

Elektronische Gesundheitskarte und Telematikinfrastruktur

Spezifikation TI-Messenger-Fachdienst

Version: 1.1.1
Revision: 866416
Stand: 31.07.2023
Status: freigegeben
Klassifizierung: öffentlich
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	29.07.2022		Überarbeitung folgender Features: - Erreichbarkeit einzelner Organisationseinheiten mittels Funktionsaccounts - Öffnung des TI-Messengers für Drittssysteme durch clientseitige Schnittstellen zur Integration z.B. ins Praxisverwaltungssystem - schnelles Finden von Kontaktdaten durch Zugriff auf FHIR-basiertes Adressbuch	gematik
	16.08.2022		Möglichkeit einer Art Zugriffskontrolle für Org-Admin	gematik
1.1.1	31.07.2023		Einarbeitung TI-Messenger Maintenance 23.1 / VZD FHIR Maintenance_23.1	gematik

Inhaltsverzeichnis

1 Einordnung des Dokumentes.....	5
1.1 Zielsetzung.....	5
1.2 Zielgruppe.....	5
1.3 Geltungsbereich.....	5
1.4 Abgrenzungen.....	6
1.5 Methodik.....	6
2 Systemüberblick.....	8
3 Systemkontext.....	10
3.1 Nachbarsysteme.....	10
3.2 Messenger-Services.....	10
3.2.1 Authentifizierungsverfahren.....	11
4 Übergreifende Festlegungen.....	12
4.1 Datenschutz und Sicherheit.....	12
4.2 Authentisierung und Authentifizierung.....	16
4.2.1 Authentisierungssverfahren für die Registrierung eines Messenger-Services...16	
4.2.1.1 OpenID Connect.....	16
4.2.1.2 KIM-Verfahren.....	17
4.2.2 Verhinderung unautorisierter Registrierung eines Messenger-Services.....	17
4.2.3 Authentifizierung der Akteure am Messenger-Service.....	18
4.2.3.1 Verwaltung der Nutzersession.....	18
4.2.3.2 2-Faktor-Authentifizierung.....	18
4.3 DNS-Namensauflösung.....	18
4.3.1 Identifizierung von Messenger-Services.....	19
4.4 Test.....	19
4.5 Betrieb.....	20
4.5.1 Monitoring und Betriebssteuerung.....	20
4.5.2 Kontrollierte Außerbetriebnahme.....	21
5 Funktionsmerkmale.....	22
5.1 Funktionen der Systemkomponenten.....	23
5.1.1 Registrierungs-Dienst.....	23
5.1.1.1 Schnittstellen.....	24
5.1.1.1.1 I_Registration.....	24
5.1.1.1.2 I_requestToken.....	24
5.1.1.1.3 I_internVerification.....	25
5.1.1.1.4 I_VZD_TIM_Provider_Services.....	27
5.1.1.1.5 OAuth / Auth-Service.....	28

5.1.1.2 Bereitstellung eines Org-Admin Accounts.....	28
5.1.1.2.1 Authentisierung einer Organisation.....	28
5.1.1.2.2 Anlegen des Administrations-Accounts.....	29
5.1.2 Messenger-Service.....	29
5.1.2.1 Messenger-Proxy.....	31
5.1.2.1.1 TLS-Terminierung.....	31
5.1.2.1.2 Prüfung des verwendeten Clients.....	31
5.1.2.1.3 HTTP(S)-Forwarding.....	31
5.1.2.1.4 Schnittstelle für Authentifizierungsverfahren.....	31
5.1.2.1.5 Föderationsliste.....	32
5.1.2.1.6 Bereitstellen und Administration der Freigabeliste.....	33
5.1.2.1.7 Ausnahmeregeln.....	33
5.1.2.1.8 Umsetzung von Prüfregeln.....	33
5.1.2.2 Matrix-Homeserver.....	35
5.1.2.2.1 Server Discovery.....	36
5.1.2.2.2 Öffentliche Räume.....	36
5.1.2.2.3 Custom Room Types und Custom State Events.....	36
5.1.3 Push-Gateway.....	37
6 Anhang A - Verzeichnisse.....	38
6.1 Abkürzungen.....	38
6.2 Glossar.....	39
6.3 Abbildungsverzeichnis.....	39
6.4 Tabellenverzeichnis.....	39
6.5 Referenzierte Dokumente.....	40
6.5.1 Dokumente der gematik.....	40
6.5.2 Weitere Dokumente.....	41

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 Leistungserbringereinrichtungen betrachtet. Festlegungen zur Nutzergruppe der Versicherten und Anforderungen an Krankenversicherungsorganisationen werden in der zweiten Ausbaustufe des TI-Messengers Berücksichtigung finden und daher im vorliegenden Dokument nicht weiter betrachtet.

Die vorliegende Spezifikation definiert die Anforderungen zu Herstellung, Test und Betrieb des Produkttyps TI-Messenger-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 Produktypspezifikation 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, Produktypsteckbrief, 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 Anwendungsfalles 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 (Berechtigungsprüfung – Stufe 1 der Client-Server Kommunikation). 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. Ebenfalls stellt der Messenger-Proxy eine Freigabeliste für die Berechtigungsprüfung (Stufe 2 der Server-Server Kommunikation) bereit. Für die Administration dieser Freigabeliste durch die Akteure bietet der Messenger-Proxy den TI-Messenger-Clients eine Schnittstelle an.

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 Funktion die Bereitstellung einer Föderationsliste für die Messenger Proxies seiner Messenger-Services an. 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.

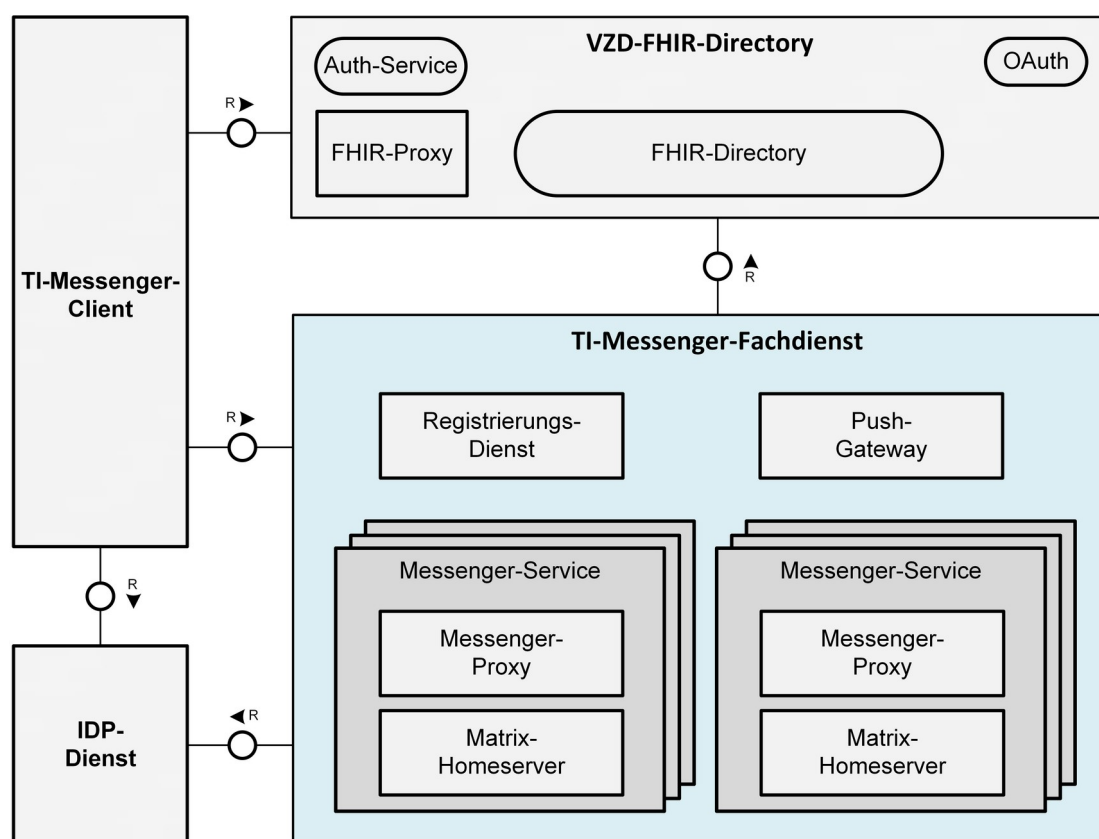


Abbildung 1: Systemüberblick (Vereinfachte Darstellung)

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 gehört der zentrale IDP-Dienst welcher Authentifizierungen und Autorisierungen auf Basis von Smartcard-Identitäten durchführt, sowie das VZD-FHIR-Directory. Die in Kapitel 2-Systemüberblick zu findende Abbildung zeigt deren Beziehung zum TI-Messenger-Fachdienst.

Der zentrale IDP-Dienst stellt allen berechtigten Akteuren ID_TOKEN, gemäß des durch die OpenID Foundation [OpenID] spezifizierten Protokolls, zur Verfügung. Diese können alternativ zum KIM-Verfahren (siehe Kapitel 4.2.1-Authentisierungssverfahren für die Registrierung eines Messenger-Services) für den Nachweis des Besitzes einer SMC-B bei der Bestellung eines Messenger-Services und für die Authentisierung von Leistungserbringern beim Schreibzugriff auf das FHIR-Directory verwendet werden.

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-Service 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.

3.2.1 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.

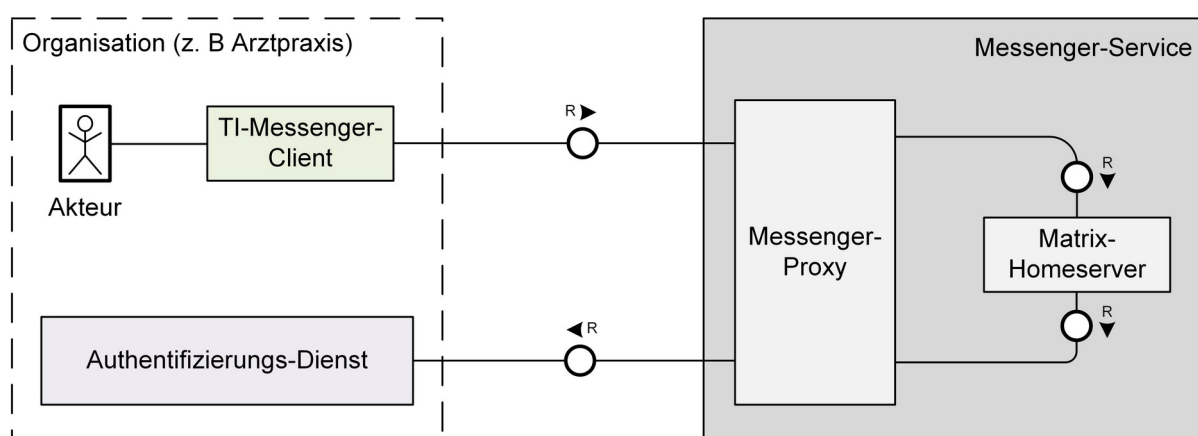


Abbildung 2: Beispiel - Authentifizierung von Akteuren einer Organisation

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 - Vertragsverpflichtungen

Der TI-Messenger-Anbieter MUSS Kunden vertraglich verpflichten, dass organisationsbasierte TI-Messenger-Accounts nicht an Dritte vergeben werden und nur Accounts für Akteure der Organisation erstellt werden, mit denen ein Beschäftigungsverhältnis oder Dienstleistervertragsverhältnis besteht. Funktionsaccounts (in Verbindung mit einem Chatbot) sind von den Vertragsverpflichtungen ausgenommen.
[<=]

A_22809 - Flächendeckende Verwendung von TLS für Hersteller

TI-Messenger-Fachdienst-Hersteller 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 serverseitiges 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 serverseitiges 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 und gesperrt werden können. Der Anbieter MUSS sicherstellen, dass zur Authentifizierung mindestens zwei Faktoren verwendet werden und die Sicherheitsempfehlungen des BSI [BSI 2-Faktor] Berücksichtigung finden. Zur Vermeidung von Angriffen aus der Ferne auf den 2. Faktor ist ein Verfahren zu wählen, das mindestens mit "mittel" bewertet ist. Der Anbieter MUSS sicherstellen, dass mindestens eine Authentisierung mittels OIDC-Authenticator unterstützt wird und technische Optionen für die Organisation gegeben sind, damit beide Faktoren nicht durch einen Angriffsvektor kompromittiert 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_23611 - Vorgaben zur minimalen Qualität von Passwörtern

Der Anbieter des TI-Messenger-Fachdienstes MUSS Vorgaben zur minimalen Qualität von Passwörtern entsprechend [BSI ORP.4] A.22 machen und die Einhaltung dieser Vorgaben an allen Stellen gewährleisten, an denen Passwörter im Rahmen der Konfiguration festzulegen sind. Weiterhin MUSS der Anbieter die Leistungserbringerinstitution (LEI), welche den TI-Messenger Dienst von ihm bezieht, über die Notwendigkeit der Einhaltung der Vorgaben aus [BSI ORP.4] A8 instruieren. Diese beinhalten sicherheitsrelevante Anforderungen hinsichtlich der Nutzung und des Umgangs mit Passwörtern, richten sich jedoch an den operativen Betrieb in der LEI, der vom Anbieter nicht kontrolliert werden kann. Unter Passwörtern werden in diesem Kontext sowohl Kennwörter als auch Passphrasen verstanden, auf welche das Dokument [BSI ORP.4] gleichermaßen anwendbar ist. [≤]

A_23613 - Zwangsabmeldung und Sperrung von Akteuren

Wird ein Akteur in der Rolle "User" des TI-Messenger-Dienstes einer Organisation durch einen Akteur in der Rolle "Org-Admin" der Organisation gesperrt oder seine aktive Sitzung beendet - das heißt, er wird zwangsweise ausgeloggt -, so MUSS der TI-Messenger-Fachdienst die Weiterleitung von Nachrichten, die an diesen Akteur in der Rolle "User" gesendet werden oder von diesem gesendet werden, mit sofortiger Wirkung einstellen. [≤]

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. Zum Nachweis der Umsetzung ist eine Prüfung des Prozesses zur Einbringung des kryptografischen Materials erforderlich. Die Prüfung umfasst die Beschreibung und Durchführung des Prozesses. Eine Auditierung der Umsetzung ist optional. [≤]

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.

Hinweis: 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 zeitlich begrenzte 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.

Hinweis: Die gematik kann nach § 331 Abs. 2 SGB V Daten festlegen, die Anbieter von Komponenten und Dienste der gematik offenzulegen bzw. zu übermitteln haben, sofern diese erforderlich sind, um den gesetzlichen Auftrag der gematik zur Überwachung des Betriebs zur Gewährleistung der Sicherheit, Verfügbarkeit und Nutzbarkeit der

Telematikinfrastruktur zu erfüllen. Nur die hierfür erforderlichen personenbezogenen Daten dürfen von den Anbietern und Herstellern als zeitlich begrenzte 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_22811 - Löschfristen für Matrix-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 Akteur in der Rolle "Org-Admin" konfigurierbar ist. Diese Funktion DARF über Opt-Out durch den Akteur in der Rolle "Org-Admin" 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 sicherstellen, 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.

[<=]

A_22965 - Push-Benachrichtigungen Messenger-Anbieter

TI-Messenger-Anbieter MÜSSEN sicherstellen, 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).
- Es MÜSSEN Push-Anbieter gewählt werden, die eine Wahrung der Betroffenenrechte gemäß DSGVO gewährleisten.

[<=]

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 zu A_22818: 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_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 zu A_22810: 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 Authentisierung und 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 authentisieren, um einen oder mehrere Messenger-Services für seine Organisation registrieren zu können. Um die Organisation gegenüber dem Registrierungs-Dienst zu authentifizieren, KÖNNEN die im folgenden Kapitel beschriebenen Verfahren OpenID Connect oder KIM verwendet werden.

4.2.1 Authentisierungsverfahren für die Registrierung eines Messenger-Services

4.2.1.1 OpenID Connect

Beim OpenID Connect Verfahren wird der zentrale IDP-Dienst der gematik benötigt, um eine Organisation am Registrierungs-Dienst zu authentifizieren sowie Leistungserbringer über ihren TI-Messenger-Clients Schreibzugriff auf das VZD-FHIR-Directory zu ermöglichen. Hierfür MÜSSEN der Registrierungs-Dienst und die TI-Messenger-Clients am zentralen 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 zentralen 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 zentralen IDP-Dienst folgende Claims im ID_TOKEN vereinbaren:

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

Leistungserbringerinstitutionen (SMC-B)	Leistungserbringer (HBA)
<ul style="list-style-type: none"> • ProfessionOID • idNummer • organizationName • acr • aud 	<ul style="list-style-type: none"> • 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.

Hinweis: Detaillierte Erläuterungen zu den Abläufen zur Authentifizierung sind in [api-messenger] in einem spezifischen Howto beschrieben.

4.2.1.2 KIM-Verfahren

Bei der Authentifizierung über das KIM-Verfahren MUSS sowohl der Anbieter des TI-Messengers, als auch die Organisation die am TI-Messenger-Dienst teilnehmen möchte, über funktionierende KIM-Accounts verfügen. Für die Nutzung des KIM-Verfahrens ist eine gültige SMC-B Org sowie eine KIM-Installation notwendig.

Der Akteur in der Rolle "Org-Admin" wird im Bestellvorgang aufgefordert, seine KIM Mail-Adresse in eine Eingabemaske einzutragen. Daraufhin MUSS zur angegebenen KIM-Adresse im Verzeichnisdienst (z. B. im LDAP-VZD gemäß gemSpec_VZD) dieTelematikID sowie die ProfessionOID abgerufen werden. Anschließend MUSS der Registrierungs-Dienst prüfen, ob die ProfessionOID zu einer Organisation des Gesundheitswesens gehört. Der Registrierungs-Dienst sendet der Organisation nach einem positiven Prüfergebnis eine KIM-Nachricht mit einer URL an die angegebene KIM-Adresse und

fordert den Akteur in der Rolle "Org-Admin" auf, die KIM-Nachricht zu lesen und die darin befindliche URL zu öffnen. Um sicherzustellen, dass derselbe Akteur, welcher die Registrierung gestartet hat, auch der-/diejenige ist, welcher die URL aufruft, MUSS der Registrierungs-Dienst einen zufälligen sechsstelligen Code anzeigen, welcher beim URL-Aufruf geprüft werden MUSS. Bei einem negativen Prüfergebnis MUSS der Registrierungs-Dienst eine aussagekräftige Fehlermeldung anzeigen. Durch folgen des Links wird der Akteur wieder in den Bestellprozess zurückgeführt, gibt den zuvor angezeigten Code ein und die Authentisierung ist abgeschlossen. Durch das Entschlüsseln der KIM-Nachricht und die Eingabe des sechsstelligen Codes ist nachgewiesen, dass es sich hierbei um die antragstellende Organisation des Gesundheitswesens handelt.

4.2.2 Verhinderung unautorisierter Registrierung eines Messenger-Services

Der Nachweis des Besitzes einer SMC-B im Zuge der Authentifizierung einer Organisation am Registrierungs-Dienst ist ein notwendiges Kriterium, damit der dazugehörige Prozess überhaupt initiiert werden kann. Da der Nachweis einer SMC-B in beiden der zuvor genannten Verfahren jedoch nicht zwangsläufig von jemandem erbracht wird, der innerhalb der Leistungserbringerinstitution auch zur Registrierung eines Messenger-Dienstes befugt ist, MUSS der Anbieter Maßnahmen ergreifen, welche die Erfüllung einer unautorisierten Bestellung verhindert.

A_23521 - Verhinderung unautorisierter Registrierung

Der TI-Messenger Anbieter MUSS einen organisatorischen oder technischen Prozess etablieren, der die erfolgreiche Registrierung eines Messenger-Service durch einen unautorisierten Akteur verhindert. [≤]

Beispiel: Um sicherzustellen, dass nur solche Bestellungen zur erfolgreichen Registrierung und Inbetriebnahme des Messenger-Dienstes führen, die willentlich und mit Befugnis ausgeführt wurden, könnte der Anbieter auf Basis des Eingangs einer Bestellung einen nachgelagerten Prozess etablieren, der eine postalische Bestätigung bei der LEI vorsieht. Dabei würde diejenige Stelle adressiert werden, die befugt ist über die Legitimität der Bestellung zu entscheiden.

4.2.3 Authentifizierung der Akteure am Messenger-Service

Damit Akteure Ad-Hoc-Nachrichten austauschen können, MÜSSEN sich diese an ihrem Messenger-Service authentisieren. Die Authentisierung MUSS hierbei über ein zwischen der Organisation und dem Anbieter vereinbartes Verfahren erfolgen. Wurden die 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.

4.2.3.1 Verwaltung der Nutzersession

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

4.2.3.2 2-Faktor-Authentifizierung

Der TI-Messenger-Service MUSS zur Authentisierung der Akteure mindestens eine 2-Faktor-Authentifizierung durchsetzen. Der zweite Faktor MUSS den Sicherheitsempfehlungen des BSI gemäß [BSI 2-Faktor] zur Resilienz gegen Angriffe aus der Ferne, mindestens mit mittlerer Bewertung genügen. Der Anbieter MUSS sicherstellen, dass mindestens eine Authentisierung mittels OIDC-Authenticator unterstützt wird und technische Optionen für die Organisation gegeben sind, damit beide Faktoren nicht durch einen Angriffsvektor kompromittiert werden können.

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 Benennung gewählt, erfolgt die Eintragung der notwendigen DNS-Records auf DNS-Server im Internet durch die Administration der Organisation.

4.3.1 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 auch an Unterauftragnehmer aus- bzw. verlagert werden oder *on-premise* gehostet werden. 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.

Anforderungen zu Performance und Reporting sind den entsprechenden Produkt- und Anbietertypsteckbriefen u.a. den Dokumenten [gemSpec_Perf] und [gemKPT_Betr] zu entnehmen.

4.5.1 Monitoring und Betriebssteuerung

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.

A_23092 - TI-M Gültigkeitsprüfung der Organisation am VZD-FHIR-Directory

Der TI-Messenger Fachdienst MUSS mindestens alle 24 Stunden, für alle bei ihm registrierten Organisationen mit einem Messenger-Service, prüfen, ob diese im VZD-FHIR-Directory als "active" (Organization.active) eingetragen sind.

[<=]

A_23093 - TI-M Information an Nutzer bei ausgetragener Organisation am VZD-FHIR-Directory

Wenn die Organisation nicht mehr im VZD-FHIR-Directory "active" (Organization.active) ist, MUSS der TI-Messenger-Anbieter diese darüber informieren.

[<=]

A_23094 - TI-M Sperrung der Organisation mit ungültiger SMC-B

Wenn die Organisation länger als 30 Kalendertage nicht im VZD-FHIR-Directory "active" (Organization.active) ist, MUSS der TI-Messenger-Anbieter die Domäne dieses Messenger-Service aus der Föderation löschen (siehe FHIR-VZD: I_VZD_TIM_Provider_Services, DELETE /federation/{domain}). Dann DARF erst nach erneuter Authentifizierung mit der SMC-B der Dienst wieder genutzt werden, siehe AF_10103.

[<=]

4.5.2 Kontrollierte Außerbetriebnahme

Wenn z. B. das Vertragsverhältnis zwischen Kunde und TI-Messenger-Anbieter ausläuft, so MUSS der TI-Messenger-Anbieter die dazugehörige Domäne dieses Messenger-Service aus der Föderation löschen (siehe FHIR-VZD: I_VZD_TIM_Provider_Services, DELETE /federation/{domain}) und den Messenger-Service abschalten, so dass dieser nicht mehr erreicht werden kann.

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:

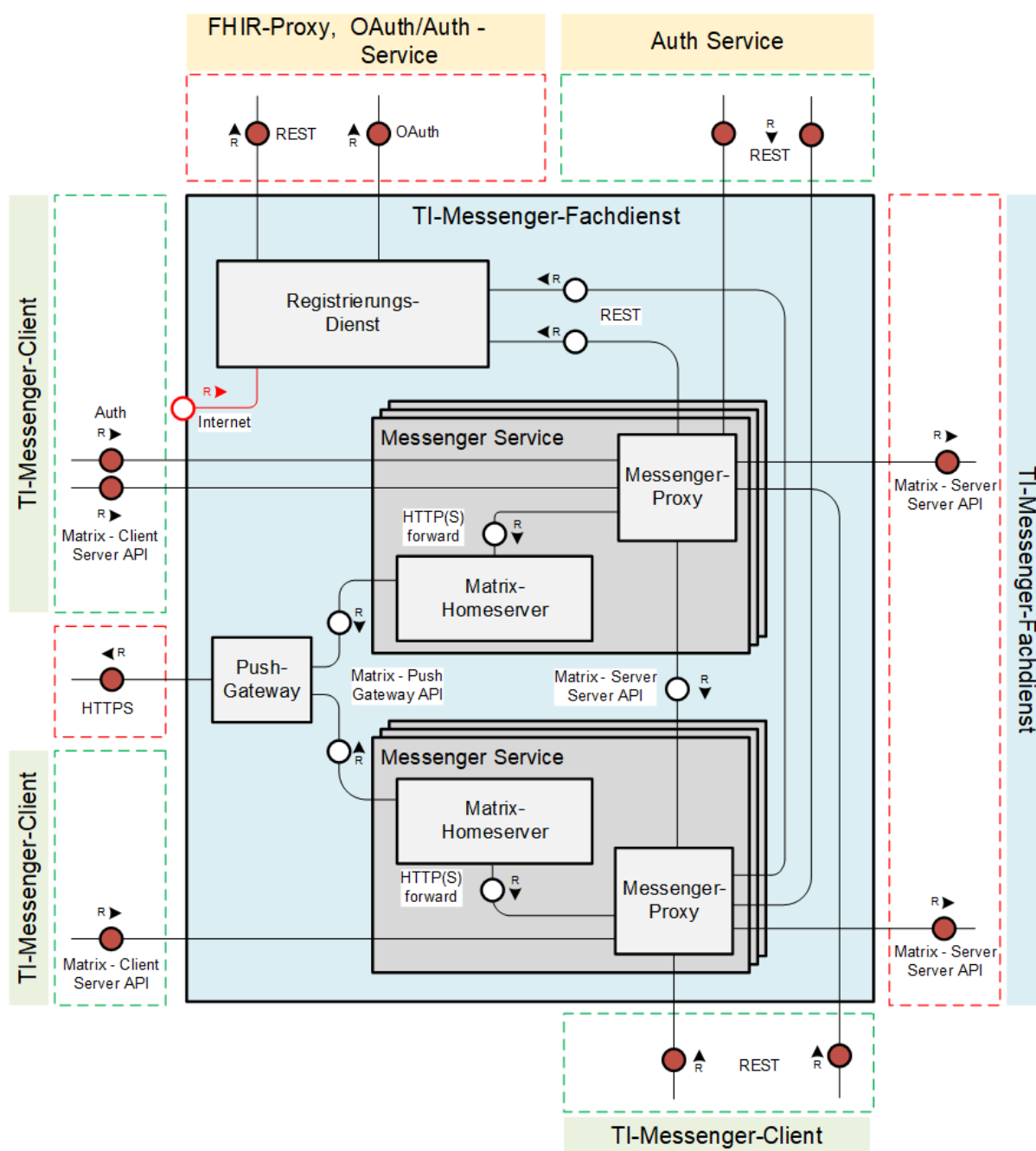


Abbildung 3: Funktionaler Aufbau des TI-Messenger-Fachdienstes

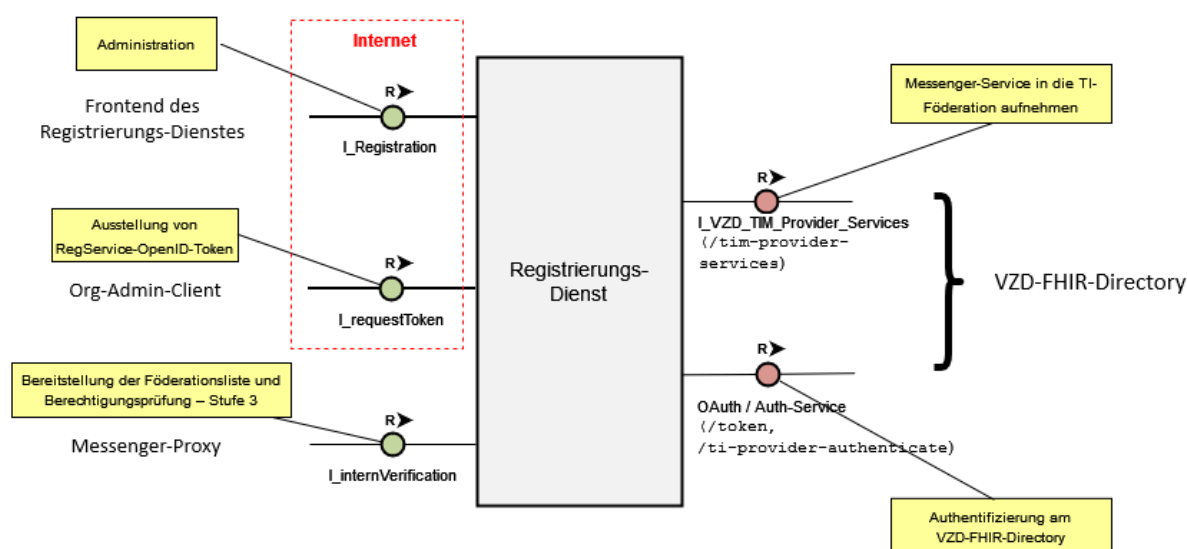
Die in der Abbildung grün dargestellten Boxen zeigen die Schnittstellen, die am TI-Messenger-Fachdienst aufgerufen werden. Rot dargestellte Boxen zeigen die Schnittstellen, über die der TI-Messenger-Fachdienst weitere Services anderer Komponenten nutzt. Eine Ausnahme bildet die Kommunikation zwischen 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 bzw. die vom TI-Messenger-Client mit Org-Admin Funktionalität verwendete Schnittstelle zur Administration bzw. zur Ausstellung eines RegService-OpenID-Tokens. 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 (Bereitstellung der Föderationsliste und Berechtigungsprüfung - Stufe 3) am Registrierungs-Dienst kann auch über separate Schnittstellen erfolgen. Bei den beiden Schnittstellen `I_Registration` und `I_requestToken` handelt es sich um die Schnittstellen die der TI-Messenger-Anbieter im Internet anbieten MUSS. Diese werden nicht normativ von der gematik spezifiziert.

5.1.1.1 Schnittstellen

In den folgenden Kapiteln werden die Schnittstellen beschrieben, die der Registrierungs-Dienst bereitstellen und aufrufen MUSS.

5.1.1.1.1 `I_Registration`

Der TI-Messenger-Fachdienst MUSS eine Schnittstelle für die Administration am Registrierungs-Dienst 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.

5.1.1.1.2 `I_requestToken`

Der TI-Messenger-Fachdienst MUSS eine Schnittstelle für die Ausstellung eines ID_TOKENS (RegService-OpenID-Token) am Registrierungs-Dienst bereitstellen. Das Token wird für die Authentifizierung am FHIR-Proxy des VZD-FHIR-Directory benötigt, damit ein Akteur in der Rolle "Org-Admin" Organisationseinträge ändern kann. Die Ausgestaltung der Schnittstelle am Registrierungs-Dienst (`I_requestToken`) ist dem jeweiligen TI-Messenger-Anbieter überlassen. Der Registrierungs-Dienst MUSS dafür sorgen, dass nur für authentifizierte Akteure in der Rolle "Org-Admin" ein Token ausgestellt wird. Die Gültigkeit des RegService-OpenID-Tokens MUSS kleiner oder maximal gleich einer Stunde betragen.

5.1.1.1.2.1 Aufbau des RegService-OpenID-Token

Das RegService-OpenID-Token ist ein JSON-Web-Token und MUSS folgende Attribute enthalten:

```
HEADER
{
  "alg": "BP256R1",
  "typ": "JWT"
  "x5c": [
    "<X.509 Sig-Cert, base64-encoded DER>" ]
}
PAYLOAD
{
  "sub": "1234567890",
  "iss": "<url des Registrierungs-Dienst-Endpunkts, über den das Token
ausgestellt wurde>",
  "aud": "<url des owner-authenticate-Endpunkte am VZD-FHIR-Directory>",
  "professionOID": "<ProfessionOID der Organisation>",
  "idNummer": "<TelematikID der Organisation>",
  "iat": "1516239022",
```



```
"exp": "1516242622"  
}
```

5.1.1.1.2.2 Signatur des RegService-OpenID-Token

Für die Signatur des RegService-OpenID-Token MUSS der private Schlüssel des Zertifikats C.FD.SIG verwendet werden. Das Zertifikat wird durch einen TI-ITSM Service Request beantragt. Bevor das Zertifikat abläuft MUSS ein neues beantragt werden und das neue Zertifikat an das VZD-FHIR-Directory übergeben werden.

5.1.1.1.3 I_internVerification

Der Registrierungs-Dienst MUSS eine Schnittstelle für die Bereitstellung sowie der Aktualisierung der Föderationsliste und die Überprüfung auf MXID-Einträge im VZD-FHIR-Directory zur Verfügung stellen. Die Ausgestaltung der Schnittstelle am Registrierungs-Dienst (I_internVerification) ist dem jeweiligen TI-Messenger-Anbieter überlassen.

5.1.1.1.3.1 Bereitstellung und Aktualisierung der Föderationsliste

Inhalt der Föderationsliste, die der Registrierungs-Dienst über die Schnittstelle den Messenger-Proxies bereitstellen MUSS, sind alle 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 `getFederationList` (GET `/tim-provider-services/FederationList/federationList.jws`) aufgerufen werden. Im Aufruf der Schnittstelle MUSS ein `provider-accesstoken` enthalten sein. Optional kann auch die aktuell verwendete Version mit in den Aufruf übergeben werden. Wenn die Version übergeben wird, dann wird nur bei einer veralteten Version eine neue Föderationsliste vom VZD-FHIR-Directory bereitgestellt. 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, sofern die durch den Registrierungs-Dienst vorgehaltene Föderationsliste älter als eine Stunde ist. 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 Föderationszugehörigkeit über die interne Schnittstelle I_internVerification bereitgestellt werden.

Der Registrierungs-Dienst MUSS regelmäßig jede Stunde die Aktualität der Föderationsliste am VZD-FHIR-Directory prüfen. Ist das VZD-FHIR-Directory nicht innerhalb einer definierten Antwortzeit erreichbar und es bleiben auch weitere Aktualisierungsversuche erfolglos (`HealthState_VZD` und `HealthStateCheck_VZD`), MUSS der Registrierungs-Dienst seine eigene Vorhaltezeit der Föderationsliste auf einen festgelegten Wert von 72 Stunden (`TTL_Föderationsliste`) verlängern und ein Incident-Event erzeugen, welches durch ein Drittsystem aufgefangen werden kann (z. B. ein ITSM-System). Falls die Föderationsliste nicht nach weiteren Aktualisierungsversuchen aktualisiert werden konnte, MUSS ein Incident beim VZD-FHIR-Directory-Anbieter eingestellt werden. Die vorhandene Föderationsliste SOLL bis zur Behebung des Incidents weiter genutzt werden, jedoch maximal für 72 Stunden. Nach dem Ablauf dieser Zeitspanne darf der Messenger-Proxy die Kommunikation zu anderen Matrix-Homeservern nicht mehr erlauben, bis wieder eine aktuelle Föderationsliste vom Registrierungs-Dienst abgerufen werden kann.

Hinweis: Die Vorhaltung einer aktuellen Föderationsliste ist aus sicherheitstechnischer Perspektive sinnvoll, um das Zeitfenster klein zu halten, in welchem ein Fachdienst "unwissentlich" mit einem anderen Fachdienst interagiert, der nicht mehr Teil der Föderation ist. Die Wahl einer geeigneten Frist, innerhalb welcher das Arbeiten mit einer alten Liste noch akzeptabel ist, weil diese nicht aktualisiert werden konnte, berücksichtigt zu erwartende Zeitaufwände der Wiederherstellung bei Nichtverfügbarkeit des VZD und ist dabei nicht großzügiger gewählt, als Fristen, die für andere Kommunikationsdienste innerhalb der TI eingeräumt werden.

In der folgenden Tabelle werden Attribute und ihre Typen definiert, die am Registrierungs-Dienst vorgehalten werden MÜSSEN:

Tabelle 2 Spezifische Attribute für das Handling der Föderationsliste am Registrierungs-Dienst

Attribut	Typ	Beschreibung	Wertebereich
HealthState_VZD	Zustand	Typ hält Gesundheitszustand von Komponenten des VZD-FHIR-Directorys auf Basis ihres Antwortverhaltens vor	[gesund, ungesund]
HealthStateCheck_VZD	hochzählender Iterator	Typ hält die Menge der Wiederholungsversuche der Prüfung des Gesundheitszustandes des VZD-FHIR-Directory	$0 \leq \text{HealthStateCheck_VZD} \leq 3$
Alter_Föderationsliste	hochzählender Zeitzähler	Typ hält das aktuelle Alter der Föderationsliste vor ab dem Zeitpunkt der letzten Aktualisierung.	min: 0s
TTL_Föderationsliste	Lebensdauer	Typ beschreibt den oberen Grenzwert, den eine Föderationsliste alt sein darf	Konstanter Wert: 72h

Die hier beschriebenen Attribute und ihre Verwendung sind in Sequenzdiagramm [gemSpec_TI_Messenger-Dienst#Aktualisierung der Föderationsliste] erläutert. Sobald durch den Messenger-Proxy ein Request zur Aktualisierung der Föderationsliste am Registrierungs-Dienst initiiert wird, MUSS der Registrierungs-Dienst die aktuelle Liste vom FHIR-Proxy abfragen, sofern die vom Registrierungs-Dienst vorgehaltene Liste zu alt ist (Alter_Föderationsliste). Sollte die Liste des Registrierungs-Dienstes nicht zu alt sein,

so MUSS dessen Föderationsliste an den Messenger-Proxy ausgeliefert werden. Das geschieht jedoch nur, wenn die Liste des Registrierungs-Dienstes aktueller ist als die des Messenger-Proxy. Erhält der Messenger-Proxy eine aktuelle Föderationsliste, so MUSS eine Signaturprüfung lokal anhand des mitgelieferten Signaturzertifikates durchgeführt werden. Beim Signaturzertifikat handelt es sich um das erste Element aus der - gemeinsam mit der Föderationsliste übertragenen - x5c-Zertifikatsliste.

5.1.1.1.3.2 Berechtigungsprüfung - Stufe 3

Der Registrierungs-Dienst MUSS eine Funktion anbieten, mit der die Überprüfung auf MXID-Einträge im VZD-FHIR-Directory möglich ist. Hierfür MUSS der Registrierungs-Dienst die Operation `whereIs` (GET `/tim-provider-services/localization`) am FHIR-Proxy des VZD-FHIR-Directory verwenden.

Die Prüfung ist erfolgreich wenn:

- die MXID des einzuladenden Akteurs im Organisationsverzeichnis hinterlegt und seine Sichtbarkeit in diesem Verzeichnis nicht eingeschränkt ist oder
- der einladende sowie der einzuladende Akteur im Personenverzeichnis hinterlegt sind und der einladende Akteur seine Sichtbarkeit in diesem Verzeichnis nicht eingeschränkt hat

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

5.1.1.1.4 I_VZD_TIM_Provider_Services

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 `addTiMessengerDomain` (POST `/tim-provider-services/federation`), am VZD-FHIR-Directory, eingetragen werden. Im Aufruf der Schnittstelle MUSS ein `provider-accesstoken` enthalten sein.

5.1.1.1.5 OAuth / Auth-Service

Für den Zugriff des Registrierungs-Dienstes auf das VZD-FHIR-Directory über die Schnittstelle `I_VZD_TIM_Provider_Services` (`/tim-provider-services`) des FHIR-Proxy ist eine vorherige Authentifizierung unter Verwendung des 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 des `/tim-provider-services` Endpunktes enthalten sein MUSS. Der Authentifizierungsprozess besteht aus den nacheinander stattfindenden Aufrufen:

- POST `/auth/realms/TI-Provider/protocol/openid-connect/token` (OAuth-Service)
- GET `/ti-provider-authenticate` (Auth-Service)

Beim ersten Aufruf werden die Client-Credentials übergeben, beim zweiten Aufruf ein TI-Provider-Accessstoken, welches man beim ersten Aufruf als Rückgabewert erhalten hat.

5.1.1.2 Bereitstellung eines Org-Admin Accounts

Für die Bereitstellung eines Org-Admin Accounts sind die in den folgenden Kapiteln beschriebenen Schritte erforderlich.

5.1.1.2.1 Authentisierung einer Organisation

Bei der Authentisierung einer Organisation KÖNNEN die im Kapitel 4.2.1-Authentisierungsverfahren für die Registrierung eines Messenger-Services genannten Verfahren verwendet werden. Im Folgenden werden diese Verfahren weiter beschrieben:

5.1.1.2.1.1 OpenID Connect

Gemäß des OpenID Connect Standards MUSS bei der Erzeugung eines Authorization Codes eine PKCE-Code-Challenge durchgeführt werden. Dazu MUSS der Registrierungs-Dienst den PKCE Code erzeugen und später den Verifier dieser Challenge zusammen mit dem Authorization Code beim zentralen IDP-Dienst gegen ein ID_TOKEN einlösen. Der Registrierungs-Dienst MUSS bei einer neuen Registrierungsanfrage automatisiert den durch den zentralen IDP-Dienst ausgestellten ID_TOKEN validieren. Bei der Validierung MUSS der Registrierungs-Dienst die im ID_TOKEN enthaltene ProfessionOID gegen die in der Tabelle "Tab_PKI_403-x OID-Festlegung Institutionen im X.509-Zertifikat der SMC-B" gelisteten OIDs gemäß [gemSpec_OID] prüfen.

5.1.1.2.1.2 KIM-Verfahren

Das Frontend des Registrierungs-Dienst MUSS dem Akteur eine Eingabemaske für die zu verwendende KIM-Adresse anbieten. Am Verzeichnisdienst (z. B. LDAP-VZD gemäß [gemSpec_VZD]) MUSS anhand der KIM-Adresse die ProfessionOID sowie die TelematikID abgefragt werden. Der ermittelte Datensatz MUSS anschließend dem Registrierungs-Dienst bereitgestellt werden. Diese MÜSSEN zusammen mit dem Admin-Account-Daten dieser Organisation gespeichert werden. Der Registrierungs-Dienst MUSS die ProfessionOID gegen die in der Tabelle "Tab_PKI_403-x OID-Festlegung Institutionen im X.509-Zertifikat der SMC-B" gelisteten OIDs gemäß [gemSpec_OID] prüfen. Anschließend MUSS der Registrierungs-Dienst eine KIM-Nachricht mit einer URL die auf den Bestellprozess zurückführt, generieren. Dabei MUSS die URL aus dem FQDN des Registrierungs-Dienstes und einer eindeutigen ID (UUID) gemäß [RFC4122] bestehen. Zusätzlich MUSS in der KIM-Nachricht das E-Mail-Header Element X-KIM-Dienstkennung: Auth;Verification;V1.0 mit aufgenommen werden. In der KIM-Nachricht MUSS ersichtlich sein, dass es sich hierbei um eine Authentifizierungsmail handelt. Neben dem Aufruf der URL MUSS zusätzlich durch den Registrierungs-Dienst ein sechs stelliger PIN-Code geprüft werden, der zuvor in der Bestellmaske angezeigt wurde und zufällig ist.

5.1.1.2.2 Anlegen des Administrations-Accounts

Nach erfolgreicher Authentifizierung einer Organisation am Registrierungs-Dienst MUSS ein Admin-Account für die Organisation auf dem Registrierungs-Dienst angelegt werden. Dieser MUSS für die Authentisierung des Akteurs in der Rolle "Org-Admin" eine 2-Faktor-Authentifizierung verwenden und die Sicherheitsempfehlungen des BSI [BSI 2-Faktor] berücksichtigen. Zur Vermeidung von Angriffen aus der Ferne auf den 2. Faktor ist ein Verfahren zu wählen, das mindestens mit "mittel" bewertet ist. Der Anbieter MUSS sicherstellen, dass mindestens eine Authentisierung mittels Authenticator unterstützt

wird und technische Optionen für die Organisation gegeben sind, damit beide Faktoren nicht durch einen Angriffsvektor kompromittiert werden können. Ist für die Organisation bereits ein Admin-Account vorhanden, DARF eine erneute initiale Authentifizierung der Organisation mit Hilfe der SMC-B für diese Organisation NICHT möglich sein und DARF NICHT dazu führen, dass ein weiterer Admin-Account angelegt, oder der bisherige überschrieben wird.

Der Admin-Account ermöglicht es einem Akteurs in der Rolle "Org-Admin" einen oder mehrere Messenger-Services für seine Organisation zu registrieren. Die in der Registrierungsanfrage für eine Domain übergebene Matrix-Domain MUSS durch den Registrierungs-Dienst über die Schnittstelle `I_VZD_TIM_Provider_Services` gemäß [VZD_Provider_Services#Version 1.3.0] am VZD FHIR-Proxy in die Föderation eingetragen werden. Ebenfalls MUSS der Registrierungs-Dienst dem Frontend des Registrierungs-Dienstes die erstellte Matrix-Domain für den Zugriff auf den beantragten Messenger-Service übergeben

5.1.2 Messenger-Service

Ein Messenger-Service besteht aus den Teilkomponenten Matrix-Homeserver und 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. Welche APIs der Matrix-Spezifikation im Messenger-Service nachgenutzt werden, ist in der folgenden Abbildung dargestellt:

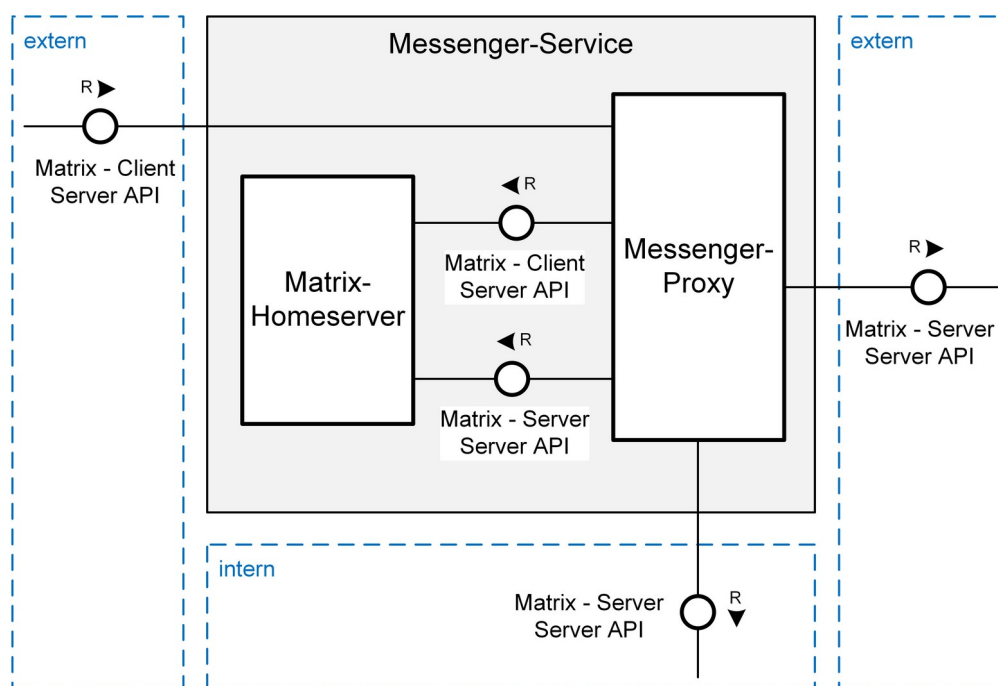


Abbildung 5: Matrix-API des Messenger-Service

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

- [Server-Server API] und
- [Client-Server API]

umgesetzt werden.

Der Aufruf der Client-Server-API am Matrix-Homeserver MUSS immer über den Messenger-Proxy erfolgen. Der Messenger-Proxy übernimmt hierbei die Aufgabe eines Reverse-Proxys. Dieser leitet alle durch ihn autorisierten Aufrufe der TI-Messenger-Clients an den Matrix-Homeserver weiter. Die Kommunikation der Matrix-Homeserver über die Server-Server-API MUSS ebenfalls über den Messenger-Proxy erfolgen. Hierbei MUSS der Proxy die Funktion als Forward-Proxy (Sender-Seite) sowie als Reverse-Proxy (Empfänger-Seite) einnehmen. 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 als Forward sowie Reverse-Proxy 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. Die Matrix-Server-Server-API (Server-Server Kommunikation) und Matrix-Client-Server-API (Client-Server Kommunikation) 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.

5.1.2.1.1 TLS-Terminierung

Alle Anfragen der TI-Messenger-Clients und anderer Messenger-Services an den Matrix-Homeserver MÜSSEN über den Messenger-Proxy (in der Funktion als Reverse-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.

5.1.2.1.2 Prüfung des verwendeten Clients

Der Messenger-Proxy MUSS prüfen, ob die Anfrage von einem zugelassen TI-Messenger-Client erfolgt. Die Überprüfung erfolgt anhand des 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.

5.1.2.1.3 HTTP(S)-Forwarding

Sämtliche TLS-Verbindungen, die über den Messenger-Proxy weitergeleitet werden, MÜSSEN von diesem aufgebrochen werden. Die Kommunikation des Matrix Homeservers in das Internet MUSS immer über den eigenen Messenger Proxy (in der Funktion als Forward-Proxy) erfolgen. Das Forwarding KANN hierbei sowohl über HTTP als auch über HTTPS erfolgen, wobei HTTP NICHT verwendet werden DARF, wenn die Kommunikation zwischen Matrix Homeserver und Messenger Proxy unter Verwendung nicht-vertrauenswürdiger Infrastruktur zustande kommt.

5.1.2.1.4 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.

5.1.2.1.5 Föderationsliste

Der Messenger-Proxy MUSS bei seinem zuständigen Registrierungs-Dienst die Föderationsliste über die interne Schnittstelle `I_internVerification` abrufen, die Signatur der Föderationsliste gemäß RFC7797 prüfen und diese lokal speichern. Zur Prüfung der Signatur der Föderationsliste ist das im Signatur-Header enthaltene Signaturzertifikat (öffentliche Schlüssel) und das X.509-Root-CA Zertifikat der TI erforderlich. Das X.509-Root-CA Zertifikat MUSS im Truststore des Messenger-Proxies gespeichert sein. Die Struktur der Föderationsliste ist in [gemSpec_VZD_FHIR_Directory#Erzeugung und Bereitstellung der Föderationsliste] beschrieben.

Hinweis: Die gematik plant, einen OCSP-Responder für die Prüfung des Zertifikatsstatus im Internet bereitzustellen. Sobald dieser vorhanden ist MUSS dieser für die Prüfung zusätzlich verwendet werden.

Der Messenger-Proxy MUSS wöchentlich prüfen, ob neue X.509-Root-CA-Versionen existieren und Cross-Zertifikate verfügbar sind. Falls dies der Fall ist, so MUSS der Messenger-Proxy diese neue Root-Versionen in seinen Truststore importieren.

Nach der Erzeugung einer neuen Root-Version der X.509-Root-CA der TI werden dessen selbstsigniertes Zertifikat und Cross-Zertifikate auf den Download-Punkt gemäß [ROOT-CA] abgelegt. Automatisiert kann der Messenger-Proxy von dort die Verfügbarkeit neuer Versionen überwachen. Zusätzlich kann der folgende Download-Punkt unter [ROOT-CA-JSON] verwendet werden. Dort werden die aktuellen Root-Zertifikate inkl. deren Cross-Zertifikate gepflegt. Im Regelfall wird alle zwei Jahre eine neue Root-Version erzeugt. Die Dateigröße der heruntergeladenen JSON-Datei kann man als Hashfunktion verwenden. Hiermit kann man beispielsweise mit Hilfe des Tools `curl` die HTTP-Methode `HEAD` verwenden und damit erfahren ob die lokale Kopie der JSON-Datei noch aktuell ist. Die JSON-Datei ist ein Array, in dem Associative Arrays als Elemente aufgeführt werden. Diese Elemente enthalten je ein Root-Zertifikat inkl. Cross-Zertifikate für das chronologisch vorhergehende und das nachfolgende Root-Zertifikat. D. h., kryptographisch gesehen stellt dies eine doppelt verkettete Liste dar. Die Elemente im Array sind in chronologischer Ordnung sortiert. Im Folgenden wird ein Beispiel dargestellt.

```
{  
  [  

```

```
{
  {
    "name" : "RCA1",
    "CN" : "GEM.RCA1",
    "cert" : "...base64...",
    "prev" : "",
    "next" : "...base64...",
    "SKI" : "Subject-Key-Identifizier als Hexwert"
  },
  {
    "name" : "RCA2",
    ...
  },
  {
    "name" : "RCA3",
    ...
  },
  ...
}
```

5.1.2.1.6 Bereitstellen und Administration der Freigabeliste

Der Messenger-Proxy MUSS eine Freigabeliste vorhalten (z. B. in Form einer Lookup-Table). Die Freigabeliste dient zur Prüfung, ob einem eingehenden Invite-Event am Messenger-Proxy zugestimmt wird (siehe Berechtigungsprüfung - Stufe 2). Der Messenger-Proxy MUSS die Schnittstelle `I_TiMessengerContactManagement` als REST-Webservice über HTTPS gemäß `[api-messenger#TiMessengerContactManagement.yaml]` in der Version 1.0.0 umsetzen. Ebenfalls MUSS es möglich sein, dass der Akteur die Freigabeliste über seinen TI-Messenger-Client administrieren kann. Darüber hinaus MUSS der Messenger-Proxy sicherstellen, dass abgelaufene Freigaben aus der Freigabeliste entfernt werden.

5.1.2.1.7 Ausnahmeregeln

Der Messenger-Proxy MUSS es ermöglichen, Ausnahmeregeln definieren zu können. Dies ist notwendig, damit Anfragen nicht durch die Berechtigungsprüfung des Messenger-Proxys abgelehnt werden. So MUSS der Messenger-Proxy dem VZD-FHIR-Directory Zugriff auf den Endpunkt `/_matrix/federation/v1/openid/userinfo` der Matrix-Homeserver ermöglichen. Weitere Ausnahmeregeln könnten zum Beispiel für das Monitoring/Reporting definiert werden.

5.1.2.1.8 Umsetzung von Prüfregeln

Der Messenger-Proxy MUSS das Berechtigungskonzept gemäß `[gemSpec_TI_Messenger-Dienst#Berechtigungskonzept]` unterstützen. Der Messenger-Proxy MUSS den Inhalt der Anfrage an den Matrix-Homeserver prüfen. Die Art der Prüfung ist abhängig davon, ob es sich um Client-Server oder Server-Server Kommunikation handelt. Im Folgenden werden die Prüfregeln beschrieben.

5.1.2.1.8.1 Prüfregeln Client-Server Kommunikation

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

5.1.2.1.8.1.1 Stufe 1 - Prüfung der TI-Föderationszugehörigkeit

In dieser Stufe 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 das Invite-Event an den einladenden Matrix-Homeserver weiterleiten. Ist die Prüfung nicht erfolgreich, MUSS der Messenger-Proxy an den TI-Messenger-Client das folgenden JSON-Objekt zurückgeben:

```
Responsecode 403
{
  "errcode": "M_FORBIDDEN",
  "error": "<Matrix-Domain> konnte nicht eingeladen werden"
}
```

Bei einer erfolgreichen Föderationsprüfung wird das Invite-Event durch den Matrix-Homeserver verarbeitet. Dieser prüft, ob die Sender und Empfänger-Matrix-Domain gleich sind. Ist dies der Fall, dann befinden sich die Akteure auf demselben Messenger-Service und der einzuladende Akteur wird in einen gemeinsamen Chatraum eingeladen. Wenn die Matrix-Domains 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 Prüfregele der Server-Server Kommunikation anwenden.

5.1.2.1.8.1.2 Weitere Prüfregele der Client-Server Kommunikation

Neben der Föderationszugehörigkeit MUSS der Messenger-Proxy weitere Prüfregele unterstützen. Der Messenger-Proxy MUSS bei jedem `createRoom`-Event gemäß [Client-Server API#Rooms] den Inhalt der Anfrage an den Matrix-Homeserver prüfen. Hierbei MUSS der Messenger-Proxy prüfen, ob das im Event enthaltene Attribut `"invite"` mit maximal einem Element befüllt ist. Ist die Prüfung nicht erfolgreich, MUSS der Messenger-Proxy an den TI-Messenger-Client das folgenden JSON-Objekt zurückgeben:

```
Responsecode 400
{
  "errcode": "M_FORBIDDEN",
  "error": "Beim Starten der Kommunikation ist ein Fehler aufgetreten. Bitte wenden Sie sich an Ihren Administrator."
}
```

5.1.2.1.8.2 Prüfregele Server-Server Kommunikation

Der Messenger-Proxy MUSS Prüfregele für Server-Server Anfragen unterstützen und MUSS bei jedem Event den Inhalt der Anfrage prüfen. Für eingehende Server-to-Server Anfragen anderer Messenger-Proxies MUSS der Messenger-Proxy diese an den

zuständigen Matrix-Homeserver weiterleiten, damit dieser die Authentisierung gemäß [Server-Server API#Request Authentication] durchführt. Im Folgenden werden die Prüfregele beschrieben.

5.1.2.1.8.2.1 Stufe 1 - Prüfung der TI-Föderationszugehörigkeit

In der 1. Stufe MUSS der Messenger-Proxy für jedes ausgehende und eingehende Event prüfen, ob die Matrix-Domain Teil der TI-Föderation ist. Zur Prüfung der Föderationszugehörigkeit MUSS der Messenger-Proxy gemäß [Server-Server API#Request Authentication] die im Authorization-Header Attribut "origin" enthaltene Domain bei eingehender Kommunikation und im Authorization-Header Attribut "destination" bei ausgehender Kommunikation, gegen die Domains in seiner lokalen Föderationsliste prüfen. Ist die Prüfung fehlgeschlagen, 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 mit dem folgenden JSON-Objekt ablehnen:

```
Responsecode 403
{
  "errcode": " M_FORBIDDEN ",
  "error": "Die Gegenpartei konnte nicht kontaktiert werden"
}
```

Ist die Prüfung erfolgreich, MUSS der Messenger-Proxy das Event an den Matrix-Homeserver weiterleiten. Handelt es sich um ein Invite-Event, dann MUSS die weitere Prüfung gemäß der Stufe 2 erfolgen.

5.1.2.1.8.2.2 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 Abfrage seiner Freigabeliste 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.

5.1.2.1.8.2.3 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] gemäß der Matrix-Spezifikationen in der Version v1.3 umsetzen.

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.

5.1.2.2.1 Server Discovery

Der Matrix-Homeserver MUSS Server Discovery gemäß [Server-Server API#server-discovery] unterstützen. Hierfür MUSS der TI-Messenger Anbieter den Endpunkt `/well-known/matrix/` bereitstellen und darüber den Hostname sowie den Port, unter dem der Matrix-Homeserver erreichbar ist, zurückliefern.

5.1.2.2.2 Öffentliche Räume

Der Matrix-Homeserver MUSS es erlauben, öffentliche Räume erstellen zu können. Hierbei DARF im Gegensatz zu privaten Räumen auf die Ende-zu-Ende Verschlüsselung verzichtet werden.

5.1.2.2.3 Custom Room Types und Custom State Events

Der Matrix-Homeserver MUSS die folgenden *Custom Room Types* sowie die folgenden *Event Types* der *Custom State Events* entgegennehmen können, ohne diese auszuwerten, abzuweisen oder auf diese mit einer Fehlermeldung zu reagieren:

- Custom Room Types
 - `de.gematik.tim.roomtype.casereference.v1`
 - `de.gematik.tim.roomtype.default.v1`
- Custom State Events
 - `de.gematik.tim.room.casereference.v1`
 - `de.gematik.tim.room.default.v1`
 - `de.gematik.tim.room.name`
 - `de.gematik.tim.room.topic`

Die Erzeugung von *Custom Room Types* sowie von *Custom State Events* dieser *Event Types* DARF NICHT die Definition einer neuen oder angepassten Matrix Room Version zur Folge haben. Vorhandene Raumdefinitionen MÜSSEN gemäß der Default Room Version

der anzuwendenden Matrix-Protokollversion vollständig erhalten bleiben. Dabei MUSS das *Custom State Event* dieses *Event Types* kompatibel sein mit dessen Wurzel-Event (`m.room.create`).

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, ob eine Push-Funktion unterstützt wird.

6 Anhang A - Verzeichnisse

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	Telematikinfrastuktur
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

Abbildung 1: Systemüberblick (Vereinfachte Darstellung).....	9
Abbildung 2: Beispiel - Authentifizierung von Akteuren einer Organisation.....	11
Abbildung 3: Funktionaler Aufbau des TI-Messenger-Fachdienstes.....	23

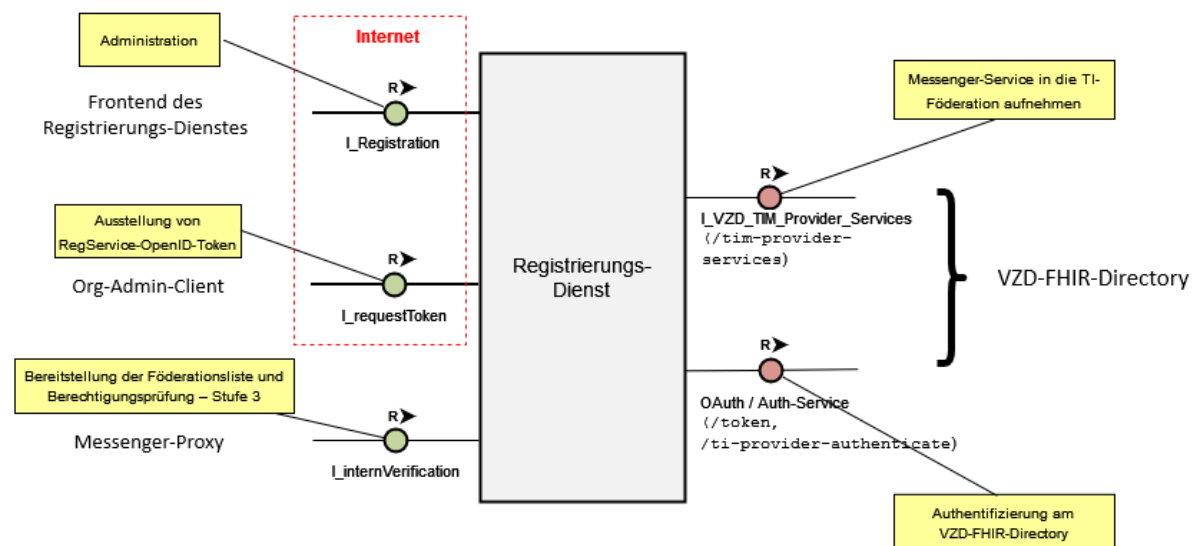


Abbildung 4: Übersicht der Schnittstellen am Registrierungs-Dienst.....	23
Abbildung 5: Matrix-API des Messenger-Service.....	30

6.4 Tabellenverzeichnis

Tabelle 1: Inhalte der Claims für SMC-B/HBA.....	16
--	----

Tabelle 2 Spezifische Attribute für das Handling der Föderationsliste am Registrierungs-Dienst..... 26

6.5 Referenzierte Dokumente

6.5.1 Dokumente der gematik

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

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

-Client]	
[gemSpec_TI_Messenger-Dienst]	gematik: Spezifikation TI-Messenger-Dienst
[VZD_Provider_Services]	gematik: api-vzd https://github.com/gematik/api-vzd/blob/main/src/openapi/I_VZD_TIM_Provider_Services.yaml

6.5.2 Weitere Dokumente

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[BSI 2-Faktor]	BSI 2-Faktor Authentisierung für mehr Datensicherheit https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Zwei-Faktor-Authentisierung/Bewertung-2FA-Verfahren/bewertung-2fa-verfahren_node.html
[BSI ORP.4]	BSI ORP.4: Identitäts- und Berechtigungsmanagement (Stand Februar 2021) https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompodium_Einzel_PDFs_2021/02_ORP_Organisation_und_Personal/ORP_4_Identitaets_und_Berechtigungsmanagement_Edition_2021.html
[Client-Server API]	Matrix Foundation: Matrix Specification - Client-Server API https://spec.matrix.org/v1.3/client-server-api/
[Matrix Specification]	Matrix Foundation: Matrix Specification https://spec.matrix.org/v1.3/
[OpenID]	OpenID Foundation https://openid.net/developers/specs/
[OWASP Proactive Control]	OWASP Proactive Controls https://owasp.org/www-project-proactive-controls/
[ROOT-CA]	ROOT-CA Download Punkt https://download.tsl.ti-dienste.de/ECC/ROOT-CA/
[ROOT-CA]	ROOT-CA Download Punkt als JSON-Datei

T-CA-JSON]	https://download.tsl.ti-dienste.de/ECC/ROOT-CA/roots.json
[Server-Server API]	Matrix Foundation: Matrix Specification - Server-Server API https://spec.matrix.org/v1.3/server-server-api/