.
O.Tokn_10	Diese Funktion wird über das Matrix-Protokoll mittels Devices unterstützt.
O.Data_5 erster Satz	Für den TI-Messenger-Client wurde eine Funktion vorgesehen, die eine Standardlöschfrist für Inhalte setzt und Nutzern die Möglichkeit gibt selbst über die Aufbewahrungsdauer ihrer Gesprächsinhalte zu bestimmen.
O.Data_6	Diese Maßnahme steht den Sicherheitszielen des TI-Messengers diametral entgegen.
O.Data_12	Diese Maßnahme ist bereits in ML-123585 geregelt.
O.Data_19	Diese Maßnahme richtet sich nicht an den 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 - 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
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 - Sichere Softwareverteilung
Der Hersteller eines TI-Messenger-Clients MUSS Nutzer über die vertrauenswürdigen Quellen informieren, von denen Nutzer den TI-Messenger-Client beziehen können und wie sie die Vertrauenswürdigkeit der Quelle erkennen können. Der Hersteller MUSS sicherstellen, dass der Nutzer 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.
[<=]

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 - Datenschutzkonformes Tracking
Der TI-Messenger-Client DARF NICHT Werbe-Tracking verwenden.
Im Folgenden wird unter Tracking 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 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 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 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 nutzt, den Nutzer 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 nutzt, für jede Clientnutzung neue Nutzungsidentifier zufällig generieren. Der Nutzer 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 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 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 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 erfolgt ist und MUSS jederzeit durch diese deaktivierbar sein.
Ein Verweis auf AGBs oder Nutzungsbedingungen des TI-Messengers 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 DARF NICHT wiederholt beim Nutzer anfragen um eine Einwilligung durch Belästigung zu erzwingen. Nach einmaliger Ablehnung durch den Nutzer MUSS jede Anzeige des Dialogs explizit durch den Nutzer initiiert werden.
[<=]

ML-123632 - CC-Evaluierung als Ersatz für 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,
- die in den zusätzlichen Funktionen verarbeiteten Daten,

- die Schnittstellen zwischen dem TI-Messenger-Client des Nutzers und den ggf. genutzten Backend-Diensten der zusätzlichen Funktionen inklusive ihrer Sicherheitsmaßnahmen und
- die Sicherheitsannahmen an das TI-Messenger-Client des Nutzers 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
TI-Messenger-Clients MÜSSEN verhindern, dass Nutzer mittels Nutzereingaben Informationen in Room-States bringen. Sobald durch die geplante Matrix-Spec-Changes (MSCs) die Möglichkeit geschaffen wurde, vertrauliche Informationen sicher im Room-State zu speichern, wird dies direkt durch die Matrix-Spezifikation abgedeckt. **[<=]**

4.2 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 Funktionen durch den Hersteller bereitgestellt werden, um ein Mindestmaß an Nutzererfahrung zu erreichen.

Präsenzanzeige

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

Erwähnungen

TI-Messenger-Clients MÜSSEN es ermöglichen, dass über das Eingabefeld andere Nutzer gemäß [Erwähnung] 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, MUSS der 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 implementieren. TI-Messenger-Clients für Nutzer MÜSSEN diese Funktion des Anzeigens und 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) standardmäßig deaktiviert sein.

Eingabebenachrichtigungen

Mobile TI-Messenger-Clients MÜSSEN die Matrix-Spezifikation gemäß [Eingabebenachrichtigungen] vollständig 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) 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.
[<=]

4.3 Konfiguration des TI-Messenger-Clients

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

Einstellung von Push-Benachrichtigungen

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

4.4 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, Testspezifikationen, Testfälle sowie 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 IOP-Tests, die Synchronisierung von Meilensteinen und regelmäßige industriepartnerübergreifenden Test-Sessions. Die Test-Sessions umfassen gegenseitige IOP- und E2E Tests.

Die gematik stellt eine TI-Messenger-Fachdienst 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 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.

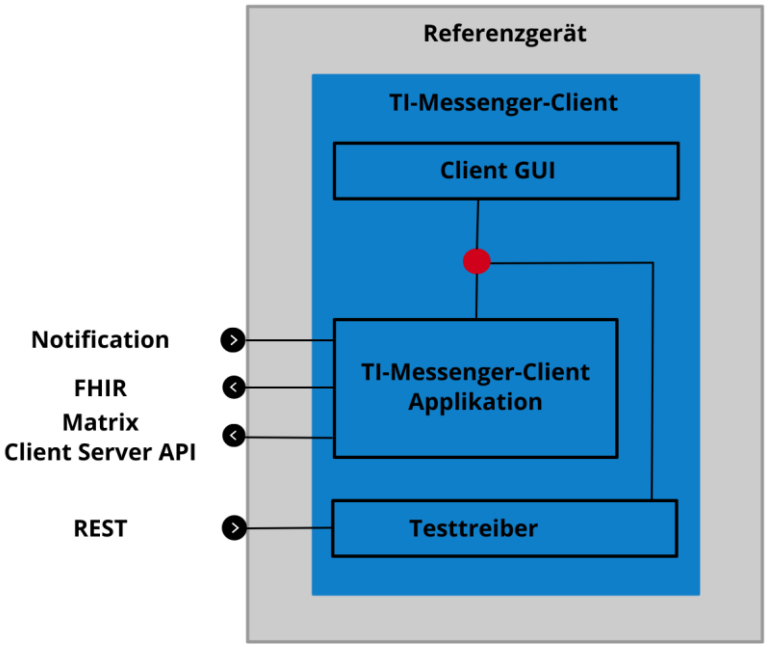

Abbildung 3: Testtreiberschnittstelle

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. 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 die Inhalte nicht verfälschen. Die konkrete Ausgestaltung der Schnittstellen wird im Fachportal der gematik und in GitHub zur Verfügung gestellt.

ML-124878 - Beschränkung Einsatz Testtreiber-Modul
Der produktive TI-Messenger-Client DARF 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 des TI-Messenger-Clients umsetzen.
[<=]

4.5 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 des TI-Messengers.

Der TI-Messenger-Anbieter MUSS seine Nutzer 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 MUSS sein Produkt TI-Messenger-Client mit einer vollumfänglich-funktionalen Verfügbarkeit von 98% seinen Nutzern anbieten.

5 Funktionsmerkmale

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

5.1 Authentisierung

SSO Login

TI-Messenger-Clients MÜSSEN die Matrix-Spezifikation gemäß [SSO Login] vollständig implementieren.

OpenID

TI-Messenger-Clients MÜSSEN die Matrix-Spezifikation gemäß [OpenID] vollständig implementieren.

Gäste Accounts

Der Hersteller eines TI-Messenger-Client MUSS 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] umsetzen.

Room Upgrades

TI-Messenger-Clients MÜSSEN die Matrix-Spezifikation gemäß [Room Upgrades] vollständig implementieren. TI-Messenger-Clients MÜSSEN mit Raum 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 [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 die Matrix-Spezifikation gemäß [Geräteverwaltung] vollständig implementieren.

Ende-zu-Ende-Verschlüsselung

TI-Messenger-Clients MÜSSEN die Matrix-Spezifikation gemäß [Ende-zu-Ende-Verschlüsselung] vollständig implementieren. 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 Nachrichten versendet werden.

Reporting von Inhalten

TI-Messenger-Clients MÜSSEN die Matrix-Spezifikation gemäß [Reporting-content] implementieren und den Nutzern die Möglichkeit geben, unerwünschten Inhalt an Nutzer in der Rolle *Org-Admin* zu melden.

5.3 Instant Messaging

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

Folgende Events und `Msgtypes` MÜSSEN 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 Client keine formatierten Nachrichten unterstützt, ist ein Fallback im Plaintext für beispielsweise Replies spezifiziert:

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

TI-Messenger-Clients MÜSSEN Fallbacks für folgende Events unterstützen:

- Fallback für Antworten/Zitieren
- 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

TI-Messenger-Clients MÜSSEN eine Funktion anbieten, um Direktnachrichten gemäß [Direct Messaging] mit anderen Nutzern des TI-Messenger-Dienstes auszutauschen. Direktnachrichten bedeutet, dass ein Chatraum nur zwischen zwei Personen erstellt wird. Dieser Chatraum kann nicht um weitere Teilnehmer erweitert werden. Soll ein Chatraum für mehr als zwei Teilnehmer erstellt werden, ist Group Messaging zu 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:

Direktnachrichten innerhalb eines Messenger-Services	
Userstory	1. Nutzer möchte neue Unterhaltung starten 2. Client zeigt Nutzerverzeichnis an 3. Nutzer wählt Gesprächspartner aus und startet Chat
Direktnachrichten zwischen verschiedenen Messenger-Services	
Userstory mittels VZD-FHIR-Directory	1. Nutzer A (verifizierter HBA-Inhaber) möchte eine neue Unterhaltung mit Nutzer B (verifizierten HBA-Inhaber) starten

	2. Nutzer A durchsucht VZD-FHIR-Directory nach Nutzer B 3. TI-Messenger-Client zeigt Profil (Name, Organisationszugehörigkeit, Berufsgruppe) von Nutzer B an 4. Nutzer A startet Chat mit Nutzer B Client zeigt an, dass es sich um einen Direktchat handelt. Eine Umwandlung in Gruppe ist nicht möglich.
Userstory mittels QR-Scan	1. Nutzer A und Nutzer B treffen sich in Person 2. Nutzer A und Nutzer B wählen "neue Unterhaltung starten" aus 3. Nutzer A wählt "QR-Code teilen" aus 4. Nutzer B wählt "QR-Code scannen" aus und scannt "QR-Code" von Nutzer A 5. Nutzer A und Nutzer B klicken "weiter" 6. Nutzer B bekommt QR-Code angezeigt, Nutzer A bekommt QR-Code Scanner angezeigt 7. Nutzer A scannt Nutzer B 8. Nutzer A bekommt Dialog, dass Chatraum erstell wird, Nutzer B kann QR-Code schließen 9. Die in diesem Ablauf ausgetauschten Token haben eine Gültigkeit von 10 Minuten.

5.5 Group Messaging

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

Gruppenunterhaltungen innerhalb eines Messenger-Services	
Neue Gruppenunterhaltung	1. Nutzer möchte eine neue Gruppenunterhaltung starten 2. Client zeigt Nutzerverzeichnis an 3. Nutzer wählt Gesprächspartner aus

	4. Gesprächspartner werden in die Gruppenunterhaltung eingeladen 5. Nutzer kann weitere Gesprächspartner hinzufügen
Gruppenunterhaltungen zwischen verschiedenen Messenger-Services	
Nachricht an Organisation	1. Nutzer möchte eine Nachricht an eine Organisation senden 2. Nutzer durchsucht VZD-FHIR-Directory nach Organisation 3. TI-Messenger-Client zeigt Profil der Organisation (Name, Typ, Kontaktmöglichkeiten) 4. Nutzer startet Chat mit Organisation, hinterlegte MXID der Organisation wird in Chatgruppe eingeladen (Nutzer, Bot)
Einladen weiterer Personen	1. Nutzer wollen weitere Personen in Chatgruppe einladen 2. Nutzer durchsucht Nutzerverzeichnis oder VZD-FHIR-Directory (Wenn HBA-Inhaber) 3. Nutzer wählt Person aus 4. Person wird in bestehende Chatgruppe eingeladen
Einladen weiterer Organisationen	1. Nutzer wollen weitere Organisationen in Chatgruppen einladen 2. Nutzer durchsucht VZD-FHIR-Directory nach Organisation 3. TI-Messenger-Client zeigt Profil der Organisation (Name, Typ, Kontaktmöglichkeiten) 4. Nutzer lädt Organisation in bestehende Gruppenunterhaltung ein

5.6 Push-Benachrichtigungen

Mobile TI-Messenger-Clients MÜSSEN die Matrix-Spezifikation gemäß [Push-Benachrichtigungen] vollständig implementieren.

5.6.1 Allgemein

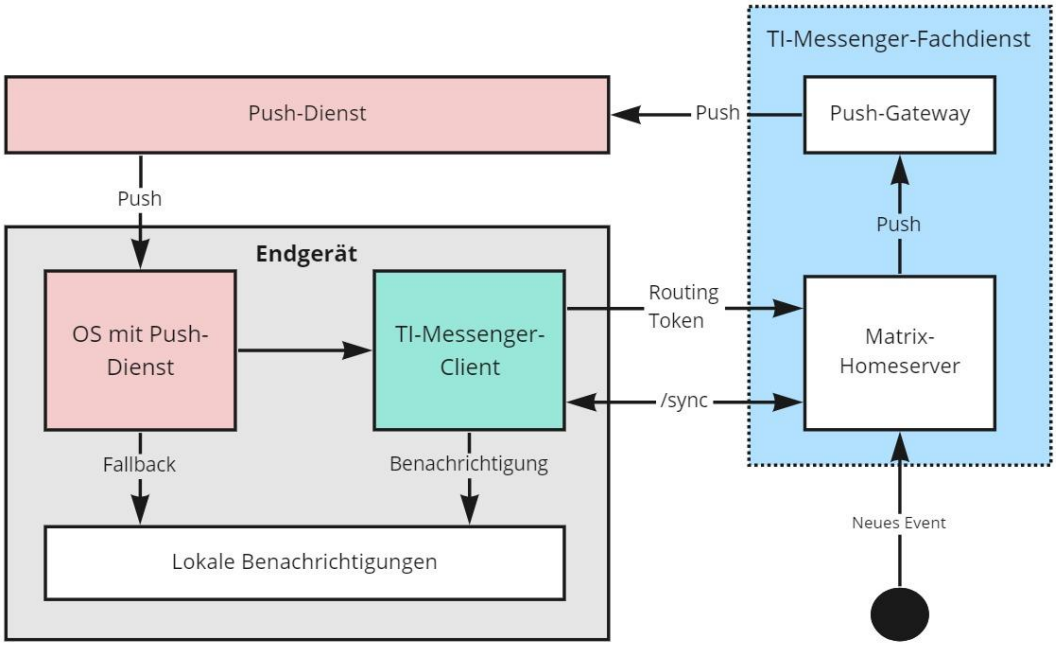

Abbildung 4: Push-Benachrichtigung für Mobilgeräte

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:

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.
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 mit dem Matrix-Homeserver und zeigt die Benachrichtigung lokal an.

5.6.2 Push-Anbieter

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

5.6.3 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 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.

5.6.4 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.

5.6.5 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 MUSS dem Nutzer Möglichkeiten anbieten Push-Regelsätze zu verwalten.

5.6.6 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.

5.7 Weitere Funktionen

Erstellung des Localparts

Der TI-Messenger-Client MUSS bei der Erstellung des Localparts der MXID eines Nutzers sicherstellen, dass keine personenbezogenen Daten entstehen. Dazu MUSS der TI-Messenger-Client den local-Part der verwendeten MXID des Nutzers als Base32 SHA256 Hash berechnen.

Beispiel einer MXID

`@74c1fecc710ce4c8a8bbe310fbc5954c2a5e1e9ef5f70d651da1bfc4c9abe43f:<domain>.de`

ML-124045 - Base32 SHA256 Hash

Der Client MUSS für die MXID einen Hash-Wert mittels Base32 SHA256 zu berechnen.
[<=]

Displayname

Der TI-Messenger-Client MUSS sicherstellen, dass nur Nutzer in der Rolle *Org-Admin* den Displaynamen von Nutzern bearbeiten können. Es MUSS sichergestellt werden, dass Nutzer den eigenen Displaynamen nicht ändern können.

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. 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 direkt ausgeloggt werden.

Ende-zu-Ende Verschlüsselung

Der TI-Messenger-Client MUSS sicherstellen, dass sämtliche Nachrichteninhalte Ende-zu-Ende [Ende-zu-Ende Verschlüsselung] verschlüsselt werden. Das Senden von Nachrichten ohne Ende-zu-Ende Verschlüsselung MUSS technisch unterbunden werden.

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.

6 Anhang A – Verzeichnisse

6.1 Abkürzungen

Kürzel	Erläuterung
CC	Common Criteria
FHIR	Fast Healthcare Interoperable Resources
IDP	Identity Provider
JSON	JavaScript Object Notation
MXID	Matrix-ID
OAuth	Open Authorization
PASSporT	Personal Assertion Token
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
[gemGlossar]	gematik: Einführung der Gesundheitskarte – Glossar
[gemSpec_TI-Messenger-Dienst]	gematik: Spezifikation TI-Messenger-Dienst
[gemSpec_TI-Messenger-FD]	gematik: Spezifikation TI-Messenger-Fachdienst
[gemSpec_Krypt]	gematik: Übergreifende Spezifikation - Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur
[gemSpec_VZD_FHIR_Directory]	gematik: Spezifikation Verzeichnisdienst FHIR-Directory
[gemKPT_Betr]	gematik: Betriebskonzept Online-Produktivbetrieb

6.5.2 Weitere Dokumente

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[Matrix Foundation]	Matrix Foundation https://matrix.org/docs/spec/
[Instant Messaging]	Matrix Foundation https://matrix.org/docs/spec/client_server/r0.6.1#id42
[Direct Messaging]	Matrix Foundation https://matrix.org/docs/spec/client_server/r0.6.1#id140
[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 Foundation https://matrix.org/docs/spec/client_server/r0.6.1#id129
[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
[OWASPMobileTop 10]	OWASP Mobile Top 10 https://owasp.org/www-project-mobile-top-10/
[OWASP Proactive Control]	OWASP Proactive Controls https://owasp.org/www-project-proactive-controls/
[ISO 9241]	Ergonomics of human-system interaction https://www.iso.org
[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