Elektronische Gesundheitskarte und Telematikinfrastruktur

Spezifikation
TI-Messenger-Fachdienst

Version:	1.1.0 CC
Revision:	469910
Stand:	13.06.2022
Status:	zur Abstimmung freigegeben
Klassifizierung:	öffentlich_Entwurf
Referenzierung:	gemSpec_TI-Messenger-FD

Dokumentinformationen

Änderungen zur Vorversion

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

Dokumentenhistorie

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

Inhaltsverzeichnis

1 Einordnung des Dokumentes

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-Fachdienst. Der Fachdienst ermöglicht die sichere Ad-hoc-Kommunikation zwischen Teilnehmern. Aus den Kommunikationsbeziehungen mit dem TI-Messenger-Client und dem VZD-FHIR-Directory resultieren vom TI-Messenger-Fachdienst anzubietende Schnittstellen, die in diesem Dokument normativ beschrieben werden. Vom TI-Messenger-Fachdienst genutzte Schnittstellen liegen zumeist in anderen Verantwortungsbereichen (z. B. IDP-Dienst). Diese werden in der entsprechenden Produkttypspezifikation definiert.

1.2 Zielgruppe

Das Dokument richtet sich zwecks der Realisierung an Hersteller des Produkttypen Fachdienst TI-Messenger 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 Fachdienst TI-Messenger 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, Kapitel 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-Fachdienst 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-Fachdienst ermöglicht eine sichere Kommunikation zwischen verschiedenen Akteuren im deutschen Gesundheitswesen. Dieser basiert auf dem offenen und dezentralen Kommunikationsprotokoll Matrix. Dabei stellt der Matrix Standard RESTful-APIs für die sichere Übertragung von JSON-Objekten zwischen Matrix-Clients und weiteren Diensten bereit. Die sichere Kommunikation zwischen den einzelnen Akteuren findet in verschlüsselter Form in Räumen auf den beteiligten Matrix-Homeservern statt.

Der TI-Messenger-Fachdienst besteht aus dezentralen und zentralen Teilkomponenten, welche bei der Produktzulassung getestet werden und die ein TI-Messenger-Anbieter bereitstellen MUSS. Bei den dezentralen Teilkomponenten handelt es sich um die Messenger-Services. Ein Messenger-Service besteht aus einem Matrix-Homeserver und einem Messenger-Proxy, der dafür sorgt, dass eine Föderation der Matrix-Homeserver nur zwischen verifizierten Domains stattfindet. Messenger-Services werden für einzelne Organisationen (z. B. Leistungserbringerinstitutionen, Verbände) bereitgestellt und erlauben die Nutzung durch alle berechtigten Akteure einer Organisation. Weiterhin KÖNNEN Messenger-Services Authentifizierungsverfahren anbieten, die nicht einer Organisation zugeordnet sind. Diese unterscheiden sich technisch nicht von anderen Messenger-Services. Einzig die zugeordnete Organisation bietet ein für diese Akteure notwendiges Authentifizierungsverfahren an.

Die Kommunikation zwischen einem TI-Messenger-Client und einem TI-Messenger-Fachdienst erfolgt immer über den Messenger-Proxy der Messenger-Services. Am Messenger-Proxy eines Messenger-Service findet zunächst die TLS-Terminierung der Verbindungen von den TI-Messenger-Clients statt. Der Messenger-Proxy kontrolliert die Zugehörigkeit zur TI-Föderation durch den Abgleich mit einer durch seinen Registrierungs-Dienst bereitgestellten Föderationsliste. Hierbei prüft der Messenger-Proxy, ob die beteiligten Matrix-Homeserver registrierte Mitglieder der Föderation sind und ein Akteur berechtigt ist, Anfragen auf dem Matrix-Homeserver auszulösen.

Neben den dezentralen Messenger-Services besteht ein TI-Messenger-Fachdienst aus den zentralen Teilkomponenten Registrierungs-Dienst und Push-Gateway. Über den Registrierungs-Dienst bekommt der TI-Messenger-Anbieter die Möglichkeit Messenger-Services automatisiert Organisationen zur Verfügung zu stellen und die Matrix-Domain der von ihm bereitgestellten Messenger-Services in deren Organisationsressource in das zentrale VZD-FHIR-Directory einzutragen. Der Registrierungs-Dienst eines TI-Messenger-Fachdienstes bietet als weitere Funktionen die Bereitstellung einer Föderationsliste für die Messenger Proxies seiner Messenger-Services und die Möglichkeit zur Administration einer Freigabeliste. Das Push-Gateway dient zur Übertragung von Benachrichtigungen (Notifications) an die jeweiligen TI-Messenger-Clients um den Eingang einer neuen Nachricht zu signalisieren.

In der folgenden Abbildung sind alle beteiligten Komponenten der TI-Messenger-Architektur in vereinfachter Form dargestellt. Der in der Abbildung blau dargestellte TI-Messenger-Fachdienst zeigt alle Komponenten die in dieser Spezifikation beschrieben werden.

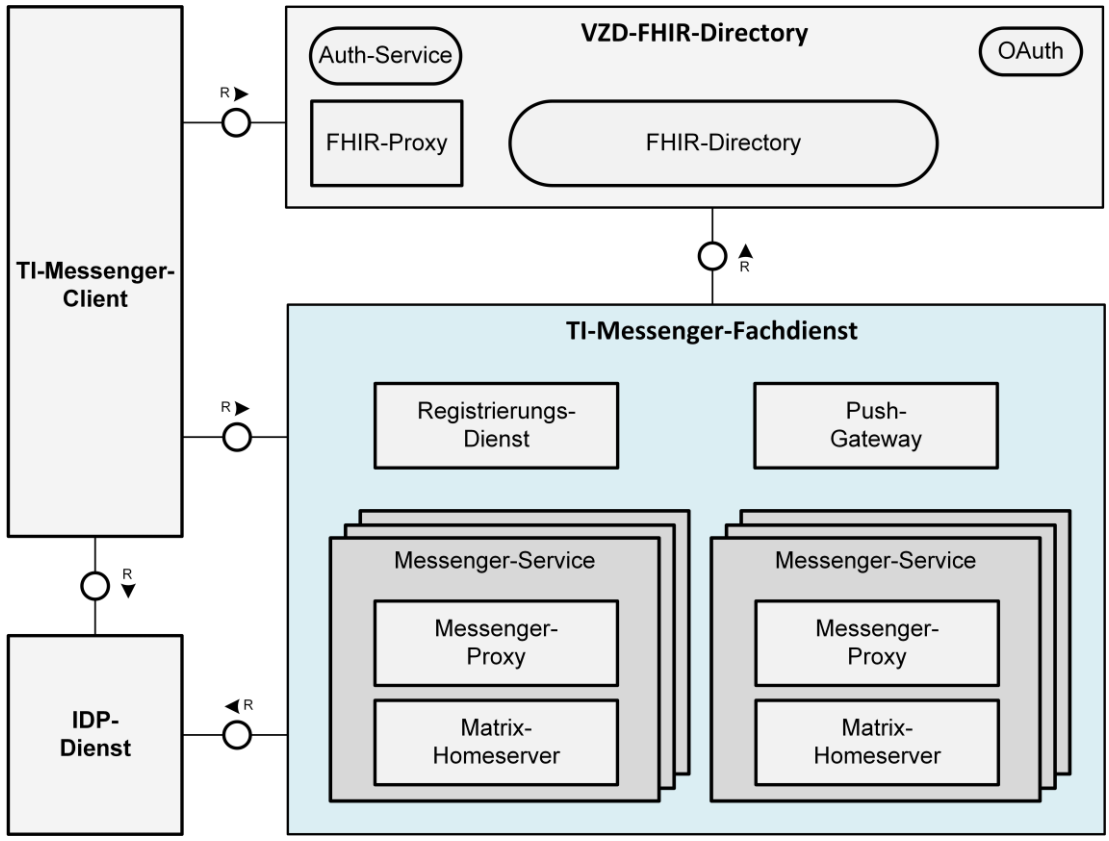

Abbildung 1: Systemüberblick (Vereinfachte Darstellung)

3 Systemkontext

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

3.1 Nachbarsysteme

Für den Betrieb des TI-Messenger-Fachdienstes werden weitere Systeme benötigt. Dazu gehören zuständige IDP-Dienste welche Authentisierungen und Autorisierungen auf Basis von SmartCard-Identitäten durchführen, sowie das VZD-FHIR-Directory. Die in Kapitel 2 zu findende Abbildung *"Systemüberblick"* zeigt deren Beziehung zum TI-Messenger-Fachdienst.

Ein IDP-Dienst stellt allen berechtigten Akteuren ID_TOKEN, gemäß des durch die OpenID Foundation [OpenID] spezifizierten Protokolls, zur Verfügung. Dieses wird vom Auth-Service des VZD-FHIR-Directory verwendet, um ein search-accesstoken oder ein owner-accesstoken für den Lese- bzw. Schreibzugriff auf das FHIR-Directory zu erhalten.

Das zentrale VZD-FHIR-Directory bildet ein Verzeichnis aller TI-Messenger-Fachdienste, Organisationen und Leistungserbringer und bietet die Möglichkeit der Suche von Teilnehmern anhand konfigurierter Merkmale. Der Registrierungs-Dienst des TI-Messenger-Fachdienstes trägt bei erfolgreicher Verifizierung einer Organisation die Matrix-Domain des zugehörigen Messenger-Services der Organisation im VZD-FHIR-Directory ein. Durch diesen Eintrag kann der Messenger-Service an der Föderation des TI-Messenger-Dienstes teilnehmen. Das VZD-FHIR-Directory vertraut den Matrix-Homerservern der jeweiligen Messenger-Services, wenn die Domain des Messenger-Service erfolgreich in das VZD-FHIR-Directory eingetragen wurde.

3.2 Messenger-Services

Durch TI-Messenger-Anbieter werden Messenger-Services für Organisationen des Gesundheitswesens (z. B. Arztpraxis, Krankenhaus, Apotheke, Verband, etc.) bereitgestellt. Die Bereitstellung der Messenger-Services erfolgt über den Registrierungs-Dienst eines TI-Messenger-Fachdienstes und KANN *on-premise* oder zentral innerhalb von Rechenzentren stattfinden. Jeder Messenger-Service MUSS einer Organisation logisch zugeordnet sein. Die Messenger-Services KÖNNEN sich lediglich durch die je Organisation verwendeten Authentifizierungsverfahren unterscheiden. Diese werden durch die jeweilige Organisation festgelegt und bereitgestellt und ermöglichen damit die Nachnutzung bereits innerhalb der Organisation existierender Authentifizierungsverfahren. Die jeweilige Organisation MUSS die Kontrolle über die Benutzerverwaltung haben, um zu jedem Zeitpunkt Nutzer aus dem TI-Messenger ausschließen zu können. Dabei MÜSSEN Akteure vom Messenger-Service gelöscht/gesperrt werden, wenn der Nutzer innerhalb der Nutzerverwaltung gelöscht/gesperrt wurde.

Authentifizierungsverfahren

Messenger-Services MÜSSEN je nach Art der Organisation den Akteuren ein Authentifizierungsverfahren anbieten. Sind zum Beispiel bereits Systeme wie Active-

Directory oder LDAP basierende Nutzerverzeichnisse innerhalb einer Organisation verfügbar, KÖNNEN diese verwendet werden, indem der jeweilige Matrix-Homeserver bei diesen registriert wird. Sind keine Authentifizierungsverfahren in der Organisation vorhanden KÖNNEN TI-Messenger-Anbieter entsprechende Authentifizierungsverfahren zur Verfügung stellen. Diese erlauben eine Authentifizierung von Akteure (z. B. durch Benutzername/Passwort und einen zweiten Faktor) und können auch von weiteren Systemen nachgenutzt werden.

Die nachfolgende Abbildung verdeutlicht die Nachnutzung eines existierenden Authentifizierungsverfahrens von Akteuren innerhalb einer Organisation durch einen Messenger-Service.

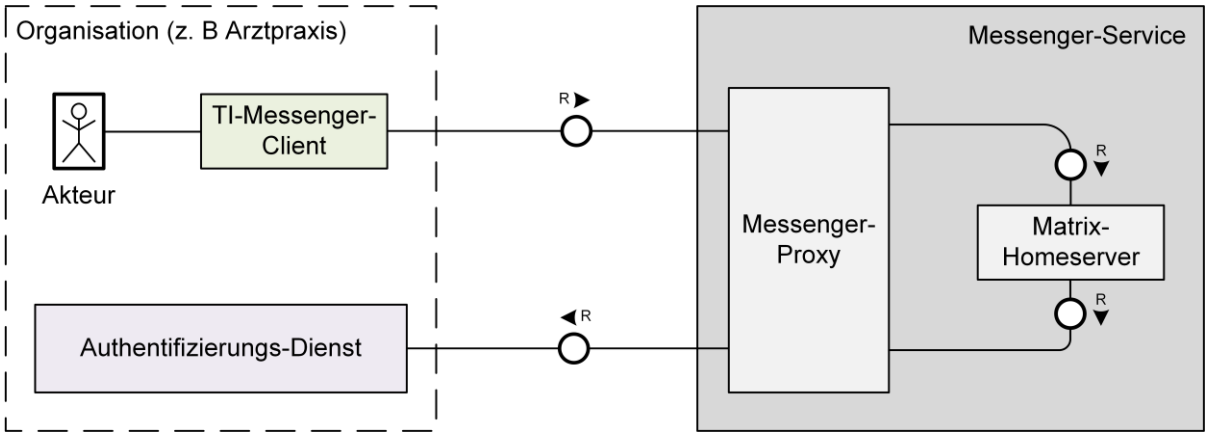

Abbildung 2: Beispiel - Authentifizierung von Akteuren einer Organisation

4 Übergreifende Festlegungen

4.1 Datenschutz und Sicherheit

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

A_22807 - Verbot von Organisationsaccounts für Versicherte
Der TI-Messenger-Anbieter MUSS Kunden vertraglich verpflichten, dass organisationsbasierte TI-Messenger-Accounts nicht an Dritte vergeben werden. Der Anbieter MUSS fordern, dass sichergestellt wird, dass nur Accounts an Akteure vergeben werden, mit denen ein Beschäftigungsverhältnis oder Dienstleistervertragsverhältnis besteht.
[<=]

A_22809 - Flächendeckende Verwendung von TLS für Hersteller
TI-Messenger-Fachdienst-Hersteller MÜSSEN sicherstellen, dass sämtliche Verbindungen zwischen Komponenten des TI-Messenger-Fachdienst mittels TLS kommunizieren, sofern diese Kommunikation die Grenzen einer virtuellen/physischen Maschine überschreitet. Hierzu MUSS mindestens serverseitig authentizitätsgeschütztes TLS verwendet werden. Sofern kein beidseitiges TLS verwendet wird, MUSS die Authentizität der Clientseite mit gleichwertiger Sicherheit sichergestellt werden. Es gelten die Festlegungen gemäß [gemSpec_Krypt].
[<=]

A_22929 - Flächendeckende Verwendung von TLS für Anbieter
TI-Messenger-Anbieter MÜSSEN sicherstellen, dass sämtliche Verbindungen zwischen Komponenten des TI-Messenger-Fachdienstes mittels TLS kommunizieren, sofern diese Kommunikation die Grenzen einer virtuellen/physischen Maschine überschreitet. Hierzu MUSS mindestens serverseitig authentizitätsgeschütztes TLS verwendet werden. Es gelten die Festlegungen gemäß [gemSpec_Krypt].
[<=]

A_22936 - Authentifizierungsverfahren für Akteure in Organisationen
TI-Messenger-Anbieter KÖNNEN für die Authentisierung von Akteuren in der Rolle "User" bestehende Authentifizierungsverfahren der Organisation nachnutzen.
Sollte dies der Fall sein, MÜSSEN Anbieter die Organisation und die Administratoren explizit darauf hinweisen, dass die Sicherheit der Nutzerauthentisierung damit in die Verantwortung der Organisation gegeben wird. Hierzu MUSS der Anbieter sicherstellen, dass er nur Authentifizierungsverfahren akzeptiert, die in der Hand der Organisation sind und deren Authentisierungsmittel von dieser verwaltet werden und gesperrt werden können. Der Anbieter MUSS sicherstellen, dass zur Authentifizierung mindestens zwei Faktoren verwendet werden.
Sofern Anbieter und Organisation die Nachnutzung bestehender Authentifizierungsverfahren nicht vereinbart haben MUSS der Anbieter sicherstellen, dass keine nachgenutzten Authentifizierungsverfahren verwendet werden können.
[<=]

Hinweis: A_22936 regelt lediglich die Authentisierung, die notwendig ist um ein Token zu erhalten, mit dem sich Nutzer gegen den Messenger-Service authentisieren können.

A_22815 - Behandlung von kryptographischem Material für OAuth
TI-Messenger-Anbieter MÜSSEN sicherstellen, dass kryptographisches Material zur Authentisierung gegen das VZD-FHIR-Directory sicher eingebracht wird. Dieses Material MUSS in Hardware Security Modules sicher gespeichert werden.**[<=]**

Zum Nachweis der Umsetzung ist lediglich eine Prüfung der Prozesse zur Einbringung erforderlich. Eine Auditierung der Umsetzung ist optional.

Hinweis: Es ist lediglich ein HSM je Messenger-Anbieter notwendig. Die Verwendung von HSM-Modulen wird für die Lagerung von kryptographischem Material bei den Fachdiensten vorgeschrieben. Sofern eine Mandantentrennung gewährleistet werden kann, ist es nicht erforderlich, mehrere getrennte HSM-Umgebungen zu betreiben.

A_22817 - Explizites Verbot von Profiling für TI-Messenger-Fachdienste
TI-Messenger-Fachdienst-Hersteller DÜRFEN NICHT Daten zu Profilingzwecken 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 Hersteller von Komponenten und Dienste der gematik offenzulegen bzw. zu übermitteln haben, sofern diese erforderlich sind, um den gesetzlichen Auftrag der gematik zur Überwachung des Betriebs zur Gewährleistung der Sicherheit, Verfügbarkeit und Nutzbarkeit der Telematikinfrastruktur zu erfüllen. Nur die hierfür erforderlichen personenbezogenen Daten dürfen von den Anbietern und Herstellern als Ausnahme vom Profilingverbot erhoben und ausschließlich für den genannten Zweck verwendet werden.
[<=]

A_22814 - Explizites Verbot von Profiling für TI-Messenger-Anbieter
TI-Messenger-Anbieter DÜRFEN NICHT Daten zu Profilingzwecken sammeln. Dies betrifft insbesondere eine Überwachung welche Akteure mit welchen anderen Akteuren kommunizieren.

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

A_22813 - Protokollierung zum Zwecke der Fehler- bzw. Störungsbehebung
Falls im TI-Messenger-Fachdienst eine Protokollierung zum Zwecke der Fehler- bzw. Störungsbehebung erfolgt, MUSS der Fachdienst unter Berücksichtigung des Art. 25 Abs. 2 DSGVO sicherstellen, dass in den Protokolldaten entsprechend dem Datenschutzgrundsatz nach Art. 5 DSGVO nur personenbezogene Daten in der Art und dem Umfang enthalten sind, wie sie zur Behebung erforderlich sind und dass die erzeugten Protokolldaten im Fachdienst nach der Behebung unverzüglich gelöscht werden. Sofern andere gesetzliche Grundlagen wie §331 SGB V nicht überwiegen sind hierzu nur anonymisierte Daten zu protokollieren.
[<=]

A_22820 - Kein Einbringen vertraulicher Informationen in Room-States durch Administratoren einer Organisation
TI-Messenger-Anbieter MÜSSEN sicherstellen, dass sie als Organisations-Administratoren keine sensiblen Informationen in Room-States einbringen. Ebenso MÜSSEN Organisations-Administratoren von Matrix-Homeservern unter Kundenverwaltung informieren, dass im Room-State sichtbare Informationen gegenwärtig nicht verschlüsselt sind.
[<=]

A_22811 - Löschfristen für Homeserver
TI-Messenger-Fachdienst-Hersteller MÜSSEN sicherstellen, dass ihre Matrix-Homeserver eine Funktion anbieten, durch die Events, Gesprächsinhalte und mit einzelnen Gesprächen assoziierte Daten (z. B. versandte Dateien) nach einem Zeitraum von 6 Monaten seit letzter Aktivität in einem Raum gelöscht werden. Hersteller MÜSSEN sicherstellen, dass der Zeitraum durch den Kunden konfigurierbar ist. Diese Funktion DARF über Opt-Out durch den Kunden deaktivierbar sein. Diese Funktion DARF darüber realisierbar sein, dass nach Verstreichen der Frist Teilnehmer einen Gesprächsraum verlassen und der Raum nach Verlassen aller Teilnehmer automatisch gelöscht wird.
[<=]

A_22808 - Push-Benachrichtigungen Messenger-Service
TI-Messenger-Services MÜSSEN dafür sorgen, dass die Push-Gateways externe Push-Dienste datenschutzkonform nutzen. Hierzu werden folgende Kriterien definiert, die in jedem Fall beachtet werden MÜSSEN:

- Alle Push-Nachrichteninhalte, auf die der Push-Anbieter nicht zugreifen können muss, MÜSSEN verschlüsselt werden.
- Push-Nachrichten MÜSSEN vor dem Versenden um einen Zufallswert von 0-10 Sekunden verzögert werden um timingbasierte Profilbildung zu erschweren.
- Wenn ein Ziel-Client gerade aktiv ist, soll dieser selbsttätig auf einkommende Nachrichten lauschen und nicht per Push benachrichtigt werden.
- Push-Nachrichten dürfen keine Nachrichteninhalte enthalten, ihre Funktion besteht lediglich darin Clientsysteme zu informieren, dass Nachrichten abrufbar sind und eine Synchronisierung mit dem Homeserver nötig ist. Es DARF nur die Room-ID und Event-ID enthalten sein

[<=]

A_22965 - Push-Benachrichtigungen Messenger-Anbieter

TI-Messenger-Anbieter MÜSSEN dafür sorgen, dass die Push-Gateways externe Push-Dienste datenschutzkonform nutzen. Hierzu werden folgende Kriterien definiert, die in jedem Fall beachtet werden MÜSSEN:

- Push-Benachrichtigungen dürfen erst nach expliziter Zustimmung der Nutzer erfolgen (Opt-In).
- Wo möglich, MÜSSEN Push-Anbieter gewählt werden, die eine Wahrung der Betroffenenrechte für personenbezogene Informationen ermöglichen.

[<=]

A_22818 - Sicherheitsrisiken von Software-Bibliotheken minimieren
TI-Messenger-Fachdienst-Hersteller MÜSSEN Maßnahmen umsetzen, um die Auswirkung von unentdeckten Schwachstellen in benutzten Software-Bibliotheken zu minimieren.

Hinweis: Beispielmaßnahmen sind in [OWASP Proactive Control#C2] zu finden. Das

gewählte Verfahren MUSS die gleiche Wirksamkeit aufweisen, wie die Kapselung gemäß [OWASP Proactive Control#C2 Punkt 4].
[<=]

A_22819 - CC-Evaluierung als Ersatz für das Gutachten
Falls der TI-Messenger-Fachdienst-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-Fachdienstes,
- die in den zusätzlichen Funktionen verarbeiteten Daten,
- die Schnittstellen zwischen dem TI-Messenger-Fachdient des Akteurs und den ggf. genutzten Backend-Diensten der zusätzlichen Funktionen inklusive ihrer Sicherheitsmaßnahmen und
- die Sicherheitsannahmen an den TI-Messenger-Fachdienst des Akteurs und die Ausführungsumgebung.

[<=]

A_22810 - Abweichungen vom Matrix-Standard
TI-Messenger-Fachdienst-Hersteller MÜSSEN sämtliche, nicht in der TI-Messenger-Spezifikation beschriebenen, Abweichungen vom Matrix-Protokoll oder den MUST- oder SHOULD-Empfehlungen des Matrix-Protokolls dokumentieren und begründen.
[<=]

Hinweis: Gemeint sind hier nur tatsächliche Abweichungen von Setzungen der Matrix-Spezifikation und nicht zusätzliche Funktionen, die auf dem TI-Messenger-Dienst aufbauen und produktspezifisch sind.

A_22812 - Interoperabilität von Zusatzfunktionen für den TI-Messenger-Fachdienst
TI-Messenger-Fachdienst-Hersteller MÜSSEN sicherstellen, dass alle implementierten Funktionen, die über den gewöhnlichen Funktionsumfang einer TI-Messenger-Komponente hinausgehen die Sicherheit des Produkts nicht gefährden und die Interoperabilität mit anderen TI-Messenger-Produkten gewährleisten.
[<=]

A_22928 - Einsatz geschulter Administratoren für Org-Admins
TI-Messenger-Anbieter MÜSSEN als Administratoren Personal einsetzen, welches für die damit verbundenen Aufgaben und Themen der Informationssicherheit geschult und sensibilisiert wurden. Anbieter MÜSSEN technisch sicherstellen, dass nur die berechtigten Administratoren administrativen Zugriff auf die zu verwaltenden Messenger-Services haben.
[<=]

A_22816 - Device Verification, Cross-Signing und SSSS für TI-Messenger-Fachdienste
TI-Messenger-Hersteller MÜSSEN sicherstellen, dass die Funktionen Cross-Signing und Secure Secret Storage and Sharing (SSSS) zur Device Verification vom Fachdienst unterstützt werden. Es MUSS die Spezifikation hinsichtlich Ende-zu-Ende Verschlüsselung vollständig befolgt werden.
[<=]

4.2 Authentifizierung

Ein Akteur in der Rolle "Org-Admin" MUSS sich über das vom TI-Messenger-Anbieter bereitgestellte Frontend eines Registrierungs-Dienstes mit der Identität (SMC-B) der Organisation gegenüber dem Registrierungs-Dienst authentifizieren, um einen oder mehrere Messenger-Services für seine Organisation registrieren zu können.

Damit Akteure Ad-Hoc-Nachrichten austauschen können, MÜSSEN sich diese an ihrem Messenger-Service authentifizieren. Die Authentifizierung MUSS hierbei über ein zwischen der Organisation und dem Anbieter vereinbartes Authentifizierungsverfahren erfolgen. Haben sich Akteure erfolgreich an ihrem Messenger-Service authentifiziert, erhalten sie ein von ihrem Homeserver ausgestelltes Matrix-ACCESS_TOKEN, welches für die spätere Authentifizierung des TI-Messenger-Clients verwendet wird.

IDP-Dienst

Der zentrale IDP-Dienst der gematik wird benötigt, um eine Organisation am Registrierungs-Dienst zu authentifizieren und den TI-Messenger-Clients Schreibzugriff auf das VZD-FHIR-Directory zu ermöglichen. Hierfür MÜSSEN der Registrierungs-Dienst und die TI-Messenger-Clients am zugelassenen IDP-Dienst der gematik gemäß [gemSpec_IDP_FD] registriert sein. Diese MÜSSEN den ausgestellten Security Tokens (ID_TOKEN) dieses IDP-Dienstes vertrauen.

Im Rahmen der Registrierung des VZD-FHIR-Directory am IDP-Dienst werden notwendige Claims für das ID_TOKEN (bestätigte Identifikationsmerkmale für den Akteur) festgelegt. Der Anbieter des TI-Messengers MUSS über einen organisatorischen Prozess beim zugelassenen IDP-Dienst folgende Claims im ID_TOKEN vereinbaren:

Tabelle 1: Inhalte der Claims für SMC-B/HBA

Leistungserbringerinstitutionen (SMC-B)	Leistungserbringer (HBA)
• `ProfessionOID` • `idNummer` • `organizationName` • `acr` • `aud`	• `ProfessionOID` • `idNummer` • `given_name` • `family_name` • `acr` • `aud`

Die `ProfessionOID` gibt an um welche Art von Leistungserbringer (z. B. Arzt, Zahnarzt etc.) es sich handelt. Die `idNummer` beinhaltet die Telematik-ID für Organisationen des Gesundheitswesens und Leistungserbringer.

Verwaltung der Nutzersession

Die Verwaltung der Nutzersession MUSS wie in der Matrix-Spezifikation beschrieben erfolgen.

4.3 DNS-Namensauflösung

Für die Namensauflösung der vom TI-Messenger-Fachdienst angebotenen Außenschnittstellen, werden DNS-Server im Internet verwendet. Der vereinbarte Abfrage-Record MUSS durch den jeweiligen TI-Messenger-Anbieter bereitgestellt werden und MUSS in öffentlichen DNS-Servern eingetragen sein.

Wird bei der Nutzung eines Messenger-Service für eine Organisation eine auf die Domain der Organisation bezogene Benamung gewählt, erfolgt die Eintragung der notwendigen DNS-Records auf DNS-Server im Internet durch die Administration der Organisation.

Identifizierung von Messenger-Services

Jeder Messenger-Service MUSS durch einen Matrix-Homeservernamen identifiziert werden, der aus einem Hostnamen und einem optionalen Port besteht. Weitere Informationen finden sich in [Server-Server API#Server discovery].

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, der Testspezifikationen, der Testfälle und mit dem Review der Testprotokolle (Log- und Trace-Daten) überprüfen kann.

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

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

ML-124200 - Test des TI-Messenger-Fachdienstes gegen die Referenzimplementierung

Der Hersteller des TI-Messenger-Fachdienstes MUSS den Fachdienst gegen die Referenzimplementierung erfolgreich testen. Die Testergebnisse sind der gematik

vorzulegen.
[<=]

Für die Anbieter Zulassung MÜSSEN die TI-Messenger-Fachdienste und TI-Messenger-Clients vom TI-Messenger-Anbieter bereitgestellt werden. Um einen automatisierten Test für den TI-Messenger-Dienst zu ermöglichen, MUSS die Test-App des TI-Messenger-Clients zusätzlich ein Testtreiber-Modul intern oder extern zur Verfügung stellen. Dieses MUSS die Funktionalitäten der produktspezifischen Schnittstelle des TI-Messenger-Clients über eine standardisierte Schnittstelle von außen zugänglich machen und einen Fernzugriff ermöglichen. Das Testtreiber-Modul darf die Ausgaben des TI-Messenger-Clients gemäß der technischen Schnittstelle aufarbeiten, aber darf die Inhalte nicht verfälschen. Eine genaue Beschreibung des Testvorgehens ist in der [gemSpec_TI_Messenger-Client] zu finden.

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-Dienste geprüft. Anschließend wird mit den IOP- und E2E Tests die Interoperabilität zwischen den verschiedenen 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 diese IOP- und E2E Tests selbständig und eigenverantwortlich durchführen. Bei Problemen im Rahmen der Zulassung MÜSSEN die Anbieter bei der Analyse unterstützen.

4.5 Betrieb

Der Betrieb des Fachdienstes wird durch den TI-Messenger-Anbieter verantwortet. Entsprechend dem Betriebskonzept [gemKPT_Betr#Anbieterkonstellationen], KANN der Betrieb jedoch aus- bzw. verlagert werden, zum Beispiel für ein *on-premise* Hosting. Die Koordination der jeweiligen Komponenten sowie die Erfüllung der Anforderungen verbleiben jedoch beim Anbieter. Dieser KANN in Abstimmung mit seinen Nutzern und Dienstleistern Verträge abschließen um den sicheren Betrieb aufrecht zu erhalten.

4.5.1 Performance

Der TI-Messenger-Fachdienst MUSS mit einer vollumfänglich-funktionalen Verfügbarkeit von mindestens 99% betreibbar sein.

Der Anbieter TI-Messenger MUSS sein Produkt TI-Messenger-Fachdienst mit einer vollumfänglich-funktionalen Verfügbarkeit von 99,8% in der Hauptzeit und 99,0 % in der Nebenzeit betreiben.

Die Hauptzeit ist Montag bis Freitag von 6 bis 22 Uhr, ausgenommen bundeseinheitliche Feiertage. Alle übrigen Zeiten gelten als Nebenzeit.

Wenn der Betrieb von Homeservern *on-premise* bei den Nutzern realisiert wird, KANN der Anbieter TI-Messenger für diese Produktinstanzen von den Performancevorgaben in Abstimmung mit seinen Kunden abweichen. Die Abweichungen und die betroffenen Instanzen MÜSSEN dem GTI im Rahmen der betrieblichen Prozesse bekannt gemacht werden.

4.5.2 Reporting

A_22946 - Rohdatenerfassung und -lieferung
Der TI-Messenger-Fachdienst MUSS die Rohdatenerfassung und -lieferung entsprechend der Vorgaben aus [gemSpec_Perf#Rohdaten-Performance-Reporting (Rohdatenerfassung v.02)] umsetzen.
Die Rohdatenerfassung am TI-Messenger-Fachdienst bzw. VZD-FHIR-Directory SOLL anhand folgender Messpunkte und Kriterien erfolgen:

Tabelle 2: Rohdatenerfassung TI-Messenger und VZD-FHIR-Directory

Messung am Produkt	Anwendungsfall (=$TIM-Operation)	Beschreibung	Start der Messung	Ende der Messung (siehe Hinweis *1)	ID Tab_gemKPT_Betr_Performance-Groessen
TI-Messenger-Fachdienst	AF_10103_01	6.1 AF - Authentisieren einer Organisation am TI-Messenger-Dienst: Redirect to IdP	Request: POST /register (Frontend des Registrierungs-Dienstes an Registrierungs-Dienst)	Response: Redirect to IDP Authorization Endpoint (Antwort an Frontend des Registrierungs-Dienstes)	D3-G14 D3-G16 D3-G30 D3-G31
TI-Messenger-Fachdienst	AF_10103_02	6.1 AF - Authentisieren einer Organisation am TI-Messenger-Dienst: Authentisierung	Request: POST /register (Authorization code) (Frontend des Registrierungs-Dienstes an Registrierungs-Dienst)	Response: status, id_token (Antwort an Frontend des Registrierungs-Dienstes)	D2-G08 D3-G14 D3-G16 D3-G30 D3-G31
TI-Messenger-Fachdienst	AF_10103_03	6.1 AF - Authentisieren einer Organisation am TI-Messenger-Dienst: Admin Account anlegen	Request: POST /register (id_token, Client-Credentials) (Frontend des Registrierungs-Dienstes an Registrierungs-Dienst)	Response: status, Admin-Account (Antwort an Frontend des Registrierungs-Dienstes)	D2-G08 D3-G14 D3-G16 D3-G30 D3-G31
TI-Messenger-Fachdienst	AF_10060_01	6.2 AF - Bereitstellung eines Messenger-Service für eine Organisation: Login	Request: POST /login (Client-Credentials) (Frontend des Registrierungs-Dienstes an Registrierungs-Dienst)	Response: status (Antwort an Frontend des Registrierungs-Dienstes)	D2-G08 D3-G14 D3-G16 D3-G30 D3-G31

Messung am Produkt	Anwendungsfall (=$TIM-Operation)	Beschreibung	Start der Messung	Ende der Messung (siehe Hinweis *1)	ID Tab_gemKPT_Betr_Performance-Groessen
TI-Messenger-Fachdienst	AF_10060_02	6.2 AF - Bereitstellung eines Messenger-Service für eine Organisation: Messenger-Service erstellen	Request: POST /create (Matrix-Domain) (Frontend des Registrierungs-Dienstes an Registrierungs-Dienst)	Response von Messenger-Service: status (Antwort an Registrierungs-Dienstes)	D2-G08 D3-G14 D3-G16 D3-G30 D3-G31
TI-Messenger-Fachdienst	AF_10060_03	6.2 AF - Bereitstellung eines Messenger-Service für eine Organisation: Messenger-Service in die Föderation aufnehmen	Request: POST /token (client_id) (Registrierungs-Dienst an OAuth-Service des VZD-FHIR-Directory)	Response: status (Antwort an Frontend des Registrierungs-Dienstes)	D2-G08 D3-G14 D3-G16 D3-G30 D3-G31
VZD-FHIR-Directory	AF_10059_01	6.3 AF - Organisationsressourcen im Verzeichnisdienst hinzufügen: Redirect to IdP	Request: GET /owner-authenticate (TI-Messenger-Client mit Org-Admin Funktionalität an Auth-Service des VZD-FHIR-Directory)	Response: Redirect to IdP Authorization Endpoint (Antwort an TI-Messenger-Client mit Org-Admin Funktionalität)	-
VZD-FHIR-Directory	AF_10059_02	6.3 AF - Organisationsressourcen im Verzeichnisdienst hinzufügen: Get owner-accesstoken	Request: GET /owner-authenticate with Authorization code (TI-Messenger-Client mit Org-Admin Funktionalität an Auth-Service des VZD-FHIR-Directory)	Response: owner-accesstoken (Antwort an TI-Messenger-Client mit Org-Admin Funktionalität)	-
VZD-FHIR-Directory	AF_10059_03	6.3 AF - Organisationsressourcen im Verzeichnisdienst hinzufügen: FHIR-Ressource lesen (SMC-B)	Request: POST /owner/HealthcareService/? (TI-Messenger-Client mit Org-Admin Funktionalität an FHIR-Proxy des VZD-FHIR-Directory)	Response: HTTPS Forward inkl. result body json (Antwort an TI-Messenger-Client mit Org-Admin Funktionalität)	-

Messung am Produkt	Anwendungsfall (=$TIM-Operation)	Beschreibung	Start der Messung	Ende der Messung (siehe Hinweis *1)	ID Tab_gemKPT_Betr_Performance-Groessen
VZD-FHIR-Directory	AF_10059_04	6.3 AF - Organisationsressourcen im Verzeichnisdienst hinzufügen: FHIR-Ressource schreiben (SMC-B)	Request: FHIR-Operation um eigenen Datensatz zu verwalten (TI-Messenger-Client mit Org-Admin Funktionalität an FHIR-Proxy des VZD-FHIR-Directory)	Response: HTTPS Forward inkl. result body json (Antwort an TI-Messenger-Client mit Org-Admin Funktionalität)	-
TI-Messenger-Fachdienst	AF_10057_01	6.4 AF - Anmeldung eines Akteurs am Messenger-Service: Client-Login, Auswahl Authentifizierungsverfahren	Request: GET /_matrix/client/login (TI-Messenger-Client an Messenger-Proxy)	Response: HTTPS Forward inkl. unterstützte Authentifizierungsverfahren (Antwort an TI-Messenger-Client)	D2-G08 D3-G14 D3-G16 D3-G30 D3-G31
TI-Messenger-Fachdienst	AF_10057_02	6.4 AF - Anmeldung eines Akteurs am Messenger-Service: Erstellung Matrix-ACCESS_TOKEN	Request: POST /_matrix/client/login (TI-Messenger-Client an Messenger-Proxy)	Response: HTTPS Forward inkl. Matrix-ACCESS_TOKEN, device_ID, MXID (Antwort an TI-Messenger-Client)	D2-G08 D3-G14 D3-G16 D3-G30 D3-G31
TI-Messenger-Fachdienst	AF_10057_03	6.4 AF - Anmeldung eines Akteurs am Messenger-Service: Erstellung Matrix-OpenID-Token	Request: POST /_matrix/client/user/{userid}/openid/request_token (TI-Messenger-Client an Messenger-Proxy)	Response: HTTPS Forward inkl. Matrix-OpenID-Token (Antwort an TI-Messenger-Client)	D2-G08 D3-G14 D3-G16 D3-G30 D3-G31
VZD-FHIR-Directory	AF_10057_04	6.4 AF - Anmeldung eines Akteurs am Messenger-Service: Validitätsprüfung Messenger-Service	Request: GET /tim-authenticate (Matrix-OpenID-Token) (TI-Messenger-Client an Auth-Service des VZD-FHIR-Directory)	Response: HTTP 401/200 (Antwort an TI-Messenger-Client)	-

Messung am Produkt	Anwendungsfall (=$TIM-Operation)	Beschreibung	Start der Messung	Ende der Messung (siehe Hinweis *1)	ID Tab_gemKPT_Betr_Performance-Groessen
VZD-FHIR-Directory	AF_10058_01	6.5 AF - Akteur (User-HBA) im Verzeichnisdienst hinzufügen: Redirect to IdP	Request: GET /owner-authenticate (TI-Messenger-Client an Auth-Service des VZD-FHIR-Directory)	Response: Redirect to IdP Authorization Endpoint (Antwort an TI-Messenger-Client)	-
VZD-FHIR-Directory	AF_10058_02	6.5 AF - Akteur (User-HBA) im Verzeichnisdienst hinzufügen: Get owner-accesstoken	Request: GET /owner-authenticate with Authorization code (TI-Messenger-Client an Auth-Service des VZD-FHIR-Directory)	Response: owner-accesstoken (Antwort an TI-Messenger-Client)	-
VZD-FHIR-Directory	AF_10058_03	6.5 AF - Akteur (User-HBA) im Verzeichnisdienst hinzufügen: FHIR-Ressource lesen (HBA)	Request: POST /owner/PractitionerRole/? (TI-Messenger-Client an FHIR-Proxy des VZD-FHIR-Directory)	Response: HTTPS Forward inkl. result body json (Antwort an TI-Messenger-Client)	-
VZD-FHIR-Directory	AF_10058_04	6.5 AF - Akteur (User-HBA) im Verzeichnisdienst hinzufügen: FHIR-Ressource schreiben (HBA)	Request: FHIR-Operation um eigenen Datensatz zu verwalten (TI-Messenger-Client an FHIR-Proxy des VZD-FHIR-Directory)	Response: HTTPS Forward inkl. result body json (Antwort an TI-Messenger-Client)	-
VZD-FHIR-Directory	AF_10064_01	6.6 AF - Föderationszugehörigkeit eines Messenger-Service prüfen: Get provider-accesstoken	Request: GET /token (client_id) (Registrierungs-Dienst des TI-Messenger-Fachdienstes an OAuth-Service des VZD-FHIR-Directory)	Response: status, provider-accesstoken (Antwort an Registrierungs-Dienst des TI-Messenger-Fachdienstes)	-
VZD-FHIR-Directory	AF_10064_02	6.6 AF - Föderationszugehörigkeit eines Messenger-Service prüfen: Erhalte Föderationslist	Request: GET /tim-provider-services/getFederationList (Registrierungs-Dienst des TI-Messenger-Fachdienstes an FHIR-Proxy des VZD-FHIR-Directory)	Response: status / Föderatinoslist e (Antwort an Registrierungs-Dienst des TI-Messenger-	-

Messung am Produkt	Anwendungsfall (=$TIM-Operation)	Beschreibung	Start der Messung	Ende der Messung (siehe Hinweis *1)	ID Tab_gemKPT_Betr_Performance-Groessen
		e		Fachdienstes)	
TI-Messenger-Fachdienst	AF_10104_01	6.7 AF - Einladung von Akteuren innerhalb eines Messenger-Service: Akteur suchen	Request: POST /_matrix/client/user_directory/search (TI-Messenger Client A an Messenger-Proxy)	Response: HTTPS Forward inkl MXID (Messenger-Proxy an TI-Messenger Client A)	D2-G08 D3-G14 D3-G16 D3-G30 D3-G31
TI-Messenger-Fachdienst	AF_10104_02	6.7 AF - Einladung von Akteuren innerhalb eines Messenger-Service: Akteur einladen	Request: POST /_matrix/client/r0/rooms/{roomId}/invite (TI-Messenger Client A an Messenger-Proxy)	Response: status (Messenger-Proxy an TI-Messenger-Client Akteur A)	D2-G08 D3-G14 D3-G16 D3-G30 D3-G31
TI-Messenger-Fachdienst	AF_10063_01	6.8 AF - Austausch von Events innerhalb eines Messenger-Service	Request: Matrix-Request (TI-Messenger Client an Messenger-Proxy)	Response: HTTPS Forward Status (Matrix-Request) (Antwort an TI-Messenger-Client Akteur A)	D1-G03 D1-G04 D2-G08 D3-G14 D3-G16 D3-G30 D3-G31
TI-Messenger-Fachdienst	AF_10061_01	6.9 AF - Einladung von Akteuren anderer Messenger-Services: Eintrag in Freigabeliste erzeugen	Request: POST /tim-contact-mgmt/createContactSetting (MXID, start, end) (TI-Messenger-Client an TI-Messenger Proxy)	Response: status (Antwort an TI-Messenger-Client)	D2-G08 D3-G14 D3-G16 D3-G30 D3-G31
TI-Messenger-Fachdienst (Sendersystem)	AF_10061_02	6.9 AF - Einladung von Akteuren anderer Messenger-Services: Einladung Sendersystem	Request: POST /_matrix/client/r0/rooms/{roomId}/invite (TI-Messenger Client an Messenger-Proxy)	Response: HTTPS Forward Status (Antwort an TI-Messenger-Client Akteur A)	D2-G08 D3-G14 D3-G16 D3-G30 D3-G31

Messung am Produkt	Anwendungsfall (=$TIM-Operation)	Beschreibung	Start der Messung	Ende der Messung (siehe Hinweis *1)	ID Tab_gemKPT_Betr_Performance-Groessen
TI-Messenger-Fachdienst (Sendersystem)	AF_10061_03	6.9 AF - Einladung von Akteuren anderer Messenger-Services: Einladung Empfangssystem(e)	Request: HTTPS Forward (POST /_matrix/federation/v1/invite/{roomId}/{eventId}) (Messenger-Proxy des Sendersystems an Messenger-Proxy des Empfangssystems)	Response: Status (Antwort an Messenger-Proxy des Sendersystems)	D2-G08 D3-G14 D3-G16 D3-G30 D3-G31
TI-Messenger-Fachdienst (Sendersystem)	AF_10062_01	6.10 AF - Austausch von Events zwischen anderen Messenger-Services: Event Sendersystem	Request: Matrix-Request (TI-Messenger Client an eigenen Messenger-Proxy)	Response: HTTPS Forward Status (Antwort an TI-Messenger-Client Akteur A	D1-G03 D1-G04 D2-G08 D3-G14 D3-G16 D3-G30 D3-G31
TI-Messenger-Fachdienst (Sendersystem)	AF_10062_02	6.10 AF - Austausch von Events zwischen anderen Messenger-Services: Event Empfangssystem(e)	Request: HTTPS Forward Matrix-Request (Messenger-Proxy Sendersystem an Messenger-Proxy Empfangssystem)	Response: HTTPS Forward Status (Antwort an Messenger-Proxy des Sendersystems)	D1-G03 D1-G04 D2-G08 D3-G14 D3-G16 D3-G30 D3-G31

[<=]

**1) Hinweis: Die Beschreibung entspricht dem Ende eines erfolgreichen Anwendungsfalls. Wenn der Anwendungsfall abbricht und/oder eine Fehlermeldung erzeugt, so MUSS im JSON-message-Block für das Feld httpStatus der negative http-Statuscode entsprechend der Beschreibung im Anwendungsfall eingetragen werden. Für jede Anwendungsfall-Instanz MUSS eine eindeutige ID vergeben werden. Die ID KANN mit einem Abstand von 6 Monaten neu vergeben werden um die Operationen innerhalb eines Anwendungsfalls konsolidieren zu können und gleichzeitig von anderen Anwendungsfall-Instanzen abzugrenzen.*

A_22940 - Performance - Rohdaten - Spezifika TI-M Message (Rohdatenerfassung v.02)

Das Produkt SOLL - bei Rohdaten-Performance-Berichten im "message"-Feld – folgende Informationen im JSON-Format übermitteln:

```
{
"Anwendungsfall-ID":$Anwendungsfall-ID,
"Useragent":$useragent,
"Matrix-Domain":$Matrix-Domain,
"sizeIn":$sizeIn,
```

"sizeOut":$sizeOut,
"telematikID":$telematikID,
"professionOID":$professionOID,
"Response":$response
}
Für $useragent ist der entsprechende Wert einzutragen, welcher vom Client übermittelt wird. Falls die Anfrage von einem Matrix-Server kommt, ist hier die Matrix-Domain einzutragen.
Für $Matrix-Domain ist die eigene Matrix-Domain des Messenger-Services einzutragen.
Für $sizeIn ist das eingehende übertragene Datenvolumen in Byte als Integer anzugeben. Der Messpunkt beim TI-Messenger-Fachdienst ist dabei der Messenger-Proxy und beim FHIR-Directory der FHIR-Proxy.
Für $sizeOut ist das ausgehende übertragene Datenvolumen in Byte als Integer anzugeben. Der Messpunkt beim TI-Messenger-Fachdienst ist dabei der Messenger-Proxy und beim FHIR-Directory der FHIR-Proxy.
Für die $telematikID ist die telematikID aus dem entsprechenden Token einzutragen.
Für die $professinoOID ist die professionOID aus dem entsprechenden Token einzutragen.
Für die $response ist die Rückmeldung entsprechend der Anwendungsfälle einzutragen.
[<=]

A_22941 - Performance - Rohdaten - Spezifika TI-M - Feldtrennzeichen im Useragent (Rohdatenerfassung v.02)
Das Produkt MUSS, sofern vom Client irrtümlicherweise im Useragent-Wert das verbotene Feldtrennzeichen ";" übertragen wurde, dieses ";" gegen das Zeichen "┼" austauschen und in der Rohdatenlieferung senden. (siehe: A_21981: Feldtrennzeichen ";"
Das Zeichen ┼ ist definiert gem. Unicode U+253C (9532) - BOX DRAWINGS LIGHT VERTICAL AND HORIZONTAL - ALT-Code 197)
[<=]

Bestandsdaten
Der TI-Messenger-Fachdienst MUSS die nachfolgenden Informationen jeweils monatlich zum 01. des Monats in folgendem JSON Format als HTTP Body an die Betriebsdatenerfassung (BDE) gemäß [gemSpec_SST_LD_BD] liefern:
{
„Abfragezeitpunkt": <Zeitstempel der Abfrage als String im ISO 8601 Format>,
„CI_ID": <CI ID des abgefragten Fachdienstes gemäß TI-ITSM als String>,
„TIM-FD_Anzahl_Messenger-Service": <Anzahl der zum Abfragezeitpunkt instanziierten Messenger-Service>,
„TIM-FD_Anzahl_Nutzer": <Anzahl der zum Abfragezeitpunkt registrierten Nutzer>,
„TIM-FD_Anzahl_aktNutzer": <Anzahl der zum Abfragezeitpunkt innerhalb des letzten Monats aktiven Nutzer>
}

Da bei dieser Lieferung keine Datei übermittelt wird, sondern der Text direkt im Body, ist für diese Lieferung die Angabe des filenames im HTTP Header gemäß [A_17112] (Tab_I_LogData_002 Operation I_LogData::fileUpload) in der gemSpec_SST_LD_BD NICHT notwendig.

Service Monitoring

Der TI-Messenger-Anbieter MUSS das Service Monitoring der gematik technisch-organisatorisch unterstützen.

Dafür kann es z.B. notwendig sein, dass entsprechende Accounts auf Homeservern eingerichtet werden. Das Service Monitoring SOLL dabei zu keinen technischen Veränderungen an den Produkten führen.

5 Funktionsmerkmale

Im Folgenden Kapitel wird der TI-Messenger-Fachdienst bezogen auf seine Teilkomponenten funktional beschrieben. Der TI-Messenger-Fachdienst ist die Kernkomponente des TI-Messenger-Dienstes. Dieser stellt alle Schnittstellen bereit, die für die Kommunikation innerhalb des TI-Messenger-Dienstes benötigt werden.

In der folgenden Abbildung ist der TI-Messenger-Fachdienst als Whitebox dargestellt:

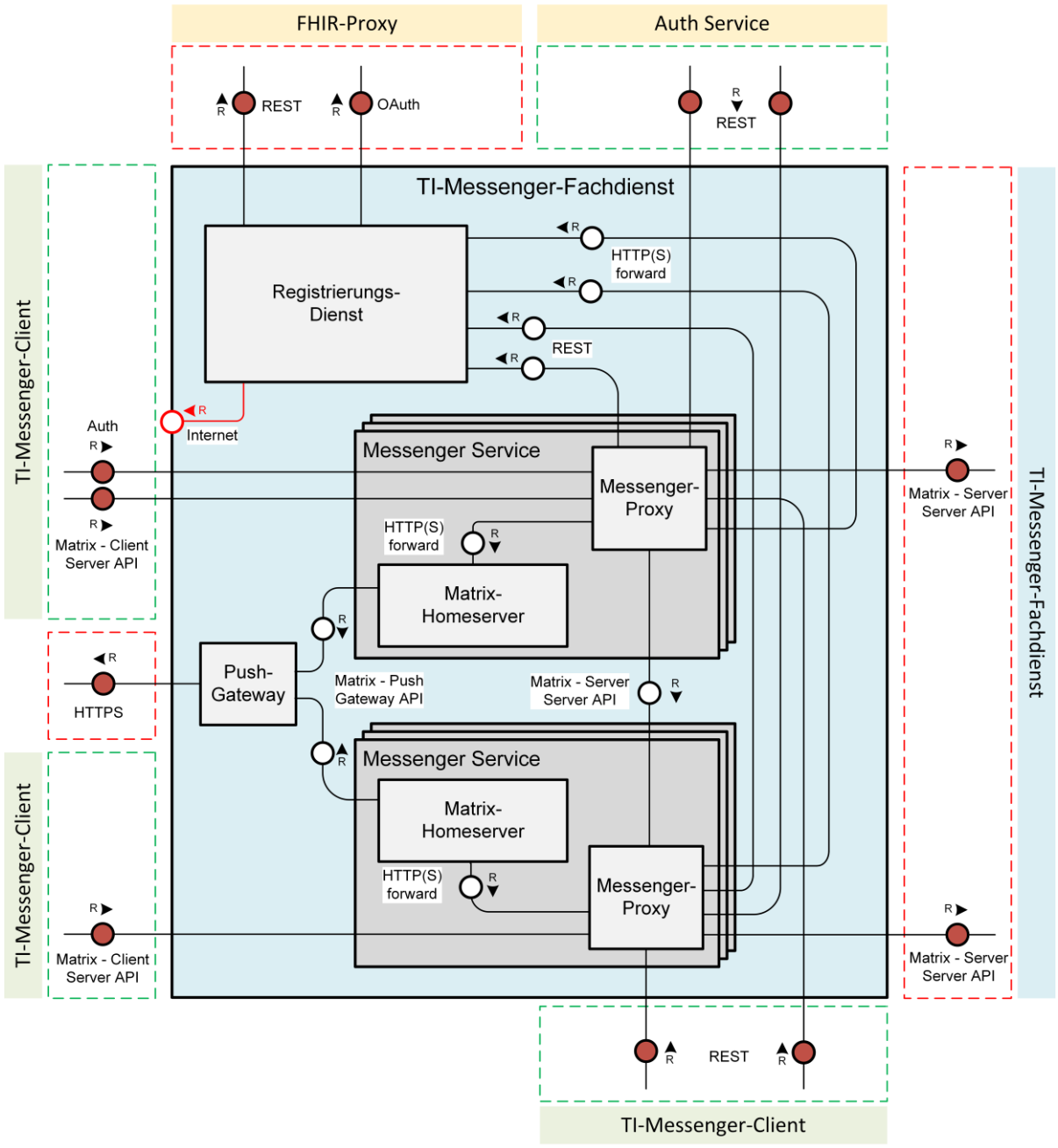

Abbildung 3: Funktionaler Aufbau des TI-Messenger-Fachdienstes

Die in der Abbildung grün dargestellten Boxen zeigen die Schnittstellen, die am TI-Messenger-Fachdienst aufgerufen werden. Rot dargestellte Boxen zeigen die Schnittstellen, über die der TI-Messenger-Fachdienst weitere Services anderer Komponenten nutzt. Eine Ausnahme bildet die Kommunikation zwischen den TI-Messenger-Fachdiensten. Hier wird die Kommunikation bilateral zwischen den zur TI-Föderation gehörenden Fachdiensten realisiert. Die in der Abbildung rot dargestellte Linie vom Registrierungs-Dienst zum Internet zeigt die vom Frontend des Registrierungs-Dienstes verwendete Schnittstelle. Diese wird nicht normativ von der gematik definiert. Die Ausgestaltung obliegt dem jeweiligen TI-Messenger-Anbieter.

5.1 Funktionen der Systemkomponenten

Im Folgenden Kapitel werden alle für den Betrieb des TI-Messenger-Fachdienstes notwendigen Komponenten funktional beschrieben.

5.1.1 Registrierungs-Dienst

Der Registrierungs-Dienst bietet drei Schnittstellen an. In der folgenden Abbildung sind die von ihm bereitgestellten (grün) und genutzten (rot) Schnittstellen dargestellt:

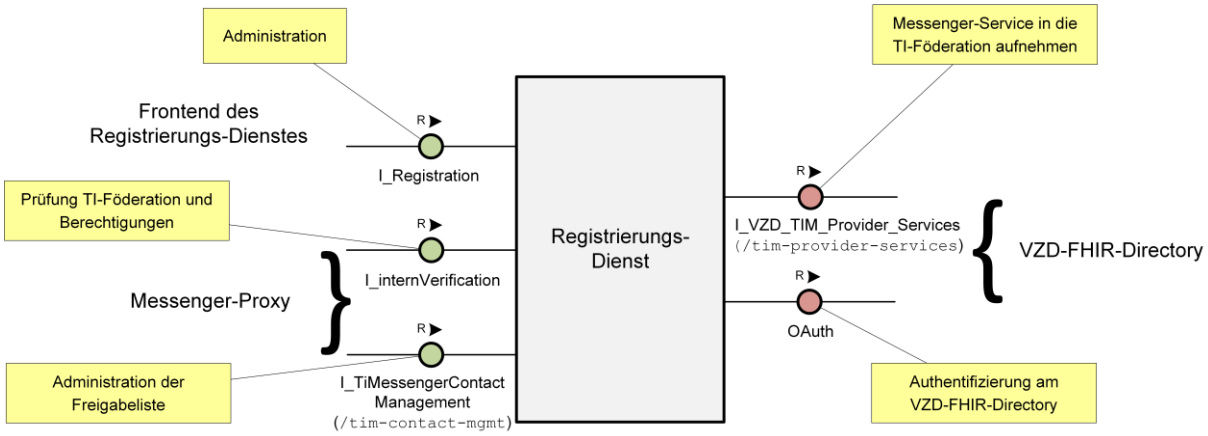

Abbildung 4: Übersicht der Schnittstellen am Registrierungs-Dienst

Hinweis: Bei der in der Abbildung dargestellte Schnittstelle `I_internVerification` handelt es sich um eine abstrakte interne Schnittstelle am Registrierungs-Dienst mit der den Messenger-Proxies mehrere Funktionalitäten bereitgestellt werden. Die Umsetzung der bereitzustellenden Funktionalitäten (Prüfung TI-Föderation und Berechtigung) am Registrierungs-Dienst kann auch über separate Schnittstellen erfolgen. `I_internVerification` *und* `I_TiMessengerContactManagement` *sind für die Umsetzung des Berechtigungsprüfung notwendig.*

Administration

Der TI-Messenger-Fachdienst MUSS eine Schnittstelle für die Administration am Registrierungs-Dienstes bereitstellen. Dies ist notwendig, damit ein Onboarding-Prozess für die Registrierung von Messenger-Services gewährleistet wird. Der Registrierungs-

Dienst MUSS es ermöglichen einen neuen Messenger-Service über ein Frontend des Registrierungs-Dienstes zu erzeugen. Die Ausgestaltung des Frontends sowie der Schnittstelle am Registrierungs-Dienst (`I_Registration`) ist dem jeweiligen TI-Messenger-Anbieter überlassen. Der Registrierungs-Dienst MUSS bei einer neuen Registrierungsanfrage automatisiert den durch den zuständigen IDP-Dienst ausgestellten ID_TOKEN (gemäß Kapitel "Authentifizierung") validieren. Bei der Validierung MUSS der Registrierungs-Dienst die im ID_TOKEN enthaltene`ProfessionOID` gegen die in der Tabelle "Tab_PKI_403-03 OID-Festlegung Institutionen im X.509-Zertifikat der SMC-B" gelisteten OIDs gemäß [gemSpec_OID] prüfen. Nach erfolgreicher Validierung MUSS der Registrierungs-Dienst einen Messenger-Service starten und die in der Registrierungsanfrage übergebene Matrix-Domain in eine Organisations-Ressource dieser Organisation (*HealthcareService*) im VZD-FHIR-Directory hinterlegen. Ebenfalls MUSS der Registrierungs-Dienst dem Frontend des Registrierungs-Dienstes die erstelle Matrix-Domain für den Zugriff auf den beantragten Messenger-Service übergeben.

Nach erfolgreicher Authentifizierung einer Organisation am Registrierungs-Dienst MUSS ein Admin-Account für den Akteur in der Rolle "Org-Admin" der Organisation auf dem Registrierungs-Dienst angelegt werden. Für die Authentifizierung des Akteurs in der Rolle "Org-Admin" MUSS eine 2-Faktor-Authentifizierung verwendet werden. Die Abstimmung bezüglich der zu verwendenden Authentifizierungsverfahren eines Messenger-Service MUSS durch den Anbieter des TI-Messengers unterstützt werden.

Authentifizierung am VZD-FHIR-Directory

Für den Zugriff des Registrierungs-Dienstes auf das VZD-FHIR-Directory über die Schnittstelle `/tim-provider-services` des FHIR-Proxy ist eine vorherige Authentifizierung mittels OAuth2 Client Credentials Flow notwendig. Die dafür notwendigen Client-Credentials MUSS der TI-Messenger-Anbieter für seinen Registrierungs-Dienst beim VZD-FHIR-Directory-Anbieter beantragen. Die Beantragung erfolgt über einen Service-Request im TI-ITSM-System. Nach erfolgreicher Authentifizierung erhält der Registrierungs-Dienst ein provider-accesstoken, welches beim Aufruf der `/tim-provider-services` Schnittstelle enthalten sein MUSS.

Messenger-Service in die TI-Föderation aufnehmen

Für die Aufnahme eines Messenger-Services eines TI-Messenger-Fachdienstes in die TI-Föderation des TI-Messenger-Dienstes, MUSS durch den Registrierungs-Dienst die vom Frontend des Registrierungs-Dienstes übergebene Matrix-Domain einer Organisation durch den Aufruf der Operation `/tim-provider-services/addTiMessengerDomain`, am VZD-FHIR-Directory, eintragen werden. Im Aufruf der Schnittstelle MUSS ein provider-accesstoken enthalten sein.

Bereitstellung der Föderationsliste

Der Registrierungs-Dienst MUSS eine Liste aller verifizierten Matrix-Domains des VZD-FHIR-Directory vorhalten und diese den Messenger-Proxies über eine interne Schnittstelle bereitstellen. Die Ausgestaltung der Schnittstelle am Registrierungs-Dienst (`I_internVerification`) ist dem jeweiligen TI-Messenger-Anbieter überlassen.

Inhalt der Föderationsliste die der Registrierungs-Dienst über die Schnittstelle den Messenger-Proxies bereitstellen MUSS, sind die Hashes aller an der Föderation beteiligten Matrix-Domainnamen. Der Registrierungs-Dienst MUSS die aktuelle TI-Föderationsliste am VZD-FHIR-Directory abfragen. Für den Abruf MUSS die am FHIR-Proxy des VZD-FHIR-Directory bereitgestellte Operation `/tim-provider-services/getFederationList` aufgerufen werden. Im Aufruf der Schnittstelle MUSS ein provider-accesstoken enthalten

sein. Die Abfrage der Föderationsliste MUSS stündlich erfolgen. Die Prüfung auf Aktualität der Föderationsliste des Registrierungs-Dienstes MUSS zusätzlich bei jeder Anfrage durch einen Messenger-Proxy zur Bereitstellung der Föderationsliste über eine Abfrage beim FHIR-Proxy des VZD-FHIR-Directory erfolgen. Die Prüfung auf Aktualität erfolgt durch den Abgleich der Versionen der Föderationslisten. Nach dem Erhalt einer neuen Föderationsliste vom VZD-FHIR-Directory MUSS diese vom Registrierungs-Dienst den Messenger-Proxies für die Prüfung der Organisationszugehörigkeit über die interne Schnittstelle `I_internVerification` bereitgestellt werden.

Berechtigungsprüfung

Der Registrierungs-Dienst MUSS eine Funktion anbieten, mit der die Überprüfung auf MXID-Einträge im VZD-FHIR-Directory möglich ist. Die Funktionalität MUSS über eine interne Schnittstelle (`I_internVerification`) den Messenger-Proxies bereitgestellt werden. Die Ausgestaltung der Schnittstelle am Registrierungs-Dienst ist dem jeweiligen TI-Messenger-Anbieter überlassen.

Über diese Schnittstelle MÜSSEN die MXID der beteiligten Akteure an die FHIR-Proxy Schnittstelle `/tim-provider-services/whereIs` des VZD-FHIR-Directory übergeben werden.

Die Prüfung ist erfolgreich wenn:

- die MXID des einzuladenden Akteurs im Organisationsverzeichnis hinterlegt ist oder
- der einladende sowie der einzuladende Akteur im Personenverzeichnis hinterlegt sind.

War die Prüfung erfolgreich, so MUSS der Registrierungs-Dienst dies an den Messenger-Proxy übergeben.

Administration / Prüfung der Freigabeliste

Die Freigabeliste dient zur Prüfung, ob einem eingehenden `Invite-Event` am Messenger-Proxy zugestimmt wird. Hierzu MUSS es möglich sein, dass der Akteur die Freigabeliste über sein TI-Messenger-Client administrieren kann. Der Registrierungs-Dienst MUSS die Schnittstelle `I_TiMessengerContactManagement` als REST-Webservice über HTTPS gemäß [api-messenger#TiMessengerContactManagement.yaml] in der Version 1.0.0 umsetzen. Der Verbindungsaufbau MUSS für die TI-Messenger-Clients hierbei über den Messenger-Proxy erfolgen. Zusätzlich MUSS der Registrierungs-Dienst den Messenger-Proxies eine Schnittstelle bereitstellen, über die die Überprüfung der hinterlegten Freigaben für jeden Akteur möglich ist. Dies KANN über eine separate Schnittstelle am Registrierungs-Dienst erfolgen. Der Registrierungs-Dienst MUSS sicherstellen, dass abgelaufene Freigaben aus der Freigabeliste entfernt werden.

5.1.2 Messenger-Service

Ein Messenger-Service besteht aus den Teilkomponenten Matrix-Homeserver und dem Messenger-Proxy. Die Teilkomponente Matrix-Homeserver basiert auf dem offenen Kommunikationsprotokoll Matrix. Der Messenger-Proxy dient als Prüfinstanz und leitet Anfragen an den Matrix-Homeserver weiter. Dieser basiert nicht auf dem Matrix Standard. Welche APIs der Matrix-Spezifikation im Messenger-Service nachgenutzt werden, ist in der folgenden Abbildung dargestellt:

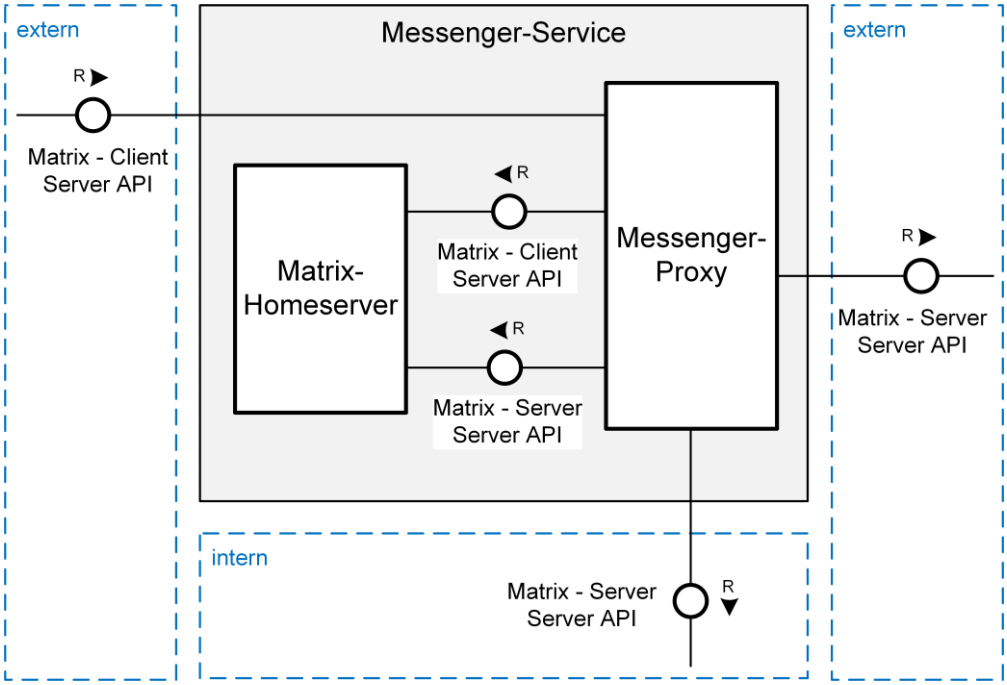

Abbildung 5: Matrix-API des Messenger-Service

Die Abbildung "*Matrix-API des Messenger Service*" zeigt die jeweils zu berücksichtigenden Matrix-APIs (Server-Server API und Client-Server API). Diese MÜSSEN gemäß

- [Matrix Specification#Server-Server API],
- [Matrix Specification#Client-Server API]

umgesetzt werden.

Der Aufruf der Client-Server-API am Matrix-Homeserver MUSS immer über den Messenger-Proxy erfolgen. Dieser leitet alle durch ihn autorisierten Aufrufe der TI-Messenger-Clients an den Matrix-Homeserver per HTTP(S)-Forward weiter. Die Kommunikation der Matrix-Homeserver MUSS ebenfalls über den Messenger-Proxy erfolgen. Auch hier MÜSSEN die Anfragen per HTTP(S)-Forward für die Matrix-Server-Server-Kommunikation zum Matrix-Homeserver weitergeleitet werden. Zum Versenden von Push-Notifications MUSS der Matrix-Homeserver das Matrix-Push-Gateway-API des Push-Gateways verwenden.

Der Messenger-Proxy agiert neben der Funktion als Proxy zur Weiterleitung aller Server-Server-API- und Client-Server-API-Aufrufe an den Matrix-Homeserver als Kontrollinstanz zur Prüfung der für die Kommunikation notwendigen Rechte. Hierfür MUSS der Messenger-Proxy für alle Server-Server- und Client-Server-API-Endpunkte genutzt werden.

Messenger-Services KÖNNEN dezentral oder "*on-premise*" von einem TI-Messenger-Anbieter bereitgestellt werden. Werden durch einen TI-Messenger-Anbieter mehrere Matrix-Domains in einem gemeinsamen Messenger-Service betrieben so MUSS die logische Trennung der Matrix-Domains sichergestellt werden.

5.1.2.1 Messenger-Proxy

Der Messenger-Proxy MUSS für jeden Messenger-Service separat bereitgestellt werden. Die Matrix-Server-Server-API (Server-Server Proxy) und Matrix-Client-Server-API (Client-Server Proxy) bezogenen Prüfungen KÖNNEN logisch im Messenger-Proxy umgesetzt werden. Die Art der Umsetzung bleibt dem TI-Messenger-Fachdienst-Hersteller überlassen. Im Folgenden wird der Funktionsumfang des Messenger-Proxies weiter beschrieben.

TLS-Terminierung

Alle Anfragen der TI-Messenger-Clients und anderer Messenger-Services an den Matrix-Homeserver MÜSSEN über den Messenger-Proxy geleitet werden. Die TLS-Kommunikation zwischen den TI-Messenger-Clients und dem Matrix-Homeserver MUSS am Messenger-Proxy terminiert werden. Die Absicherung der TLS-Kommunikation MUSS durch eine einseitige Serverauthentisierung unter Nutzung eines X.509-Zertifikats erfolgen.

Prüfung des verwendeten Clients

Der Messenger-Proxy MUSS prüfen, ob die Anfrage von einen zugelassen TI-Messenger-Client erfolgt. Die Überprüfung erfolgt anhand der übergebenen Parameters `client_id` des TI-Messenger-Clients. Für die Prüfung der `client_id` MUSS diese zuvor vom TI-Messenger-Client-Hersteller an den TI-Messenger-Anbieter übermittelt werden.

HTTP(S)-Forwarding

Die Kommunikation zwischen TI-Messenger-Client und Matrix-Homeserver erfolgt immer über den Messenger-Proxy (Forwarding). Das Forwarding KANN sowohl über HTTP als auch über HTTPS erfolgen. Der Messenger-Proxy MUSS sowohl als Reverse-Proxy als auch als Forward-Proxy fungieren. Eine Kommunikation vom Matrix-Homeserver zum TI-Messenger-Client und auch zu einem anderen Matrix-Homeserver eines anderen Messenger-Service MUSS über den Messenger-Proxy geführt werden.

Schnittstelle für Authentifizierungsverfahren

Für die Nutzung eines eigenen Authentifizierungs-Dienstes durch eine Organisation MUSS der Messenger-Proxy eine Schnittstelle für die Anbindung des Authentifizierungs-Dienstes der Organisation bereitstellen. Die Umsetzung dieser Schnittstelle MUSS durch die Organisation und dem jeweiligen TI-Messenger-Anbieter abgestimmt werden.

Vorhalten der Föderationsliste

Der Messenger-Proxy MUSS bei seinem zuständigen Registrierungs-Dienst die TI-Föderationsliste über die interne Schnittstelle (`I_internVerification`) abrufen und lokal ablegen.

Umsetzung von Prüfregeln

Der Messenger-Proxy MUSS das Berechtigungskonzept gemäß [gemSpec_TI_Messenger-Dienst#Berechtigungskonzept] unterstützen. Der Messenger-Proxy MUSS bei jedem Aufruf des RESTful-Endpunkt `Invite` den Inhalt der Anfrage an den Matrix-Homeserver prüfen. Dies betrifft sowohl die Client-Server- als auch die Server-Server-Kommunikation. Im Folgenden werden die Prüfregeln beschrieben.

- **Prüfregeln als Client-Server Proxy**

Der Messenger-Proxy MUSS Prüfregeln für Client-Server Anfragen unterstützen. Hierbei MUSS der Messenger-Proxy bei jedem `Invite-Event` gemäß [Server-Server API#Inviting to a room] den Inhalt der Anfrage an den Matrix-Homeserver wie folgt prüfen.

Stufe 1 - Prüfung der TI-Föderationszugehörigkeit

Im ersten Schritt MUSS der Messenger-Proxy prüfen, ob die Matrix-Domain im `Invite-Event` Teil der TI-Föderation ist. Hierfür MUSS der Messenger-Proxy in seiner lokalen Föderationsliste prüfen, ob die Matrix-Domain in dieser enthalten ist. Ist dies nicht der fall ,dann MUSS der Messenger-Proxy bei seinem zuständigen Registrierungs-Dienst über die interne Schnittstelle (`I_internVerification`) eine aktuelle Liste abrufen. Ist die anschließende erneute Prüfung fehlgeschlagen, dann MUSS der Messenger-Proxy die Anfrage ablehnen. Ist die Prüfung erfolgreich, dann MUSS der Messenger-Proxy den `Invite-Event` an den Matrix-Homeserver weiterleiten.

Bei einer erfolgreichen Föderationsprüfung wird das `Invite-Event` durch den Matrix-Homeserver verarbeitet. Dieser prüft, ob die Sender und Empfänger-Matrix-Domain gleich sind. Sind die Matrix-Domain gleich, dann befinden sich beide Akteure auf dem selben Messenger-Service und der einzuladende Akteur wird in einem gemeinsamen Chatraum eingeladen. Wenn die Matrix-Domain des Senders und Empfängers nicht mit der Matrix-Domain des Messenger-Services übereinstimmen wird das `Invite-Event` durch den Matrix-Homeserver an den zuständigen Messenger-Proxy des einzuladenden Empfängers weitergeleitet. Hier MUSS der Messenger-Proxy die Prüfregeln als Server-Server Proxy anwenden.

- **Prüfregeln als Server-Server Proxy**

Für eingehende Server-to-Server Anfragen anderer Messenger-Proxies MUSS der Messenger-Proxy eine Authentisierung gemäß [Server-Server API#Request Authentication] durchführen. Sobald der sendende Matrix-Homeserver authentisiert wurde, MUSS der Messenger-Proxy bei jedem `Invite-Event` gemäß [Server-Server API#Inviting to a room] den Inhalt der Anfrage an den Matrix-Homeserver prüfen. Hierfür MUSS der Messenger-Proxy Prüfregeln für Server-Server Anfragen unterstützen, die im Folgenden beschrieben werden.

Stufe 1 - Prüfung der TI-Föderationszugehörigkeit

Im ersten Schritt MUSS der Messenger-Proxy prüfen, ob die Matrix-Domain im `Invite-Event` Teil der TI-Föderation ist. Hierfür MUSS der Messenger-Proxy in seiner lokalen Föderationsliste prüfen, ob die Matrix-Domain in dieser enthalten ist. Ist dies nicht der Fall, dann MUSS der Messenger-Proxy bei seinem zuständigen Registrierungs-Dienst über die interne Schnittstelle (`I_internVerification`) eine aktuelle Liste abrufen. Ist die anschließende erneute Prüfung fehlgeschlagen, dann MUSS der Messenger-Proxy die Anfrage ablehnen. Ist die Prüfung erfolgreich, MUSS die Überprüfung gemäß der Stufe 2 erfolgen.

Stufe 2 - Prüfung der Freigabeliste

Im zweiten Schritt MUSS der Messenger-Proxy prüfen, ob die MXID des Einladenden in der Freigabeliste des einzuladenden Akteurs vorhanden ist. Hierfür MUSS der Messenger-Proxy über eine Schnittstelle an seinem zuständigen Registrierungs-Dienst prüfen, ob eine entsprechende Freigabe für den Einladenden vorliegt. Ist die Prüfung erfolgreich,

dann MUSS der Messenger-Proxy das `Invite-Event` an den Matrix-Homeserver weiterleiten. Ist dies nicht der Fall, MUSS die Überprüfung gemäß der Stufe 3 erfolgen.

Stufe 3 - Prüfung auf existierenden VZD-FHIR-Directory Eintrag
Im dritten Schritt MUSS der Messenger-Proxy prüfen, ob die MXIDs der beteiligten Akteure im VZD-FHIR-Directory enthalten sind. Hierfür MUSS der Messenger-Proxy an seinem zuständigen Registrierungs-Dienst die interne Schnittstelle `I_internVerification` aufrufen. Ist die Überprüfung erfolgreich (true), MUSS der Messenger-Proxy das `Invite-Event` an den Matrix-Homeserver weiterleiten. Ist die Überprüfung nicht erfolgreich, MUSS das `Invite-Event` abgelehnt werden.

5.1.2.2 Matrix-Homeserver

Der Matrix-Homeserver MUSS die [Server-Server API] und [Client-Server API] der Matrix-Spezifikationen umsetzen. Bereits existierende Produkte, die der Matrix Spezifikation folgen, können als Matrix-Homeserver verwendet werden.

Der Matrix-Homeserver eines Messenger-Services:

- MUSS Anfragen vom eigenen Messenger-Proxy akzeptieren und
- DARF Anfragen anderer Messenger-Proxies NICHT akzeptieren und DARF für andere Messenger-Proxies nicht erreichbar sein.

Die vom Matrix-Homeserver verwendeten Authentifizierungsverfahren MÜSSEN konfigurierbar sein. Beim Anmeldeversuch eines neuen Akteurs an einem Matrix-Homeserver MUSS dieser alle, für diese Organisation unterstützten, Authentifizierungsverfahren zur Auswahl anbieten. Nach einer erfolgreichen Anmeldung eines Akteurs an einem Matrix-Homeserver stellt dieser ein von ihm erstelltes Matrix-ACCESS_TOKEN sowie ein Matrix-OpenID-Token bereit (siehe [gemSpec_TI-Messenger-Dienst#Verwendung der Token]). Das Matrix-ACCESS_TOKEN wird zukünftig für jede weitere Autorisierung am Matrix-Homeserver verwendet. Das ausgestellte Matrix-OpenID-Token wird für eine spätere Authentisierung am Auth-Service des VZD-FHIR-Directory verwendet, um ein search-accesstoken für den Lesezugriff im VZD-FHIR-Directory zu erhalten.

ML-123905 - Umsetzung von BSI-Vorgaben für Server (Produkt)
Der TI-Messenger-Fachdienst SOLL den Vorgaben von [BSI-ISI-Server] folgen.
[<=]

ML-123956 - Umsetzung von BSI-Vorgaben für Server (Anbieter)
Der TI-Messenger-Anbieter SOLL den Vorgaben von [BSI-ISI-Server] folgen.
[<=]

ML-132863 - Erreichbarkeit des Matrix-Homeserver
Der Matrix-Homeserver ist nur über seinen zugehörigen Messenger-Proxy erreichbar.
[<=]

5.1.3 Push-Gateway

Der TI-Messenger-Fachdienst MUSS ein Push-Gateway, gemäß [Matrix Specification#Push Gateway API], für den TI-Messenger-Client bereitstellen. Es obliegt den TI-Messenger-Anbietern der einzelnen TI-Messenger-Clients, ob eine Push-Funktion unterstützt wird.

973 # 6 Anhang A – Verzeichnisse

974 ## 6.1 Abkürzungen

Kürzel	Erläuterung
API	Application Programming Interface
CC	Common Criteria
DSGVO	Datenschutz-Grundverordnung
FHIR	Fast Healthcare Interoperable Resources
HBA	Heilberufsausweis
HTTP	Hyptertext Transfer Protocol
IDP	Identity Provider
JSON	JavaScript Object Notation
MXID	Matrix-User-ID
OAuth	Open Authorization
Opt-In	Deaktiviert mit Möglichkeit zur Aktivierung
OWASP	Open Web Application Security Project
SMC-B	Institutionenkarte (Security Module Card Typ B)
SSSS	Secure Secret Storage and Sharing
TI	Telematikinfrastruktur
TI-ITSM	IT-Service-Management der TI
TI-M	TI-Messenger
TLS	Transport Layer Security
VZD	Verzeichnisdienst

6.2 Glossar

Begriff	Erläuterung
MXID	Eindeutige Identifikation eines TI-Messenger-Nutzers (Matrix-User-ID)
on-premise	Das Produkt wird auf eigener oder gemieteter Hardware betrieben
Relying Party	Vertrauenswürdige Komponente, die Zugriff auf eine sichere Anwendung ermöglicht
X.509-Zertifikat	Ein Public-Key-Zertifikat nach dem X.509-Standard

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

997 aktuellen, von der gematik veröffentlichten Dokumentenlandkarte enthalten, in der die
998 vorliegende Version aufgeführt wird.

999

[Quelle]	Herausgeber: Titel
[api-messenger]	gematik: api-ti-messenger https://github.com/gematik/api-ti-messenger/
[gemGlossar]	gematik: Einführung der Gesundheitskarte – Glossar
[gemKPT_TI_Messenger]	gematik: Konzeptpapier TI-Messenger
[gemSpec_TI_Messenger-Dienst]	gematik: Spezifikation TI-Messenger-Dienst
[gemSpec_TI_Messenger-Client]	gematik: Spezifikation TI-Messenger-Client
[gemKPT_Betr]	gematik: Betriebskonzept Online-Produktivbetrieb
[gemSpec_Perf]	gematik: Übergreifend Spezifikation Performance und Mengengerüst TI-Plattform
[gemSpec_Krypt]	gematik: Übergreifende Spezifikation Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur
[gemSpec_IDP_FD]	gematik: Spezifikation Identity Provider – Nutzungsspezifikation für Fachdienste
[gemSpec_IDP_Dienst]	gematik: Spezifikation Identity Provider-Dienst
[gemSpec_OID]	gematik: Spezifikation Festlegung von OIDs
[gemSpec_SST_LD_BD]	gematik: Spezifikation Logdaten- und Betriebsdatenerfassung

1000

1001 ### 6.5.2 Weitere Dokumente

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[Matrix Specification]	Matrix Foundation: Matrix Specification https://spec.matrix.org/v1.2/

[OpenID]	OpenID Foundation https://openid.net/developers/specs/
[OWASP Proactive Control]	OWASP Proactive Controls https://owasp.org/www-project-proactive-controls/
[Client-Server API]	Matrix Foundation: Matrix Specification - Client-Server API https://spec.matrix.org/v1.2/client-server-api/
[Server-Server API]	Matrix Foundation: Matrix Specification - Server-Server API https://spec.matrix.org/v1.2/server-server-api/

1002