Elektronische Gesundheitskarte und Telematikinfrastruktur

Spezifikation
TI-Messenger-Dienst

Version:	1.1.0~~.0~~
Revision:	~~408178~~482259
Stand:	~~01.10.2021~~29.07.2022
Status:	freigegeben
Klassifizierung:	öffentlich
Referenzierung:	gemSpec_TI-Messenger-Dienst

Dokumentinformationen

Änderungen zur Vorversion

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

Dokumentenhistorie

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
1.0.0	01.10.2021		Erstversion des Dokumentes	gematik
1.1.0	29.07.2022		Überarbeitung folgender Features: – Erreichbarkeit einzelner Organisationseinheiten mittels Funktionsaccounts – Öffnung des TI-Messengers für Drittsysteme durch clientseitige Schnittstellen zur Integration z.B. ins Praxisverwaltungssystem – schnelles Finden von Kontaktdaten durch Zugriff auf FHIR-basiertes Adressbuch	gematik

Inhaltsverzeichnis

1 Einordnung des Dokumentes

1.1 Zielsetzung

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

Dieses Dokument beschreibt basierend auf den Anforderungen des Konzeptpapiers TI-Messenger [gemKPT_TI_Messenger] die systemspezifische Lösung des TI-Messengers des deutschen Gesundheitswesens. An dieser Stelle werden insbesondere die Anforderungen des Konzeptes in Form von definierten Anwendungsfällen zu Herstellung, Test und Betrieb des TI-Messenger-Dienstes beschrieben. Die jeweiligen Anwendungsfälle beschreiben den gesamten, für die Erfüllung notwendigen, Prozess und benennen alle für die Umsetzung notwendigen Teilkomponenten. Die weitere funktionale Spezifikation erfolgt in der jeweiligen dedizierten Spezifikation des Produkttyps.

Die vorliegende Spezifikation ist als funktionale Einheit mit der jeweils auf einen konkreten Produkttyp bezogenen Spezifikation zu betrachten~~.~~.

1.2 Zielgruppe

Das Dokument richtet sich zum Zwecke der Realisierung an Hersteller von Produkttypen des TI-Messengers sowie an Anbieter, welche ~~einen oder mehrere dieser~~ die beschriebenen Produkttypen betreiben ~~[gemKPT_Betr].~~. Alle Hersteller und Anbieter von TI-Anwendungen, deren Schnittstellen einen der Produkttypen des TI-Messengers nutzen, oder Daten mit den Produkttypen des TI-Messengers 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

In diesem Dokument werden die übergreifenden Anforderungen in Form von Anwendungsfällen spezifiziert. Die Funktionsmerkmale, die für die hier beschriebenen Anwendungsfälle genutzt werden, werden in den Spezifikationen der einzelnen Produkttypen des TI-Messenger-Dienstes weiter definiert.

Die vom TI-Messenger-Dienst bereitgestellten Schnittstellen werden in den Spezifikationen der einzelnen Komponenten des TI-Messenger-Dienstes definiert. Von anderen Produkttypen benutzte Schnittstellen werden hingegen in der Spezifikation desjenigen Produkttypen beschrieben, der diese Schnittstelle bereitstellt. Auf die entsprechenden Dokumente wird referenziert.

Die vollständige Anforderungslage für den TI-Messenger-Dienst ergibt sich aus mehreren Spezifikationsdokumenten. Diese sind in den einzelnen Produkt- und Anbietertypsteckbriefen des TI-Messengers 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-Dienst als auch für den betreibenden Anbieter entsprechend [gemKPT_Betr] verbindlich zu betrachten und gilt 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-Dienst des deutschen Gesundheitswesens wird durch TI-Messenger-Anbieter betrieben. Dabei werden von jedem Anbieter die benötigten Produkttypen bereitgestellt. Für den~~ sichere Nachrichtenaustausch ~~wird von den~~zwischen beteiligten Akteuren ~~ein TI-Messenger-Client verwendet. Hierbei findet die sichere Ad-hoc-Kommunikation zwischen den Nutzern~~des deutschen Gesundheitswesens erfolgt über die von TI-Messenger-~~Clients und die vom TI-Messenger-Anbieter~~Anbietern bereitgestellten TI-Messenger-Fachdienste und TI-Messenger-Clients. Die Ad-Hoc Kommunikation zwischen den Akteuren findet hierbei über zugelassene TI-Messenger-Clients statt. Die Produkttypen TI-Messenger-Fachdienst sowie TI-Messenger-Client werden durch von der gematik zugelassene TI-Messenger-Anbieter bereitgestellt.

Ein TI-Messenger-Fachdienst besteht aus einem oder mehreren Messenger-Services ~~werden immer~~(basierend auf dem Matrix-Protokoll) die jeweils für eine Organisation (SMC-B-Inhaber) des Gesundheitswesens bereitgestellt ~~und~~ werden. Diese unterscheiden sich lediglich in der Art des verwendeten Authentifizierungsverfahrens. Akteure, die zugehörig zu einer Organisation agieren, KÖNNEN den durch diese Organisation bereitgestellten Messenger-Service verwenden und die innerhalb dieser Organisation bereits eigesetzten Authentifizierungsmethoden nachnutzen. Dies ermöglicht eine nahtlose Integration in den Alltag~~, da bestehende sichere Authentifizierungsverfahren nachgenutzt werden können. Nutzer~~. Akteure, die nicht zugehörig zu einer Organisation agieren, KÖNNEN Messenger-Services von Verbänden nutzen, falls diese durch einen Verband für ihre Mitglieder zur Verfügung gestellt werden. Hierbei kann das bestehende Authentifizierungsverfahren des Verbandes ~~nachgenutzt~~verwendet werden. ~~Nutzer die zugehörig zu einer Organisation agieren,~~ Messenger-Services KÖNNEN ~~den durch diese Organisation bereitgestellten Messenger-Service nutzen und die innerhalb dieser Organisation verwendeten Authentifizierungsmethoden verwenden. Es ist für Nutzer möglich verschiedene~~mit unterschiedlichen TI-Messenger-Clients ~~unterschiedlicher Organisationen zu nutzen (Beispiel: Ärztin ist~~verwendet werden. So ist es beispielweise möglich, dass ein Arzt, der parallel in einer Klinik und in einer niedergelassenen Praxis tätig ~~und bekommt von beiden~~ist, durch beide Organisationen jeweils einen ~~TI-~~Messenger-Service zur Verfügung gestellt~~). Messenger-Services werden durch TI-Messenger-Anbieter dezentral für Organisationen (SMC-B-Inhaber) bereitgestellt, die über das Matrix-Protokoll Nachrichten austauschen.~~ bekommt.

Die Messenger-Services des TI-Messenger-Dienstes werden in einer TI-Föderation zusammengefasst, um nicht zugehörige Messenger-Dienste auszuschließen. Um Teil der Föderation des TI-Messenger-Dienstes ~~des deutschen Gesundheitswesens~~ zu werden, MUSS die jeweilige Domain eines Messenger-Services vom TI-Messenger-Anbieter durch ~~einen~~den Registrierungs-Dienst ~~in dem~~des TI-Messenger-Fachdienstes im VZD-FHIR-Directory hinterlegt werden. Ist dies erfolgt, erhalten dessen ~~Nutzer~~Akteure Lesezugriff auf das VZD-FHIR-Directory und KÖNNEN je nach Berechtigung die Kommunikation mit ~~Nutzern~~Akteuren in anderen Organisationen ~~und/oder Leistungserbringern~~ starten. Die Kommunikation findet dabei Ende-zu-Ende-verschlüsselt zwischen den jeweiligen beteiligten Messenger-Services und TI-Messenger-Clients statt. Die Adressierung der Akteure innerhalb eines Messenger-Services erfolgt über die Matrix-User-ID und wird im Kontext des TI-Messenger-Dienstes als MXID bezeichnet. Um die beteiligten Akteure über den Eingang neuer Nachrichten zu informieren, ~~MÜSSEN die~~MUSS der TI-Messenger-Fachdienst ~~Anbieter~~ über ein Push-Gateway ~~betreiben.~~
verfügen.

In der folgenden Abbildung sind alle beteiligten Komponenten der TI-Messenger-Architektur dargestellt:

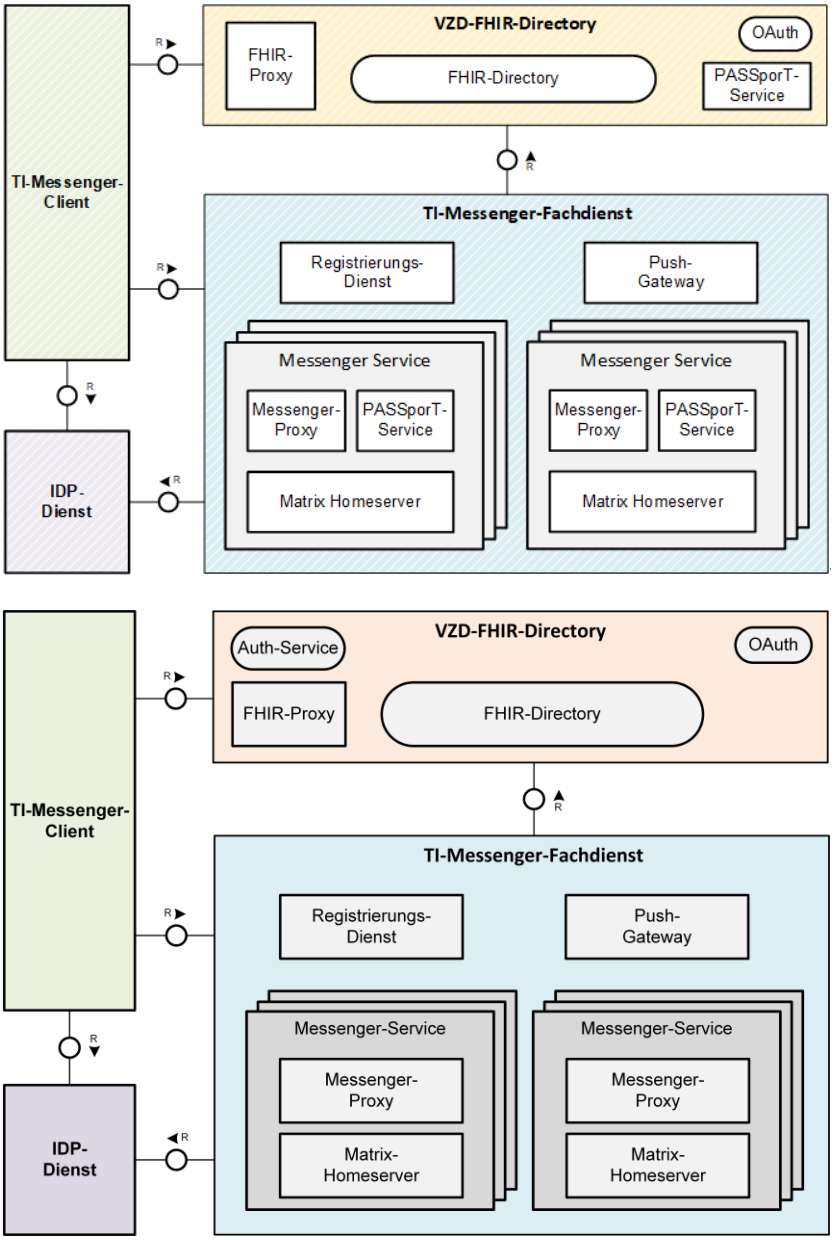


Abbildung 1: Komponenten der TI-Messenger-Architektur (vereinfachte Darstellung)

Der TI-Messenger-Dienst basiert auf dem offenen Kommunikationsprotokoll Matrix, das bereits von der Matrix Foundation gemäß [Matrix ~~Foundation~~Specification] spezifiziert ist. In den von der Matrix Foundation erstellten Spezifikationen ist sowohl die Client-Server- , die Server-Server-Kommunikation ~~und~~als auch die API des Matrix-Push-Gateways beschrieben. Für die Sicherstellung der föderalen und dezentralen Struktur des TI-Messenger-Dienstes im deutschen Gesundheitswesen und zur ~~Kontrolle~~Einschränkung des Nutzerkreises werden weitere Komponenten benötigt, welche in der jeweiligen durch die gematik veröffentlichten Spezifikation ~~dieser Komponenten~~ beschrieben werden. ~~Die Komponenten sind so ausgelegt, dass diese der Matrix Spezifikation entsprechen und somit die Funktionen des TI-Messengers mit der Funktionalität der Matrix Spezifikation weiterentwickelt werden können.~~

3 Systemkontext

3.1 Akteure und Rollen

Im Kontext des TI-Messenger-Dienstes werden verschiedene Akteure und Rollen ~~betrachtet.~~definiert. Ein Akteur ist eine natürliche Person (Leistungserbringer / Mitarbeiter einer Organisation im Gesundheitswesen) oder ein technisches System (Chatbot) die mit einem TI-Messenger-Fachdienst interagieren. Abhängig von dem verwendeten Authentifizierungsverfahren am Messenger-Service eines TI-Messenger-Fachdienstes ergeben sich unterschiedliche Rollen, die ein Akteur einnehmen kann. ~~Diese sind in der Tabelle "*Akteure und*~~Im Folgenden werden diese Rollen~~"~~ weiter beschrieben.

Rolle: "User"

Die Rolle "User" kann von einem Leistungserbringer sowie von einem Mitarbeiter im Gesundheitswesen eingenommen werden. Die Authentifizierung des Akteurs erfolgt hierbei nicht über eine SMC-B oder einen HBA, sondern über ein vom Messenger-Service bereitgestelltes Authentifizierungsverfahren. Für einen Akteur in der Rolle "User" KANN dessen MXID im Organisationsverzeichnis auf dem VZD-FHIR-Directory hinterlegt werden, um für Akteure außerhalb seiner Organisation auffindbar zu werden. Chatbots zur Abbildung von Funktionsaccounts nehmen ebenfalls die Rolle "User" ein und werden im Kapitel *5.6- Funktionsaccounts* näher beschrieben.

In dieser Rolle kann ein Akteur:

- sich gegenüber einem Messenger-Service authentisieren und
- sich an einem Messenger-Service anmelden.

Rolle: "User-HBA"

Die Rolle "User-HBA" kann ausschließlich von einem Leistungserbringer eingenommen werden. Die Authentifizierung des Akteurs erfolgt hierbei über seinen HBA. Ein Akteur in der Rolle"User-HBA" KANN seine MXID im Personenverzeichnis im VZD-FHIR-Directory hinterlegen, damit andere Akteure in der Rolle "User-HBA", die ebenfalls die eigene MXID auf dem VZD-FHIR-Directory hinterlegt haben, ihn kontaktieren können.

In dieser Rolle kann ein Akteur:

- sich am zuständigen IDP-Dienst authentisieren,
- sich am Messenger-Service anmelden und
- seine MXID auf dem VZD-FHIR-Directory hinterlegen, um sich damit persönlich, sektorübergreifend erreichbar zu machen.

Rolle: "Org-Admin"

Die Rolle "Org-Admin" stellt eine besondere Rolle im TI-Messenger Kontext dar. Leistungserbringer oder Mitarbeiter einer Organisation können diese Rolle einnehmen,

nachdem sie ihre Organisation zuvor erfolgreich am Registrierungs-Dienst unter Verwendung ihrer SMC-B authentifiziert haben (siehe Anwendungsfall "10103 - *Authentisieren einer Organisation am TI-Messenger Dienst*"). Nach der erfolgreichen Authentifizierung wird ein Admin-Account am Registrierungs-Dienst vom TI-Messenger-Fachdienst angelegt. Mit der Anmeldung am Registrierungs-Dienst über den Admin-Account nimmt ein Akteur die Rolle "Org-Admin" ein. Dieser KANN Messenger-Services für seine Organisation registrieren und Einträge im VZD-FHIR-Directory verwalten. Für die Rolle "Org-Admin" besteht die Notwendigkeit, Administratoren einzusetzen, welche für Themen der Informationssicherheit geschult und sensibilisiert wurden. Ebenfalls ist es möglich, dass die Organisation den TI-Messenger-Anbieter beauftragt, die Rolle "Org-Admin" zu übernehmen.

In dieser Rolle kann ein Akteur:

- Messenger-Services für seine Organisation registrieren,
- die Kontaktpunkte seiner Organisation auf dem VZD-FHIR-Server administrieren und damit sektorübergreifend erreichbar machen,
- die Mitarbeiter der eigenen Organisation als Akteure dieses Messenger-Services im Matrix-Homeserver administrieren (Benutzerverwaltung) sowie für seine Organisation Funktionsaccounts einrichten und
- Matrix-Homeserver-Konfigurationen für seine Organisation vornehmen.

Die folgende Tabelle "*Akteure und Rollen*" gibt einen Überblick über die im Kontext des TI-Messenger-Dienstes definierten Rollen, abhängig vom verwendeten Authentifizierungsverfahren, die ein Akteur einnehmen kann. Die Tabelle stellt alle möglichen Nutzerszenarien nach der Authentisierung mit Hilfe der SMC-B und erfolgreicher Authentifizierung einer Organisation am Registrierungs-Dienst dar.

Tabelle 1: Akteure und Rollen

Welcher Akteur bin ich	Wie authentisiere ich mich	Welcher Dienst authentifiziert mich	Welche Rolle nehme ich ein	~~Beschreibung und Berechtigungen~~
Leistungserbringer ~~im Besitz eines HBAs~~ (z. B. Ärzte, Zahnärzte, Apotheker, psychologische Psychotherapeuten~~)~~, Pflegepersonal, Hebammen, Mitarbeiter	~~User~~ HBA	VZD-FHIR-Directory~~Ein LE im Besitz eines HBAs kann~~ ~~• sich am Smartcard-IDP authentisieren~~	User-HBA	

Eingefügte Zellen
Eingefügte Zellen
Gelöschte Zellen
Eingefügte Zellen

einer Kasse) im Sinne SGB V		~~sich am Messenger-Service anmelden~~ ~~seine MXID auf dem VZD-FHIR Server hinterlegen und sich damit sektorübergreifend erreichbar machen~~ ~~den TI-Messenger-Dienst nutzen~~ ~~Kommunikationen innerhalb seiner Organisation aufbauen und entgegennehmen~~ ~~Kommunikationen mit anderen Organisationen aufbauen~~ ~~Kommunikationen mit LEs aufbauen und entgegenneh~~	

		~~men, die ebenfalls mit HBA authentisiert und somit für ihn auf dem VZD-FHIR-Server auffindbar sind~~ • ~~*Direct Messaging [Direct Messaging] mit allen Teilnehmern der TI-Messenger-Dienste~~ • ~~**Group Messaging [Group Messaging] mit allen Teilnehmern der TI-Messenger-Dienste~~ ~~im Namen der Organisation Kommunikation empfangen~~	

	~~Org-Admin~~Authentifizierungsverfahren der Organisation	~~Ein LE im Besitz eines HBAs und einer SMC-B kann~~ • ~~sich am Smartcard-IDP authentisieren~~ • ~~einen~~ Messenger-Service ~~für seine Organisation (korrespondierend zu seiner SMC-B) anlegen~~ • ~~seine Organisation auf dem VZD-FHIR Server administrieren und damit sektorübergreifend erreichbar machen~~ • ~~die User dieses Messenger-Services administrieren~~ ~~Homeserver-Konfigurationen vornehmen~~	User
	Admin-Account Credentials	Registrierungs-Dienst	Org-Admin
Mitarbeiter einer Organisation im Gesundheitswesen ~~(z. B. Pflegepersonal, Hebammen, Arzt,~~	~~User~~Authentifizierungsverfahren der Organisation	~~Ein Mitarbeiter einer Organisation im Gesundheitswesen kann~~	User

Eingefügte Zellen

die keine Leistungserbringer im ~~Krankenhaus, Mitarbeiter einer Kasse~~ Sinne SGB V sind.		• ~~sich gegenüber dem~~ Messenger-Service ~~authentisieren~~
		• ~~sich am Messenger-Service anmelden~~
		• ~~den TI-Messenger-Dienst nutzen~~
		  • ~~Kommunikationen innerhalb seiner Organisation aufbauen und entgegennehmen~~
		  • ~~Kommunikationen mit anderen Organisationen aufbauen~~
		  • ~~Direct Messaging [Direct Messaging] mit allen Teilnehmern der TI-Messenger-Dienste~~	

				• ~~Group Messaging [Group Messaging] mit allen Teilnehmern der TI-Messenger-Dienste im Namen der Organisation Kommunikation empfangen~~	
			Admin-Account Credentials	Registrierungs-Dienst	Org-Admin
	~~Org-Admin~~	~~Ein Mitarbeiter einer Organisation im Gesundheitswesen mit Zugriff auf eine SMC-B~~ • ~~sich am Smartcard-IDP authentisieren~~ • ~~einen Messenger-Service für seine Organisation (korrespondiered zu seiner SMC-B) anlegen~~ • ~~seine Organisation auf dem VZD-~~	Admin-Account Credentials	Registrierungs-Dienst	Org-Admin

Gelöschte Zellen
Gelöschte Zellen
Eingefügte Zellen
Eingefügte Zellen
Eingefügte Zellen

		~~FHIR Server administrieren und damit sektorübergreifend erreichbar machen~~ • ~~die User dieses Messenger-Services administrieren~~ ~~Homeserver-Konfigurationen vornehmen~~Beauftragter Administrator eines TI-Messenger-Anbieters			
~~TI-Messenger-Anbieter~~Chatbot		~~Org-Admin~~Authentifizierungsverfahren der Organisation		~~Ein TI-Messenger-Anbieter kann, auf Wunsch des LEs im Besitz einer SMC-B~~ • ~~einen~~ Messenger-Service ~~für die Organisation (korrespondierend zur SMC-B des LEs) anlegen~~ • ~~diese Organisation auf dem VZD-FHIR Server administrieren und damit~~	User

		~~sektorübergreifend erreichbar machen~~ • ~~die User dieses Messenger-Services administrieren~~ ~~Homeserver-Konfigurationen für LEs vornehmen~~	

~~*) Unter dem Begriff Direct Messaging versteht man im Kontext der Matrix-Spezifikation eine Kommunikation zwischen zwei Teilnehmern [gemSpec_TI-Messenger-Client].~~

~~**) Unter dem Begriff Group Messaging versteht man im Kontext der Matrix-Spezifikation eine Kommunikation zwischen mehr als zwei Teilnehmern[gemSpec_TI-Messenger-Client].~~

~~Es besteht kein notwendiger Rollenausschluss zwischen den einzelnen Rollen, auch wenn sich User und User-HBA rein logisch ausschließen.~~

~~Für Org-Admins besteht die Notwendigkeit einen Administrator einzusetzen, welcher für Themen der Informationssicherheit geschult und sensibilisiert wurde. Sofern eine Organisation nicht über solches Personal verfügt, kann hierzu auf Org-Admins vom Anbieter zurückgegriffen werden.~~

~~Ein Akteur ist eine Person oder eine Organisation, die mit dem TI-Messenger-Fachdienst interagiert. Diese Interaktion wird durch einen Anwendungsfall ausgelöst.~~

~~Leistungserbringer im Besitz eines HBAs KÖNNEN ihre MXID im VZD-FHIR-Directory hinterlegen, um für andere Leistungserbringer, die ebenfalls die eigene MXID auf dem VZD-FHIR-Directory hinterlegt haben, auffindbar zu sein (Rolle: *User-HBA*). Hinterlegt ein Leistungserbringer im Besitz eines HBAs seine MXID nicht im VZD-FHIR-Directory, so kann er lediglich als Mitarbeiter einer Organisation gefunden werden oder Chatnachrichten im Namen seiner Organisation empfangen (Rolle: *User*).~~

~~Mitarbeiter einer Organisation im Gesundheitswesen in der Rolle *User* KÖNNEN zunächst nur Akteuren schreiben, die ihrer Organisation zugeordnet sind. Um mit Mitarbeitern außerhalb dieser Organisation kommunizieren zu können, MUSS zwischen den Teilnehmern ein gültiges PASSporT ausgetauscht werden. Dieses Token wird je nach Anwendungsfall entweder vom PASSporT-Service des VZD-FHIR-Directory oder des jeweiligen Messenger-Service bereitgestellt. Neben der direkten Kommunikation zwischen Personen, haben Mitarbeiter einer Organisation zusätzlich die Möglichkeit eine andere Organisation anzuschreiben (z. B. Kardiologie eines Krankenhauses). Dabei KANN hinter der Organisation eine Person oder eine Gruppe von Personen stehen. Hiermit wird vor allem der Kommunikation zwischen Organisationen Sorge getragen und weitergehende Prozesse vorbereitet.~~

~~Leistungserbringer im Besitz eines HBAs oder ein Mitarbeiter einer Organisation im Gesundheitswesen, mit Zugriff auf eine SMC-B der Organisation, bekommen in der Rolle *Org-Admin* die Möglichkeit auf dem VZD-FHIR-Directory Einträge zu erstellen und zu administrieren. Ein TI-Messenger-Anbieter kann im Auftrag als *Org-Admin* die in der Tabelle "*Akteure und Rollen*" beschriebenen Services anbieten.~~

Hinweis: Versicherte DÜRFEN aktuell NICHT als ~~Nutzer~~Akteure auf einem Messenger-Service eingetragen werden. Für die Nutzung eines Messenger-Service sind nur ~~Nutzer~~Akteure zugelassen, die durch ein bestehendes Vertragsverhältnis ~~mit~~ der jeweiligen Organisation zugeordnet werden können~~. Ein Nutzer-Account MUSS einer juristischen Person eindeutig zugeordnet sein. Das Teilen von Passwörtern~~ oder ~~Zugangsdaten für die gleichzeitige Nutzung~~im Besitz eines HBAs sind.

Im Folgenden wird die Kommunikation für eingehende und ausgehende Nachrichten aus der Sicht eines Akteurs in den verschiedenen Rollen in einer Kommunikationsmatrix verdeutlicht.

Tabelle 2: Kommunikationsmatrix

~~Accounts ist nicht erlaubt.~~

Org-Admin	User	User-HBA	Kommunikationsart
Ausgehende Kommunikation an:			
x	x	x	Akteure in der Rolle "User" innerhalb seiner Organisation
-	x	x	Akteure in der Rolle "User" außerhalb seiner Organisation
-	-	x	Akteure in der Rolle "User-HBA" außerhalb seiner Organisation
-	x	x	Akteure in der Rolle "User" und "User-HBA" durch Scan eines QR-Codes
Eingehende Kommunikation von:			
x	x	x	Akteuren in der Rolle "User" innerhalb seiner Organisation
-	x	-	Akteuren in der Rolle "User" außerhalb seiner Organisation
-	-	x	Akteure in der Rolle "User-HBA" außerhalb seiner Organisation
-	x	x	Akteuren in der Rolle "User" und "User-HBA" durch Scan eines QR-Codes

3.2 Nachbarsysteme

Die folgende Abbildung zeigt die benachbarten Produkttypen des TI-Messenger-Dienstes:

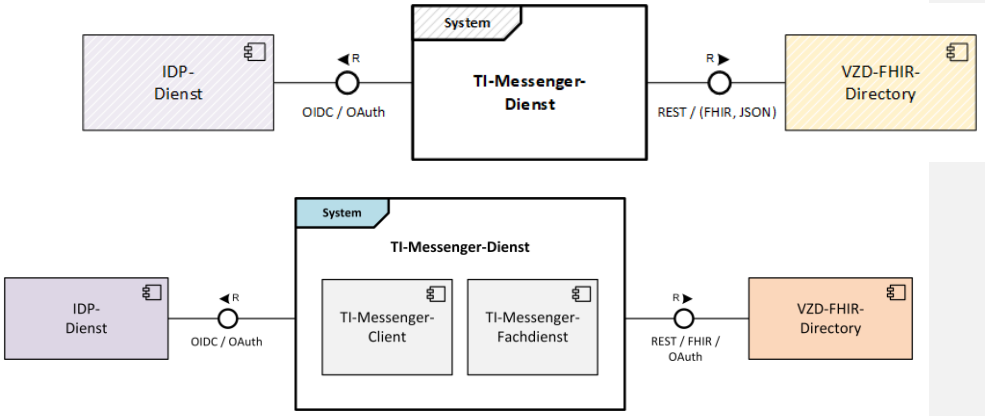


Abbildung 2: Benachbarten Produkttypen des TI-Messenger-Dienstes

Der TI-Messenger-Dienst als System besteht aus den Komponenten TI-Messenger-Fachdienst und TI-Messenger-Client.
Der Registrierungs-Dienst des TI-Messenger-Fachdienstes nutzt die OAuth- und REST-Schnittstellen ~~vom Smartcard~~des VZD-FHIR-Directory, um sich mittels OAuth Client Credential Flow zu authentisieren um somit Zugriff auf das FHIR-Directory zu erhalten.
Der TI-Messenger-Client nutzt die Schnittstellen eines zuständigen IDP-~~Dienst der gematik~~Dienstes zur Authentifizierung ~~von Akteuren~~eines Akteurs sowie Schnittstellen des ~~gesondert spezifizierten~~ VZD-FHIR-Directory, um z. B. ~~Nutzer und deren MXIDs~~ FHIR-Ressourcen zu finden~~.~~ oder zu ändern.

3.3 Ausprägungen des Messenger-~~Service~~Services

Der Messenger-Service ist eine Teilkomponente des TI-Messenger-Fachdienstes und wird ~~dezentral~~ durch den jeweiligen Anbieter für Organisationen bereitgestellt. Der Messenger-Service besteht aus einem Matrix-Homeserver (basierend auf dem Matrix-Protokoll) und~~ Komponenten die sicherstellen~~ einem Messenger-Proxy der sicherstellt, dass eine ~~Föderation~~Kommunikation mit anderen Messenger-Services, als Teil des TI-Messenger-Dienstes, nur innerhalb der gemeinsamen TI-Föderation erfolgt. ~~Bei diesen zusätzlichen Komponenten handelt es sich jeweils um einen Messenger-Proxy und einen PASSporT-Service.~~ Die Messenger-Services KÖNNEN den~~ Nutzern aufgrund der Vielzahl an verschiedenen~~ Akteuren unterschiedliche Authentifizierungsverfahren anbieten, bei denen der Besitz einer SMC-B oder eines ~~HBA~~HBAs nicht vorausgesetzt ~~werden kann~~wird. Messenger-Services MÜSSEN immer Organisationen bzw. Verbänden zugeordnet ~~werden~~sein, die über die Kontrolle ~~der verbundenen~~des verwendeten Authentifizierungsverfahren verfügen.

Abhängig vom jeweiligen Messenger-Service gibt es verschiedene Abläufe bei der Anmeldung an einem TI-Messenger-Fachdienst. Dabei können diverse Authentifizierungsmechanismen durch eine Organisation für Ihre ~~Nutzer~~Akteure bereitgestellt werden. Die Organisation und der von ihr gewählte TI-Messenger-Anbieter vereinbaren ~~den Authentifizierungsmechanismus~~das zur Anwendung kommende Authentifizierungsverfahren bilateral und stimmen sich über die technische Realisierung der ~~Authentifizierung~~dafür notwendigen Anbindung ab. Möglich ist beispielsweise die Nachnutzung eines in der Organisation betriebenen Active Directory~~-Servers~~ (AD/LDAP) oder eines geeigneten Single-Sign-On-Verfahrens (SSO). Der Anbieter MUSS sicherstellen, dass die Organisation die Kontrolle über die jeweiligen Authentifizierungsmechanismen besitzt~~, um~~ und die Möglichkeit erhält eine ~~mögliche Nutzerlöschung~~notwendige Löschung oder Sperrung eines Nutzer-Accounts sicherzustellen.

Zum besseren Verständnis werden im Folgenden ~~vier Anwendungsbeispiele dargestellt~~verschiedene, beispielhafte Anwendungsszenarien für den TI-Messenger skizziert und mögliche Ausprägungen eines Messenger-Service erläutert. Es besteht hierbei kein Anspruch auf Vollständigkeit :

Anwendungsbeispiel für eine Arztpraxis

~~Eine~~Die folgenden User Stories sollen die Bedarfe von niedergelassenen Leistungserbringern an asynchrone Ad-hoc-Kommunikation beispielhaft verdeutlichen:

User Story 1 - Nutzung des TI-Messengers unabhängig von der HBA-Verfügbarkeit
Als niedergelassener Arzt in einer Praxis stehe ich den Großteil meines Tages in direktem Patientenkontakt. Einen großen Teil der Organisation in der Praxis und der Kommunikation mit externen Stakeholdern übernimmt daher das Praxisteam. Als niedergelassener Arzt möchte ich meinem ganzen Praxisteam unabhängig von der Verfügbarkeit eines HBAs die Nutzung des TI-Messengers ermöglichen.

User Story 2 - Persönliche Erreichbarkeit als Arzt
Als niedergelassener Arzt in einer Praxis möchte ich persönlich nicht immer für alle anderen TI-Messenger-Nutzer erreichbar sein. Vor allem für medizinische Anfragen von ärztlichen Kollegen möchte ich in der Nutzersuche intersektoral gefunden werden können.

User Story 3 - Erreichbarkeit der eigenen Praxis für externe Leistungserbringer
Als niedergelassener Arzt in einer Praxis möchte ich, dass meine Praxis als Einrichtung im Gesundheitswesen für andere TI-Messenger-Nutzer erreichbar ist und adressiert werden kann. Dabei möchte ich selbst entscheiden, wie ich die individuelle Struktur meiner Praxis bei der Kontaktsuche abbilde und ob ich selbst oder mein Praxisteam initial in die Kommunikation eingebunden wird.

User Story 4 - Erreichbarkeit anderer Einrichtungen im Gesundheitswesen
Als niedergelassener Arzt in einer Praxis bekomme ich Patienten aus anderen Einrichtungen im Gesundheitswesen überwiesen und habe Rückfragen zu Befunden oder Verschreibungen. Besonders bei Einrichtungen, mit denen ich nicht regelmäßig im Kontakt stehe, möchte ich auch ohne bekannte Kontaktdaten eine Kommunikation aufbauen können und dabei sowohl die richtige Unterstruktur der Einrichtung (z. B. bestimmte Station in einem Krankenhaus) als auch den richtigen Ansprechpartner in dieser Unterstruktur (z. B. diensthabender Entscheider) erreichen können.

User Story 5 - Herstellung des Fallbezugs bei Kommunikationen
Als niedergelassener Arzt in einer Praxis findet ein großer Teil meiner Kommunikation mit anderen Leistungserbringern unter Bezugnahme zu einem Patienten oder Fall statt. Meine Nachrichten möchte ich unter diesem Aspekt verwalten können.

User Story 6 - Archivieren von Kommunikationen
Als niedergelassener Arzt in einer Praxis möchte ich fallbezogene Kommunikation in meinem Praxisverwaltungssystem in der jeweiligen Akte dokumentieren und somit nachvollziehbar speichern können.

User Story 7 - Geräte unabhängige Nutzung des TI-Messengers
Als Arzt in einer niedergelassenen Praxis arbeite ich vorrangig in meinem Praxisverwaltungssystem an meinem stationären Arbeitsplatz und möchte den TI-Messenger in diesem System integriert nutzen können. Wenn ich Hausbesuche mache, möchte ich zusätzlich die Möglichkeit haben, auch mobil auf alle meine Kommunikationen zuzugreifen und den TI-Messenger so überall nutzen können.

User Story 8 - Archivierbarkeit von Kommunikationen

Als Arzt in einer Praxis möchte ich fallbezogene Kommunikation in meinem Praxisverwaltungssystem in der jeweiligen lokalen Akte des Patienten dokumentieren und somit nachvollziehbar speichern können.

Aus den aufgezeigten User Stories ergibt sich der nachfolgende Ablauf für die Einrichtung und die Administration eines TI-Messenger-Services:

Ein Akteur in einer Arztpraxis ~~registriert sich mittels~~ authentisiert seine Organisation unter Verwendung der SMC-B bei einem Registrierungs-Dienst eines ~~Messenger-Anbieters.~~TI-Messenger-Anbieters. Nach erfolgreicher Authentifizierung durch den Registrierungs-Dienst wird für die Organisation ein Administrator-Account angelegt. Nach erfolgreicher Anmeldung am Registrierungs-Dienst nimmt der Akteur die Rolle "Org-Admin" ein und registriert einen Messenger-Service, der in einem Rechenzentrum bereitgestellt wird. Der Anbieter stellt daraufhin der Arztpraxis einen Messenger-Service mit einem sicheren Authentifizierungsverfahren bereit. ~~Durch die Dezentralität KANN dieser Service sowohl *on premise,* als auch in einem Rechenzentrum installiert werden. Zusätzlich wird einen Account für einen Akteur in der Rolle *Org-Admin* durch den Messenger-Anbieter erstellt. Der~~ Zusätzlich kann der Akteur in der Rolle "Org-Admin ~~meldet sich am Messenger-Service an und hinterlegt sämtliche Nutzer einer Arztpraxis (z.~~ "Akteure für seine Organisation auf den Matrix-Homeserver einrichten (z. B. MFA, Ärzte). Die angelegten ~~Nutzer~~Akteure melden sich am Messenger-Service an und können den TI-Messenger in der ~~Roller~~Rolle "User" direkt nutzen.

~~Die Arztpraxis wird als Organisation für Nutzer~~Ein Akteur in der Rolle "Org-Admin" richtet für seine Organisation Funktionsaccounts im Organisationsverzeichnis auf dem VZD-FHIR-Directory ein, um diese für Akteure anderer Organisationen des TI-Messenger-Dienstes erreichbar~~. Dazu KANN ein Akteur in der Rolle Org-Admin Kontaktpunkte auf dem VZD-FHIR-Directory einrichten. Nutzer~~ zu machen. Einem Funktionsaccount wird ein Akteur der Einrichtung (z. B. MFA) zugeordnet, der weitere Akteure in den Chatraum einladen kann. Akteure der Arztpraxis im Besitz eines HBAs ~~KÖNNEN~~(Rolle "User-HBA") können sich zusätzlich im TI-Messenger-Client mittels HBA authentisieren und so die eigene MXID als Practitioner-Eintrag im Personenverzeichnis auf dem VZD-FHIR-Directory hinterlegen. ~~Damit können~~Somit haben sie zusätzlich die ~~Nutzer~~Möglichkeit andere, auf dem VZD-FHIR-Directory hinterlegte, HBA-Inhaber ~~per Direct/Group-Messaging erreichen,~~(Rolle "User-HBA") in einen Chatraum einzuladen oder für diese erreichbar zu werden.

Anwendungsbeispiel für ein Krankenhaus

~~Ein Krankenhaus registriert~~ Die folgenden User Stories sollen die Bedarfe innerhalb eines Krankenhauses an asynchrone Ad-hoc-Kommunikation beispielhaft verdeutlichen:

User Story 1 - Einfache Administration der Nutzer
Als IT-Administrator der Klinik möchte ich die Administration der Nutzer meiner Organisation beim TI-Messenger möglichst automatisiert abbilden können, um Arbeitsaufwand bei der regelmäßigen Pflege der Nutzereinträgen zu minimieren.

User Story 2 - Einfache Bereitstellung und Anmeldung am Dienst
Als Arzt in einer Klinik möchte ich die bereits vorhandenen Mittel zur Anmeldung an den IT-Systemen für den TI-Messenger nachnutzen können. Die Anmeldung am Dienst sollte für mich analog zu den Anmeldungen an anderen IT-Systemen ablaufen, die ich in der Klinik nutze.

User Story 3 - Abbildbarkeit der unterschiedlichen Funktionsbereiche in einer Klinik
Als Arzt in einer Klinik habe ich Rückfragen an einen anderen Fachbereich und möchte die entsprechende Abteilung oder Station erreichen können, ohne dass ich bei der Kontaktsuche weiß, welche anderen Kollegen dort beschäftigt sind oder Dienst haben.

User Story 4 - Interdisziplinäre Teams
Als Arzt in einer Klinik bin ich in einem interdisziplinären Team mit Kollegen anderer Fachrichtungen tätig und möchte dabei zu einem Fall neue Laborbefunde oder neu verfügbare Bilddaten mit den Kollegen austauschen können.

User Story 5 - Fallbasierte Kommunikation
Als Pflegefachkraft auf einer Station möchte ich die Kollegen auf meiner Station über Neuigkeiten zu einem Patienten informieren und relevante Informationen (z. B. anstehende To-Dos bei einem Schichtwechsel) teilen.

Aus den aufgezeigten User Stories ergibt sich der nachfolgende Ablauf für die Einrichtung und die Administration eines TI-Messenger-Services innerhalb eines Krankenhauses:

Ein Akteur eines Krankenhauses authentisiert sich mittels SMC-B bei ~~einem~~dem Registrierungs-Dienst eines TI-Messenger-Anbieters. Der ~~Anbieter prüft~~Registrierungs-Dienst verifiziert die ~~bereitgestellte~~verwendete SMC-B ~~und~~ der Organisation. Bei Erfolg stellt ~~dem~~der Registrierungs-Dienst der Organisation einen Administrator-Account bereit. Nach erfolgreicher Anmeldung am Registrierungs-Dienst nimmt der Akteur die Rolle "Org-Admin" ein und registriert einen Messenger-Service für das Krankenhaus~~ einen Messenger-Service bereit. Durch die Dezentralität KANN dieser Service sowohl *on-premise*, als auch in einem Rechenzentrum installiert werden.~~. Dieser Service wird *on-premise* im Krankenhaus bereitgestellt. Der Messenger-Service ~~KANN~~ verwendet bei der Registrierung der Akteure am Matrix-Homeserver das bestehende Authentifizierungsverfahren des Krankenhauses (z. B. Active Directory~~) nutzen.~~). Die ~~Nutzer~~Akteure des Krankenhauses können anschließend mit den bestehenden Anmeldedaten den TI-Messenger-Dienst nahtlos verwenden, auch ohne im Besitz eines HBAs (Pflege, Therapeuten~~, Ärzte ohne HBA = Rolle: *User*~~) zu sein.

~~Das Krankenhaus wird als Organisation für andere Nutzer des TI-Messenger-Dienstes erreichbar. Dazu KANN ein Akteur in der Rolle Org-Admin Kontaktpunkte auf dem VZD-FHIR-Directory einrichten. Nutzer des Krankenhauses im Besitz eines HBAs KÖNNEN zusätzlich mittels des TI-Messenger-Clients die eigene MXID als Practitioner-Eintrag auf dem~~ Ein Akteur in der Rolle "Org-Admin" richtet für die Abteilungen in seinem Krankenhaus Funktionsaccounts im VZD-FHIR-Directory ein, um diese für Akteure außerhalb des Krankenhauses erreichbar zu machen. Einem Funktionsaccount wird ein Chatbot zugeordnet, der automatisiert den diensthabenden Arzt ermittelt und in den Chatraum einlädt.

~~VZD-FHIR-Directory hinterlegen (Rolle = *User-HBA*). Damit können die Nutzer andere hinterlegte HBA-Inhaber per Direct/Group-Messaging erreichen, oder für diese erreichbar werden.~~

Anwendungsbeispiel ~~Apotheke~~für Apotheken

~~Der Anbieter~~Die folgenden User Stories sollen die Bedarfe von Apotheken an asynchrone Ad-hoc-Kommunikation beispielhaft verdeutlichen:

User Story 1 - Versand von Fotos
Als Apotheker bin ich mit einem fehlerhaften Rezept konfrontiert und möchte den Sachverhalt mit dem verschreibenden Leistungserbringer klären. Dazu mache ich ein Foto von betreffenden Rezept und stelle meine Rückfrage per Chat an die Organisation des ausstellenden Leistungserbringers.

User Story 2 - Gruppenchats zur regelmäßigen Informationsweitergabe

Als Apotheker möchte ich die Leistungserbringer in räumlicher Nähe zu meiner Apotheke in einer gemeinsamen Gruppe über die Wiederverfügbarkeit eines vergriffenen Präparates informieren.

Aus den aufgezeigten User Stories ergibt sich der nachfolgende Ablauf für die Einrichtung und die Administration eines TI-Messenger-Services innerhalb einer Apotheke:

Ein Akteur einer Apotheke authentisiert sich mittels SMC-B bei dem Registrierungs-Dienst eines TI-Messenger-Anbieters. Der Registrierungs-Dienst verifiziert die verwendete SMC-B der Organisation. Bei Erfolg stellt der ~~Apotheke~~Registrierungs-Dienst der Organisation einen Administrator-Account bereit. Nach erfolgreicher Anmeldung am Registrierungs-Dienst nimmt der Akteur die Rolle "Org-Admin" ein und registriert einen Messenger-Service ~~bereit. Durch die Dezentralität KANN dieser Service sowohl *on-premise*, als auch~~für die Apotheke, der in einem Rechenzentrum ~~installiert werden. Der~~ bereitgestellt wird. Für die Authentifizierung der Akteure am Messenger-Service wird ~~mit dem bestehenden~~ der zuständige IDP-Dienst der Apotheken verwendet~~.~~, so dass die dort hinterlegten ~~Nutzer~~Akteure der ~~Apotheke können den~~Apotheken sich am TI-Messenger mittels OpenID-Connect ~~verwenden auch ohne im Besitz eines HBA zu sein (z. B. PTA, angestellte Apotheker ohne HBA).~~anmelden können.

Die Apotheke wird als Organisation für andere ~~Nutzer~~Akteure des TI-Messengers erreichbar, indem ein Akteur in der Rolle "Org-Admin" MXIDs von Akteuren seiner Apotheke im Organisationsverzeichnis~~*Org-Admin* Kontaktpunkte~~ auf dem VZD-FHIR-Directory einrichtet. ~~Nutzer~~Akteure der Apotheke im Besitz eines HBAs ~~KÖNNEN~~ (Rolle "User-HBA") hinterlegen zusätzlich mittels des TI-Messenger-Clients die eigene MXID als Practitioner-Eintrag im Personenverzeichnis auf dem VZD-FHIR-Directory. Somit haben sie zusätzlich ~~mittels~~die Möglichkeit andere, auf dem VZD-FHIR-Directory hinterlegte, HBA-Inhaber (Rolle "User-HBA") in einen Chatraum einzuladen oder für diese erreichbar zu werden.

Anwendungsbeispiel für einen Verband für HBA-Inhaber

Die folgenden User Stories sollen die Bedarfe von Verbänden an asynchrone Ad-hoc-Kommunikation beispielhaft verdeutlichen:

User Story 1 - Diskussion von Fällen
Als Verband möchte ich meinen Mitgliedern eine Plattform geben, um schwierige Fälle gemeinschaftlich diskutieren zu können.

User Story 2 - Sichere Kommunikation unabhängig von der Einrichtung in der das Mitglied tätig ist
Als Verband möchte ich meinen Mitgliedern die Möglichkeit geben, persönlich im TI-Messenger erreichbar zu werden und so unabhängig von der Einrichtung, in der das jeweilige Mitglied tätig ist, den Dienst nutzen zu können.

Aus den aufgezeigten User Stories ergibt sich der nachfolgende Ablauf für die Einrichtung und die Administration eines TI-Messenger-Services innerhalb eines Verbandes:

Der Verband hat eine SMC-B ORG beantragt, die für die Authentisierung am Registrierungs-Dienst eines TI-Messenger-Anbieters verwendet wurde. Der Registrierungs-Dienst verifiziert die verwendete SMC-B des Verbandes. Bei Erfolg stellt der Registrierungs-Dienst dem Verband einen Administrator-Account bereit. Nach erfolgreicher Anmeldung am Registrierungs-Dienst nimmt der Akteur die Rolle "Org-Admin" ein und registriert einen Messenger-Service für den Verband, der in einem Rechenzentrum bereitgestellt wird. Dieser Service wird für Mitarbeiter im Gesundheitswesen verfügbar gemacht, die nicht einer Organisation mit Zugriff auf eine SMC-B zugehörig sind.

Akteure des Verbandes im Besitz eines HBAs (Rolle "User-HBA") KÖNNEN zusätzlich mit dem TI-Messenger-Clients die eigene MXID als Practitioner-Eintrag im Personenverzeichnis auf dem VZD-FHIR-Directory hinterlegen. ~~Somit haben Sie die Möglichkeit~~ Damit können sie andere, auf dem VZD-FHIR-Directory hinterlegte, HBA-Inhaber ~~per Direct-Messaging zu erreichen~~(Rolle "User-HBA") in einen Chatraum einladen oder für diese erreichbar ~~zu~~ werden.

~~**Anwendungsbeispiel Verbände**~~

~~Der Anbieter eines TI-Messenger-Dienstes stellt Verbänden einen Messenger-Service zur Verfügung. Durch die Dezentralität KANN dieser Service sowohl *on-premise*, als auch in einem Rechenzentrum installiert werden. Der Messenger-Service KANN mit dem bestehenden Authentifizierungsverfahren des Verbandes verbunden werden. Die dort hinterlegten Mitglieder haben die Möglichkeit ihre bestehenden Authentifizierungsdaten des TI-Messenger-Dienstes zu verwenden.~~

~~Nutzer des Verbandes im Besitz eines HBAs KÖNNEN zusätzlich mittels des TI-Messenger-Clients die eigene MXID als Practitioner-Eintrag auf dem VZD-FHIR-Directory hinterlegen. Damit können die Nutzer andere hinterlegte HBA-Inhaber per Direct-Messaging erreichen, oder für diese erreichbar werden~~

3.4 ~~Im Folgenden wird noch einmal die Kommunikation für eingehende und ausgehende Nachrichten~~TI-Messenger Föderation

Da der TI-Messenger-Dienst auf dem offenen und dezentralen Kommunikationsprotokoll Matrix basiert, MUSS gewährleistet werden, dass nur berechtigte Matrix-Homeserver eines Messenger-Services teilnehmen.

Um allen berechtigten Akteuren des deutschen Gesundheitswesens den Zugang zum TI-Messenger-Dienst zu gewähren, MUSS ein Anbieter eines TI-Messengers für Leistungserbringerinstitutionen und/oder Organisationen eigene Messenger-Services bereitstellen. Um nicht zum TI-Messenger-Dienst gehörende Matrix-Homeserver

ausschließen zu können, werden die Domainnamen (im Weiteren auch als Matrix-Domain bezeichnet) der Matrix-Homeserver der Messenger-Services in einer Föderationsliste zusammengefasst. Diese wird durch das VZD-FHIR-Directory bereitgestellt. Voraussetzung für die Aufnahme in die Föderation ist der Betrieb eines Messenger-Proxies als Teil des Messenger-Services, der sicherstellen MUSS, dass nur zugelassene TI-Messenger-Fachdienste Zugang in die Föderation erhalten. Für die Aufnahme in die Föderation MÜSSEN ausschließlich Matrix-Homeserver verwendet werden. Es MUSS für die Aufnahme in die Föderation eine erfolgreiche Zulassung des TI-Messenger-Anbieters mit ebenfalls erfolgreichen Zulassungen für die Produkttypen TI-Messenger-Fachdienst und TI-Messenger-Client durch die gematik erfolgt sein. Nach einer erfolgreichen Zulassung erhält der Registrierungs-Dienst des jeweiligen Fachdienstes die Möglichkeit die Matrix-Domains der jeweiligen Messenger-Services einer entsprechenden Organisation auf dem VZD-FHIR-Directory zuzuordnen. Ein serverseitiges Bridging zu anderen Messaging-Protokollen DARF NICHT stattfinden. Um eine Integration eines TI-Messenger-Clients in bestehende Systemumgebungen (Primärsysteme oder alternative Messenger-Clients) zu ermöglichen, ist der clientseitige bidirektionale Austausch mit Drittsystemen erlaubt.

3.5 Berechtigungskonzept

Wie im Kapitel "TI-Messenger Föderation" beschrieben, dient die TI-Messenger-Föderation dazu, nicht zugelassene Matrix-Homeserver aus ~~der Nutzersicht in der Rolle *User* und *User-HBA* in einer Kommunikationsmatrix verdeutlicht.~~

~~**Tabelle 2: Kommunikationsmatrix**~~

~~**Rolle**~~	~~**Ausgehende Kommunikation**~~	~~**Eingehende Kommunikation**~~
~~User~~	~~• Start der Kommunikation mit anderen Organisationen~~ ~~• Start der Kommunikation mit Nutzern in der Rolle *User* und *User-HBA* innerhalb einer Organisation~~ ~~• Start der Kommunikation mit Nutzern in der Rolle *User* und *User-HBA* anderer Messenger-Services durch Scan eines QR-Codes~~	~~• Kommunikationsanfragen durch Nutzer in der Rolle *User* und *User-HBA* innerhalb einer Organisation~~ ~~• Kommunikationsanfragen durch Nutzer in der Rolle *User* und *User-HBA* anderer Messenger-Services durch Scan eines QR-Codes~~ ~~• Kommunikationsanfragen durch Nutzer in der Rolle *User* und *User-HBA* anderer Messenger-Services als Ansprechpartner der Organisation. Die MXID wurde durch einen Nutzer in der Rolle *Org-Admin* bei entsprechender Ressource der Organisation auf das VZD-FHIR-Directory hinterlegt~~

User-HBA	• Start der Kommunikation mit anderen Organisationen • Start der Kommunikation mit Nutzern in der Rolle *User* und *User-HBA* innerhalb einer Organisation • Start der Kommunikation mit Nutzern in der Rolle *User* und *User-HBA* anderer Messenger-Services durch Scan eines QR-Codes • Start der Kommunikation mit Nutzern in der Rolle *User-HBA* anderer Messenger-Services durch Nutzersuche auf VZD-FHIR-Directory	• Kommunikationsanfragen durch Nutzer in der Rolle *User* und *User-HBA* innerhalb einer Organisation • Kommunikationsanfragen durch Nutzer in der Rolle *User* und *User-HBA* anderer Messenger-Services durch Scan eines QR-Codes • Kommunikationsanfragen durch Nutzer in der Rolle *User-HBA* anderer Messenger-Services durch Auffindbarkeit auf VZD-FHIR-Directory • Kommunikationsanfragen durch Nutzer in der Rolle *User* und *User-HBA* anderer Messenger-Services als Ansprechpartner der Organisation. Die MXID wurde durch einen Nutzer in der Rolle *Org-Admin* bei entsprechender Ressource der Organisation auf das VZD-FHIR-Directory hinterlegt

3.4 Nutzung von Personal Assertion Token (PASSporT)

Für die dem TI-Messenger-Dienst auszuschließen. Ebenfalls MUSS es möglich sein, dass nur die im Kapitel *3.1- Akteure und Rollen* genannten berechtigten Akteure miteinander kommunizieren dürfen. Hierfür ist die Etablierung eines Rechtekonzeptes innerhalb des TI-Messenger-Dienstes ist es notwendig ein geeignetes Verfahren vorzusehen. Es wird ein Personal Assertion Token (PASSporT) gemäß [*RFC 8225#PASSporT: Personal Assertion Token*] in Anfragen an den Matrix-Homeserver hinzugefügt. Bestandteil des PASSporT ist sowohl die MXID des einladenden Nutzers, als auch die MXID des eingeladenen Nutzers. Aufgrund des Domain-Parts der MXID und der Rolle eines Nutzers entscheidet das VZD-FHIR-Directory, ob ein PASSporT ausgestellt wird. Das PASSporT, das in der Anfrage an einen Matrix-Homeserver enthalten ist, wird durch den Messenger-Proxy bei der Einladung eines Nutzers in einen Chatraum (eingehend/ausgehend) überprüft. Ein PASSporT wird zentral durch den PASSporT-Service des VZD-FHIR-Directory, aber auch, abhängig von der beabsichtigten Kommunikation, lokal bei den PASSporT-Services des Messenger-Services ausgestellt. Die Nutzung des lokalen PASSporT-Service ermöglicht es Nutzern eine Kommunikation ohne eine vorherige Abfrage am VZD-FHIR-Directory aufzubauen, wenn beide Gesprächspartner aktiv in eine Kommunikation einwilligen. Die Bereitstellung des PASSporT durch den Messenger-Server erfolgt analog zum PASSporT-Service des VZD-FHIR-Directorynotwendig.

Das Rechtekonzept basiert auf einer mehrstufigen Prüfung. Mit Hilfe des Berechtigungskonzeptes wird nachgewiesen, ob ein Akteur berechtigt ist, innerhalb der TI-Messenger-Föderation einen Akteur in einen Chatraum einzuladen.

Die einzelnen Stufen werden im Folgenden weiter beschrieben:

Berechtigungskonzept - Stufe 1

In der 1. Stufe MUSS geprüft werden, ob die in der Anfrage enthaltenen Matrix-Domains zugehörig zur TI-Föderation sind. Ist dies der Fall, MUSS die Anfrage an den Matrix-Homeserver des Einladenden weitergeleitet werden. Ist dies nicht der Fall, MUSS die beabsichtigte Anfrage des Akteurs vom Messenger-Proxy des Einladenden abgelehnt werden. Nach der Weiterleitung an den Matrix-Homeserver prüft dieser, ob der eingeladene Akteur der gleichen Organisation angehört. Stellt der Matrix-Homeserver fest das der eingeladene Akteur nicht zu seiner Domain gehört wird das `Invite-Event` an den Messenger-Proxy des einzuladenden Akteurs weitergeleitet. Dieser prüft erneut die Zugehörigkeit zur TI-Föderation (Stufe 1). Bei erfolgreicher Prüfung erfolgt dann die Weiterverarbeitung gemäß der Stufe 2.

Berechtigungskonzept - Stufe 2

In dieser Stufe prüft der Messenger-Proxy des Einzuladenden auf eine vorliegende Freigabe. Hierbei handelt es sich um eine Lookup-Table, in der alle erlaubten Akteure hinterlegt sind, von denen man eine Einladung in einen Chatraum akzeptiert. Ist ein Eintrag vom einladenden Akteur vorhanden, dann MUSS die beabsichtigte Einladung des Akteurs zugelassen werden. Ist dies nicht der Fall, MUSS die weitere Überprüfung gemäß der 3. Stufe erfolgen.

Berechtigungskonzept - Stufe 3

In der letzten Stufe erfolgt die Prüfung ausgehend von den Einträgen der beteiligten Akteure im VZD-FHIR-Directory. Die Einladung MUSS zugelassen werden, 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 einzuladende Akteur seine Sichtbarkeit in diesem Verzeichnis nicht eingeschränkt hat

Ist die Prüfung nicht erfolgreich, dann MUSS die beabsichtigte Einladung des Akteurs vom Messenger-Proxy abgelehnt werden.

~~3.5~~3.6 Verwendung der Token

Für die Nutzung des TI-Messenger-Dienstes kommen unterschiedliche Arten von Token zur Authentisierung und Autorisierung an weiteren Diensten zum Einsatz ~~und werden~~die in verschiedenen Anwendungsfällen verwendet~~. Es existieren die~~ werden. Aus diesem Grund werden in der folgenden ~~für eine Authentisierung benötigten~~Tabelle die verschiedenen Token~~:~~ näher beschrieben.

~~- ID_TOKEN und ACCESS_TOKEN ausgestellt vom Smartcard IDP Dienst~~

~~Matrix ACCESS_TOKEN ausgestellt~~

Tabelle 3: Arten von ~~den Matrix-Homeservern~~ ~~Matrix-OpenID-~~**Token** ~~ausgestellt vom Matrix-Homeserver~~

~~**ID_TOKEN (Smartcard-IDP-Dienst)**~~

~~Das vom Smartcard-IDP-Dienst ausgestellte ID_TOKEN, wird vom Registrierungs-Dienst verwendet, um eine Organisation zu verifizieren.~~

~~**ACCESS_TOKEN (Smartcard-IDP-Dienst)**~~

~~TI-Messenger-Clients verwenden das vom Smartcard-IDP-Dienst ausgestellte ACCESS_TOKEN , um schreibenden Zugriff auf das VZD-FHIR-Directory zu erhalten.~~

~~**Matrix-ACCESS_TOKEN (Matrix-Homeserver)**~~

~~Nach der erfolgreichen initialen Anmeldung eines Nutzers am Matrix-Homeserver wird ein Matrix-ACCESS_TOKEN vom Matrix-Homeserver ausgestellt. Mit diesem Token MUSS sich ein Nutzer, mit einem existierenden Matrix-Account, an seinem Matrix-Homeserver erneut authentisieren. Dieses Token wird im lokalen Speicher des TI-Messenger-Clients sicher abgespeichert und MUSS bei jeder weiteren Interaktion mit seinem Matrix-Homeserver verwendet werden und ist an die Session des jeweiligen Clients gebunden.~~

~~**Matrix-OpenID-Token (Matrix-Homeserver)**~~

~~Bei Bedarf MUSS sich ein Nutzer ein Matrix-OpenID-Token gemäß [Nutzer-Token] von seinem Matrix-Homeserver ausstellen lassen. Dieses Token MUSS für die Autorisierung bei einem Third-Party-Dienst verwendet werden. Als Beispiel wird auf die Anmeldung am FHIR-Proxy des VZD-FHIR-Directory verwiesen. Mit dem Matrix-OpenID-Token, ausgestellt durch seinen Matrix-Homeserver, authentisiert sich ein Nutzer am FHIR-Proxy und erhält lesenden Zugriff auf das VZD-FHIR-Directory.~~

Token	ausgestellt vom	Beschreibung
ID_TOKEN	IDP-Dienst	Dieses Token wird auf Basis von SmartCard-Identitäten vom zuständigen IDP-Dienst ausgestellt. Dieses Token wird vom Frontend des Registrierungs-Dienstes sowie den TI-Messenger-Clients verwendet, um sich gegenüber dem Registrierungs-Dienst oder dem Auth-Service des VZD-FHIR-Directory zu authentifizieren.
Matrix-ACCESS_TOKEN	Matrix-Homeserver	Nach der erfolgreichen Anmeldung eines Akteurs am Matrix-Homeserver wird ein Access-Token vom Matrix-Homeserver ausgestellt. Im Kontext des TI-Messenger-Dienstes wird das vom Matrix-Homeserver ausgestellte Access-Token als Matrix-ACCESS_TOKEN bezeichnet.

		Dieses Token MUSS im lokalen Speicher des TI-Messenger-Clients sicher abgespeichert werden. Dieses Token wird bei jeder weiteren Interaktion mit dem ausstellenden Matrix-Homeserver verwendet, um den TI-Messenger-Client zu berechtigen bestimmte Dienste des Servers zu nutzen. Es ist an die Session des jeweiligen TI-Messenger-Clients gebunden.
Matrix-OpenID-Token	Matrix-Homeserver	Bei dem Matrix-OpenID-Token handelt es sich um ein 3rd-Party-Token, welches von einem Matrix-Homeserver gemäß [Client-Server API#OpenID] bei Bedarf für einen Akteur ausgestellt wird. Im Kontext des TI-Messenger-Dienstes wird das 3rd-Party-Token als Matrix-OpenID-Token bezeichnet. Das Matrix-OpenID-Token wird für die Verifizierung eines Messenger-Services sowie für das Suchen von FHIR-Ressourcen im VZD-FHIR-Directory benötigt. Hierfür wird das Matrix-OpenID-Token im Auth-Service des Verzeichnisdienstes gegen ein search-accesstoken ersetzt, welches am FHIR-Proxy für die weitere Verarbeitung benötigt wird. Das ursprünglich ausgestellte Matrix-OpenID-Token wird dann nicht mehr benötigt. Zur Überprüfung der Gültigkeit des Matrix-OpenID-Token ruft der Auth-Service den Userinfo-Endpoint am jeweiligen Matrix-Homeserver auf.
provider-accesstoken	OAuth des VZD-FHIR-Directory	Das provider-accesstoken wird dem Registrierungs-Dienst durch den OAuth-Service des VZD-FHIR-Directory bereitgestellt. Ein provider-accesstoken wird benötigt, wenn der Registrierungs-Dienst eines TI-Messenger-Fachdienstes, nach der Bereitstellung eines neuen Messenger-Service für eine Organisation, einen neuen Eintrag für diese Ressource im VZD-FHIR-Directory anlegen oder der Registrierungs-Dienst eine Föderationsliste vom FHIR-Proxy abfragen möchte. Der Registrierung-Dienst übergibt dazu vereinbarte Client-Credentials an den OAuth-Service des VZD-FHIR-Directory und erhält nach der erfolgreichen Prüfung dieser Credentials das provider-accesstoken.
search-accesstoken	Auth-Service des VZD-FHIR-Directory	Das search-accesstoken wird einem berechtigten Akteur durch den Auth-Service das VZD-FHIR-Directory bereitgestellt. Dieses wird für die Suche im VZD-FHIR-Directory benötigt und stellt sicher, dass nur berechtigte Akteure im VZD-FHIR-Directory eine Suche

		auslösen können. Dazu wird das vom Matrix-Homeserver ausgestellte Matrix-OpenID-Token an den Auth-Service des VZD-FHIR-Directory übergeben. Dieses dient in diesem Fall als Nachweis, dass ein Akteur bei einem der TI-Föderation angehörenden Messenger-Service registriert ist. Nur dann wird durch den Auth-Service des VZD-FHIR-Directory ein search-accesstoken bereitgestellt. Es muss bei der dann folgenden Suche im VZD-FHIR-Directory im Aufruf enthalten sein. Die Prüfung erfolgt durch den FHIR-Proxy.
owner-accesstoken	Auth-Service des VZD-FHIR-Directory	Das owner-accesstoken wird einem berechtigten Akteur durch den Auth-Service das VZD-FHIR-Directory bereitgestellt. Dieses wird von einem Akteur in der Rolle "User-HBA" zur Verwaltung seiner FHIR-Ressource im Personenverzeichnis sowie von einem Akteur in der Rolle "Org-Admin" zum Hinzufügen der Organisations-Ressourcen im VZD-FHIR-Directory benötigt. Es dient zum Nachweis das die beabsichtigten Änderungen durch einen Akteur durchgeführt werden dürfen. Für die Authentifizierung MUSS der jeweilige Akteur einen zuständigen IDP-Dienst benutzen. Das durch den IDP ausgestellte ID_TOKEN wird durch den Auth-Service des VZD-FHIR-Directory geprüft. Bei erfolgreicher Prüfung wird das owner-accesstoken vom Auth-Service ausgestellt.

4 Systemzerlegung

Wie bereits im Kapitel "*Systemüberblick*" dargestellt sind bei der Umsetzung der Funktionalitäten des TI-Messenger-Dienstes ~~des deutschen Gesundheitswesens sind~~ mehrere Komponenten beteiligt, die durch verschiedene Anbieter bereitgestellt werden ~~können~~. Im Folgenden werden die jeweiligen beteiligten Komponenten des TI-Messenger-Dienstes weiter beschrieben.

Die folgende Abbildung zeigt alle an der TI-Messenger-Architektur beteiligten Komponenten mit deren Schnittstellen~~:~~.

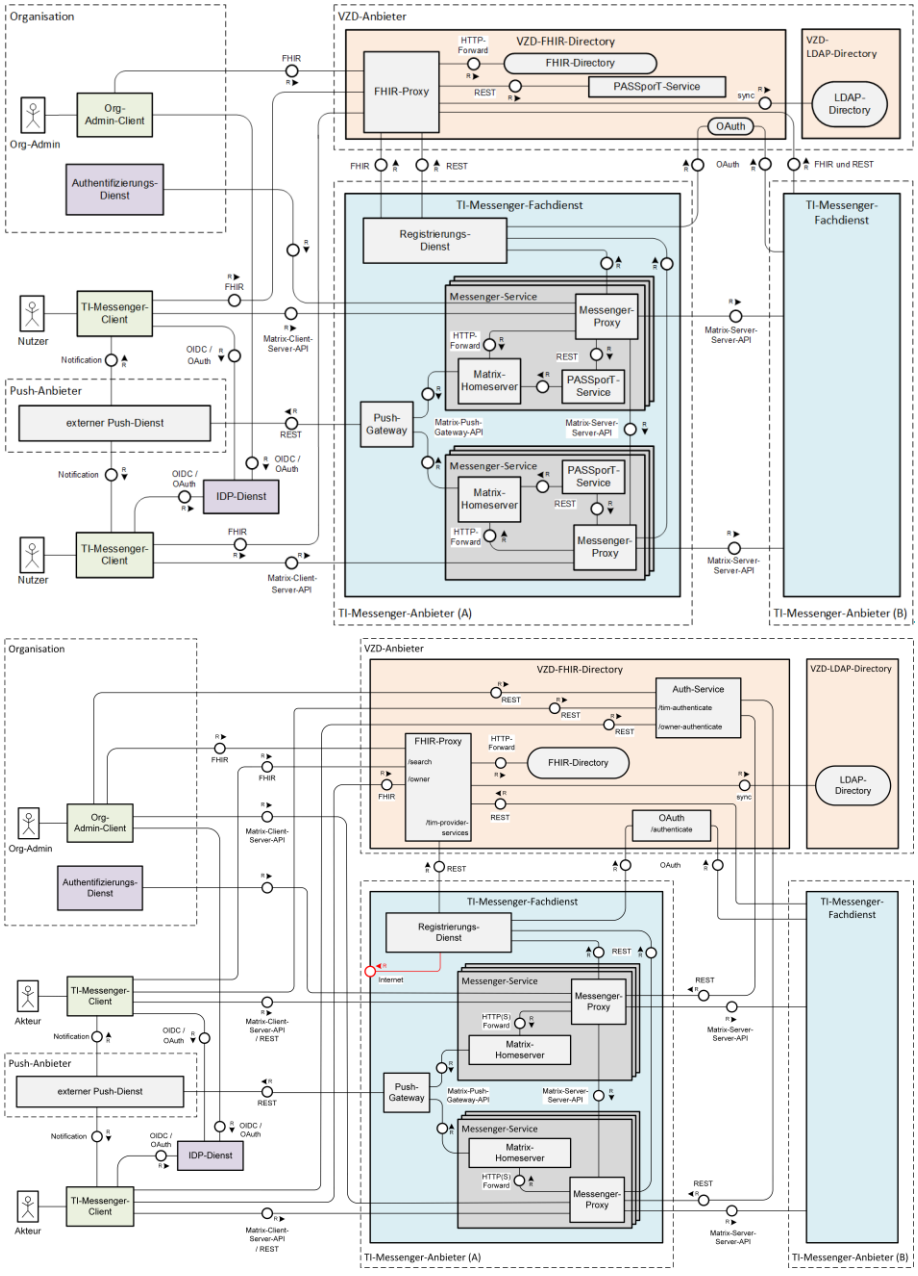


Abbildung 3: Komponenten der TI-Messenger-Architektur und deren Schnittstellen

Die in der Abbildung rot dargestellte Schnittstelle am Registrierungs-Dienst wird nicht durch die gematik normativ vorgegeben. Sie bietet einem Akteur in der Rolle "Org-Admin" die Möglichkeit, Messenger-Services für seine Organisation zu administrieren. Bei dieser Schnittstelle bleibt es dem TI-Messenger-Fachdienst Hersteller überlassen diese in geeigneter Form umzusetzen. Die gematik gibt lediglich grundlegende bereitzustellende Funktionen vor.

Hinweis: Weitere Informationen über das Zusammenspiel der Komponenten sind im Kapitel 6- Anwendungsfälle zu finden.

4.1 IDP-Dienst

Ein IDP-Dienst stellt JSON Web Token (JWT) für attestierte Identitäten aus. Er übernimmt die Aufgabe der Identifikation der Akteure für den Fachdienst. Das bedeutet, Fachdienste MÜSSEN keine Überprüfung der Akteure selbst implementieren, sondern KÖNNEN davon ausgehen, dass der Besitzer des bei ihnen vorgetragenen "ID_TOKEN" bereits identifiziert und authentifiziert wurde. Anwendungsfrontends können über die Authentifizierung des Akteurs am IDP-Dienst Zugriff (gegen Vorlage des ausgestellten ID_TOKEN) zu den von den Fachdiensten angebotenen Daten erhalten.

In der ersten Ausbaustufe des TI-Messengers-Dienstes MUSS der von der gematik spezifizierte zentrale IDP-Dienst verwendet werden. Dieser ermöglicht die sichere Identifikation der Akteure anhand der ihnen bereitgestellten Identifikationsmittel (SMC-B / HBA). Die Identifikation des Akteurs wird anhand einer Smartcard und der Auswertung des vom Authenticator-Modul an den IDP-Dienst übergebenen Authentifizierungszertifikats (aus der Smartcard) sichergestellt. Der Authenticator wird auf dezentraler Hardware in Windows-Systemumgebungen zusammen mit dem Primärsystem betrieben. Das Authenticator-Modul für den zentralen IDP-Dienst wird von der gematik bereitgestellt [gematik Authenticator]. Hersteller KÖNNEN eigene Authenticator Lösungen entwickeln.

Werden zukünftig weitere zugelassene IDP-Dienste verfügbar KÖNNEN diese ebenfalls für die Authentifizierung von Akteuren genutzt werden. Im Folgenden wird nur noch der Begriff IDP-Dienst verwendet.

4.2 VZD-FHIR-Directory

Beim VZD-FHIR-Directory handelt es sich um einen zentralen Verzeichnisdient der TI, der die deutschlandweite Suche von Organisationen und Akteuren des TI-Messenger-Dienstes ermöglicht. Das VZD-FHIR-Directory basiert auf dem FHIR-Standard zum Austausch von definierten Informationsobjekten (FHIR-Ressourcen).

Der Verzeichnisdienst bietet zwei Arten von Verzeichnistypen an, die durchsucht werden können. Für die Suche von Organisationseinträgen wird das Organisationsverzeichnis (*HealthcareService*) und für die Suche von Akteuren das Personenverzeichnis (*PractitionerRole*) verwendet. Im Organisationsverzeichnis sind alle auf eine Organisation bezogenen Ressourcen hinterlegt die durch einen Akteur in der Rolle "Org-Admin" der Organisation gepflegt werden. Das Personenverzeichnis bietet Akteuren in der Rolle "User-HBA" die Möglichkeit, alle zu seiner *PractitionerRole* gehörenden FHIR-Einträge zu konfigurieren. Für die Suche nach FHIR-Einträgen werden durch die TI-Messenger-Clients FHIR-Schnittstellen am VZD-FHIR-Directory aufgerufen. Bei der Verwendung der Schnittstellen MUSS sich der TI-Messenger-Client gegenüber dem VZD-FHIR-Directory authentifizieren. Für die Authentifizierung werden die im Kapitel "*Verwendung der Token*"

beschriebenen accesstoken (search-accesstoken und owner-accesstoken) verwendet. In der folgenden Tabelle werden die beiden Verzeichnistypen in Abhängigkeit der jeweiligen Identität und den sich daraus ergebenden Berechtigungen gezeigt.

Tabelle 4: Verzeichnistypen - Rechtekonzept

Verzeichnistyp	FHIR-Ressource	Identität	Rolle	Berechtigungen
Organisationsverzeichnis	HealthcareService	SMC-B	Org-Admin	Lese- und Schreibzugriff
		-	User	Lesezugriff
		-	User-HBA	Lesezugriff
Personenverzeichnis	PractitionerRole	HBA	User-HBA	Lese- und Schreibzugriff
		-	User	Lesezugriff

Zusätzlich zur Bereitstellung der Verzeichnistypen ermöglicht das VZD-FHIR-Directory ebenfalls die sektorenübergreifende Kommunikation. Hierfür wird die Matrix-Domain eines Messenger-Services durch einen Eintrag in das VZD-FHIR-Dircetory durch den Registrierungs-Dienst in die TI-Föderation aufgenommen. Für die Registrierung der Matrix-Domain wird durch den Registrierungs-Dienst eine REST-Schnittstelle am VZD-FHIR-Directory aufgerufen, die mittels OAuth2 Client Credentials Flow gesichert ist. Dies ermöglicht es TI-Messenger-Anbietern ihre betriebenen Messenger-Services in die TI-Messenger-Föderation aufzunehmen und zu verwalten.

Allgemein besteht das VZD-FHIR-Directory aus mehreren Teilkomponenten (FHIR-Proxy, Auth-Service, OAuth-Service und FHIR-Directory) die benötigt werden, um alle Funktionsmerkmale abbilden zu können. Im Folgenden werden die Teilkomponenten weiter beschrieben. Weiterführende Informationen zum VZD-FHIR-Directory sind in [api-vzd] zu finden.

FHIR-Proxy

Der FHIR-Proxy ist eine Teilkomponente des VZD-FHIR-Directory. Alle Anfragen an das FHIR-Directory werden über den FHIR-Proxy verarbeitet. Der FHIR-Proxy stellt die folgenden drei Schnittstellen zur Verfügung, die durch die TI-Messenger-Clients sowie durch den Registrierungs-Dienst aufgerufen werden:

- `/search` (FHIR-Schnittstelle zur Suche)
- `/owner` (FHIR-Schnittstelle zur Pflege eigener Einträge)
- `/tim-provider-services` (REST-Schnittstelle zur Pflege eigener TIM Provider Einträge)

Bei Aufruf der Schnittstellen MUSS ein entsprechendes access-token mit übergeben werden. Bei erfolgreicher Authentifizierung leitet der FHIR-Proxy die Anfragen an das FHIR-Directory weiter.

Auth-Service

Die Teilkomponente Auth-Service stellt den TI-Messenger-Clients die für den Aufruf der FHIR-Schnittstellen am FHIR-Proxy benötigen access-token aus. Hierbei werden die zwei folgenden REST-Schnittstellen:

- `/tim-authenticate` und
- `/owner-authenticate`

verwendet. Die Schnittstelle `/tim-authenticate` erwartet ein Matrix-OpenID-Token, wohingegen bei der Schnittstelle `/owner-authenticate` ein ID_TOKEN übergeben werden muss.

OAuth

Bei Aufruf der REST-Schnittstelle `/tim-provider-services` durch den Registrierungs-Dienst am FHIR-Proxy wird ein accesstoken (provider-accesstoken) benötigt, welches von der Teilkomponente OAuth ausgestellt wird. Hierfür MUSS sich der Registrierungs-Dienst des TI-Messenger-Fachdienstes bei der Teilkomponente OAuth des VZD-FHIR-Directory mittels OAuth2 Client Credentials Flow authentisieren. Zuvor MUSS der TI-Messenger-Anbieter für seinen Registrierungs-Dienst beim VZD-Anbieter Client-Credentials beantragen.

FHIR-Directory

Die Teilkomponente FHIR-Directory stellt das zentrale Verzeichnis der FHIR-Ressourcen bereit.

~~4.1~~4.3 TI-Messenger-Fachdienst

Der TI-Messenger-Fachdienst ist die zentrale Komponente des TI-Messenger-Dienstes zur Ad-hoc-Kommunikation zwischen mehreren Akteuren. Für die Kommunikation mit den TI-Messenger-Clients stellt der Fachdienst alle notwendigen Schnittstellen bereit. Für eine fachdienstübergreifende Kommunikation werden alle Nachrichten an ~~weitere~~ die in der TI-Föderation gelisteten TI-Messenger-Fachdienste übermittelt. ~~Der Zugriff auf den TI-Messenger-Fachdienst ist durch unterschiedliche Authentifizierungsverfahren abgesichert und ist abhängig vom Messenger-Service, der verwendet wird.~~ Es MUSS sichergestellt werden, dass die Organisation die ~~Nutzer~~Akteure jederzeit identifizieren kann und das die Organisationen ~~Nutzer~~Akteure jederzeit aus dem TI-Messenger-Dienst ausschließen können. Daher MUSS die Kontrolle über die Identitäten bei der Organisation liegen. Hierbei ist eine Delegierung, z. B. an einen Dienstleister zulässig. Jeder Anbieter, der einen TI-Messenger-Fachdienst bereitstellt, MUSS einen Registrierungs-Dienst, ein Push-Gateway sowie einen oder mehrere Messenger-Services betreiben. Im Folgenden werden die einzelnen Komponenten weiter beschrieben.

Hinweis: Die Komponenten sind als logische Dienste zu verstehen, welche letztendlich die in der Spezifikation beschriebenen Funktionalitäten umsetzen MÜSSEN. Die tatsächliche Realisierung bzw. Trennung dieser Dienste darf variabel durch die Produkthersteller erfolgen, solange alle Anforderungen an die Funktionalität, Sicherheit und Interoperabilität stets erfüllt sind und eingehalten werden.

~~4.1.1~~4.3.1 Registrierungs-Dienst

Der Registrierungs-Dienst ist eine Komponente, die vom ~~Anbieter~~Hersteller des TI-Messenger-Fachdienstes ~~bereitgestellt~~umgesetzt werden MUSS. Durch ~~diesen KÖNNEN~~diese MÜSSEN im VZD-FHIR-Directory die Matrix-Domains der TI-Messenger-Fachdienste, die an der Föderation des TI-Messengers teilnehmen, eingetragen werden. Die Eintragung der Matrix-Domain ~~SOLLTE~~SOLL automatisch erfolgen. Ebenfalls KANN über den Registrierungs-Dienst das Accounting durchgeführt werden. Dies wird von der gematik nicht normativ festgelegt.

Um einen ~~interoperablen~~benutzerfreundlichen Onboarding-Prozess zu gewährleisten MUSS der Registrierungs-Dienst die Bereitstellung eines Messenger-Service über ein Frontend ermöglichen~~. So MUSS~~ (im Folgenden auch als Frontend des Registrierungs-Dienstes bezeichnet). Nach der ~~Dienst bei~~erfolgreichen Authentisierung einer ~~neuen Registrierungsanfrage den~~Organisation, durch ~~den Smartcard IDP-Dienst~~Validierung eines ausgestellten ~~ACCESS_TOKEN und~~ ID_TOKEN ~~validieren und~~von einem zuständigen IDP-Dienst, wird für einen ~~dezentralen~~Akteur in der Rolle "Org-Admin" ein Administrations-Account im Registrierungs-Dienst angelegt. Das ermöglicht es einem Akteur in der Rolle "Org-Admin" einen oder mehrere Messenger-~~Service starten.~~Services für seine Organisation zu registrieren. Dazu MUSS das Frontend des Registrierungs-Dienstes ~~am Smartcard~~bei allen durch ihn unterstützten IDP-~~Dienst~~Diensten registriert sein. Vor dem Anlegen eines neuen Messenger-Service MUSS der Registrierungs-Dienst prüfen, ob der beantragte Domain-Name verfügbar ist und diesen ~~in die~~zur TI-Messenger Föderation ~~eintragen~~hinzufügen.

Neben der Registrierung neuer Messenger-Services, dient der Registrierungs-Dienst ~~ebenfalls~~ als Middleware zwischen TI-Messenger-~~Client~~Services und dem VZD-FHIR-Directory und speichert eine aktuelle Liste aller verifizierten Domains~~,~~ (Föderationsliste), damit diese von ~~dem Messenger-Proxy abgerufen werden können. Für die Prüfung der Signatur der durch~~ den ~~PASSporT-Service im VZD-FHIR-Directory ausgestellten PASSporT wird das öffentliche Zertifikat des PASSporT-Service im Registrierungs-Dienst abgelegt. Die~~ Messenger-Proxies ~~aller Messenger-Services~~ des TI-Messenger-~~Fachdienst-Anbieters MÜSSEN dieses Zertifikat am Registrierungs-Dienst für die Prüfung der vom PASSporT-Service im VZD-FHIR-Directory ausgestellten PASSporT nutzen.~~Fachdienstes abgerufen werden können (siehe Kapitel 3.5- Berechtigungskonzept - Stufe 1). Eine weitere Funktion des Registrierungs-Dienstes ist die Überprüfung auf Einträge im VZD-FHIR-Directory. Diese dient ebenfalls dem Messenger-Proxy zur Prüfung von Berechtigungen bei der Kontaktaufnahme von anderen Akteuren (siehe Kapitel 3.5- Berechtigungskonzept - Stufe 3).

~~4.1.2~~4.3.2 Push-Gateway

Jeder Anbieter eines TI-Messenger-Fachdienstes MUSS ein Push-Gateway bereitstellen, um seinen registrierten ~~Nutzern~~Akteuren den Eingang neuer Nachrichten zu signalisieren. Das Push-Gateway ist gemäß der Matrix-Foundation-Spezifikation [~~Matrix-PushGW]~~ Push Gateway API] zu implementieren. Dieses leitet die Benachrichtigung an Push-Dienste im Internet weiter~~.~~.

~~4.1.3~~4.3.3 Messenger-Service

Ein Messenger-Service besteht aus einem Messenger-Proxy~~, einem PASSporT-Service~~ und einem Matrix-Homeserver der gemäß der Spezifikation der Matrix Foundation implementiert ist. Messenger-Services unterscheiden sich lediglich durch die jeweils unterstützten Authentifizierungsverfahren. Es ist notwendig, dass sich die Messenger-

Services mit steigender Last skalieren lassen. ~~Ein Messenger-Service wird immer einer~~Eine Organisation des Gesundheitswesens wird logisch einem Messenger-Service zugeordnet. Näheres zur Absicherung der Komponenten der Messenger-Services findet sich in der Spezifikation des TI-Messenger-Fachdienstes [gemSpec_TI-Messenger-FD]. Im Folgenden werden die Komponenten beschrieben.

~~4.1.3.1~~4.3.3.1 Messenger-Proxy

Der Messenger-Proxy ~~schließt nicht zur TI~~ als Prüfinstanz aller eingehenden Anfragen zum Messenger-Service ist für die Regelung der gemäß Matrix Client-Server-API und Matrix-Server-Server-API geltenden Aufrufe zuständig. Die hierbei jeweils umzusetzenden Prüfregeln unterscheiden sich und werden im Folgenden näher beschrieben. Die folgende Abbildung zeigt die durchzuführenden Prüfungen in Abhängigkeit der beabsichtigten Kommunikation.

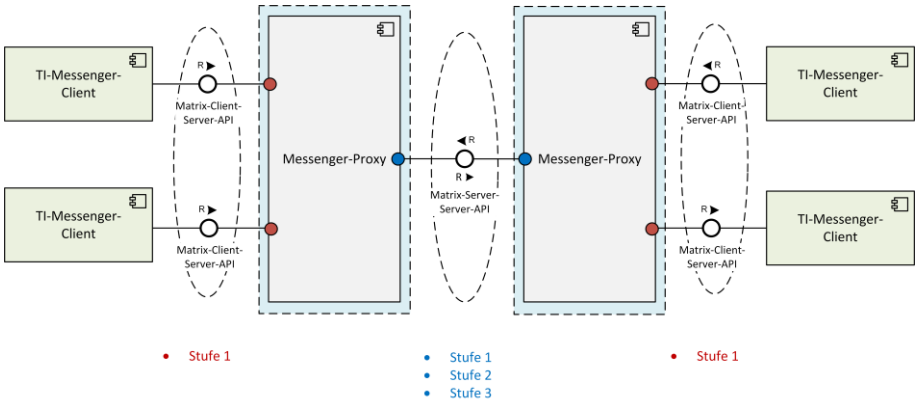


Abbildung 4: Darstellung der Berechtigungsprüfung am Messenger-Proxy

Client-Server Proxy
In der Funktion als Client-Server Proxy prüft der Messenger-Proxy eingehende `Invite-Events` der TI-Messenger-Clients (in der Abbildung rot dargestellt). Hierbei MUSS der Messenger-Proxy prüfen, ob die in der Anfrage enthaltenen Matrix-Domains zur TI-Föderation ~~gehörende~~ gehören (siehe Kapitel *3.5- Berechtigungskonzept* - Stufe 1). Nach erfolgreicher Prüfung, wird das `Invite-Event` an den Matrix-Homeserver ~~aus. Für die Prüfung der Berechtigung hat der Messenger-Proxy Zugriff auf den~~ weitergeleitet. Der Matrix-Homeserver prüft daraufhin, ob die beteiligten Akteure auf dem selben Matrix-Homeserver registriert sind. Ist dies nicht der Fall, wird das `Invite-Event` an den zuständigen Messenger-Proxy des Einzuladenden weitergeleitet. In diesem Fall findet die weitere Prüfung beim Messenger-Proxy des Einzuladenden statt (Server-Server Proxy).

Server-Server Proxy
In der Funktion als Server-Server Proxy prüft der Messenger-Proxy eingehende `Invite-Events` anderer Messenger-Proxies. Hierbei MÜSSEN alle Stufen gemäß Kapitel *3.5-*

Berechtigungskonzept vom Messenger-Proxy geprüft werden (in der Abbildung blau dargestellt). Ist keine der drei Stufen erfolgreich geprüft worden, dann MUSS der Messenger-Proxy die Verbindung ablehnen.

Weiterführende Vorgaben

Der Messenger-Proxy MUSS eine Freigabeliste bereitstellen. Diese dient zur Prüfung von Berechtigungen bei der Kontaktaufnahme von anderen Akteuren (siehe Kapitel 3.5 - Berechtigungskonzept - Stufe 2). Ebenfalls MUSS der Messenger-Proxy eine Schnittstelle bereitstellen, mit der TI-Messenger-Clients Berechtigungen in der Freigabeliste hinterlegen können.

Der Messenger-Proxy MUSS nach dem Erhalt einer neuen Föderationsliste vom Registrierungs-Dienst ~~des zugehörigen TI-Messenger-Anbieters. Durch eine Anfrage bei jedem `Transaction-Event` an den Registrierungs-Dienst erfolgt die Prüfung auf Zugehörigkeit zur TI-Messenger-Föderation.~~ die Signatur der erhaltenen Datei prüfen und diese nur nach erfolgreicher Prüfung verwenden.

Die Komponente Messenger-Proxy MUSS für jeden Messenger-Service separat bereitgestellt werden. Es ist nicht zwingend notwendig, diese auf die Matrix-Server-Server-API und Matrix-Client-Server-API bezogenen Prüfungen durch getrennte Komponenten zu realisieren. Die Art der Umsetzung bleibt dem TI-Messenger-Fachdienst-Hersteller überlassen.

~~Neben der stetigen Überprüfung bei `Transactions-Requests`, prüft der Messenger-Proxy zudem, ob ein Nutzer berechtigt ist eine Kommunikation mit anderen Nutzern aufzubauen (`Invite-Request`). Dazu benötigen Leistungserbringer und Mitarbeiter von Organisationen PASSporT, die vom VZD-FHIR-Directory, oder dem Messenger-Service ausgestellt werden. Diese PASSporT zeigen die Berechtigung zum Kommunikationsaufbau an.~~

Bei einer Nutzung des Messenger-Services für eine Organisation dient der Messenger-Proxy zusätzlich als ~~Interface~~Schnittstelle für den Anschluss des Authentifizierungs-Dienstes der Organisation ~~mit dem~~an den Ziel Matrix-Homeserver.

~~Der Messenger-Proxy MUSS eine Funktionalität bereitstellen, die das Ändern des Displaynamens durch den Nutzer verhindert. Änderungen des Displaynamens SOLL nur durch einen Akteur in der Rolle *Org-Admin* möglich sein.~~

~~4.1.3.2 PASSporT-Service des Messenger-Service~~

~~Der PASSporT-Service des TI-Messenger-Fachdienstes wird verwendet, wenn Akteure, die nicht im VZD-FHIR-Directory gefunden werden, eine Kommunikation aufbauen möchten. In diesem Fall kann kein PASSporT durch den VZD-FHIR-Directory PASSporT-Service ausgestellt werden. Dies MUSS dann durch den PASSporT-Service des TI-Messenger-Fachdienstes gemäß [gemSpec_TI-Messenger-FD#5.2.3] bereitgestellt werden.~~

~~4.1.3.3~~4.3.3.2 Matrix-Homeserver

Für den Betrieb des TI-Messenger-Dienstes MUSS der TI-Messenger-Anbieter mindestens einen Matrix-Homeserver gemäß der Matrix-Foundation Spezifikation in der sektorübergreifenden TI-Föderation betreiben. Es MÜSSEN alle Matrix-Homeserver die in der Föderation verwendet werden den Anforderungen der Matrix Foundation Spezifikation entsprechen. Über den Matrix-Homeserver findet die Ad-hoc-Kommunikation der

~~Nutzer~~Akteure sowie weitere Nutzerinteraktionen (z. B. Starten neuer Räume etc.) statt. ~~Der TI-Messenger-Anbieter MUSS sicherstellen, dass folgende Matrix-Spec-Changes (MSCs) [MatrixSpecProposal] zum Thema Push-Benachrichtigungen von dem Matrix-Homeserver unterstützt wird:~~

- ~~Encrypted Push – https://github.com/matrix-org/matrix-doc/pull/3013~~
- ~~Delayed Push – https://github.com/matrix-org/matrix-doc/pull/3359~~
- ~~Opportunistic Direct Push – https://github.com/matrix-org/matrix-doc/pull/3361~~

~~4.2~~4.4 TI-Messenger-Client

~~Beim~~Ein TI-Messenger-Client ~~handelt es sich um~~ ist eine mobile oder stationäre Anwendung ~~auf einem mobilen Gerät oder auf einem Desktop. Der TI-Messenger-Client ermöglicht die Ad-hoc-Kommunikation im TI-Messenger-Dienst. Die Akteure KÖNNEN über entsprechende Suchanfragen im VZD-FHIR-Directory durch den TI-Messenger-Client gesucht werden. Der TI-Messenger-Client~~. Diese basiert auf der von der Matrix-Foundation definierten Spezifikation ~~.~~

~~Der TI-Messenger-Anbieter MUSS mindestens einen mobilen~~ und ~~einen desktopfähigen TI-Messenger-Client anbieten. Welche Art des Clients angeboten wird, ist dem Anbieter überlassen.~~

~~Der TI-Messenger-Client MUSS am Smartcard-IDP-Dienst registriert sein, damit mittels SMC-B oder HBA Änderungen am VZD-FHIR-Directory durch einen Akteur in der Rolle *Org-Admin* vorgenommen werden können.~~

~~4.31.1 VZD-FHIR-Directory~~

~~Beim VZD-FHIR-Directory handelt es sich um einen zentralen Verzeichnisdient, der die deutschlandweite Nutzersuche des TI-Messenger-Dienstes ermöglicht. Das VZD-FHIR-Directory basiert auf dem FHIR-Standard zum Austausch~~ ermöglicht die Ad-hoc-Kommunikation von ~~definierten Informationsobjekten. Das VZD-FHIR-Directory bietet eine FHIR-Schnittstelle zur Suche nach Leistungserbringern (*Practitioner*) und Organisationen an. Somit wird eine einfache Suche nach~~ Akteuren~~, die an dem TI-Messenger teilnehmen, gewährleistet. Der Zugriff auf das VZD-FHIR-Directory ist mittels OAuth2 Client Credentials Flow gesichert. Ebenfalls ermöglicht das VZD-FHIR-Directory die sektorenübergreifende Kommunikation. Hierzu wird die Domain der Matrix-Homeserver durch einen Eintrag im VZD-FHIR-Directory registriert. Für die Nutzung des TI-Messenger-Dienstes bietet das zentrale VZD-FHIR-Directory einen FHIR-Proxy sowie einen PASSporT-Service an~~ über den TI-Messenger-Dienst. Im Kontext des TI-Messenger-Dienstes wird zwischen zwei Ausprägungen des TI-Messenger-Clients unterschieden. Diese ergeben sich aus den jeweiligen Rollen der Akteure, die im Folgenden weiter beschrieben werden.

~~FHIR-Proxy~~

~~Der FHIR-Proxy ist das zentrale Interface der TI-Messenger-Fachdienste zum VZD-FHIR-Directory. Der FHIR-Proxy leitet autorisierte Anfragen und Kommandos vom TI-Messenger-Client an das VZD-FHIR-Directory weiter. Die Komponente~~ Für die Realisierung von Anwendungsfällen, die ausschließlich ein Administrator der Organisation

ausführt (siehe Kapitel *6- Anwendungsfälle*, dem Akteur "Org-Admin" zugeordneten Anwendungsfälle), MUSS ein TI-Messenger-Anbieter einen TI-Messenger-Client mit Administrationsfunktionen anbieten (auch als Org-Admin-Client bezeichnet). Diese erweiterte Funktionalität KANN auch in den TI-Messenger-Client für Akteure integriert sein. TI-Messenger-Clients für Akteure (Akteure in der Rolle User / User-HBA) unterstützen die von der Matrix-Spezifikation festgelegten Funktionalitäten sowie die Abfragen im VZD-FHIR-Directory. Der geforderte mindestens bereitzustellende Funktionsumfang wird in der [gemSpec_TI-Messenger-Client] beschrieben.

~~Registrierungs-Dienst benutzt den FHIR-Proxy ebenfalls für den Zugriff auf das VZD-FHIR-Directory. Der Kommunikationsablauf für den Zugriff auf das VZD-FHIR-Directory durch den TI-Messenger-Client ist in [gemSpec_VZD_FHIR_Directory#6.2] beschrieben.~~

~~PASSporT-Service des VZD-FHIR-Directory~~

~~Im TI-Messenger-Kontext werden für die Prüfungen von Berechtigungen PASSporT verwendet. Berechtigte Akteure erhalten vom PASSporT-Service des VZD-FHIR-Directory ein PASSporT. Das PASSporT wird durch die Messenger-Proxies für das `Invite`-`Event` geprüft. Der PASSporT-Service stellt automatisiert PASSporT aus, sollte die gesuchte Ressource vom VZD-FHIR-Directory erfolgreich zurückgegeben werden. Das PASSporT wird als Query-Parameter in der Matrix-User-URI angehängt. Dies wird in der [gemSpec_VZD_FHIR_Directory] festgelegt.~~

~~OAuth~~

~~Der Registrierungs-Dienst des TI-Messenger-Fachdienst MUSS sich beim VZD-FHIR-Directory mit OAuth2-Client-Credentials-Flow authentisieren.~~

5 Übergreifende Festlegungen

5.1 Datenschutz und Sicherheit

Der TI-Messenger-Dienst baut auf flächendeckender Verwendung von Transportverschlüsselung mittels TLS (gemäß den Vorgaben aus [gemSpec_Krypt~~]) ,~~]), zusätzlicher moderner Ende-zu-Ende-Verschlüsselung von Chatinhalten mittels OLM/MEGOLM und einer dezentralen Gesprächsarchitektur mittels föderierten Matrix-Homeservern auf.

Die Vorgaben für die Absicherung des TI-Messengers bestehen aus komponentenbezogenen ~~Akzeptanzkriterien~~Anforderungen, die in den jeweiligen Dokumenten in eigenen Kapiteln untergebracht sind, funktionsbezogenen ~~Akzeptanzkriterien~~Anforderungen, die im Rahmen der jeweiligen Funktionsbeschreibungen zu finden sind~~,~~ und ergänzenden übergreifenden Anforderungen, die aus anderen Spezifikationen stammen und den Steckbriefen zugeordnet werden.

5.2 Verwendete Standards

Matrix

Für den TI-Messenger-Dienst wird das offene Kommunikationsprotokoll der Matrix-Foundation~~ gemäß [Matrix Foundation]~~ verwendet. Im Rahmen der Spezifikation wird ~~daher~~ das Server-Server- (gemäß [Server-Server API]) und das Client-Server-Protokoll (gemäß [~~Matrix Foundation~~]Client-Server API]) nachgenutzt. Für die Kommunikation der Matrix-Homeserver in der Föderation wird ~~somit~~ die API gemäß ~~Matrix~~ [Server-Server~~-Protokoll~~ API] verwendet. Der TI-Messenger-Client setzt bei der Kommunikation mit den ~~TI-Messenger~~ Matrix-Homeservern die API des Matrix-Client-Server-Protokolls um. Für die Benachrichtigung der Akteure über eingehende Nachrichten wird ein Push-Gateway verwendet, welches gemäß [Push Gateway API] nachgenutzt wird. Bei der Kommunikation werden REST-Webservices über HTTPS (JSON-Objekte) aufgerufen.

OpenID-Connect

Das VZD-FHIR-Directory~~ nutzt als Authorisierungsserver den Smartcard IDP~~, der Registrierungs-Dienst ~~der TI. Hierfür stellt~~sowie die TI-Messenger-Clients nutzen im Rahmen der ~~IDP-Dienst ein~~Authentifizierung ID~~ und ACCESS~~_TOKEN ~~für Nutzer~~ in Form eines JSON-Web-Token (JWT) gemäß [OpenID~~] aus.~~

].

FHIR

~~Der~~Die TI-Messenger-~~Client nutzt~~Clients nutzen die FHIR-Schnittstellen der Teilkomponente FHIR-Proxy des VZD-FHIR-Directorys gemäß dem FHIR-Standard [FHIR] mit einer RESTful API.

~~**PASSporT**~~

~~Für die Prüfung von Rechten der beteiligten Nutzer innerhalb einer beabsichtigten Kommunikation verwendet der TI-Messenger-Dienst PASSporT gemäß [RFC 8225]. Die Verwendung des PASSPorTs im Kontext des TI-Messenger-Dienstes wird im Kapitel "*Nutzung von Personal Assertion Token*" weiter beschrieben.~~

5.3 Authentifizierung und Autorisierung

5.3.1 Authentifizierung von ~~Nutzern~~Akteuren am Messenger-Service

Für die Authentifizierung von ~~Nutzern, also z. B. Mitarbeiter in einer Organisation, oder Leistungserbringer~~Akteuren werden die durch den jeweiligen Matrix-Homeserver bereitgestellten Authentifizierungsverfahren genutzt. Dies ermöglicht es z. B. Krankenhäusern ihre eigene Benutzerverwaltung (z. B. Active Directory) zu nutzen, oder Verbänden ~~eigene~~ihre eigenen Identitätsserver (IDP-Dienst) zu verwenden. Die Abstimmung, welches Authentifizierungsverfahren verwendet wird, trifft die Organisation mit dem jeweiligen TI-Messenger-~~Fachdienst~~ Anbieter. Die Benutzerverwaltung erfolgt durch autorisierte Mitarbeiter in der jeweiligen Organisation (Akteur in der Rolle "Org-Admin~~).~~"). Die Administration der verwendeten Authentifizierungsmethoden MÜSSEN unter der Kontrolle der jeweiligen Organisation sein.

~~Bezüglich der Einschränkung der Authentisierungsmittel, welche von einer Organisation verwendet werden dürfen, befindet sich die gematik derzeit noch in Abstimmung mit dem BSI, weswegen mit einer verbindlichen Regelung erst im geplanten Hotfix 1 zu rechnen ist. Bis dahin MUSS zusätzlich zur Prüfung der SMC-B als erstem Faktor noch ein zweiter Faktor nach [BSI TR-03107] Kap. 4 geprüft werden, bis die übliche Kombination aus Gerätebindung und Homeserver Access Token erreicht sind.~~

5.3.2 Authentifizierung am VZD-FHIR-Directory

Die Authentifizierung für den Lese- und Schreibzugriff ~~der Nutzer gegenüber dem VZD~~ auf das FHIR-Directory erfolgt ~~für Leistungserbringer und Organisationen des Gesundheitswesens mittels SMC-B/HBA. Die Bestätigung der Authentizität erfolgt am Smartcard-IDP-Dienst. Mitarbeiter einer Organisation (in den Rollen *User, User-HBA* und *Org-Admin*) verwenden die durch die Organisation festgelegten Authentifizierungsmethoden und erhalten Lesezugriff auf das~~ mit Hilfe von Identitätstoken. Die jeweilige Überprüfung der Identitätstoken erfolgt am FHIR-Proxy des VZD-FHIR-Directory ~~für Organisations-Ressourcen.~~

~~Für~~. Die Authentifizierung ~~von Leistungserbringern und Organisationen des Gesundheitswesens, die im Besitz einer SMC-B/HBA sind, wird~~ der ~~durch die gematik spezifizierte IDP~~Komponenten Registrierungs-Dienst ~~verwendet [gemSpec_IDP_Dienst]. Dazu MUSS der verwendete~~ und TI-Messenger-Client ~~beim Smartcard-IDP-Dienst~~

registriert sein. Der Leistungserbringer oder Akteur in der Rolle *Org-Admin* KANN mittels des ACCESS_TOKEN die MXID als Telecom Eintrag der Practitioner-Ressource oder Organisations-Ressource zuordnen. Diese Zuordnung verifiziert die MXID des Leistungserbringers, oder macht die jeweilige Organisationsressource anschreibbar durch Nutzer anderer Organisationen.wird im Folgenden weiter beschrieben.

Registrierungs-Dienst

Die Authentifizierung des Registrierungs-Dienstes am VZD-FHIR-Directory erfolgt mittels OAuth am OAuth-Service des VZD-FHIR-Directory. Nach erfolgreicher Authentifizierung mit vereinbarten Client-Credentials wird dem Registrierungs-Dienst ein provider-accesstoken ausgestellt.

TI-Messenger-Client

TI-Messenger-Clients MÜSSEN sich gegenüber dem Auth-Service des VZD-FHIR-Directory mit Hilfe eines ID_TOKENS oder des Matrix-OpenID-Token authentifizieren. Dem Matrix-OpenID-Token des Matrix-Homeservers wird vertraut, wenn der ausstellende Matrix-Homeserver als Matrix-Domain einer verifizierten Organisations-Ressource im VZD-FHIR-Directory eingetragen wurde. Der Auth-Service des VZD-FHIR-Directory stellt nach erfolgreicher Prüfung des jeweiligen Matrix-OpenID-Token ein search-accesstoken aus. Dem ID_TOKEN wird vertraut, wenn der ausstellende IDP-Dienst beim VZD-FHIR-Directory registriert ist und somit das Token durch den Auth-Service validiert werden kann. Nach erfolgreicher Prüfung des ID_TOKEN durch den Auth-Service des VZD-FHIR-Directory wird ein owner-accesstoken ausgestellt.

5.3.25.3.3 Autorisierung am Messenger-Service

Durch die Übergabe eines Matrix-ACCESS_TOKENS erhalten TI-Messenger-Clients erhalten Zugriff auf den Messenger-Service einer, in der Föderation registrierten, Organisation durch Übergabe eines Matrix-ACCESS_TOKENS.. Dieses wird durch den Matrix-Homeserver ausgestellt nachdem ein NutzerAkteur erfolgreich authentifiziert wurde. Das Matrix-ACCESS_TOKEN MUSS sicher auf dem Endgerät gespeichert werden.

5.3.35.3.4 Autorisierung am VZD-FHIR-ProxyDirectory

TI-Messenger-Clients autorisieren sich **Registrierungs-Dienst**

Für den Schreibzugriff des Registrierungs-Dienstes autorisiert dieser sich gegenüber dem FHIR-Proxy des VZD-FHIR-Directory für lesenden Zugriff mittels Matrix-OpenID-Tokenmit einem provider-accesstoken, welches vom Matrix-Homeserver ausgestellt wird. Für schreibenden Zugriff nutzen TI-Messenger-Clients ein ACCESS_TOKEN, welches durch den Smartcard-IDP-Dienst ausgestellt wird. Der Ablauf der Autorisierung amOAuth-Service des VZD FHIR-Proxy wird in der [gemSpec_VZD_FHIR_Directory] im Anwendungsfall "*Nutzer sucht TIOrganization- und TIPractitioner-Einträge im VZD-FHIR-*Directory" beschrieben. Eine Erläuterung zu dem Rechtekonzept des VZD-FHIR-Directoy findet sich in dieser Spezifikation im Kapitel "*Rechtekonzept VZD-FHIR-Directory*".

~~5.4 Föderation~~

~~Da der TI-Messenger-Dienst auf dem offenen und dezentralen Kommunikationsprotokoll Matrix basiert, MUSS gewährleistet werden, dass nur die im Kapitel "*Akteure und Rollen*" genannten berechtigten Akteure teilnehmen können.~~

~~Um allen berechtigten Akteuren des deutschen Gesundheitswesens~~ ausgestellt wurde.

TI-Messenger-Client

Für den ~~Zugang zum TI-Messenger zu gewähren, MUSS ein Anbieter eines TI-Messenger-Fachdienstes für Leistungserbringerinstitutionen und/oder einer Organisation entsprechende Messenger-Services bereitstellen.~~

~~Um nicht zum TI-Messenger gehörende Matrix-Server ausschließen zu können, werden die TI-Messenger-Fachdienste in einer Föderation zusammengefasst. Voraussetzung für die Aufnahme in die Föderation ist der Betrieb eines Messenger-Proxies als Teil des Messenger-Services, der sicherstellen MUSS, dass nur zugelassene TI-Messenger-Fachdienste Zugang in die Föderation erhalten. Voraussetzung für die Aufnahme in die Föderation ist eine erfolgreiche Zulassung durch die gematik. Nach einer erfolgreichen Zulassung erhält der Registrierungs-Dienst~~Lesezugriff autorisieren sich TI-Messenger-Clients gegenüber dem FHIR-Proxy des VZD-FHIR-Directory mit einem search-accesstoken, welches vom Auth-Service des ~~jeweiligen Fachdienstes die Möglichkeit die Domains des jeweiligen Messenger-Services der entsprechenden Organisation auf dem VZD~~ VZD FHIR-Directory ~~zuzuordnen~~ausgestellt wurde. Für den Schreibzugriff nutzen TI-Messenger-Clients das owner-accesstoken, welches vom Auth-Service des VZD FHIR-Directory ausgestellt wurde.

~~Für die Aufnahme in die Föderation MÜSSEN ausschließlich Matrix-Homeserver verwendet werden. Ein Bridging anderer Messaging-Protokolle DARF NICHT stattfinden.~~

~~5.5~~5.4 Rechtekonzept VZD-FHIR-Directory

Im folgenden Kapitel wird ~~beschreiben~~beschrieben, wie der ~~Schreib~~Lese- und ~~Lesezugriff~~ Schreibzugriff durch die TI-Messenger-Clients ~~des TI-Messenger-Fachdienstes~~ und dem Registrierungs-Dienst auf dem VZD-FHIR-Directory erfolgt.

~~5.5.1 Schreibzugriffe für TI-Messenger-Fachdienste~~

5.4.1 Lesezugriff

Registrierungs-Dienst

Die TI-Messenger-Fachdienste erhalten die Möglichkeit, mittels ihres Registrierungs-Dienstes die ~~bereits bestehende Föderation um weitere Messenger-Services zu erweitern. Die Autorisierung am~~ Föderationsliste vom FHIR-Proxy des VZD-FHIR-Directory ~~des Registrierungs-Dienstes erfolgt mittels OAuth und ermöglicht es Fachdiensten~~ abzurufen. Hierfür MUSS die ~~eigene Organisations-Ressource um Endpoint-Ressourcen zu erweitern. Eine Endpoint-Ressource stellt dabei einen Messenger-Service da, welcher durch die Matrix-Domain auf einen Host verweist und auf eine Organisation referenziert wird. Der Registrierungs-Dienst MUSS durch die Überprüfung der SMC-B sicherstellen, dass es sich um eine zugelassene Organisation handelt.~~

5.5.2 Schreibzugriff für TI-Messenger-Clients

Nutzer MÜSSEN sich als Leistungserbringer, oder Organisation mittels OpenID-Connect authentifizieren. Diese Authentifizierung gewährt schreibenden Zugriff auf die jeweils eigene, für den Leistungserbringer, oder Organisation angelegte FHIR-Ressource (Practitoner, Organization).

Schreibzugriff für Nutzer in der Rolle Org-Admin

Um die Schnittstelle `/tim-provider-services` am FHIR-Ressource der jeweiligen Organisation bearbeiten zu können MUSS die Identität der Organisation bestätigt werden. Dies erfolgt aktuell durch eine SMC-B. Die Nutzung einer SMC-B ermöglicht es einem Akteur in der Rolle *Org-Admin* mit Hilfe eines TI-Messenger-Clients FHIR-Ressourcen im Namen der Organisation anzulegen. Die FHIR-Ressourcen werden als *part of* zu der entsprechenden Stamm-Organisationsressource referenziert.

Schreibzugriff für Nutzer in der Rolle User-HBA

Ein Leistungserbringer KANN die eigene, bereits bestehende FHIR-Ressource *Practitioner* erweitern, um für andere Leistungserbringer aus der Ferne anschreibbar zu werden, oder um andere Leistungserbringer anzuschreiben. Dafür MUSS sich der Leistungserbringer entsprechend mit einem TI-Messenger-Client am Smartcard-Proxy des IDP-Dienst authentifizieren. Dieser Vorgang verifiziert den Nutzer als Leistungsbringer innerhalb des TI-Messengers.

5.5.3 Lesezugriff für TI-Messenger-Clients

Für lesenden Zugriff auf das VZD-FHIR-Directory wird das Matrix-OpenID-Token des jeweiligen Matrix-Homeservers unter Vorlage des provider-accesstoken aufgerufen werden verwendet. Ein Nutzer KANN somit Suchanfragen an das VZD-FHIR-Directory senden. Dem Matrix-OpenID-Token des Matrix-Homeservers wird vertraut, wenn der Matrix-Homeserver als Matrix-Domain einer verifizierten Organisations-Ressource im VZD-FHIR-Directory zugeordnet wurde und ihm somit auch vertraut werden kann. Der Lesezugriff wird mittels Berechtigungen (*Policies*) auf dem VZD-FHIR-Directory geregelt.

Es gilt:

- die Sichtbarkeit auf die Organisations-Ressourcen KANN für andere Organisationen oder Practitioners eingeschränkt werden und

die Sichtbarkeit auf Practitoner

TI-Messenger-Clients

Durch den Aufruf der Schnittstelle `/search` am FHIR-Proxy des VZD-FHIR-Directory KANN ein TI-Messenger-Client unter Vorlage des search-accesstoken Suchanfragen an das FHIR-Directory stellen. Die Suchergebnisse sind abhängig von den eingetragenen FHIR-Ressourcen und deren Sichtbarkeit.

5.4.2 Schreibzugriff

Registrierungs-Dienst

Die TI-Messenger-Fachdienste erhalten die Möglichkeit, mittels ihres Registrierungs-Dienstes Messenger-Services in die TI-Föderation aufzunehmen. Hierfür MUSS die Schnittstelle `/tim-provider-services` am FHIR-Proxy des VZD-FHIR-Directory unter Vorlage des provider-accesstoken aufgerufen werden.

TI-Messenger-Clients

Durch den Aufruf der Schnittstelle `/owner` am FHIR-Proxy des VZD-FHIR-Directory erhält ein Akteur unter Vorlage des owner-accesstoken Schreibzugriffe auf das FHIR-Directory. In der folgenden Tabelle wird die zu verändernde FHIR-Ressource in Abhängigkeit zu der verwendeten Identität eines Akteurs beschrieben (siehe dazu auch die Tabelle "Verzeichnistypen - Rechtekonzept").

Tabelle 5: Schreibzugriff - VZD-FHIR-Ressourcen ~~ist nur möglich, wenn der~~

Rolle	Identität	FHIR-Ressource	Beschreibung
Org-Admin	SMC-B	HealthcareService	Die Nutzung einer SMC-B ermöglicht es einem Akteur in der Rolle "Org-Admin" mit Hilfe eines TI-Messenger-Clients mit Administrationsfunktion FHIR-Ressourcen (*Endpoint*) im Namen der Organisation in das Organisationsverzeichnis einzutragen. Die Einträge im Organisationsverzeichnis beginnen immer mit einer *HealthcareService* Ressource.
User-HBA	HBA	PractitionerRole	Die Nutzung eines HBAs ermöglicht es einem Akteur in der Rolle "User-HBA" mit Hilfe eines TI-Messenger-Clients seine, bereits bestehende FHIR-Ressource *(Endpoint*), im Personenverzeichnis zu erweitern, um für andere Leistungserbringer anschreibbar zu werden oder um andere Leistungserbringer anzuschreiben. Die Einträge im Personenverzeichnis beginnen immer mit einer *PractitionerRole* Ressource.

5.5 User Management

Aufgrund der Vielzahl an Teilnehmern wird eine komfortable Benutzerverwaltung innerhalb des TI-Messenger-Dienstes benötigt. In diesem Kapitel werden die für das User Management notwendigen Rollen und die dafür verwendeten Nutzer-Verzeichnisse beschrieben.

Voraussetzung für die Nutzung des TI-Messenger-Dienstes ist zunächst, dass sich ein Akteur über ein Authentifizierungsverfahren am Matrix-Homeserver seiner Organisation authentifizieren kann und ein Nutzer-Account auf dem Matrix-Homeserver angelegt wurde. Der Nutzer-Account auf dem Matrix-Homeserver wird entweder vom Akteur in der Rolle "Org-Admin" seiner Organisation bereitgestellt oder vom Akteur selbst ~~mit der Matrix User URI (~~am Matrix-Homeserver registriert. Bei der Erstellung des Nutzer-Accounts wird die MXID~~) als Practitioner auf dem VZD~~ des Akteurs erzeugt sowie der Displayname des Akteurs festgelegt (siehe gemSpec_TI-Messenger-Client#Weitere Funktionen). Nach der Erstellung des Nutzer-Accounts am Matrix-Homeserver wird die MXID des Akteurs im User-Directory des Matrix-Homeservers hinterlegt. Alle im User-Directory des Matrix-Homeservers hinterlegten MXIDs sind anschließend durch andere Akteure seiner Organisation auffindbar und erreichbar. Soll der Akteur auch von außerhalb der Organisation auffindbar werden, so MUSS dieser mit seiner MXID in das Organisationsverzeichnis im VZD-FHIR-Directory hinterlegt werden. Das Hinterlegen der MXID eines Akteurs in das Organisationsverzeichnis MUSS durch den Akteur in der Rolle "Org-Admin" erfolgen. Voraussetzung ist ~~und die Period gemäß [Spec_VZD-FHIR_Directory] gesetzt wurde~~das vorhandensein einer HealthcareService-Ressource der Organisation. Die MXIDs werden in, der HealthcareService-Ressource zugeordnet, Endpoint-Ressourcen hinterlegt. Die Einrichtung einer HealthcareService-Ressource einer Organisation erfolgt durch den Akteur in der Rolle "Org-Admin". Möchte ein Akteur ohne Zugehörigkeit zu einer Organisation gefunden werden, so MUSS seine MXID in das Personenverzeichnis des VZD-FHIR-Directory hinterlegt werden. Voraussetzung hierfür ist der Besitz eines HBAs.

Die folgende Tabelle zeigt einen zusammenfassenden Überblick der Benutzerverwaltung.

Tabelle 6: Überblick der Benutzerverwaltung in Abhängigkeit der Rolle

Rolle	Client	Administration	Wo
Org-Admin	TI-Messenger Client mit Administrationsfunktionen (Org-Admin-Client)	• Nutzer-Account anlegen • Nutzer-Account verwalten	Matrix-Homeserver (User Directory)
		• HealthcareService-Ressource anlegen • Endpoint einer HealthcareService-Ressource anlegen • Endpoint einer HealthcareService-Ressource verwalten	VZD-FHIR-Directory (Organisationsverzeichnis)
User	TI-Messenger Client	• Nutzer-Account anlegen	Matrix-Homeserver (User Directory)

User-HBA	TI-Messenger Client	• Endpoint einer PractitionerRole-Ressource anlegen • Endpoint einer PractitionerRole-Ressource verwalten	VZD-FHIR-Directory (Personenverzeichnis)

5.6 Funktionsaccounts

Einrichtungen im Gesundheitswesen sind sehr unterschiedlich strukturiert und wollen hinsichtlich ihrer Erreichbarkeit flexibel eigene Strukturen abbilden können. Daher sind beim TI-Messenger-Dienst Accounts notwendig, die es ermöglichen, Akteure unterhalb der Struktur erreichbar zu machen. Der anfragende Akteur muss dann nicht die genaue interne Struktur der Organisation kennen. Diese speziellen Accounts werden im folgenden als Funktionsaccounts bezeichnet.
Ein Funktionsaccount ist als eine *Endpoint*-Ressource (mit dem `payloadType` *"TI-Messenger chat")* eines *HealthcareService* einer Organisation anzulegen. Der *HealthcareService* bildet im FHIR-Directory eine Struktur (z. B. Station in einem Krankenhaus) der Organisation ab. Zur Erreichbarkeit dieser Struktur wird die MXID eines Chatbots oder eines Akteurs (der stellvertretend für die Organisation eintritt) in das `address` Attribut der Endpoint Ressource hinterlegt. Pro *HealthcareService* darf nur eine *Endpoint*-Ressource für den `payloadType` "*TI-Messenger chat*" existieren. Somit kann die angelegte Struktur der Organisation über den Funktionsaccount und dessen hinterlegten Namen (*Endpoint.name*) im VZD-FHIR-Directory von einem Akteur gefunden werden.

Chatbot

Chatbots sind spezielle Akteure (siehe Kapitel "*Akteure und Rollen*"), die stellvertretend für eine Struktur einer Organisation von einem die Kommunikation initiierenden Akteur eingeladen werden können. Chatbots KÖNNEN die Kommunikation vollständig automatisiert abschließen (z. B. Terminvergabe) oder in der Organisation hinterlegte natürliche Personen dem Chat hinzuziehen (z. B. Ausstellen eines Rezeptes). Beispiele für Chatbots sind unter [Matrix Bots] zu finden. Treten Chatbots als Kommunikationsteilnehmer des TI-Messengers auf, so MÜSSEN diese im jeweiligen Chat als Chatbot gekennzeichnet werden.

Im Folgenden wird ein Beispiel für eine mögliche Zuordnung für die Abbildung von Funktionsaccounts mit Hilfe von Chatbots und eines Akteurs der stellvertretend für die Organisation auftritt.
Der Chatbot KANN automatisiert Anfragen von Akteuren (z. B. für Terminanfragen, Medikationsentscheidung) bearbeiten oder bei Bedarf die zugeordneten und zu diesem Zeitpunkt verfügbaren Akteure in den Chatraum einladen. Die dem Chatbot zur Verfügung stehenden Akteure (in der Spalte Akteur blau hinterlegt) sind in der Konfiguration des Chatbots zu definieren. Im abschließenden Beispiel ist ein Akteur (natürliche Person) als Endpoint hinterlegt und tritt stellvertretend für die Organisation in den Chat ein.

Tabelle 7: Beispiel für Funktionsaccounts

Abteilung	Funktionsaccount	Endpoint.address	Akteur (MXID)	Displayname
Kardiologie	Labor_Kardiologie	@MXID_Bot01:<domain>.de	@MXID_01:<domain>.de @MXID_02:<domain>.de	Empfang_Kardiologie (Chatbot) Dennert, Maltilde Fritsche, Sarah
Neurologie	Ambulanz_Neurologie	@MXID_Bot02:<domain>.de	@MXID_03:<domain>.de	Ambulanz_Neurologie (Chatbot) Gotsch, Gerd
Radiologie	Empfang_Radiologie	@MXID_04:<domain>.de	-	Fruechtl, Wilfried

Im Folgenden wird die Interaktion eines externen Akteurs mit einem Funktionsaccount gezeigt.

Prozess:

1. Vorbedingung:
   - Organisation verfügt über einen TI-Messenger-Client mit Administrationsfunktion und einen Messenger-Service
   - Chatbots stehen zur Verfügung und können vom Akteur in der Rolle "Org-Admin" verwaltet werden

2. Konfiguration von Funktionsaccounts:
   - Der Akteur in der Rolle "Org-Admin" legt einen Funktionsaccount (organisationsbezogene MXID) als einen*Endpoint* des gewünschten *HealthcareService* der Organisation an und ordnet dieser MXID einen Chatbot zu
   - Der Akteur in der Rolle "Org-Admin" weist zuständige Akteure der Organisation (personenbezogene MXIDs) dem Chatbot zu
   - Die Zuordnung von Akteuren zu einzelnen Anfragen innerhalb eines Funktionsaccounts (z. B. Terminanfragen, Medikationsentscheidung) erfolgt durch die Konfiguration im Chatbot

   Alternative: Der Akteur in der Rolle "Org-Admin" legt einen Funktionsaccount (organisationsbezogene MXID) als einen*Endpoint* des gewünschten *HealthcareService* der Organisation an und hinterlegt in diesem Endpoint die MXID von einem Akteur.

3. Beispielhafter Ablauf (siehe Abbildung "*Interaktion mit einem Chatbot*"):
   1. Ein Akteur sucht nach einer Organisation und/oder Unterstruktur dieser Organisation (z. B. in einem Krankenhaus die Abteilung Kardiologie)
   2. Der Akteur öffnet einen Chatraum mit dem Funktionsaccount der Abteilung Kardiologie
   3.
      a. Der Chatbot des Funktionsaccounts der Abteilung Kardiologie betritt den Raum
      b. Der Chatbot KANN automatisiert das Anliegen vom Akteur (z. B. Terminanfrage, Rückfrage an Arzt etc.) abfragen
   4. Der Akteur antwortet dem Chatbot
   5. Der Chatbot lädt je nach Anliegen die ihm zugeordneten und verfügbaren Akteure in den Chatraum ein
   6.
      a. Eingeladene Akteure betreten den Chatraum mit ihrem Displaynamen
      b. Eingeladene Akteure kommunizieren mit dem Akteur

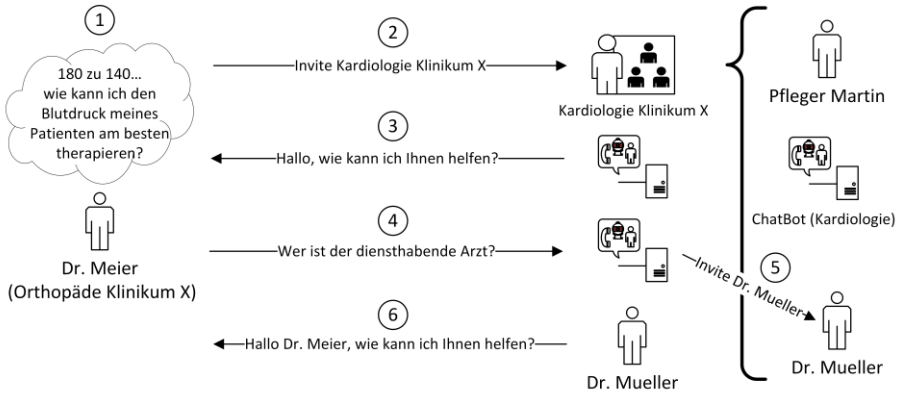


Abbildung 5: Beispiel einer Interaktion mit einem Chatbot

5.7 Test

Der TI-Messenger-Anbieter MUSS eine Referenz-Instanz und mindestens eine Test-Instanz des TI-Messenger-Fachdienstes und TI-Messenger-Clients bereitstellen und

betreiben. Die Referenz-Instanz hat die gleiche Version wie die Produktionsumgebung und kann von anderen Herstellern für Tests und Entwicklung gegen die zugelassene Version benutzt werden. Weiterhin wird die Referenz-Instanz für die Reproduktion aktueller Fehler/Probleme aus der Produktionsumgebung genutzt. Der Zugriff auf die Referenz-Instanz MUSS für die gematik zur Fehleranalyse gewährleistet sein.
Die Test-Instanz dient den Herstellern bei der Entwicklung neuer TI-Messenger-Clients und TI-Messenger Fachdienste Versionen, den IOP-Tests zwischen den verschiedenen TI-Messenger-Anbietern und wird auch von der gematik für die Zulassung genutzt.
Der TI-Messenger-Anbieter MUSS die verschiedenen Benutzer der Referenz-Instanz und der Test-Instanz koordinieren (Verwaltung eines Test-/Nutzungsplans). Bei Bedarf (Entwicklung verschiedener Versionen, hoher Auslastung durch andere Hersteller oder durch die gematik) MUSS der TI-Messenger-Anbieter auch mehrere Test-Instanzen mit der gleichen oder mit verschiedene Versionen bereitstellen und betreiben.

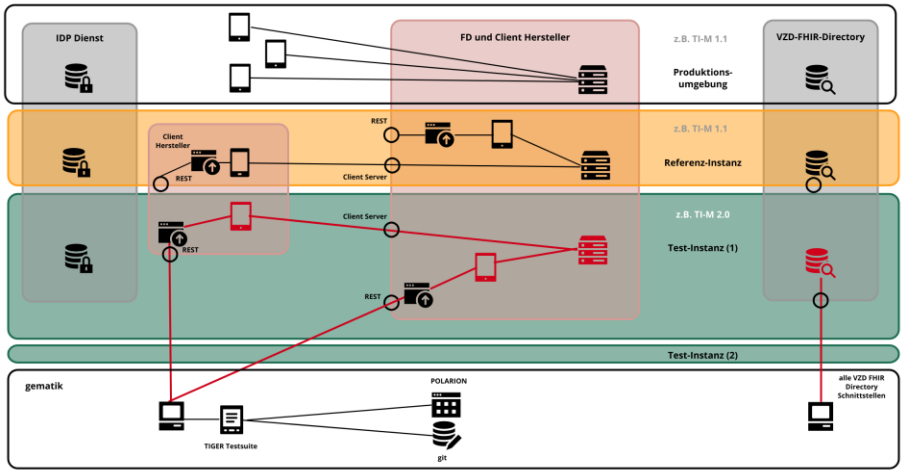


Abbildung 6: TI-Messenger-Dienst Instanzen

~~5.6~~5.8 Betrieb

Der TI-Messenger-Anbieter verantwortet im Betrieb folgende Produkte:

- TI-Messenger-Fachdienst ~~und~~ (e),
- TI-Messenger-Client(s~~),~~) für Akteure und

- TI-Messenger-Clients mit Administrationsfunktionen (Org-Admin-Client) inkl. Authenticator(-modul).

Der TI-Messenger-Anbieter MUSS mindestens einen TI-Messenger-Fachdienst, mindestens einen TI-Messenger-Client für Akteure und mindestens einen Org-Admin-Client (die Clients jeweils oder in einen TI-Messenger-Client integriert) anbieten.

Der TI-Messenger-Anbieter KANN auch mehrere TI-Messenger-Clients und mehrere TI-Messenger-Fachdienste anbieten. Der tatsächliche Betrieb kann gemäß [gemKPT_Betr#Anbieterkonstellationen] ausgelagert werden.

Der TI-Messenger-Anbieter MUSS seinen Nutzern und Organisationen einen Helpdesk entsprechend [gemKPT_Betr] anbieten, welcher auch Störungen zu allen verantworteten TI-Messenger-Clients ~~entgegen nimmt.~~ und TI-Messenger-Fachdiensten entgegennimmt.

Der TI-Messenger-Anbieter ist gemäß Betriebskonzept [gemKPT_Betr] ein Teilnehmer im TI-ITSM (IT-Service-Management der TI) mit allen damit verbundenen Rechten und Pflichten.

~~Der~~

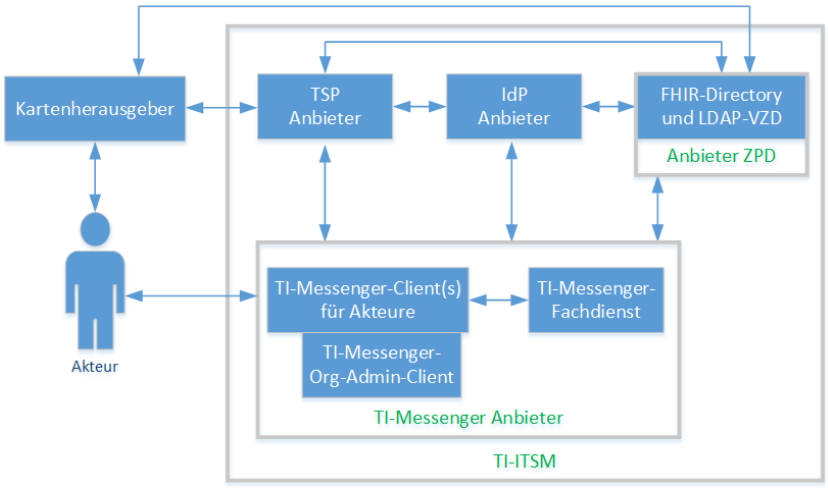


Abbildung 7: Ausschnitt - TI-Messenger-Anbieter ~~MUSS Referenzinstanzen~~im TI-ITSM

Hinweis: Die Abbildung bildet die organisatorischen Kommunikationsbeziehungen im Vordergrund des TI-~~Messenger-Fachdienstes bereitstellen und betreiben~~ITSM-System zwischen den jeweiligen Entitäten ab. Die Produkte beim TI-Messenger Anbieter können einzeln zugelassen werden, werden aber im Bundle im Sinne des Nutzers mit einem SPOC für die jeweiligen Komponenten vom jeweiligen Anbieter angeboten.

~~Dabei MUSS es eine Referenzinstanz geben welche Herstellern bei der Entwicklung neuer TI-Messenger-Clients und TI-Messenger-Fachdienste dient und eine Referenzinstanz welche ausschließlich der gematik zur Verfügung gestellt wird, gegen welche getestet werden kann.~~

6 Anwendungsfälle

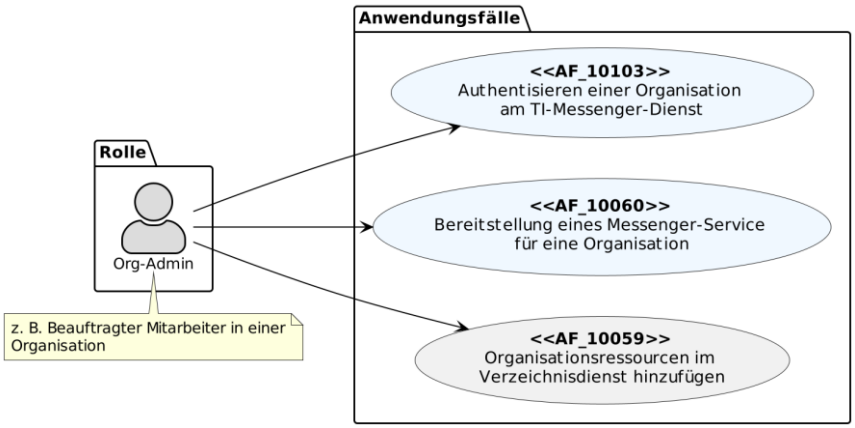
~~Alle Anwendungsfälle, die gemäß Matrix-Client-Server-Protokoll umgesetzt werden können, werden in diesem Konzept nicht aufgeführt. Stattdessen wird auf die Matrix-Client-Server-API verwiesen ([Matrix Foundation#Client_Server]).~~

Die nachfolgend beschriebenen Anwendungsfälle sind spezifisch für den TI-Messenger-Dienst und weichen daher teilweise von der Matrix-Client-Server-API ab. Das ~~gleich~~gleiche gilt für die auf dem Matrix-Server-Server-Protokoll ([~~Matrix Foundation#~~Server – Server API]) basierenden Anwendungsfälle. Das bedeutet, dass alle Anwendungsfälle, die gemäß Matrix-Client-Server-Protokoll umgesetzt werden, an dieser Stelle nicht weiter aufgeführt sind. Stattdessen wird hier auf die Matrix-Client-Server-API verwiesen ([Client-Server API]).

Im Kontext des TI-Messenger-Dienstes nehmen Akteure unterschiedliche Rollen ein (siehe Kapitel *3.1- Akteure und Rollen)*. Entsprechend der eingenommen Rolle eines Akteurs werden unterschiedliche Anwendungsfälle ausgelöst. Für die Rollen "Org-Admin und User/User-HBA" wird dies in den folgenden Abbildungen dargestellt.

Rolle: Org-Admin

Ein Akteur in der Rolle "Org-Admin" KANN ein Leistungserbringer / beauftragter Mitarbeiter in einer Organisation oder ein beauftragter Administrator des TI-Messenger-Anbieters sein. Für seine administrativen Tätigkeiten löst dieser Akteur, unter Nutzung einer freigeschalteten SMC-B, im Kontext des TI-Messenger-Dienstes die folgenden Anwendungsfälle aus.



~~Im Folgenden werden die Anwendungsfälle gemäß dem Konzeptpapier TI-Messenger [gemKPT_TI_Messenger] beschrieben.~~

~~6.1 AF – Anmeldung eines Nutzers an Messenger-Service~~

~~AF_10057 – Anmeldung eines Nutzers am Messenger-Service~~

~~Mit diesem Anwendungsfall meldet sich ein Nutzer als Person an einem Messenger-Service an. Die Anmeldung erfolgt durch den Nutzer mit einem TI-Messenger-Client und einem Authentifizierungsverfahren, das vom Messenger-Service unterstützt wird. Der TI-Messenger-Client präsentiert dem Nutzer eine Liste aller unterstützten Messenger-Services. Ebenfalls ist es möglich, dass der Nutzer die Domain eines Messenger-Service direkt eingibt, um sich an diesen zu authentifizieren. Nach erfolgreicher Anmeldung erhält der TI-Messenger-Client ein Matrix-ACCESS_TOKEN (AuthZ) vom Matrix-Homeserver, das für die spätere Autorisierungen genutzt wird. Das Matrix-ACCESS_TOKEN ist mit dem TI-Messenger-Client des Nutzers über die device_id verknüpft.~~

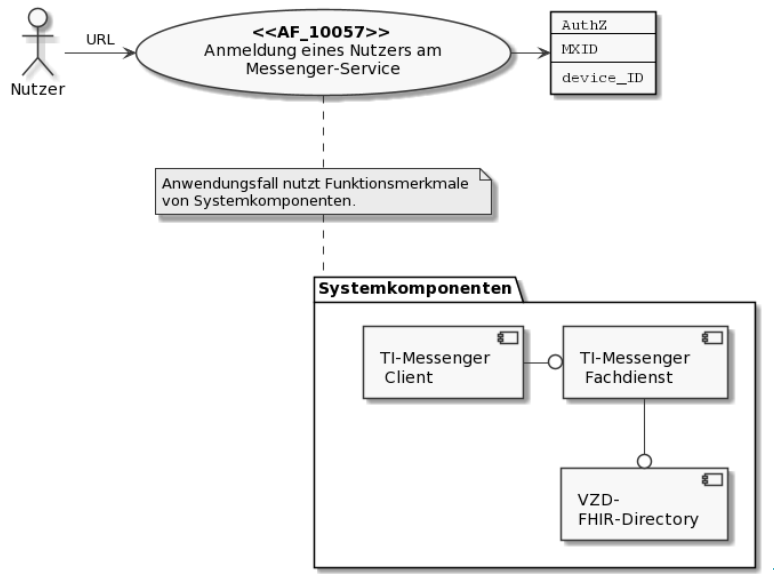


Abbildung 8: ~~Systemkomponenten des~~ Org-Admin - Übersicht Anwendungsfälle

Der Anwendungsfall "*AF ~~– Anmeldung~~ _10060 - Bereitstellung eines ~~Nutzers am~~ Messenger ~~–~~Service für eine Organisation*" setzt die erfolgreiche Authentifizierung der Organisation durch den Anwendungsfall "AF_10103 - Authentisieren einer Organisation am TI-Messenger-Dienst" voraus. Werden durch eine Organisation mehrere Messenger-Services benötigt (z. B. im Krankenhausumfeld) KANN der Anwendungsfall mehrfach ausgeführt werden. Mit der farblichen Zuordnung soll auf eine funktionale Beziehung zwischen den einzelnen Anwendungsfällen hingewiesen werden.

~~Tabelle 3: AF – Anmeldung eines Nutzers am Messenger-Service~~

Eine weitere Aufgabe des Akteurs in der Rolle "Org-Admin", welche hier nicht weiter in einem Anwendungsfall gezeigt wird, ist die Einrichtung von Funktionsaccounts und die Benutzerverwaltung.

Rolle: User / User-HBA

Ein Akteur in der Rolle "User / User-HBA" KANN die folgenden Anwendungsfälle auslösen.

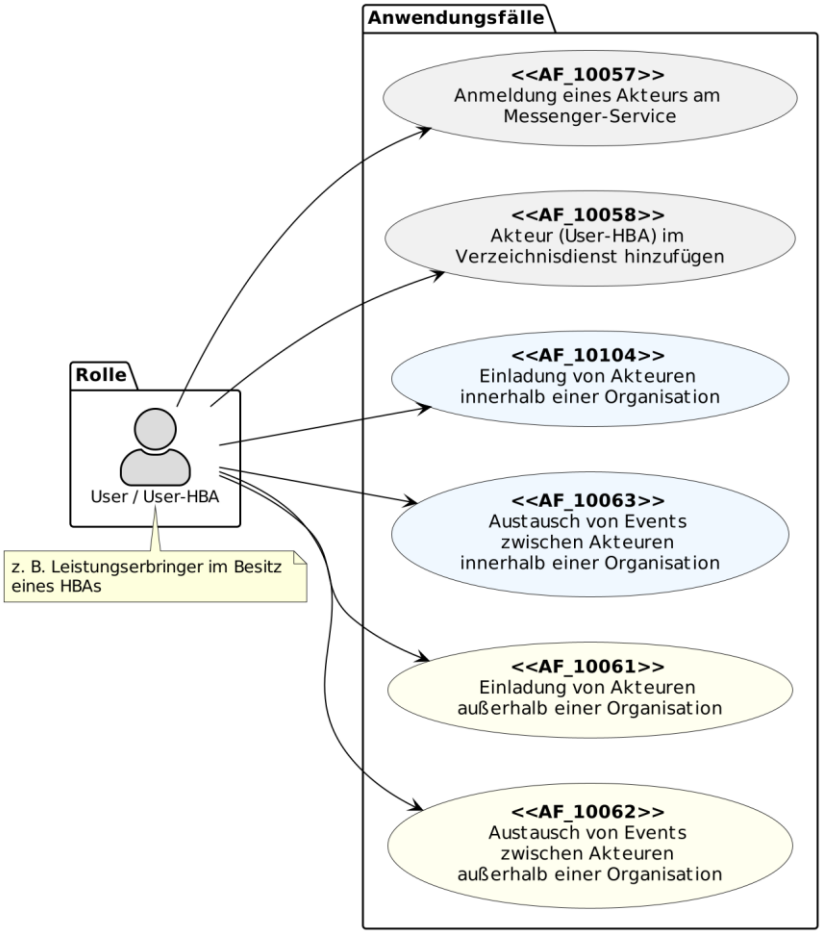


Abbildung 9: User / User HBA - Übersicht Anwendungsfälle

Der Anwendungsfall "*AF_10058 - Akteur (User-HBA) im Verzeichnisdienst hinzufügen*" KANN nur von einen Akteur in der Rolle "User-HBA" ausgeführt werden. Alle anderen gezeigten Anwendungsfälle KÖNNEN von den Akteuren in der Rolle "User / User-HBA" ausgeführt werden. Mit der farblichen Zuordnung soll auf eine funktionale Beziehung zwischen den einzelnen Anwendungsfällen hingewiesen werden.

Hinweis: In den folgenden Anwendungsfällen wird auf Abläufe verwiesen, die im Anhang B zu finden sind. Ebenfalls können für eine bessere Lesbarkeit die in den jeweiligen

Anwendungsfällen dargestellten Laufzeitsichten als PlantUML-Quelle in [api-messenger] unter `src/plantuml` und in Diagrammform unter `/images/diagrams` abgerufen werden.

6.1 AF - Authentisieren einer Organisation am TI-Messenger-Dienst

AF_10103 **- Authentisieren einer Organisation am TI-Messenger-Dienst**
Mit diesem Anwendungsfall authentisiert ein Akteur, in der Rolle "Org-Admin", seine Organisation bei einem TI-Messenger-Anbieter. Für die Authentisierung einer Organisation stellt der TI-Messenger-Fachdienst eine Schnittstelle an seinem Registrierungs-Dienst bereit. Diese wird über das Frontend des Registrierungs-Dienstes für die Authentisierung verwendet. Die Authentisierung der Organisation erfolgt individuell und nutzungsabhängig durch einen Akteur in der Rolle "Org-Admin". Für die Verifizierung der Organisation MUSS bei der Authentisierung am IDP-Dienst eine freigeschaltete SMC-B verwendet werden. Als Nachweis zur Prüfung auf eine gültige Organisation MUSS der Registrierungs-Dienst die im ID_TOKEN enthaltene *ProfessionOID* gegen die OID-Festlegung für Institutionen prüfen. Bei erfolgreicher Verifizierung der Organisation wird ein Administrator-Account für die Organisation am Registrierungs-Dienst angelegt. Dies ermöglicht es einem Administrator Messenger-Services zu registrieren und seiner Organisation am TI-Messenger-Dienst teilzunehmen.

Tabelle 8: Tabelle : AF - Authentisieren einer Organisation am TI-Messenger-Dienst

AF_~~10057~~10103	**~~Anmeldung eines Nutzers~~Authentisieren einer Organisation am TI-Messenger-~~Service~~Dienst**
Akteur	~~Nutzer~~Beauftragter Mitarbeiter einer Organisation in der Rolle "Org-Admin"
Auslöser	~~Nutzer~~Eine Organisation des deutschen Gesundheitswesens möchte ~~sich mit~~am TI-Messenger-~~Client bei einem~~Dienst teilnehmen und benötigt die Berechtigung einen Messenger-Service ~~anmelden~~zu registrieren
Komponenten	• Frontend des Registrierungs-Dienstes, • Authenticator, • Konnektor, • eHealth Kartenterminal mit gesteckter SMC-B, • Registrierungs-Dienst, • IDP-Dienst~~TI-Messenger-Client, Messenger-Service, VZD-FHIR-Directory~~
~~Vorbedingungen~~ Vorbedingung	~~1. Der Nutzer verfügt über einen TI-Messenger-Client~~

	~~1. Der Nutzer kennt die URL des Messenger-Services oder die URL ist bereits in seinem Client konfiguriert.~~ ~~2. Der Nutzer kann sich durch ein beim Matrix-Homeserver unterstütztes Authentisierungsverfahren identifizieren.~~ ~~3. Der verwendete Matrix-Homeserver unterstützt vereinbarte Authentisierungsverfahren.~~ 1. ~~Der verwendete Matrix-Homeserver ist in die Föderation integriert.~~Der Akteur kann über ein Frontend des Registrierungs-Dienstes für die Kommunikation auf den Registrierungs-Dienst zugreifen. 2. Das verwendete Frontend des Registrierungs-Dienstes ist bei einem zuständigen IDP-Dienst registriert. 3. Der Akteur kann den Authenticator des jeweiligen TI-Messenger-Anbieters verwenden. ~~1.~~4. Die im eHealth Kartenterminal gesteckte SMC-B ist freigeschaltet.
Eingangsdaten	~~URL des Matrix-Homeservers~~Identität der Organisation, SMC-B
Ergebnis	~~TI-Messenger-Account erzeugt~~Die Organisation wurde am Registrierungs-Dienst des TI-Messenger-Fachdienstes verifiziert
Ausgangsdaten	~~Matrix-ACCESS~~ID_TOKEN, ~~MXID, device_id~~ Admin-Account, Status
Akzeptanzkriterien	ML-~~123571,~~ 128757, ML-~~123576 ,~~ 128759, ML-~~123575~~128758 , ML-129853, ML-132446

In der Laufzeitsicht sind die Interaktionen zwischen den Komponenten, die durch den Anwendungsfall genutzt werden, dargestellt. Für die Authentisierung einer Organisation wird in der Laufzeitsicht der zentrale IDP-Dienst der TI verwendet. Die Nutzung anderer IDP-Dienste ist auch möglich.

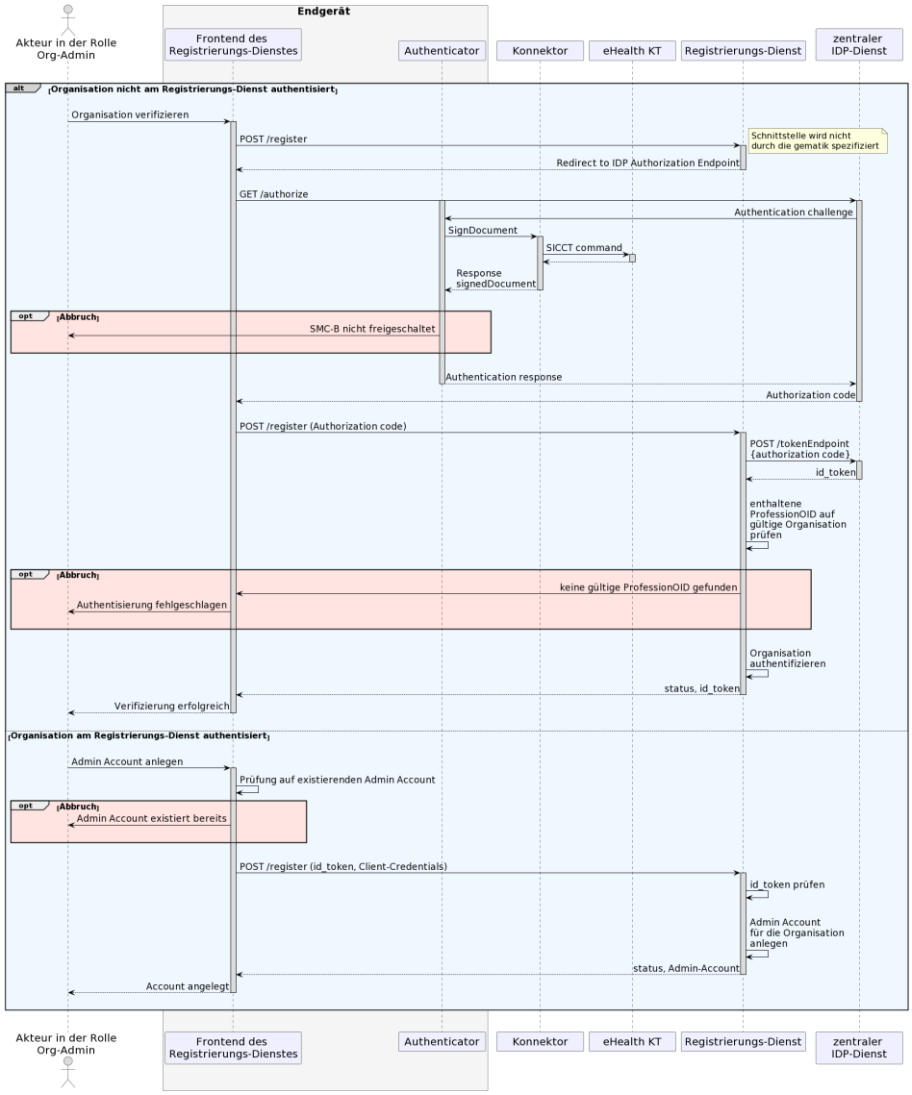


Abbildung 10: Laufzeitsicht - Authentisieren einer Organisation am TI-Messenger-Dienst [<=]

Akzeptanzkriterien für den Anwendungsfall: Authentisieren einer Organisation am TI-Messenger-Dienst (AF_10103)

ML-128757 **- AF_10103 - Verifizierung der Organisation als Akteur in der Rolle Org-Admin**
Nur ein Akteur in der Rolle "Org-Admin" darf seine Organisation gegenüber dem TI-Messenger-Fachdienst authentifizieren.
[<=]

ML-128759 **- AF_10103 - Organisation wurde erfolgreich verifiziert**
Die Organisation wurde beim TI-Messenger-Fachdienst erfolgreich mit einer Identität einer Organisation des Gesundheitswesens verifiziert
[<=]

ML-128758 **- AF_10103 - ID-Token wurden ausgestellt und übergeben**
Das vom IDP-Dienst ausgestellte ID_TOKEN ist gültig und liegt dem Frontend des Registrierungs-Dienstes vor.
[<=]

ML-129853 **- AF_10103 - Administrator Account angelegt**
Ein Administrator Account für die Organisation wurde erfolgreich am Registrierungs-Dienst angelegt.
[<=]

ML-132446 **- AF_10103 - TI-M Rohdatenerfassung und -lieferung**
Die Rohdaten wurden entsprechend der Rohdatendefinition gemäß [gemSpec_TI-Messenger-FD#Betrieb] für den TI-Messenger-Fachdienst erfolgreich erfasst und an die definierte Schnittstelle der Rohdatenerfassung versendet.**[<=]**

6.2 AF - Bereitstellung eines Messenger-Service für eine Organisation

AF_10060 **- Bereitstellung eines Messenger-Service für eine Organisation**
Mit diesem Anwendungsfall wird einer zuvor am Registrierungs-Dienst authentifizierten Organisation ein Messenger-Service für diese Organisation durch einen Akteur in der Rolle "Org-Admin" bereitgestellt. Die Beantragung zur Bereitstellung eines Messenger-Service wird durch den Akteur in der Rolle "Org-Admin" am Frontend des Registrierungs-Dienstes vorgenommen. Dieser MUSS sich zuvor mit dem Admin-Account der Organisation am Registrierungs-Dienst anmelden. Für eine zeitnahe Adaption des TI-Messenger-Dienstes MUSS eine schnelle Bereitstellung von Messenger-Services gewährleistet sein. TI-Messenger-Anbieter sind verpflichtet, Prozesse zu etablieren, damit Messenger-Services für Organisationen schnell und ggf. automatisiert bereitgestellt werden können. Nach erfolgreicher Bereitstellung eines Messenger-Service wird dieser in die Föderation des TI-Messenger-Dienstes aufgenommen. Werden mehrere Messenger-Services für eine Organisation benötigt KANN dieser Anwendungsfall mehrfach ausgeführt werden.

Tabelle 9: AF - Bereitstellung eines Messenger-Service für eine Organisation

AF_10060	**Bereitstellung eines Messenger-Service für eine Organisation**
Akteur	Beauftragter Mitarbeiter einer Organisation in der Rolle "Org-Admin"

Auslöser	Eine Organisation des deutschen Gesundheitswesen möchte am TI-Messenger-Dienst teilnehmen und benötigt die Bereitstellung eines oder mehrerer Messenger-Services
Komponenten	• Frontend des Registrierungs-Dienstes, • Registrierungs-Dienst, • VZD-FHIR-Directory, • Messenger-Service.
Vorbedingung	1. Es besteht ein Vertragsverhältnis mit einem TI-Messenger-Anbieter. 2. Der Akteur verfügt über ein Frontend des Registrierungs-Dienstes für die Kommunikation mit dem Registrierungs-Dienst. 3. Das verwendete Frontend des Registrierungs-Dienstes ist beim zuständigen IDP-Dienst registriert. 4. Die Organisation ist erfolgreich beim Registrierungs-Dienst authentifiziert und ein Admin-Account ist vorhanden. 5. Der Registrierungs-Dienst kann sich beim VZD-FHIR-Directory Server für Schreibzugriffe mit OAuth2 authentisieren.
Eingangsdaten	Admin-Account, Identität der Organisation (SMC-B)
Ergebnis	1. Der Messenger-Service für die Organisation wurde erstellt. 2. Die Matrix-Domain des neuen Messenger-Services wurde als Endpunkt im VZD-FHIR-Directory eingetragen und in die Föderation aufgenommen.
Ausgangsdaten	Neuer Messenger-Service für die Organisation, Status
Akzeptanzkriterien	ML-123648 , ML-123649 , ML-123650 , ML-132585

In der Laufzeitsicht sind die Interaktionen zwischen den Komponenten, die durch den Anwendungsfall genutzt werden, dargestellt. Für den Anwendungsfall wird die erfolgreiche Authentifizierung der Organisation mit Hilfe des Anwendungsfalls "*AF_10103 - Authentisieren einer Organisation am TI-Messenger-Dienst*" vorausgesetzt. Die Komponente Messenger-Service für die Organisation wird im Verlauf des Anwendungsfalles zu einem späteren Zeitpunkt erstellt.

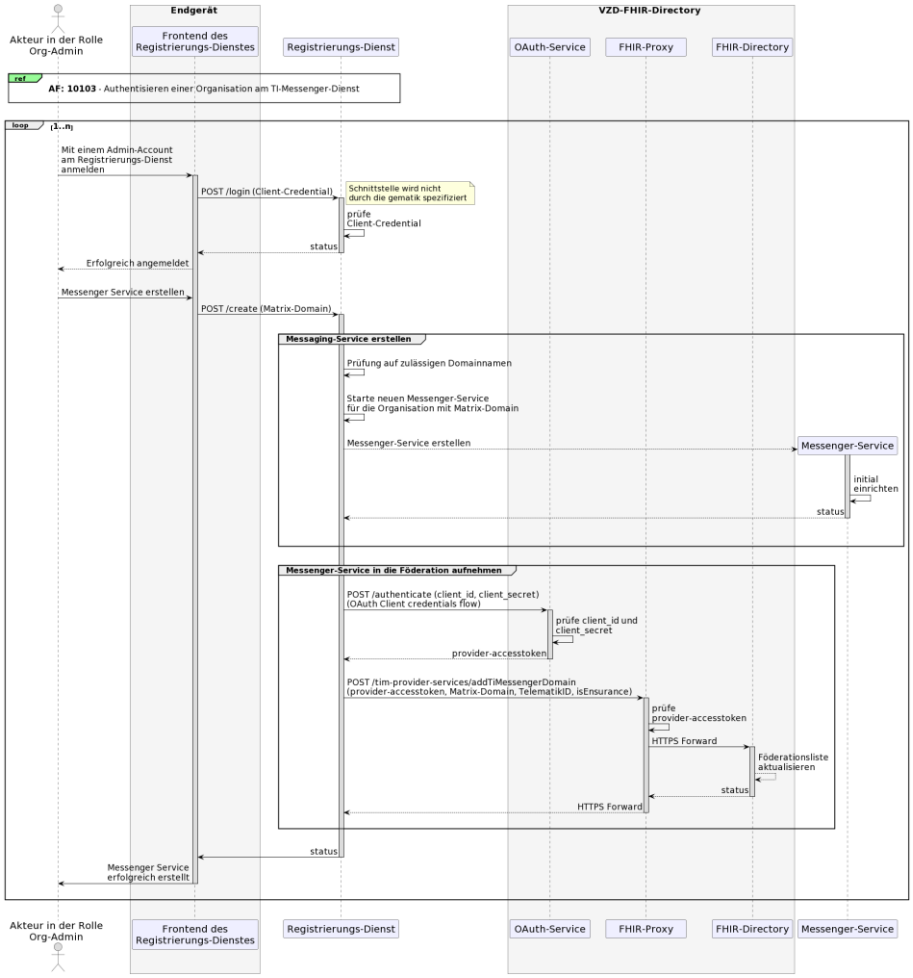


Abbildung 11: Laufzeitsicht - Bereitstellung eines Messenger-Service für eine Organisation

[<=]

Akzeptanzkriterien für den Anwendungsfall: Bereitstellung eines Messenger-Service für eine Organisation (AF_10060)

ML-123648 **- AF_10060 - Messenger-Service bereitstellen nur als Akteur in der Rolle Org-Admin**
Nur ein Akteur in der Rolle "Org-Admin" darf einen Messenger-Service bereitstellen.
[<=]

ML-123649 **- AF_10060 - Messenger-Service wurde erzeugt**
Ein neuer Messenger-Service wurde mit dem gewählten Domainbezeichner erzeugt.
[<=]

ML-123650 **- AF_10060 - Messenger-Service im VZD-FHIR-Directory existiert**
Für den erzeugten Messenger-Service wurde ein neuer Eintrag im VZD-FHIR-Directory angelegt
[<=]

ML-132585 **- AF_10060 - TI-M Rohdatenerfassung und -lieferung**
Die Rohdaten wurden entsprechend der Rohdatendefinition gemäß [gemSpec_TI-Messenger-FD#Betrieb] für den TI-Messenger-Fachdienst erfolgreich erfasst und an die definierte Schnittstelle der Rohdatenerfassung versendet.**[<=]**

6.3 AF - Organisationsressourcen im Verzeichnisdienst hinzufügen

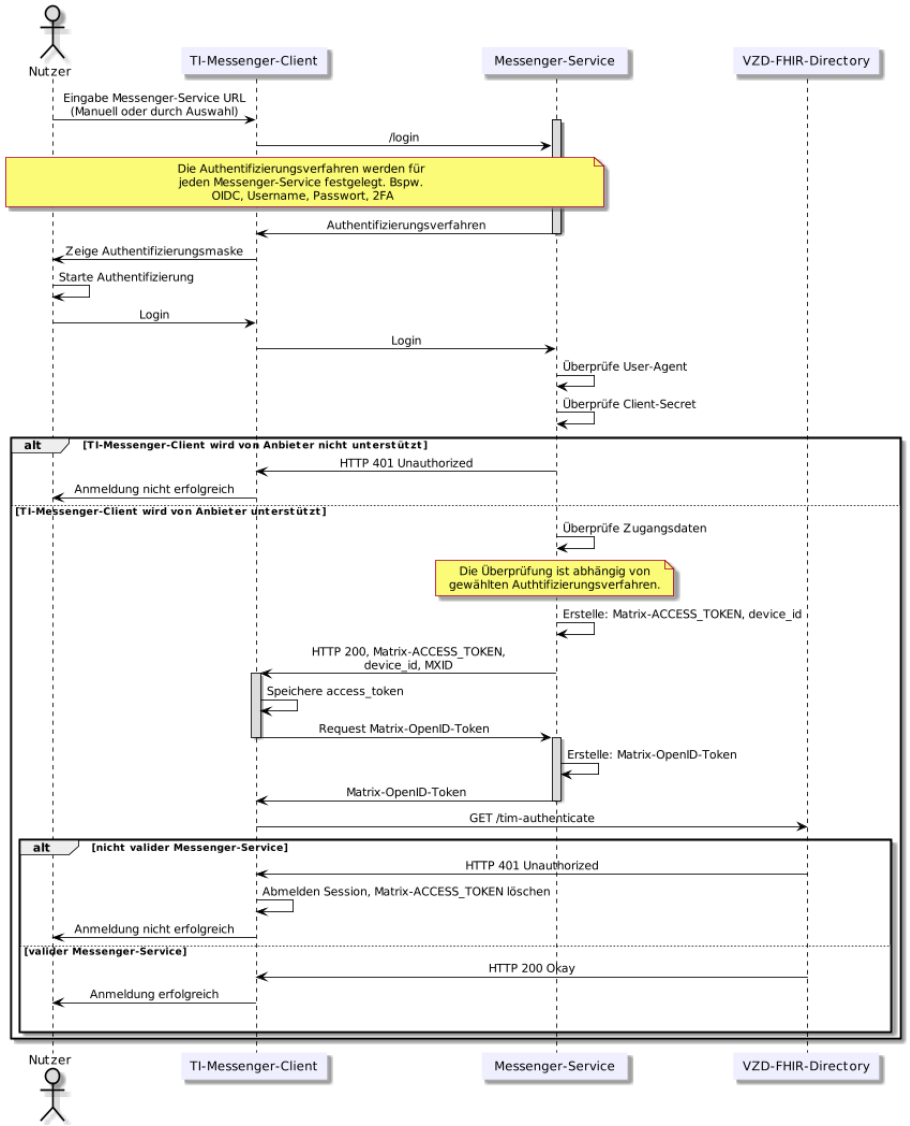
AF_10059 **- Organisationsressourcen im Verzeichnisdienst hinzufügen**
Mit diesem Anwendungsfall macht ein Akteur in der Rolle "Org-Admin" Akteure seiner Organisation im TI-Messenger-Dienst für andere Akteure auffindbar und erreichbar. Dafür werden FHIR-Ressourcen mit ihrer jeweiligen MXID im Organisationsverzeichnis (*HealthcareService*) des VZD-FHIR-Directory hinterlegt. Organisationen KÖNNEN mehrere FHIR-Ressourcen pro Organisation administrieren und somit eingehende Kommunikationsprozesse organisatorisch und thematisch strukturieren.

Tabelle 10: AF - Organisationsressourcen im Verzeichnisdienst hinzufügen

AF_10059	Organisationsressourcen im Verzeichnisdienst hinzufügen
Akteur	Beauftragter Mitarbeiter einer Organisation in der Rolle "Org-Admin"
Auslöser	Der Administrator der Organisation (Org-Admin) möchte seine Organisation erreichbar machen indem die MXIDs der Akteure der Organisation im VZD-FHIR-Directory hinterlegt werden.
Komponenten	• TI-Messenger-Client (mit erweiterter Org-Admin Funktionalität), • Authenticator des IDP-Dienst, • IDP-Dienst, • Auth-Service, • FHIR-Proxy, • FHIR-Directory.

Vorbedingungen	1. Für die Organisation wurde ein Messenger-Service bereitgestellt und eine FHIR-Ressource im VZD-FHIR-Directory erzeugt. 2. Der Administrator der Organisation verfügt über einen TI-Messenger-Client (mit erweiterter Org-Admin Funktionalität). 3. Das VZD-FHIR-Directory ist bei einem zuständigen IDP-Dienst registriert. 4. Der Administrator der Organisation kann sich an einem zuständigen IDP-Dienst authentisieren.
Eingangsdaten	SMC-B, FHIR-Organisations-Ressourcen
Ergebnis	FHIR-Organisations-Ressourcen aktualisiert, Status
Ausgangsdaten	Aktualisierte VZD-FHIR-Directory-Datensätze
Akzeptanzkriterien	ML-123626 , ML-123627 , ML-132586

In der Laufzeitsicht sind die Interaktionen zwischen den Komponenten, die durch den Anwendungsfall genutzt werden, dargestellt.



Hierbei handelt es sich um eine **vereinfachte Laufzeitansicht** in der zum Beispiel die TLS-Terminierung am FHIR-Proxy auf Grund der Übersichtlichkeit nicht berücksichtigt wurde.

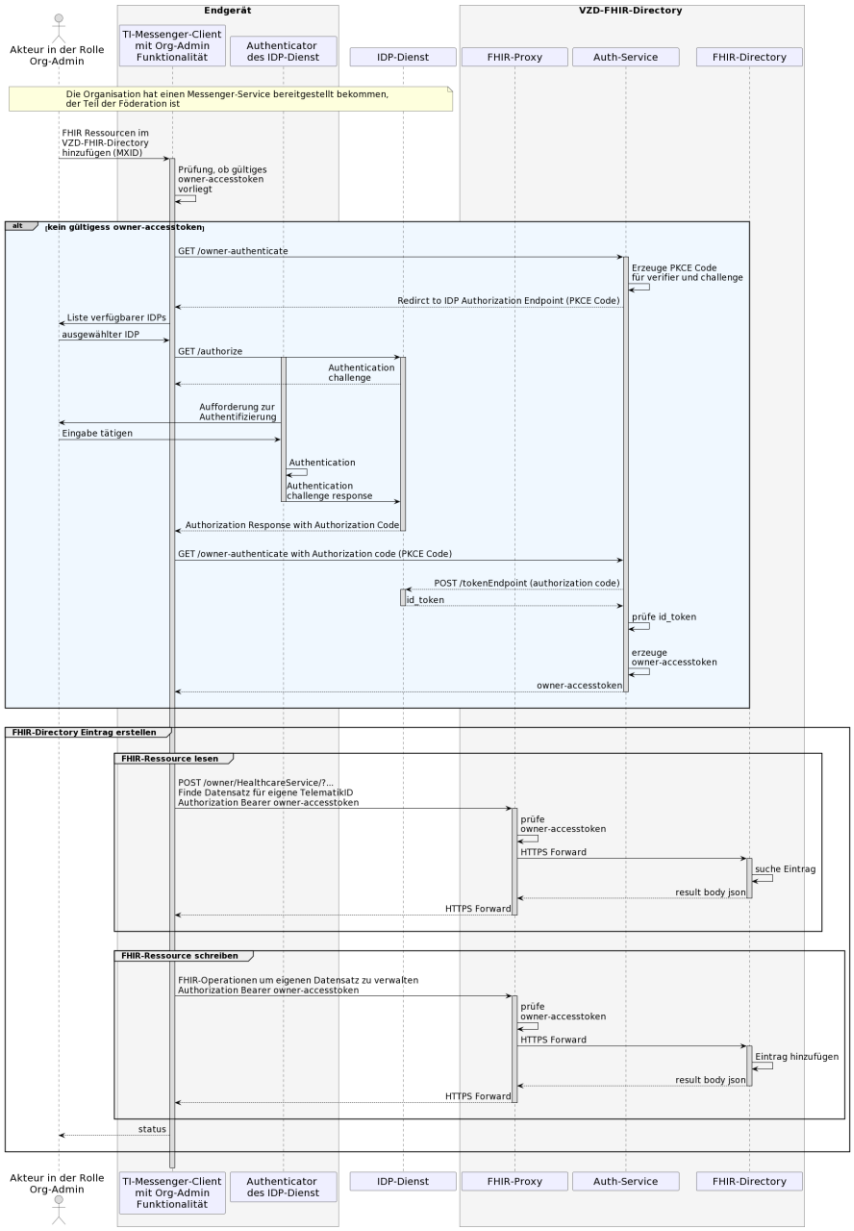


Abbildung 12: Laufzeitsicht - ~~Anmeldung eines Nutzers am Messenger-Service~~ Organisationsressourcen im Verzeichnisdienst hinzufügen

[<=]

Akzeptanzkriterien für den Anwendungsfall: ~~Anmeldung eines Nutzers am Messenger-Service~~ Organisationsressourcen im Verzeichnisdienst hinzufügen (AF_~~10057)~~10059)

ML-123627 **- AF_10059 - Organisationsressourcen im VZD-FHIR-Directory hinzufügen**
Nach erfolgreicher Authentisierung an einem zuständigen IDP-Dienst als Administrator einer Organisation kann der Akteur in der Rolle "Org-Admin" die MXID eines Akteurs seiner Organisation in den *HealthcareService* in einen *Endpoint* eintragen und Unterstrukturen für die Organisation anlegen. Der Akteur in der Rolle "Org-Admin" wird über den Erfolg der Operation informiert.
[<=]

ML-123626 **- AF_10059 - Änderungen nur für eigene Organization-FHIR-Datensätze**
Der Akteur in der "RolleOrg-Admin" darf nur FHIR-Ressourcen seiner eigenen Organisation (inklusive der Unterstrukturen) ändern. Ein Zugriff auf FHIR-Ressourcen, die nicht zu der eigenen Organisation gehören, MUSS unterbunden werden.
[<=]

ML-132586 **- AF_10059 - TI-M Rohdatenerfassung und -lieferung**
Die Rohdaten wurden entsprechend der Rohdatendefinition gemäß [gemSpec_TI-Messenger-FD#Betrieb] für den TI-Messenger-Fachdienst erfolgreich erfasst und an die definierte Schnittstelle der Rohdatenerfassung versendet.**[<=]**

6.4 AF - Anmeldung eines Akteurs am Messenger-Service

AF_10057 **- Anmeldung eines Akteurs am Messenger-Service**
Mit diesem Anwendungsfall meldet sich ein Akteur an einem in der TI-Föderation zuständigen Messenger-Service an und registriert seinen TI-Messenger-Client als Endgerät. Der Akteur MUSS die Matrix-Domain des gewünschten Messenger-Service direkt im TI-Messenger-Client eingeben können. Die Eingabe KANN dabei automatisiert oder durch andere Hilfsmittel wie beispielweise durch ein QR-Code-Scan unterstützt werden. Die Authentifizierung erfolgt hierbei nach den Vorgaben der jeweiligen Organisation. Nach der erfolgreichen Anmeldung eines Akteurs am Messenger-Service KÖNNEN die von ihm angebotenen Dienste verwendet werden.

Tabelle 11: AF - Anmeldung eines Akteurs am Messenger-Service

AF_10057	Anmeldung eines Akteurs am Messenger-Service
Akteur	Leistungserbringer, Mitarbeiter einer Organisation im Gesundheitswesen in der "Rolle User / User-HBA"
Auslöser	Ein Akteur möchte sich mit seinem TI-Messenger-Client bei einem Messenger-Service anmelden.

Komponenten	• TI-Messenger-Client, • Messenger-Proxy, • Messenger-Homeserver, • FHIR-Proxy, • FHIR-Directory.
Vorbedingungen	1. Der Akteur verfügt über einen vom Anbieter unterstützen TI-Messenger-Client. 2. Der Akteur kennt die URL des Messenger-Services oder die URL ist bereits in seinem TI-Messenger-Client konfiguriert. 3. Der Akteur kann sich durch ein beim Matrix-Homeserver unterstütztes Authentisierungsverfahren identifizieren. Wird durch die Organisation ein eigenes Authentifizierungsverfahren verwendet MUSS eine Anbindung an den Matrix-Homeserver erfolgt sein. 4. Der verwendete Matrix-Homeserver ist in die Föderation integriert (valider Messenger-Service).
Eingangsdaten	URL des Matrix-Homeservers
Ergebnis	Es wurde ein TI-Messenger Account für einen Akteur in der Rolle "User / User-HBA" erzeugt.
Ausgangsdaten	`Matrix-ACCESS_TOKEN, MXID, device_id` Status
Akzeptanzkriterien	ML-123571, ML-123576 , ML-123575 , ML-129870, ML-132587

In der Laufzeitsicht sind die Interaktionen zwischen den Komponenten, die durch den Anwendungsfall genutzt werden, dargestellt. In dieser wird der Prozess einer Anmeldung eines Akteurs an einem Messenger-Service dargestellt. Sollte ein Akteur noch nicht an einem Matrix-Homeserver registriert sein, dann wird zunächst eine Registrierung des Akteurs mit der Operation `POST /_matrix/client/register` durchgeführt. Der Ablauf der Registrierung ist analog dem des Login-Verfahrens.

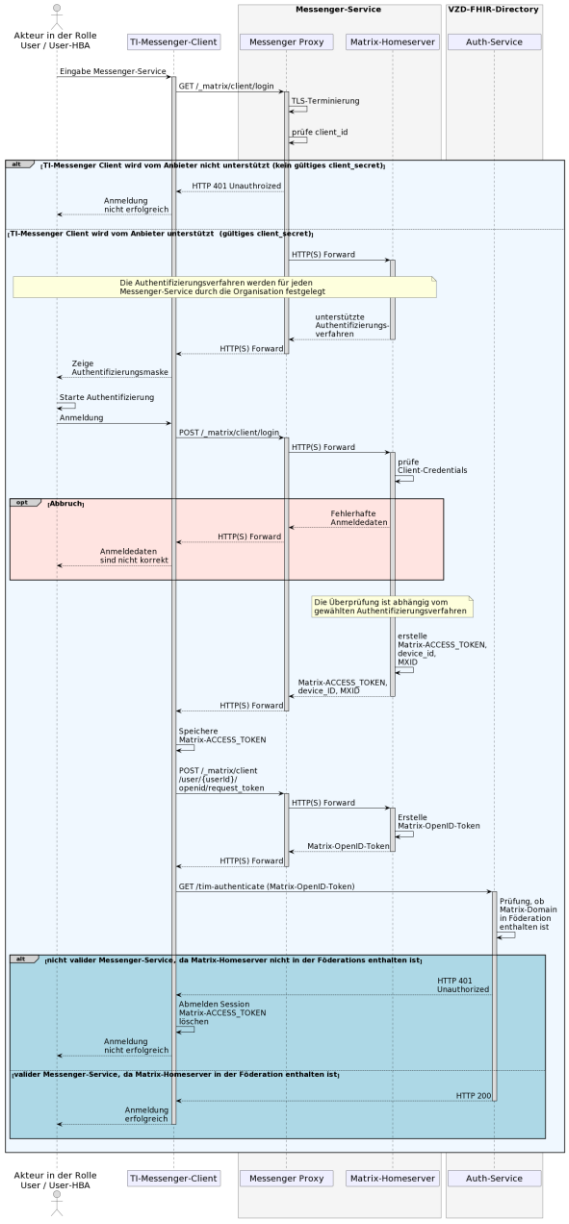


Abbildung 13: Laufzeitsicht - Anmeldung eines Akteurs am Messenger-Service

[<=]

Akzeptanzkriterien für den Anwendungsfall: Anmeldung eines Akteurs am Messenger-Service (AF_10057)

ML-123571 - ~~**AF_10057 - Nutzer kann sich erfolgreich an einem gültigen Messenger-Service anmelden**~~**AF_10057 - Akteur kann sich erfolgreich an einem gültigen Messenger-Service anmelden**
Ein ~~Nutzer kann~~Akteur hat sich erfolgreich an einem gültigen Messenger-Service ~~anmelden, wenn er sich~~angemeldet und mit einem zugelassenen ~~Authentisierungsverfahren~~Authentifizierungsverfahren erfolgreich authentisiert. Es MUSS sichergestellt werden, dass die Anmeldung an Messenger-Services, die nicht Teil der Föderation sind, nicht möglich ist.
[<=]

ML-123576 - ~~**AF_10057 - Der Messenger-Service stellt dem TI-Messenger-Client ein Access-Token aus**~~**AF_10057 - Der Messenger-Service stellt dem TI-Messenger-Client ein Access-Token aus**
~~Bei der erfolgreichen~~Nach erfolgreicher Anmeldung ~~stellt~~hat der Messenger-Service dem TI-Messenger-Client ein Matrix-ACCESS_TOKEN ausgestellt.
[<=~~Access Token aus.~~
~~**[<=**~~**]**

ML-123575 - ~~**AF_10057 - Speicherung Access-Token durch TI-Messenger-Client**~~**AF_10057 - Speicherung Access-Token durch TI-Messenger-Client**
Der TI-Messenger-Client speichert das ihm übergebene ~~Access~~ Matrix-ACCESS_TOKEN zur Verwendung in den folgenden Anwendungsfällen.
[<=]

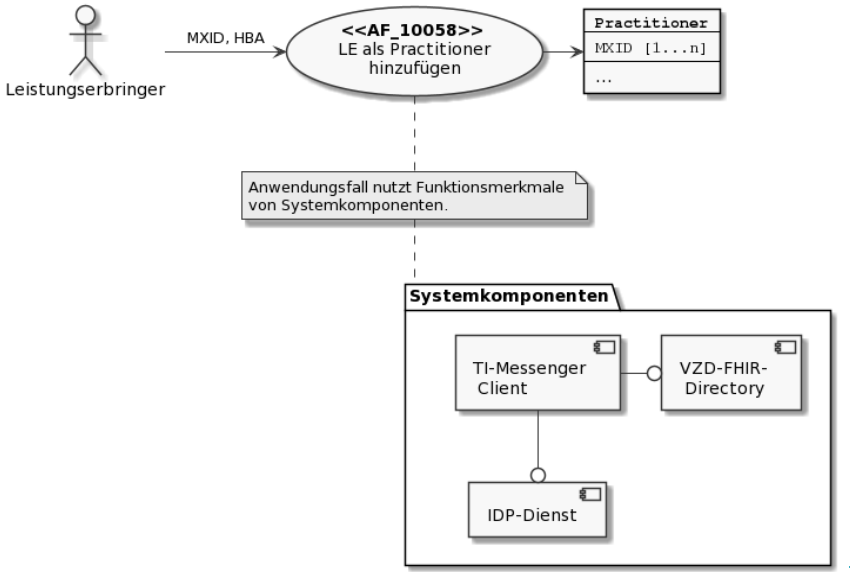
~~AF – Leistungserbringer als Practitioner~~
ML-129870 **- AF_10057 - Akteur kann sich an einen nicht validen Messenger-Service nicht anmelden**
Ein Akteur kann sich nicht bei einem öffentlichen Matrix-Homeserver anmelden, der nicht in die TI-Föderation integriert ist.
[<=]

ML-132587 **- AF_10057 - TI-M Rohdatenerfassung und -lieferung**
Die Rohdaten wurden entsprechend der Rohdatendefinition gemäß [gemSpec_TI-Messenger-FD#Betrieb] für den TI-Messenger-Fachdienst erfolgreich erfasst und an die definierte Schnittstelle der Rohdatenerfassung versendet.**[<=]**

~~6.2~~6.5 AF - Akteur (User-HBA) im Verzeichnisdienst hinzufügen

AF_10058 - ~~**Leistungserbringer als Practitioner hinzufügen**~~**Akteur (User-HBA) im Verzeichnisdienst hinzufügen**
Mit diesem Anwendungsfall ~~trägt~~wird ein ~~Leistungserbringer~~Akteur in der Rolle "User-HBA" für andere Akteure anderer Messenger-Services auffindbar und erreichbar. Dafür werden FHIR-Ressourcen mit ~~HBA seine~~ihrer jeweiligen MXID ~~in seinen Practitioner-Datensatz auf dem~~ im Personenverzeichnis (*PractitionerRole*) des VZD-FHIR-Directory ~~ein. Danach hat der Leistungserbringer~~hinterlegt. Zusätzlich besteht die Möglichkeit~~, mit anderen verifizierten LE in Kontakt zu treten und ist für andere verifizierte LE über das~~

~~VZD-FHIR-Directory erreichbar.~~ die Sichtbarkeit für andere Akteure einzuschränken. Dieser ~~Flow SOLL~~ Anwendungsfall KANN direkt mit dem initialen Anmeldevorgang eines Akteurs am Messenger Service (siehe Anwendungsfall: "AF_10057 - Anmeldung eines Akteurs am Messenger-Service") kombiniert werden. Hierfür wird der ~~LE~~Akteur in der Rolle "User-HBA" während des ~~Onboardings~~Anmeldevorgangs durch den TI-Messenger-Client gefragt, ob ~~es sich bei dem Nutzer um einen Leistungserbringer mit Zugriff auf HBA handelt. Zusätzlich KANN der LE angeben, ob er andere LE über das VZD-FHIR-Directory finden möchte und ob eine Sichtbarkeit gegenüber anderen LE gewünscht~~dieser im Besitz eines HBAs ist.



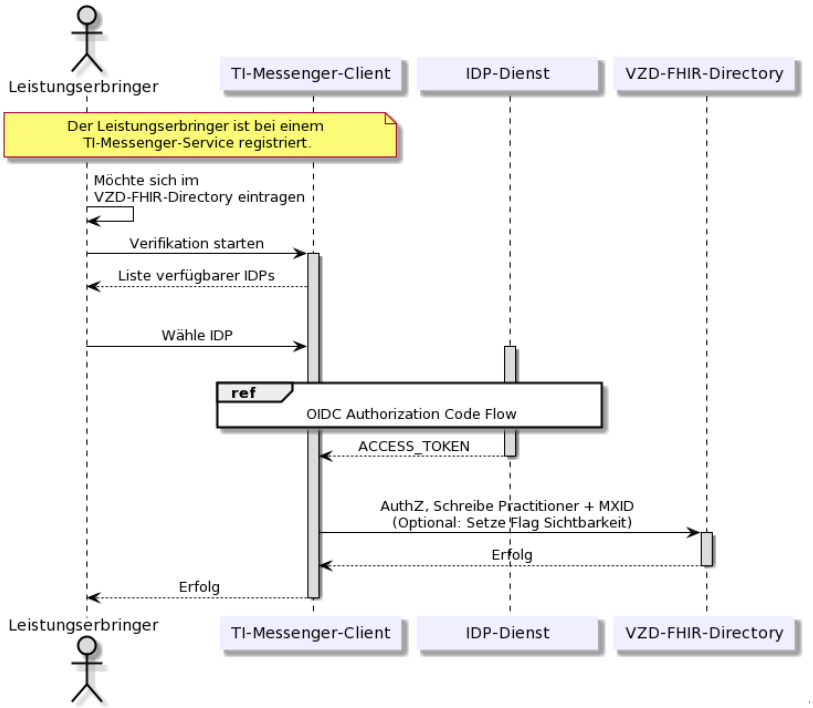
~~**Abbildung 6: Systemkomponenten des AF – Leistungserbringer als Practitioner hinzufügen**~~

Tabelle 12: AF - ~~Leistungserbringer als Practitioner~~Akteur (User-HBA) im Verzeichnisdienst hinzufügen

AF_10058	**~~Leistungserbringer als Practitioner~~Akteur (User-HBA) im Verzeichnisdienst hinzufügen**
Akteur	Leistungserbringer, Mitarbeiter einer Organisation im Gesundheitswesen in der Rolle "User-HBA"
Auslöser	~~Leistungserbringer~~Ein Akteur in der Rolle "User-HBA" möchte sich im Personenverzeichnis erreichbar machen, indem er seine MXID im seinen Practitioner-Datensatz ~~auf dem~~im VZD-FHIR-Directory ~~aktualisieren~~ hinterlegt.

Komponenten	• TI-Messenger-Client, • Authenticator des IDP-Dienst, ~~VZD~~ • IDP-Dienst, • FHIR-Proxy, • Auth-Service, • FHIR-Directory .
Vorbedingungen	~~1. Der LE verfügt über einen TI-Messenger-Client~~ ~~1. Der LE~~Akteur ist ~~beim Smartcard-IDP-Dienst der TI registriert.~~ 1. ~~Der LE ist als Nutzer im~~bei einem gültigen Messenger-Service angemeldet (siehe AF_10057). 2. Der Akteur verfügt über einen zugelassenen TI-Messenger-Client. ~~2.~~3. Das VZD-FHIR-Directory ist ~~beim Smartcard~~bei einem zuständigen IDP-Dienst registriert. ~~2. Der verwendete Matrix-Homeserver ist in die Föderation integriert.~~ ~~3.~~4. ~~Der LE~~Der Akteur kann sich am ~~(Practitioner) Smartcard~~ IDP-Dienst authentisieren.
Eingangsdaten	~~MXID des Leistungserbringers, HBA~~HBA, FHIR-Practitioner-Ressourcen
Ergebnis	~~MXID im Practitioner-Datensatz des Nutzers auf dem FHIR-Server eingetragen, (gemäß [gemSpec_VZD_FHIR_Directory])~~ FHIR-Practitioner-Ressourcen aktualisiert, Status
Ausgangsdaten	aktualisierter Practitioner-Datensatz
Akzeptanzkriterien	ML-123611, ML-123612 , ML-132588

In der Laufzeitsicht sind die Interaktionen zwischen den Komponenten, die durch den Anwendungsfall genutzt werden, dargestellt. ~~Für das zu benutzende Authentifizierungsverfahren gilt~~Hierbei handelt es sich um eine **vereinfachte Laufzeitansicht** in der zum Beispiel die ~~Spezifikation gemäß OpenID Connect. Das Verfahren OIDC wird im Anhang B beschrieben~~TLS-Terminierung am FHIR-Proxy auf Grund der Übersichtlichkeit nicht berücksichtigt wurde.


Leistungserbringer
TI-Messenger-Client
IDP-Dienst
VZD-FHIR-Directory
Der Leistungserbringer ist bei einem TI-Messenger-Service registriert.
Möchte sich im VZD-FHIR-Directory eintragen
Verifikation starten
Liste verfügbarer IDPs
Wähle IDP
ref
OIDC Authorization Code Flow
ACCESS_TOKEN
AuthZ, Schreibe Practitioner + MXID (Optional: Setze Flag Sichtbarkeit)
Erfolg
Erfolg
Leistungserbringer
TI-Messenger-Client
IDP-Dienst
VZD-FHIR-Directory

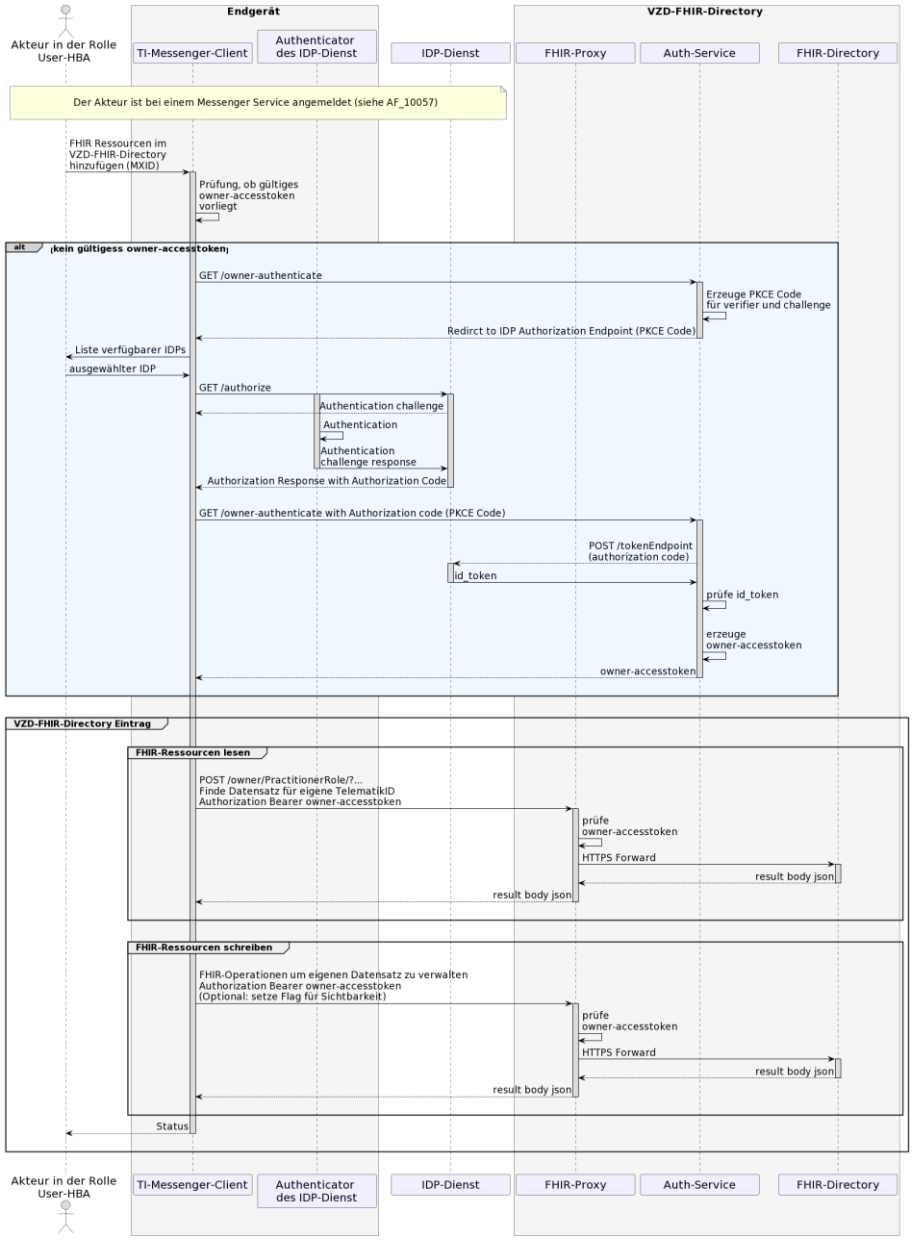


Abbildung 14: Laufzeitsicht - ~~LE als Practitioner~~ Akteur (User-HBA) im Verzeichnisdienst hinzufügen

[<=]

Akzeptanzkriterien für den Anwendungsfall: ~~LE als Practitioner~~Akteur (User-HBA) im Verzeichnisdienst hinzufügen (AF_10058)

ML-123612 **- ~~AF_10058 - LE als Practitioner hinzufügen~~AF_10058 - Akteur als Practitioner hinzufügen**
~~Nach erfolgreichen Authentisierung am IDP-Dienst wird~~Die MXID wurde in den Practitioner-FHIR-Datensatz ~~des authentifizierten Leistungserbringers die Matrix User URI~~ eingefügt und der ~~Leistungserbringer~~Akteur über den Erfolg informiert.
[<=]

ML-123611 **- AF_10058 - MXID-Eintrag nur für eigenen Practitioner-FHIR-Datensatz**
Der ~~Leistungserbringer~~Akteur in der Rolle "User-HBA" darf nur die eigene FHIR-Ressourcen ~~(AF_10037 - gemSpec_VZD_FHIR_Directory)~~ ändern.
[<=]

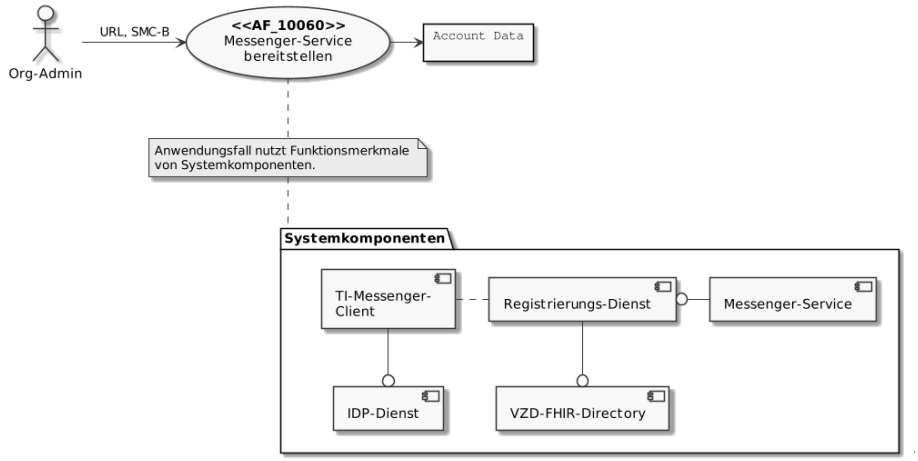
ML-132588 **- AF_10058 - TI-M Rohdatenerfassung und -lieferung**
Die Rohdaten wurden entsprechend der Rohdatendefinition gemäß [gemSpec_TI-Messenger-FD#Betrieb] für den TI-Messenger-Fachdienst erfolgreich erfasst und an die definierte Schnittstelle der Rohdatenerfassung versendet.**[<=]**

~~6.3~~6.6 AF - Föderationszugehörigkeit eines Messenger-Service ~~bereitstellen~~prüfen

AF_10064 **- Föderationszugehörigkeit eines Messenger-Service prüfen**
Dieser Anwendungsfall prüft, ob ein Messenger-Service zugehörig zur TI-Messenger-Föderation ist und gilt für alle Anwendungsfälle, welche die Matrix-Domain eines anderen Messenger-Services überprüfen müssen. Für die Prüfung der Zugehörigkeit der Matrix-Domain zur TI-Messenger-Föderation, verwendet der Messenger-Proxy
eine Föderationsliste die vom Registrierungs-Dienst seines TI-Messenger-Fachdienstes bereitgestellt wird. Die Speicherdauer der Föderationsliste des Messenger-Proxies ist limitiert. Die Aktualisierung der Föderationsliste erfolgt wie in Anhang B 8.2 "*Aktualisierung der Föderationsliste*" beschrieben.

Tabelle 13: Föderationszugehörigkeit eines

~~**AF_10060 - Messenger-Service bereitstellen**~~
~~Messenger-Services werden dezentral für Organisationen des Gesundheitswesens bereitgestellt. Nutzer einer Organisation melden sich an Messenger-Services an, um am TI-Messenger-Dienst teilnehmen zu können. Für eine schnelle Adaption des TI-Messenger-Dienstes MUSS eine schnelle Bereitstellung von Messenger-Services gewährleistet sein. TI-Messenger-Anbieter sind daher verpflichtet, Prozesse zu etablieren, damit Messenger-Services für Organisationen schnell und ggf. automatisiert bereitgestellt werden. Dazu MUSS der Registrierungs-Dienst mit einem Frontend oder Schnittstellen, welche in TI-Messenger-Clients oder anderen Services eingebunden werden in der Lage sein eine SMC-B zu validieren und anschließend einen Messenger-Service für die Organisation bereitzustellen.~~



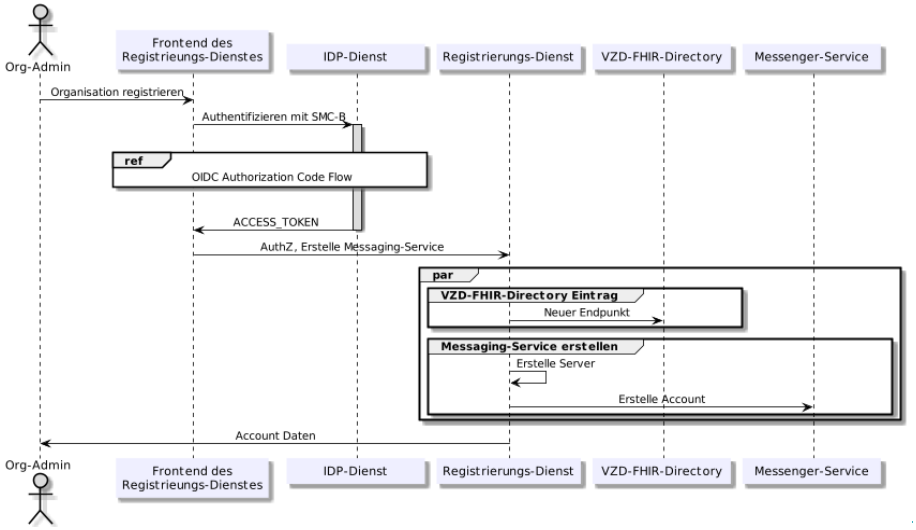
~~Abbildung 8: Systemkomponenten des AF~~ **Messenger-Service** ~~bereitstellen~~prüfen

~~Tabelle 5: AF – Messenger-Service bereitstellen~~

AF_~~10060~~10064	Föderationszugehörigkeit eines Messenger-Service ~~bereitstellen~~prüfen
Akteur	~~Beauftragter Mitarbeiter der Organisation (z. B. *Org-Admin*)~~
Auslöser	~~Eine Organisation des deutschen Gesundheitswesen möchte am TI~~Der Messenger~~-Dienst teilnehmen~~-Proxy empfängt einen `Invite-Event` und ~~benötigt~~MUSS die ~~Bereitstellung eins~~ im Request enthaltenen MXIDs auf Domain-Zugehörigkeit zur TI-Messenger-~~Service~~Föderation prüfen.
Komponenten	• ~~TI-Messenger-Client~~ ~~IDP-Dienst~~ ~~Registrierungs-Dienst~~ ~~VZD-FHIR-Directory~~ ~~Messenger-Service~~Messenger-Proxy, • Matrix-Homeserver.
~~Vorbedingung~~Vorbedingungen	~~1. Der Nutzer verfügt über ein Frontend (innerhalb oder außerhalb eines TI-Messenger-Clients) für die Kommunikation mit dem Registrierungs-Dienst~~ ~~1. Das verwendete Frontend des Registrierungs-Dienst ist beim Smartcard-IDP-Dienst registriert.~~ ~~Der verwendete Registrierungs-Dienst kann sich beim VZD-FHIR-Directory-Server für Schreibzugriffe authentifizieren.~~keine
Eingangsdaten	~~Identität der Organisation, SMC-B~~`Invite-Event`
Ergebnis	~~1. Die Domain des neuen Messenger-Services wurde als Endpunkt im VZD-FHIR-Server eingetragen.~~ ~~1.~~ Der Messenger-Proxy ermittelt mittels der Föderationsliste, ob die Matrix-Domain des anderen Messenger-Service ~~für die Organisation wurde erstellt.~~ ~~Für den beauftragten Mitarbeiter der Organisation (*Org-Admin*) wurde ein Account auf dem~~ Teil der TI-Messenger-~~Service mit Administrationsrechten erstellt~~Föderation ist.
Ausgangsdaten	~~Messenger-Service der Organisation, Account-Daten~~Status vom Matrix-Homeserver und Weiterleitung

Akzeptanzkriterien	ML-~~123648~~ , 123672 , ML-~~123649~~ , 123891 , ML-~~123650~~ , 123893 , ML-~~123651~~132589

~~Für das zu benutzende Authentifizierungsverfahren gilt die Spezifikation gemäß OpenID-Connect. Das Verfahren OIDC wird im Anhang B beschrieben.~~



~~Abbildung~~

In der Laufzeitsicht sind die Interaktionen zwischen den Komponenten, die durch den Anwendungsfall genutzt werden, dargestellt. Das auslösende Matrix-Event am Messenger-Proxy wird in der folgenden Abbildung nicht gezeigt. Die Aktualisierung der Föderationsliste ist in Anhang B "Aktualisierung der Föderationsliste" hinreichend beschrieben.

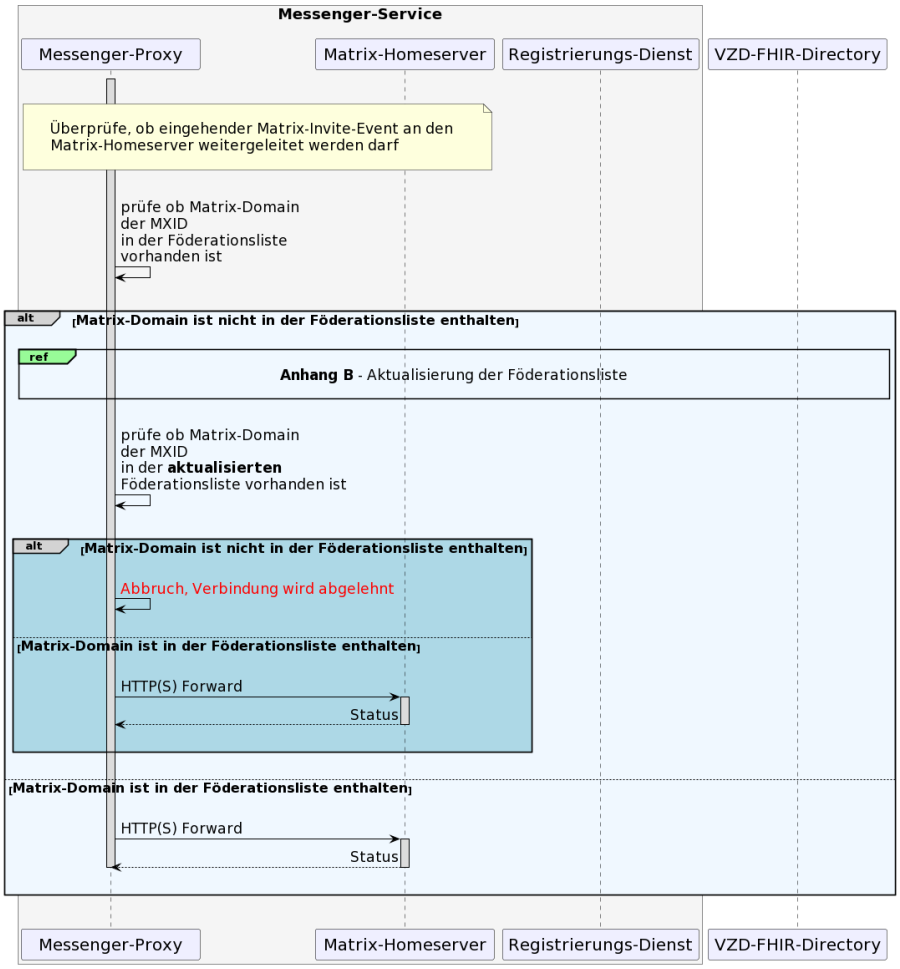


Abbildung 15: Laufzeitsicht - Föderationszugehörigkeit eines Messenger-Service ~~automatisch bereitstellen~~prüfen

~~[<=]~~[<=]

Akzeptanzkriterien für den Anwendungsfall: Föderationszugehörigkeit eines~~Messenger-Service bereitstellen (AF_10060)~~

~~ML-123648 – AF_10060 –~~ Messenger-Service ~~bereitstellen nur als Nutzer Rolle Org-Admin~~prüfen (AF_10064)

ML-123672 **- AF_10064 - Föderationsliste vom VZD-FHIR-Directory abrufen**
Der Registrierungs-Dienst des TI-Messenger-Fachdienstes MUSS die Föderationsliste erfolgreich vom FHIR-Proxy des VZD-FHIR-Directory abrufen.
[<=]

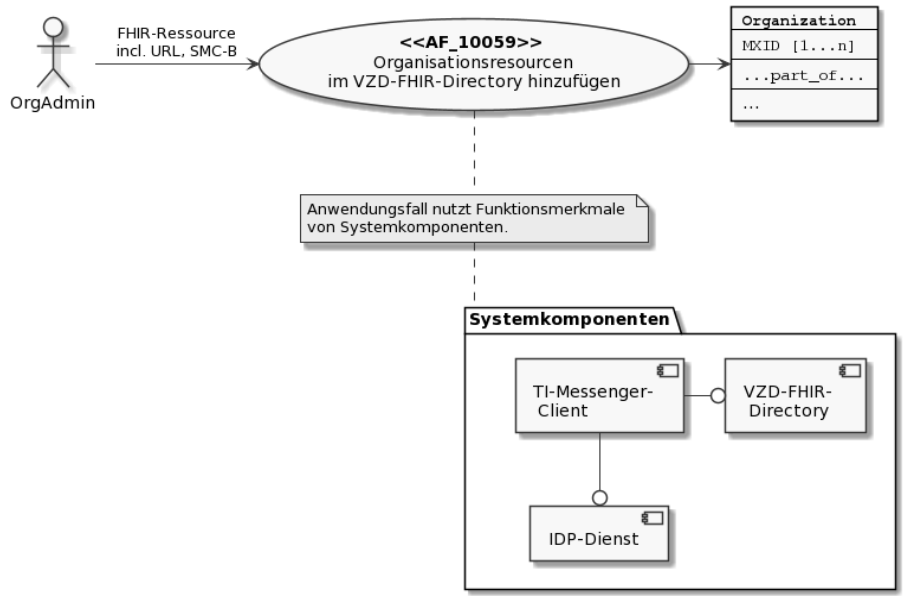
ML-123893 **- AF_10064 - Aktualität - Föderationsliste Messenger-Proxy**
Es MUSS sichergestellt werden, dass die Föderationsliste des Messenger-Proxy aktuell ist. ~~Nur ein Nutzer in~~ Dafür MUSS der Messenger-Proxy mindestens einmal täglich eine aktuelle Liste bei dem Registrierungs-Dienst anfordern.
[<=]

ML-123891 **- AF_10064 - Matrix-Domain Teil der Föderationsliste & Aktualitätscheck**
Es MUSS sichergestellt werden, dass der Registrierungs-Dienst die Föderationsliste auf Aktualität überprüft, bevor eine aktualisierte Liste durch den Messenger-Proxy abgerufen werden kann. Ebenfalls MUSS sichergestellt werden, dass der Messenger-Proxy tatsächlich überprüft, ob die Matrix-Domain des anderen ~~Rolle *Org-Admin* darf einen~~ Messenger-Service ~~automatisch bereitstellen. Es~~ Teil der Föderationsliste ist.
[<= ~~eine SMC-B-Karte für die Erstellung notwendig.~~
~~**[<=**~~**]**

~~**ML-123649 - AF_10060 - Messenger-Service wurde erzeugt**~~
~~Ein neuer Messenger-Service wurde mit dem gewählten Domainbezeichner erzeugt.~~
~~**[<=]**~~
~~**ML-123650 - AF_10060 - Messenger-Service im VZD-FHIR-Directory existiert**~~
~~Für den erzeugten Messenger-Service wurde ein neuer Eintrag im VZD-FHIR-Directory angelegt~~
~~**[<=]**~~
~~**ML-123651 - AF_10060 - Org-Admin Administrator-Account vorhanden**~~
~~Der Nutzer in der Rolle *Org-Admin* der Organisation hat einen Administrator-Account auf dem Messenger-Service seiner Organisation.~~
~~**[<=]**~~

~~6.4 AF - Organisationsressourcen im VZD-FHIR-Directory hinzufügen~~

~~**AF_10059 - Organisationsressourcen im VZD-FHIR-Directory hinzufügen**~~
~~Mit diesem Anwendungsfall haben Organisationen die Möglichkeit FHIR-Ressourcen mit MXIDs zu hinterlegen und damit für Nutzer des TI-Messenger-Dienstes kontaktierbar zu machen. Somit wird es ermöglicht, dass Nutzer Anfragen an Organisationen stellen können. Die FHIR-Ressourcen können organisatorisch und thematisch strukturiert werden.~~



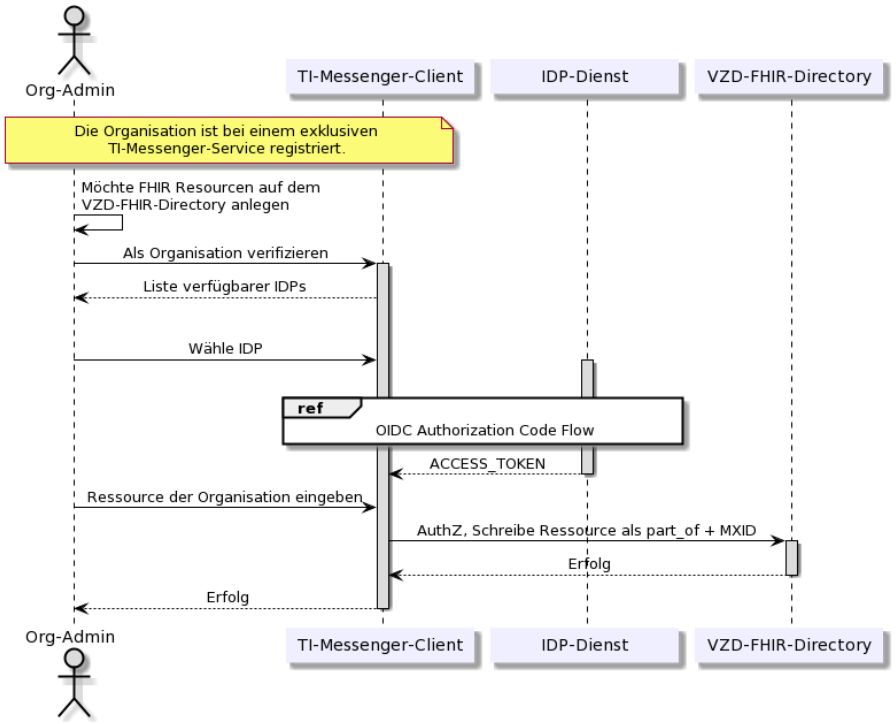
~~**Abbildung 10: Systemkomponenten des AF „Organisationsressourcen im VZD-FHIR-Directory hinzufügen**~~

~~**Tabelle 6 AF „Organisationsressourcen im VZD-FHIR-Directory hinzufügen**~~

~~AF_10059~~	~~Organisationsressourcen im VZD-FHIR-Directory hinzufügen~~
~~Akteur~~	~~Administrator der Organisation (In der Rolle *Org-Admin*)~~
~~Auslöser~~	~~Der Administrator der Organisation (*Org-Admin*) möchte seine Organisation erreichbar machen indem die Nutzer der Organisation als MXID im VZD-FHIR-Directory hinterlegt werden.~~
~~Komponenten~~	~~TI-Messenger-Client (mit erweiterter *Org-Admin* Funktionalität), IDP-Dienst, VZD-FHIR-Directory~~
~~Vorbedingungen~~	~~1. Der Administrator der Organisation verfügt über einen TI-Messenger-Client (mit erweiterter *Org-Admin* Funktionalität).~~ ~~2. Der VZD-FHIR-Directory-Server ist beim Smartcard-IDP-Dienst registriert.~~ ~~3. Der Administrator der Organisation kann sich am Smartcard-IDP-Dienst authentisieren (Zugriff SMC-B).~~

	4. Für die Organisation wurde ein Messenger-Service bereitgestellt und eine Ressource im VZD-FHIR-Directory angelegt. 5. Bei stationärer SMC-B erneute erfolgreiche PIN-Eingabe durch den Administrator der Organisation in der Rolle *Org-Admin*.
Eingangsdaten	FHIR-Organisations-Ressource mit Matrix-URL als Telecom, SMC-B
Ergebnis	Ressource `Organization` (als "part_of" Beziehung) und MXID im FHIR-Server eingetragen
Ausgangsdaten	Aktualisierte VZD-FHIR-Directory-Datensätze
Akzeptanzkriterien	ML-123626 , ML-123627

In der Laufzeitsicht sind die Interaktionen zwischen den Komponenten, die durch den Anwendungsfall genutzt werden, dargestellt. Das Verfahren OIDC wird im Anhang B beschrieben.



~~**Abbildung 11: Laufzeitsicht – Organisations-Ressourcen im VZD-FHIR-Directory hinzufügen**~~

~~**[<=]**~~

ML-132589 **- AF_10064 - TI-M Rohdatenerfassung und -lieferung**
Die Rohdaten wurden entsprechend der Rohdatendefinition gemäß [gemSpec_TI-Messenger-FD#Betrieb] für den TI-Messenger-Fachdienst erfolgreich erfasst und an die definierte Schnittstelle der Rohdatenerfassung versendet.**[<=]**

6.7 AF - Einladung von Akteuren innerhalb einer Organisation

AF_10104 **- Einladung von Akteuren innerhalb einer Organisation**
In diesem Anwendungsfall wird ein Akteur der zu einer gemeinsamen Organisation gehört in einen Raum eingeladen um Aktionen auszuführen. Für die Suche von Akteuren innerhalb einer gemeinsamen Organisation durchsucht ein TI-Messenger-Client das Nutzerverzeichnis seiner Organisation auf dem Matrix-Homeserver. In diesem Anwendungsfall prüft der Messenger-Proxy ob die im `Invite-Event` enthaltenen Matrix-Domains Teil der TI-Föderation sind (siehe Berechtigungskonzept - Stufe 1). Ist dies der Fall erfolgt die Weiterleitung an den zugehörigen Matrix-Homeserver. Dieser prüft ob die

beteiligten Akteure bei ihm registriert sind. Ist dies nicht der Fall, handelt es sich bei dem einzuladenden Akteur nicht um einen Akteur innerhalb der Organisation und das `Invite-Event` wird an den Matrix- Homeserver des einzuladenden Akteurs weitergeleitet. Der Anwendungsfall "AF_10061 - *Einladung von Akteuren außerhalb einer Organisation*" zeigt den sich daraus ergebenden Verlauf.

Tabelle 14: Einladung von Akteuren innerhalb einer Organisation

AF_10104	Einladung von Akteuren innerhalb einer Organisation
Akteur	Leistungserbringer, Mitarbeiter einer Organisation im Gesundheitswesen in der Rolle "User / User-HBA"
Auslöser	Akteur A möchte Akteur B seiner Organisation in einen gemeinsamen Raum einladen.
Komponenten	• TI-Messenger Client A + B, • Messenger-Proxy, • Matrix-Homeserver, • Push-Gateway.
Vorbedingungen	1. Die Akteure sind am selben Messenger-Service angemeldet. 2. Jeder Akteur hat einen zugelassenen TI-Messenger-Client. 3. Ein Chatraum wurde durch den Einladenden eingerichtet.
Eingangsdaten	`Invite-Event`
Ergebnis	Akteur A und Akteur B sind beide in einem gemeinsamen Chatraum. Optional erfolgt eine Benachrichtigung an Akteur B über die Einladung in den Chatraum.
Ausgangsdaten	Status
Akzeptanzkriterien	ML-123896, ML-129415, ML-129414 , ML-132590

In der Laufzeitsicht sind die Interaktionen zwischen den Komponenten, die durch den Anwendungsfall genutzt werden, dargestellt. Der für die zukünftige Kommunikation genutzte Chatraum wurde durch den einladenden Akteur bereits erstellt. Die folgende Darstellung zeigt lediglich die Einladung zwischen zwei Akteuren. Weitere Akteure können unabhängig von dieser Laufzeitsicht eingeladen werden (Hinweis: Group-Messaging). Für die vereinfachte Darstellung wird vorausgesetzt, dass die TI-Messenger-Clients der beteiligten Akteure online sind. Ebenfalls wird davon ausgegangen, dass beide Akteure am selben Matrix-Homeserver registriert sind.

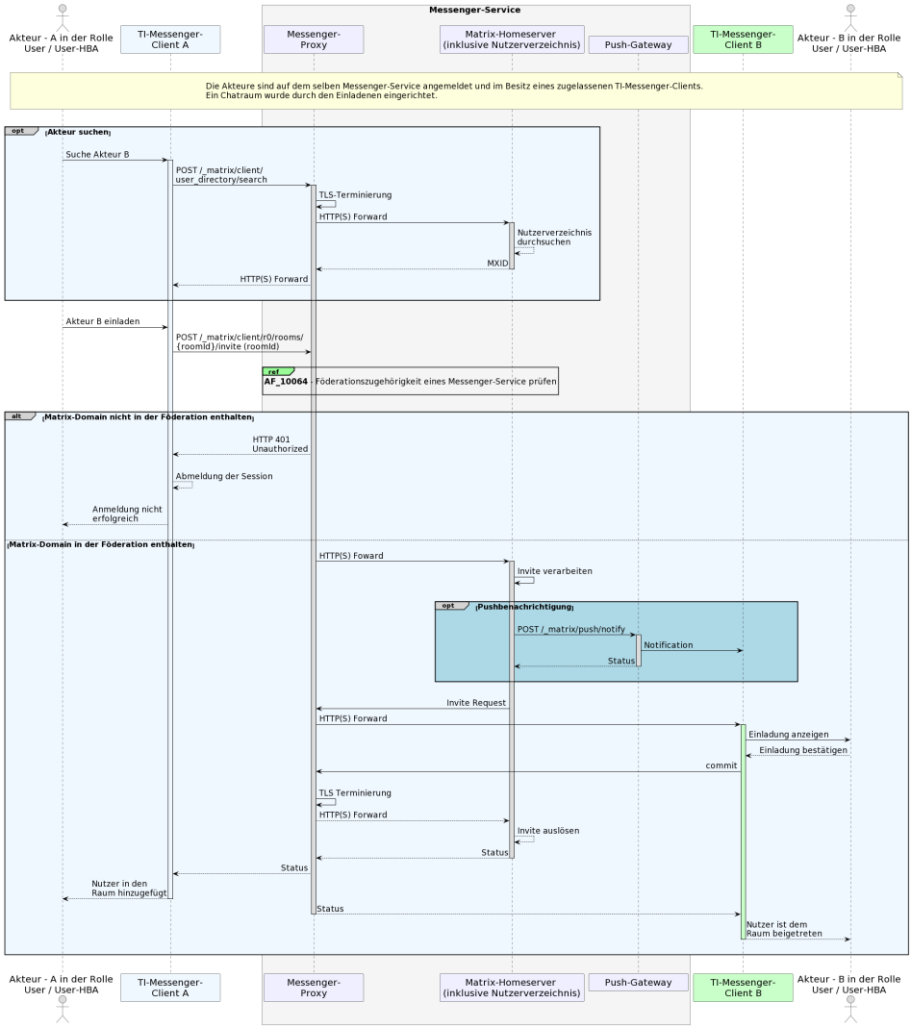


Abbildung 16: Einladung von Akteuren innerhalb einer Organisation

[<=]

Akzeptanzkriterien für den Anwendungsfall: ~~Organisationsressourcen im VZD-FHIR-Directory hinzufügen (AF_10059)~~Einladung von Akteuren innerhalb einer Organisation (AF_10104)

ML-123896 **- AF_10104 - Matrix-Homeserver nach Akteuren durchsuchen**
Der TI-Messenger-Client zeigt eine Liste aller Akteuren eines Matrix-Homeservers an.
[<=]

ML-129415 **- AF_10104 - Messenger-Proxy prüft TI-Föderationszugehörigkeit**
~~**ML-123627 - AF_10059 - Organisations-Ressourcen im VZD-FHIR-Directory hinzufügen**~~Der Messenger-Proxy lehnt den `Invite-Event` ab, wenn die Matrix-Domain nicht zur TI-~~Nach erfolgreicher Authentisierung an einem zugelassenen IDP-Dienst als Administrator einer Organisation kann der Nutzer in der Rolle *Org-Admin* die Matrix User URI (MXID) in den FHIR-Organization-Datensatz eintragen und Unterstrukturen für die Organisation anlegen. Der Nutzer in der Rolle *Org-Admin* wird über den Erfolg der Operation informiert.~~
~~**[<=]**~~Föderation gehört.
[<=]

ML-129414 **- AF_10104 - Akteure sind dem Chatraum beigetreten**
Alle Chat-Parteien sind erfolgreich im Chatraum vorhanden.
[<=]

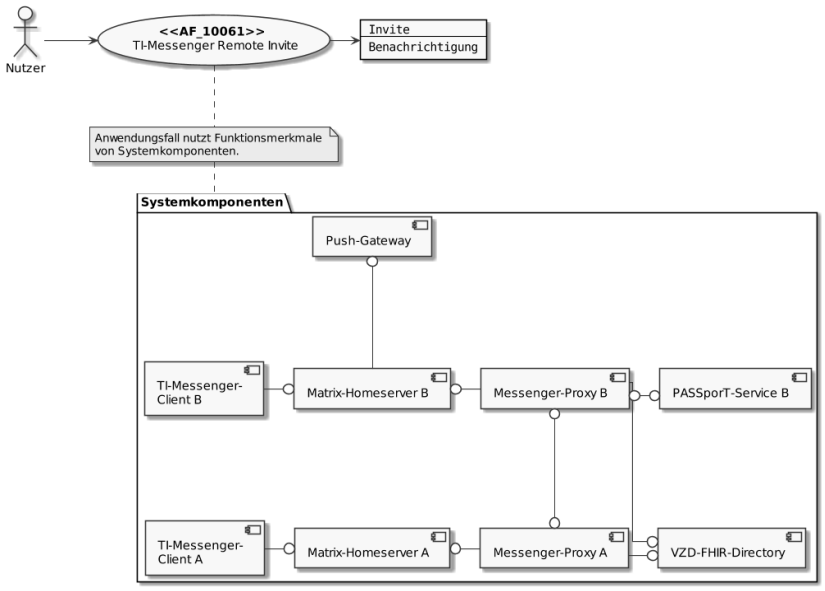
ML-132590 **- AF_10104 - TI-M Rohdatenerfassung und -lieferung**
Die Rohdaten wurden entsprechend der Rohdatendefinition gemäß [gemSpec_TI-Messenger-FD#Betrieb] für den TI-Messenger-Fachdienst erfolgreich erfasst und an die definierte Schnittstelle der Rohdatenerfassung versendet.**[<=]**

~~**ML-123626 - AF_10059 - Änderungen nur für eigene Organization-FHIR-Datensätze**~~
~~Der Nutzer in der Rolle *Org-Admin* darf nur FHIR-Ressourcen seiner eigenen Organisation (inklusive der Unterstrukturen) ändern.~~
~~**[<=]**~~

~~6.5 AF - TI-Messenger-Remote-Invite~~

6.8 ~~AF_10061 -~~ TI-Messenger-Remote-Invite**AF - Austausch von Events**~~**Nutzer haben die Möglichkeit innerhalb der Föderation des deutschen Gesundheitswesens**~~ **zwischen** ~~**Messenger-Services-Chatnachrichten und andere**~~**Akteuren innerhalb einer Organisation**

AF_10063 **- Austausch von Events zwischen Akteuren innerhalb einer Organisation**
Dieser Anwendungsfall ermöglicht es Akteuren, welche sich in einem gemeinsamen Raum innerhalb eines Messenger-Service befinden, Nachrichten auszutauschen und weitere durch die Matrix-Spezifikation festgelegte Aktionen ~~auszuführen. Dafür MUSS ein Chatraum zwischen den entsprechenden Parteien entstehen. Dieser Ablauf zeigt, wie ein Chatraum zwischen den Parteien entsteht~~(Events) auszuführen.



~~Abbildung 12: Systemkomponenten des AF - TI-Messenger-Remote Invite~~

Tabelle 7 AF_ TI-Messenger Remote Invite

AF_10061	TI-Messenger Remote Invite
Akteur	Nutzer A, Nutzer B
Auslöser	Nutzer A möchte mit Nutzer B einen gemeinsamen Chatraum einrichten
Komponenten	TI-Messenger Client Matrix-Homeserver VZD-FHIR-Directory PASSporT-Service Push-Gateway
Vorbedingungen	1. Die Nutzer verfügen über einen TI-Messenger-Client 1. Die Nutzer kennen die URL ihres Matrix-Homeservers oder die URL ist bereits in ihren Clients konfiguriert. 2. Die Nutzer sind am Messenger-Services angemeldet (AF_10057) 3. Die verwendeten Matrix-Homeserver sind in die Föderation integriert.
Eingangsdaten	beabsichtigter Nachrichtenaustausch
Ergebnis	Nutzer A und Nutzer B sind beide in einem gemeinsamen Chatraum. Optional erfolgt eine Benachrichtigung von Nutzer B über die Einladung in den Chatraum.
Ausgangsdaten	keine
Akzeptanzkriterien	ML_123654 , ML_123659 , ML_123660 , ML_123661 , ML_123663

***Hinweis: Es*Tabelle 15: Austausch von Events zwischen Akteuren innerhalb einer Organisation**

AF_10063	Austausch von Events zwischen Akteuren innerhalb einer Organisation
Akteur	Leistungserbringer, Mitarbeiter einer Organisation im Gesundheitswesen in der Rolle "User / User-HBA"
Auslöser	Alle Matrix-Events die innerhalb eines Messenger-Service einer Organisation ausgeführt werden
Komponenten	• TI-Messenger Client A + B, • Messenger-Proxy, • Matrix-Homeserver, • Push-Gateway.
Vorbedingungen	1. Die Akteure sind am selben Messenger-Service angemeldet. 2. Jeder Akteur hat einen zugelassenen TI-Messenger-Client. 3. Die Teilnehmer sind einem gemeinsamen Raum beigetreten.
Eingangsdaten	Matrix-Event
Ergebnis	Matrix-Event wurde erfolgreich verarbeitet
Ausgangsdaten	Abhängig vom Matrix-Event
Akzeptanzkriterien	ML-123669 , ML-123670 , ML-132591

In der Laufzeitsicht sind die Interaktionen zwischen den Komponenten, die durch den Anwendungsfall genutzt werden, dargestellt. Hierbei handelt es sich ~~hierbei~~ um eine **vereinfachte Laufzeitansicht**~~. Bei der Laufzeitansicht wurde nicht betrachtet~~ in der zum Beispiel die TLS-Terminierung am Messenger-Proxy auf Grund der Übersichtlichkeit nicht berücksichtigt wurde. Die in der Abbildung rot dargestellten Linien symbolisieren den Kommunikationsverlauf des auslösenden Matrix-Request. Für die vereinfachte Darstellung wird vorausgesetzt, dass die TI-Messenger-Clients der beteiligten Akteure online sind.

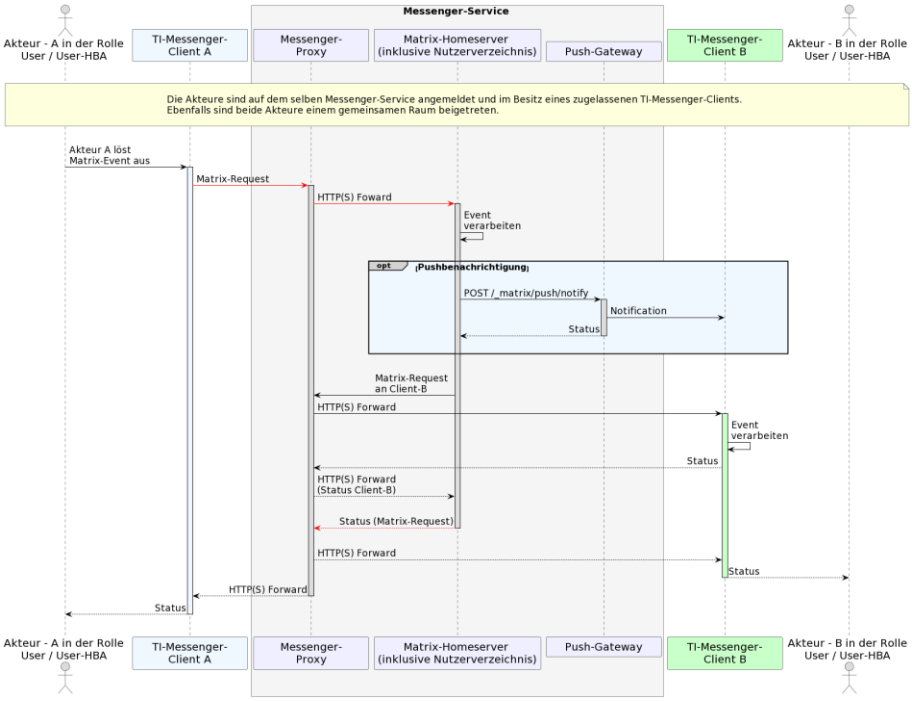


Abbildung 17: Laufzeitsicht - Austausch von Events zwischen Akteuren innerhalb einer Organisation

[<=]

Akzeptanzkriterien für den Anwendungsfall: Austausch von Events zwischen Akteuren innerhalb einer Organisation (AF_10063)

ML-123670 **- AF_10063 - Chatnachricht wird verarbeitet**
Eine Chatnachricht vom ~~*Verbindung zwischen*~~ TI-Messenger-Client A an TI-Messenger-Client B wurde vom Matrix-Homeserver erfolgreich verarbeitet.
[<=]

ML-123669 **- AF_10063 - Auslösen einer Benachrichtigung**
Der~~*und*~~ Matrix-Homeserver löst eine Benachrichtigung des TI-Messenger-Clients vom Empfänger über das mit dem TI-Messenger-Client verbundene Push-Gateway des TI-Messenger-Anbieters aus.
[<=]

ML-132591 **- AF_10063 - TI-M Rohdatenerfassung und -lieferung**
Die Rohdaten wurden entsprechend der Rohdatendefinition gemäß [gemSpec_TI-Messenger-FD#Betrieb] für den TI-Messenger-Fachdienst erfolgreich erfasst und an die definierte Schnittstelle der Rohdatenerfassung versendet.[<=]

6.9 AF - Einladung von Akteuren außerhalb einer Organisation

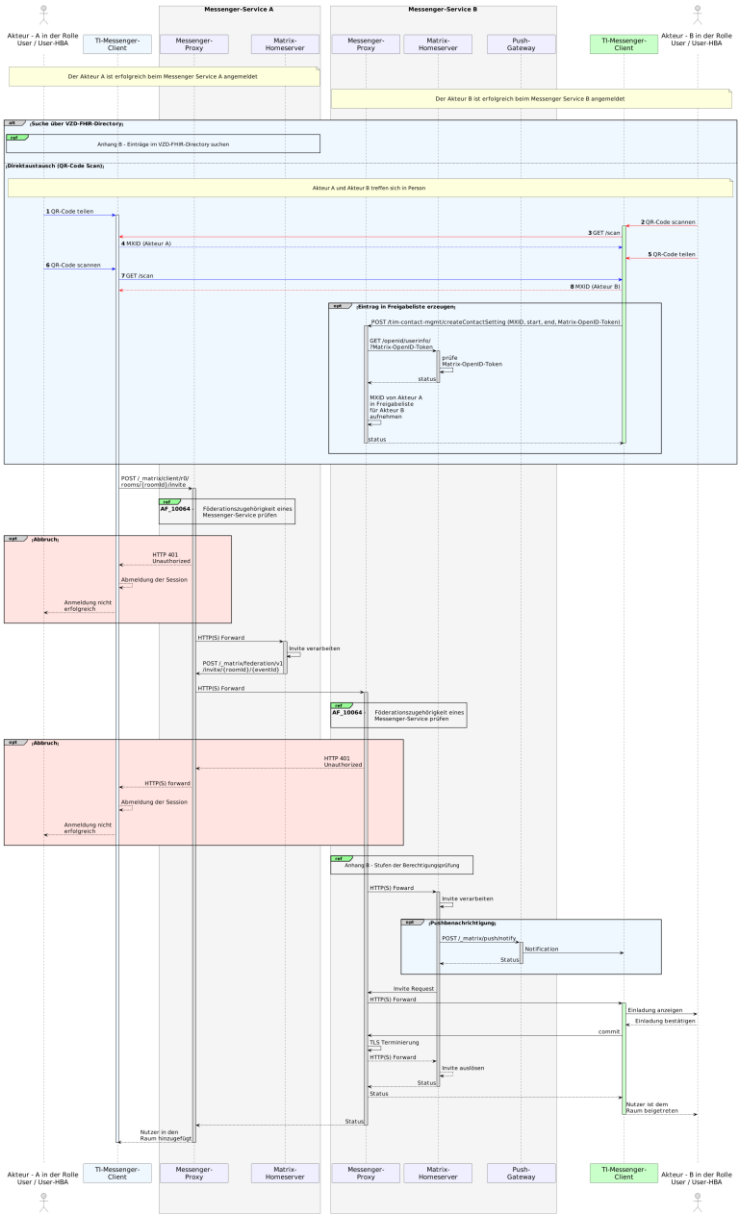
AF_10061 **- Einladung von Akteuren außerhalb einer Organisation**
In diesem Anwendungsfall wird ein Akteur außerhalb einer Organisation eingeladen. Für die Suche von Akteuren außerhalb der Organisation KANN das VZD-FHIR-Directory verwendet werden. Ist die MXID des gesuchten Akteurs dort nicht vorhanden MUSS die Kontaktaufnahme auch über einen QR-Code Scan erfolgen. Im Gegensatz zu einer Einladung von Akteuren innerhalb einer Organisation (siehe "AF_10063 -*Austausch von Events innerhalb einer Organisation*"), prüft in diesem Anwendungsfall der Messenger-Proxy ~~*läuft*~~des Einzuladenden zusätzlich die im Kapitel "*Berechtigungskonzept*" festgelegten Kriterien (Stufe 1 - 3).

Tabelle 16 AF - Einladung von Akteuren außerhalb einer Organisation

AF_10061	Einladung von Akteuren außerhalb einer Organisation
Akteur	Leistungserbringer, Mitarbeiter einer Organisation im Gesundheitswesen in der "Rolle User / User-HBA"
Auslöser	Akteur A möchte mit Akteur B außerhalb einer Organisation einen gemeinsamen Chatraum einrichten.
Komponenten	• TI-Messenger Client A + B, • Messenger-Proxy A + B, • Matrix-Homeserver A + B, • VZD-FHIR-Directory, • Push-Gateway B.
Vorbedingungen	1. Die Akteure verfügen über einen zugelassenen TI-Messenger-Client. 2. Die Akteure kennen die URL ihres Messenger-Service oder die URL ist bereits in ihren TI-Messenger-Clients konfiguriert. 3. Die Akteure sind am Messenger-Services angemeldet (siehe AF_10057) 4. Die verwendeten Messenger-Services sind Bestandteile der TI-Messenger-Föderation.
Eingangsdaten	`Invite-Event`
Ergebnis	Akteur A und Akteur B sind beide in einem gemeinsamen Chatraum. Optional erfolgt eine Benachrichtigung an Akteur B über die Einladung in den Chatraum.
Ausgangsdaten	Status
Akzeptanzkriterien	ML-123654 , ML-123663 , ML-132592

In der Laufzeitsicht sind die Interaktionen zwischen den Komponenten, die durch den Anwendungsfall genutzt werden, dargestellt. Hierbei handelt es um eine **vereinfachte Laufzeitansicht** in der zum Beispiel die TLS-Terminierung am Messenger-Proxy auf Grund der Übersichtlichkeit nicht berücksichtigt wurde. Ebenfalls wurde für eine vereinfachte Darstellung darauf verzichtet~~, dass der Messenger-Proxy die~~ eine eventuell notwendige Aktualisierung der Föderationsliste ~~bei dem~~vom eigenem Registrierungs-Dienst ~~abruft, welcher die Liste beim VZD-FHIR-Directory abruft und zur Verfügung stellt.~~zu zeigen. Der Abruf der Föderationsliste ist ~~in AF 6.8 - Check remote domain~~im Anhang B "Aktualisierung der Föderationsliste" hinreichend beschrieben. Für die vereinfachte Darstellung wird vorausgesetzt, dass die TI-Messenger-Clients der beteiligten Akteure online sind. Der in der Abbildung dargestellte Registrierungs-Dienst

gehört zu dem TI-Messenger-Fachdienst des Messenger-Service B.



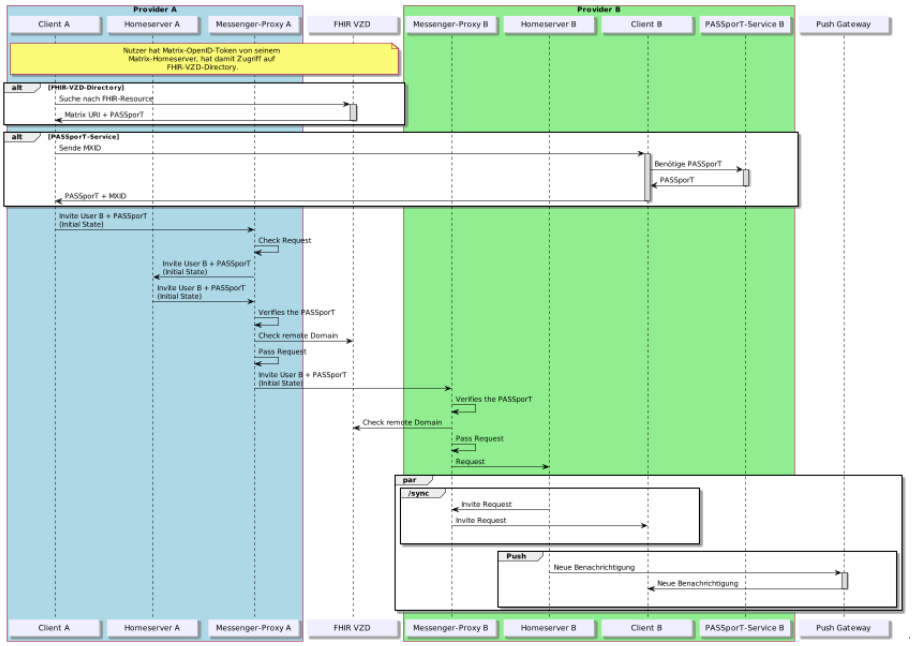


Abbildung 18: Laufzeitsicht - ~~TI-Messenger-Remote-Invite~~ Einladung von Akteuren außerhalb einer Organisation

[<=]

Akzeptanzkriterien für den Anwendungsfall: ~~TI-Messenger-Remote-Invite~~Einladung von Akteuren außerhalb einer Organisation (AF_10061)

ML-123654 **- AF_10061 - Suche im VZD-FHIR-Directory**
Ein Messenger-Client kann erfolgreich im VZD-FHIR-Directory nach einem Chatpartner suchen.
[<=]

~~**ML-123659 - AF_10061 - PASSporT Übergabe**~~
~~PASSporT wurde erfolgreich an den Messenger-Proxy übergeben, enthält alle benötigten Informationen und ist auswertbar.~~
~~**[<=]**~~

~~**ML-123660 - AF_10061 - Invite nur mit PASSporT**~~
~~Im Invite-Request steht das PASSporT an der richtigen Stelle und kann vom Messenger-Proxy ausgewertet werden.~~
~~**[<=]**~~

Ein Beispiel für einen `Invite-`~~`Request`~~`Event` ist im Dokument [gemSpec_TI-Messenger-FD~~] im Kapitel "~~#Messenger Proxy~~"~~] zu finden.

~~**ML-123661 - AF_10061 - Messenger-Proxy prüft PASSporT auf Gültigkeit**~~

~~Der Messenger-Proxy lehnt das Invite bei ungültigem PASSporT ab.~~
~~**[<=]**~~
ML-123663 **-** ~~**AF_10061 - Nutzer sind dem Chatraum beigetreten**~~**AF_10061 - Akteure sind dem Chatraum beigetreten**
Alle Chat Parteien sind erfolgreich im Chatraum vorhanden.
[<=]

ML-132864 **- Berechtigungsprüfung aller Stufen**

~~6.6 AF - Message senden (Remote)~~

Die Berechtigungsprüfung der Stufen 1-3 wurden berücksichtigt.
[<=]

ML-132592 **- AF_10061 - TI-M Rohdatenerfassung und -lieferung**
Die Rohdaten wurden entsprechend der Rohdatendefinition gemäß [gemSpec_TI-Messenger-FD#Betrieb] für den TI-Messenger-Fachdienst erfolgreich erfasst und an die definierte Schnittstelle der Rohdatenerfassung versendet.**[<=]**

6.10 AF - Austausch von Events zwischen Akteuren außerhalb einer Organisation

AF_10062 **-** ~~**Message senden (Remote)**~~**Austausch von Events zwischen Akteuren außerhalb einer Organisation**
In diesem Anwendungsfall können Akteure welche sich in einem gemeinsamen Raum befinden Nachrichten austauschen und andere durch die Matrix-Spezifikation festgelegte Aktionen ausführen. Dieser Anwendungsfall setzt ein erfolgreiches `Invite-Event` eines oder mehrerer beteiligter ~~Nutzer~~Akteure voraus~~ und führt den eigentlichen Nachrichtenaustausch durch.~~. In diesem Anwendungsfall sind die beteiligten ~~Nutzer sind mit TI-Messenger-Clients Mitglied des Chatraumes~~Akteure in einem gemeinsamen Chatraum und auf unterschiedlichen Messenger-Services verteilt.

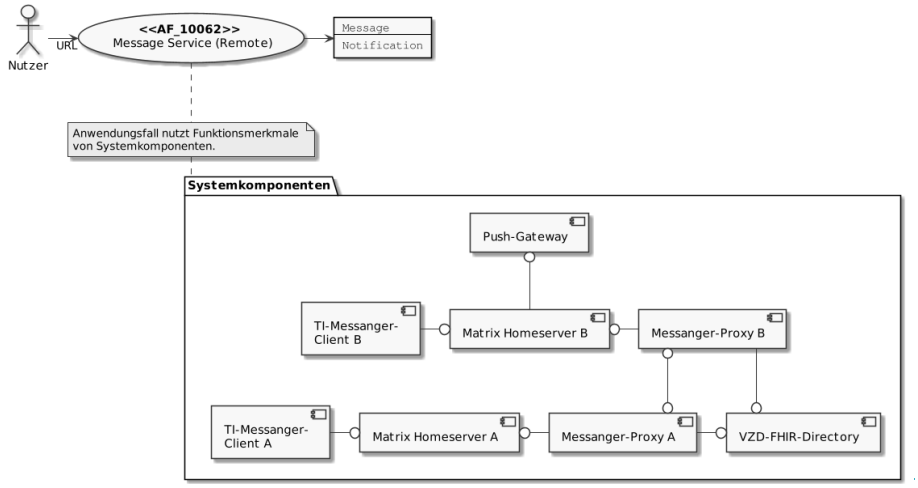


Abbildung 14: Systemkomponenten des AF – Message senden (Remote)

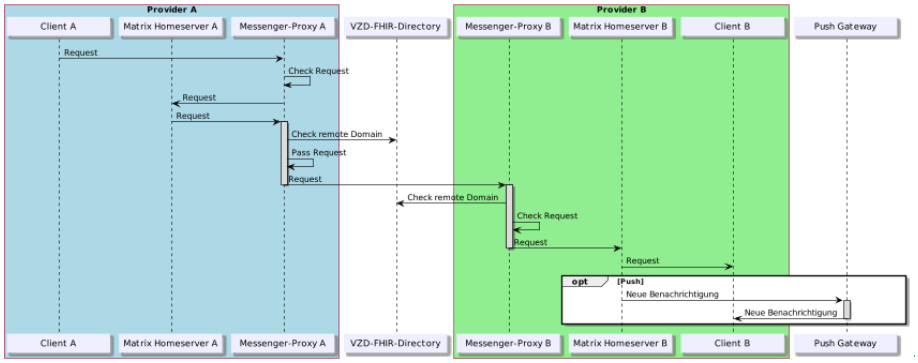
~~Tabelle 8 AF - Message senden (Remote)~~

Tabelle 17: AF - Austausch von Events zwischen Akteuren außerhalb einer Organisation

AF_10062	**~~Message senden (Remote)~~Austausch von Events zwischen Akteuren außerhalb einer Organisation**
Akteur	~~Nutzer A, Nutzer B~~Leistungserbringer, Mitarbeiter einer Organisation im Gesundheitswesen in der Rolle "User / User-HBA"
Auslöser	~~Nutzer A möchte eine Chatnachricht an Nutzer B (föderierter Matrix-Homeserver) versenden~~Alle Matrix-Events die zwischen Messenger-Services unterschiedlicher Organisationen ausgeführt werden.
Komponenten	• TI-Messenger-Client A + B, • Messenger-Proxy A + B, • Matrix-Homeserver A + B ~~Messenger-Proxy A + B~~ ~~Registrierungs-Dienst~~ ~~VZD-FHIR-Directory~~ , • Push-Gateway B.
Vorbedingungen	1. Beide ~~Nutzer~~Akteure sind ~~Mitglied~~Teilnehmer eines gemeinsamen Raumes. 2. ~~Es liegt~~Die Messenger Proxies verfügen über eine ~~aktualisierte~~aktuelle Föderationsliste ~~vor~~. 3. Die Messenger-Proxys überprüfen die ~~Remote-Domain~~Zugehörigkeit der beteiligten Messenger-Services (siehe AF~~6.8)~~_10064)
Eingangsdaten	~~Chatnachricht~~Matrix-Event
Ergebnis	~~Nutzer B erhält Chatnachricht von Nutzer A;~~ ~~optional erfolgt eine Benachrichtigung von Nutzer B über eine neue Nachricht~~Matrix-Event wurde erfolgreich verarbeitet
Ausgangsdaten	~~Chatnachricht erreicht Nutzer B~~Abhängig vom Matrix-Event, Status
Akzeptanzkriterien	ML-123665 , ML-123666 , ML-123667 , ML-123668 , ML-132593

~~*Hinweis: Es handelt sich hierbei um eine **vereinfachte Laufzeitansicht**. Bei der Laufzeitansicht wurde nicht betrachtet, dass die Verbindung zwischen TI-Messenger-Client und Matrix-Homeserver über den Messenger-Proxy läuft. Ebenfalls wurde für eine vereinfachte Darstellung darauf verzichtet, dass der Messenger-Proxy die Föderationsliste bei dem Registrierungs-Dienst abruft, welcher die Liste beim VZD-FHIR-Directory abruft*~~

~~*und zur Verfügung stellt. Der Abruf der Föderationsliste ist in AF 6.8 - Check remote domain hinreichend beschrieben.*~~



~~Abbildung~~

In der Laufzeitsicht sind die Interaktionen zwischen den Komponenten, die durch den Anwendungsfall genutzt werden, dargestellt. Hierbei handelt es um eine **vereinfachte Laufzeitansicht** in der zum Beispiel die TLS-Terminierung am Messenger-Proxy auf Grund der Übersichtlichkeit nicht berücksichtigt wurde. Es wird in dem Anwendungsfall von lediglich zwei beteiligten Akteuren ausgegangen. Auf die bei der Prüfung zur Föderationsliste, durch den Messenger-Proxy, notwendigen Interaktionen wurde in dieser Laufzeitsicht verzichtet. Für eine ausführliche Beschreibung dieser Prüfung wird auf den Anwendungsfall "AF_10064 *-Föderationszugehörigkeit eines Messenger-Service prüfen"* verwiesen. Die in der Abbildung rot dargestellten Linien symbolisieren den Kommunikationsverlauf des auslösenden Matrix-Request. Für die vereinfachte Darstellung wird vorausgesetzt, dass die TI-Messenger-Clients der beteiligten Akteure online sind.

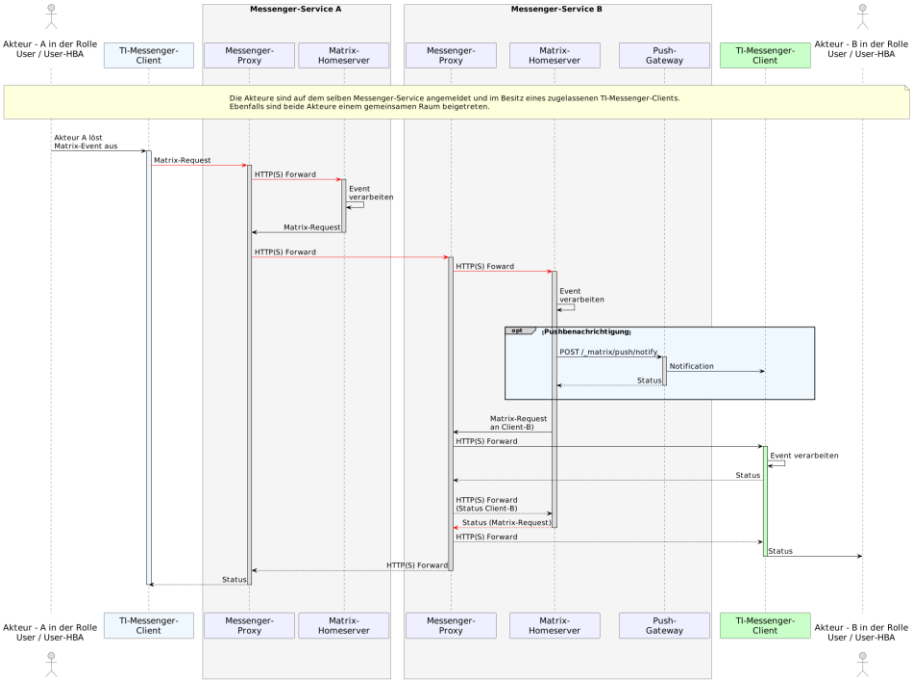


Abbildung 19: Laufzeitsicht - ~~Message senden (Remote)~~ Austausch von Events zwischen Akteuren außerhalb einer Organisation

[<=]

Akzeptanzkriterien für den Anwendungsfall: ~~Message senden~~Austausch von Nachrichten zwischen Akteuren außerhalb einer Organisation (AF_10062)

ML-123665 **- AF_10062 - Messenger-Proxy des Senders prüft Domain des Empfängers**
Der Messenger-Proxy des Senders prüft die Domain des Empfängers auf Zugehörigkeit zur TI-Messenger-Föderation.
[<=]

ML-123666 **- AF_10062 - Messenger-Proxy des Empfängers prüft Domain des Senders**
Der Messenger-Proxy des Empfängers prüft die Domain des Senders auf Zugehörigkeit zur TI-Messenger-Föderation.
[<=]

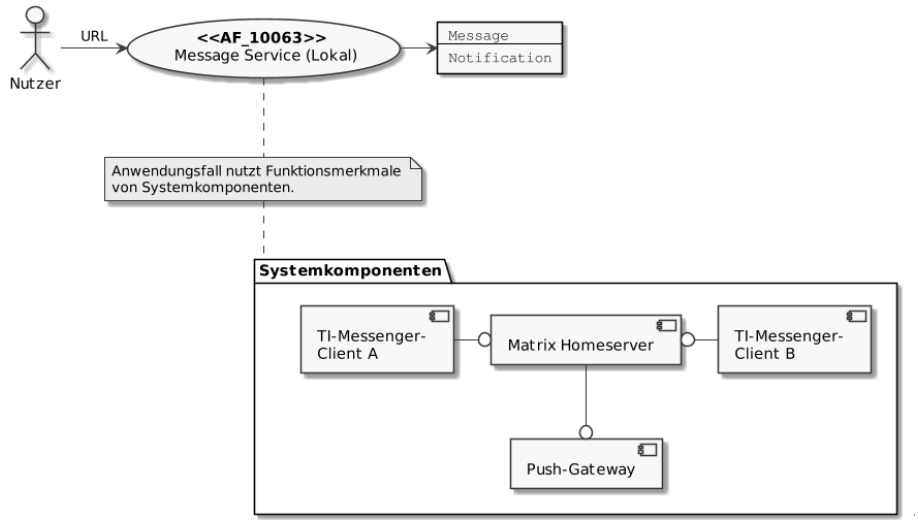
ML-123667 **- AF_10062 - Auslösen einer Notifikation**
Der Matrix-Homeserver des Empfängers löst eine Benachrichtigung des Messenger-Clients über sein Push-Gateway aus.
[<=]

ML-123668 **- AF_10062 - Nachricht wird angezeigt**
Die Nachricht wird dem Empfänger im gemeinsamen Raum angezeigt.
[<=]

~~AF~~
ML-132593 **- AF_10062 - TI-M Rohdatenerfassung und -lieferung**

~~6.7~~ Die Rohdaten wurden entsprechend der Rohdatendefinition gemäß [gemSpec_TI-Messenger-FD#Betrieb] für den ~~Service (Lokal)~~

~~**AF_10063 - Messenger-Service (Lokal)**~~
~~Nutzer haben die Möglichkeit innerhalb eines Messenger-Services Chatnachrichten auszutauschen und andere durch die Matrix-Spezifikation festgelegte Aktionen auszuführen. Zum Starten eines Chats durchsuchen Nutzer mit Hilfe des TI-Messenger-Clients das Nutzerverzeichnis eines Matrix-Homeservers. Dabei liegt folgender Ablauf vor.~~



~~**Abbildung 16: Systemkomponenten des AF - Messenger-Service (Lokal)**~~

Tabelle 9 Messenger-Service (Lokal)

AF_10063	Messenger-Service (Lokal)
Akteur	Nutzer A, Nutzer B
Auslöser	Beispiel: Nutzer A versendet eine Chatnachricht an Nutzer B auf dem selben Matrix-Homeserver
Komponenten	TI-Messenger-Client A + B Matrix-Homeserver Push-Gateway
Vorbedingungen	Beispiel: Beide Nutzer sind Mitglied eines gemeinsamen Raumes
Eingangsdaten	Beispiel: Chatnachricht
Ergebnis	Beispiel: Client Nutzer B erhält Chatnachricht von Nutzer A; optional erfolgt eine Push-Benachrichtigung von Nutzer B über den Eingang einer neuen Nachricht
Ausgangsdaten	Beispiel: Chatnachricht erreicht Client Nutzer B
Akzeptanzkriterien	ML-123669 , ML-123670 , ML-123896

Hinweis: Es handelt sich hierbei um eine ***vereinfachte Laufzeitansicht****. Bei der Laufzeitansicht wurde nicht betrachtet, dass die Verbindung zwischen* TI-Messenger-*Client und Matrix-Homeserver über den Messenger-Proxy läuft.*

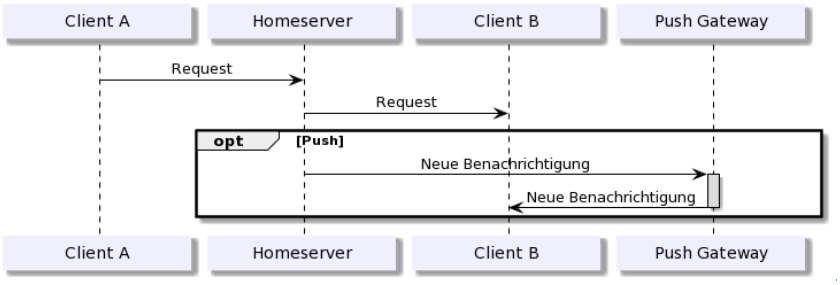


Abbildung 17: Laufzeitsicht – Messenger-Service (Lokal)

[<=]

Akzeptanzkriterien für den Anwendungsfall: Messenger-Service (Lokal) (AF_10063)

ML-123669 – AF_10063 – Auslösen einer Benachrichtigung
Der Matrix-Homeserver löst eine Benachrichtigung des TI-Messenger-Clients vom Empfänger über das mit dem TI-Messenger-Client verbundene Push-Gateway des TI-Messenger-Anbieters aus.
[<=]

ML-123896 – Matrix-Homeserver nach Nutzern durchsuchen
Der TI-Messenger-Client zeigt eine Liste aller Nutzer eines Matrix-Homeservers an.
[<=]

ML-123670 – AF_10063 – Chatnachricht wird angezeigt
Die Chatnachricht wurde dem TI-Messenger-Client zugestellt und wird im TI-Messenger-Client angezeigt.
[<=]

6.8 AF – Check remote Domain

AF_10064 – Check remote Domain FachdienstFür die Prüfung der Zugehörigkeit der Domain zu der TI-Messenger-Föderation wird durch den Registrierungs-Dienst eines TI-Messenger-Fachdienstes eine täglich aktualisierte Föderationsliste vom VZD-FHIR-Directory geladen. Der Messenger-Proxy eines Messenger-Services nutzt diese für die Prüfung der Remote-Domain. Die Speicherdauer der Föderationsliste des Messenger-Proxies ist limitiert. Die Struktur dieser Föderationsliste wird in [gemSpec_VZD_FHIR_Directory] beschrieben. Für die Prüfung durch den Messenger-Proxy gilt der folgende Ablauf. Der Ablauf gilt für alle Anwendungsfälle, welche die Remote-Domain überprüfen.

Ist die zu überprüfende Domain nicht Teil der Föderationsliste, MUSS der Messenger-Proxy zunächst eine aktualisierte Version der Liste vom Registrierungs-Dienst abfragen. Sollte der Messenger-Proxy eine aktualisierte Föderationsliste abfragen, MUSS der Registrierungs-Dienst überprüfen, ob die vorhandene Liste aktuell ist und diese gegebenenfalls aktualisieren, bevor die neue Liste zurückgegeben wird.

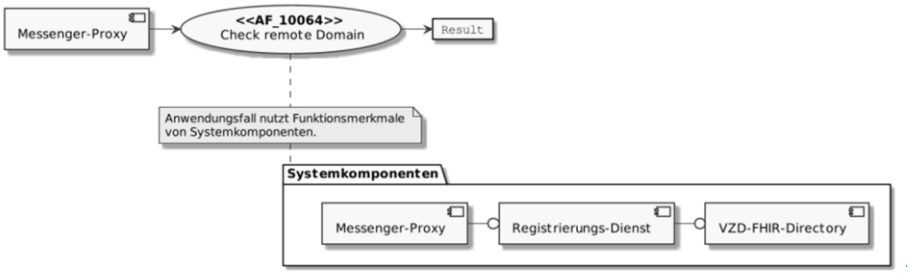


Abbildung 18: Systemkomponenten des AF – Check remote Domain

Tabelle 10 Check remote Domain

AF_10064	Check remote Domain
Akteur	Messenger-Proxy
Auslöser	Der Messenger-Proxy empfängt ein Matrix-Request und MUSS die Domain-Zugehörigkeit zur Föderation prüfen
Komponenten	Messenger-Proxy Registrierungs-Dienst VZD-FHIR-Directory
Vorbedingungen	keine
Eingangsdaten	Matrix-Request
Ergebnis	Der Messenger-Proxy ermittelt mittels der Föderationsliste, ob die Remote-Domain Teil der Föderation ist.
Ausgangsdaten	Result
Akzeptanzkriterien	ML-123672 , ML-123891 , ML-123893

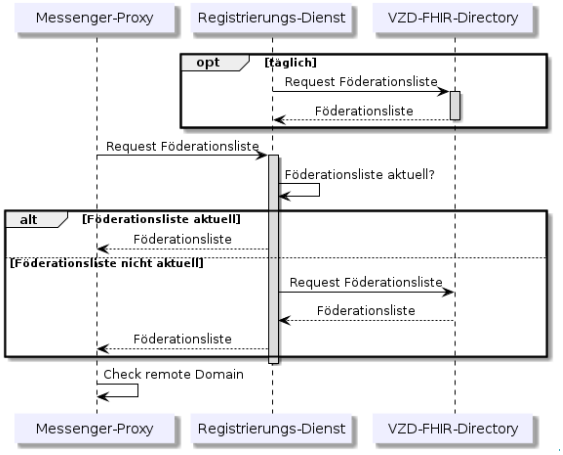


Abbildung 19: Laufzeitsicht – Ablauf Check remote Domain

[<=]

~~**Akzeptanzkriterien für den Anwendungsfall: Check remote Domain (AF_10064)**~~

~~**ML-123672 – AF_10064 – Föderationsliste vom VZD-FHIR-Directory abrufen**~~
~~Der Registrierungs-Dienst des TI-Messenger-Fachdienstes MUSS die Föderationsliste~~
erfolgreich ~~vom VZD-FHIR-Directory abrufen.~~
~~**[<=]**~~

~~**ML-123891 – Remote-Domain-Teil der Föderationsliste & Aktualitätscheck**~~
~~Es MUSS sichergestellt werden, dass der Messenger-Proxy tatsächlich überprüft, ob die Remote-Domain-Teil der Föderationsliste ist. Es MUSS sichergestellt werden, dass der Messenger-Proxy überprüft, ob die Liste aktuell ist. Es MUSS sichergestellt werden, dass der Registrierungs-Dienst die Liste auf Aktualität überprüft, bevor eine aktualisierte Liste durch den Messenger-Proxy abgerufen werden kann.~~
~~**[<=]**~~

~~**ML-123893 – Aktualität Föderationsliste Messenger-Proxy**~~~~Es MUSS sichergestellt werden, dass die Föderationsliste des Messenger-Proxy aktuell ist.~~ erfasst und an die definierte Schnittstelle der Rohdatenerfassung versendet.**[**~~Dafür MUSS der Messenger-Proxy nach einer gewissen Zeit eine aktuelle Liste bei dem Registrierungs-Dienst anfordern.~~
~~**[**~~<=**]**

7 Anhang A – Verzeichnisse

7.1 Abkürzungen

Kürzel	Erläuterung
AD	Active Directory
AF	Anwendungsfall
~~APN~~AZPD	~~Apple Push Notification Service~~ Anbieter zentrale Plattformdienste
~~AuthZ~~	~~Authorization~~
~~BSI~~	~~Bundesamt für Sicherheit in der Informationstechnik~~
~~FCM~~	~~Firebase Cloud Messaging~~
FHIR	Fast Healthcare Interoperable Resources
HBA	Heilberufsausweis
HTTP	~~Hyptertext~~Hypertext Transfer Protocol
IDP ~~Dienst~~	Identity Provider
JSON	JavaScript Object Notation
JWT	JSON Web Token
~~KV~~	~~Kassenärztliche Vereinigung~~
LDAP	Lightweight Directory Access Protocol
LE	Leistungserbringer
~~MSC~~MXID	Matrix ~~Spec Change~~ User-ID

OAuth	Open Authorization
~~OIDC~~PTA	~~OpenID Connect~~ Pharmazeutisch-technischer Assistent
~~PASSporT~~	~~Personal Assertion Token~~
REST	Representational State Transfer
SMC-B	Institutionenkarte (Security Module Card Typ B)
SMC-B ORG	Security Module Card für Organisationen
SPOC	Single Point of Contact
SSO	Single Sign-on
TI	Telematikinfrastruktur
~~UIA~~TI-ITSM	~~User Interactive Authorization Flow~~IT-Service-Management der TI
TI-M	TI-Messenger
TSP	Trust Service Provider
VZD	Verzeichnisdienst

7.2 Glossar

Begriff	Erläuterung
MXID	eindeutige Identifikation eines TI-Messenger~~-Nutzers~~ Teilnehmers (Matrix-User-ID)
on-premise	das Produkt wird auf eigener oder gemieteter Hardware betrieben
Third-Party	Drittanbieter, der Zusatzleistungen oder Komponenten beisteuert

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

7.3 Abbildungsverzeichnis

7.4 Tabellenverzeichnis

7.5 Referenzierte Dokumente

7.5.1 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
[~~gemKPT_TI_~~api-messenger]	~~gematik: Konzeptpapier TI-Messenger~~gematik: api-ti-messenger https://github.com/gematik/api-ti-messenger/
[api-vzd]	gematik: Verzeichnisdienst der Telematikinfrastruktur https://github.com/gematik/api-vzd
[gemKPT_Betr]	gematik: Betriebskonzept Online-Produktivbetrieb
[gemKPT_TI_Messenger]	gematik: Konzeptpapier TI-Messenger
[gemSpec_IDP_Dienst]	gematik: Spezifikation Identity Provider-Dienst
[gemSpec_TI-Messenger-FD]	gematik: Spezifikation TI-Messenger-Fachdienst
[gemSpec_VZD_FHIR_Directory]	gematik: Spezifikation Verzeichnisdienst FHIR-Directory

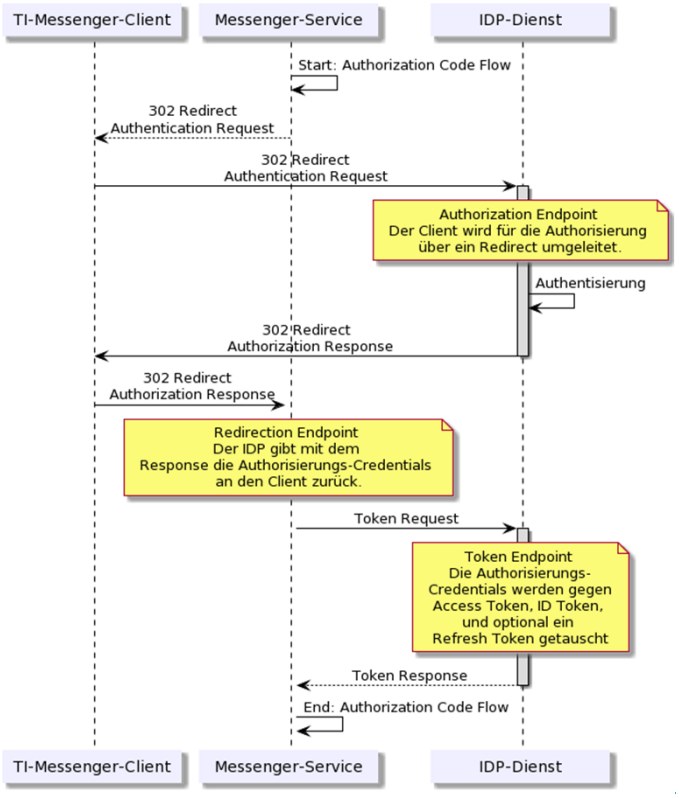
7.5.2 Weitere Dokumente

[Quelle]	Herausgeber (Erscheinungsdatum): Titel

~~[Direct Messaging]~~	~~Matrix Foundation https://matrix.org/docs/spec/client_server/r0.6.1~~
[~~Matrix Foundation~~Client-Server API]	~~Matrix Foundation https://matrix.org/docs/spec/~~ Matrix Foundation: Matrix Specification - Client-Server API https://spec.matrix.org/v1.3/client-server-api/
~~[Nutzer Token]~~	~~Matrix Foundation https://matrix.org/docs/spec/client_server/r0.6.1~~
~~[Matrix PushGW]~~	~~Matrix Foundation https://matrix.org/docs/spec/push_gateway/r0.1.1~~
~~[MatrixSpecProposal]~~	~~Matrix Foundation https://spec.matrix.org/unstable/proposals/~~
~~[RFC 8225]~~	~~IETF https://datatracker.ietf.org/doc/html/rfc8225~~
~~[OpenID]~~	~~OpenID Foundation https://openid.net/developers/specs/~~
[FHIR]	HL7 FHIR Dokumentation https://www.hl7.org/fhir/documentation.html
[gematik Authenticator]	gematik Authenticator https://cloud.gematik.de/index.php/s/23ebxa75z3s7zGt?path=%2Fv2.1.0
[Matrix Bots]	Matrix Bot Implementierungen https://matrix.org/bots/
[Matrix Specification]	Matrix Foundation: Matrix Specification https://spec.matrix.org/v1.3/
[OpenID]	OpenID Foundation https://openid.net/developers/specs/
[Push Gateway API]	Matrix Foundation: Matrix Specification - Push Gateway API https://spec.matrix.org/v1.3/push-gateway-api/
[RFC 8225]	IETF https://datatracker.ietf.org/doc/html/rfc8225
[Server-Server API]	Matrix Foundation: Matrix Specification - Server-Server API https://spec.matrix.org/v1.3/server-server-api/

8 Anhang B - Abläufe

~~8.1 OIDC – Authorization Code Flow~~



8.1 Einträge im VZD-FHIR-Directory suchen

Die folgende Abbildung beschreibt, wie ein Akteur im VZD-FHIR-Directory nach *HealthcareService*- und *PractitionerRole* Ressourcen sucht. Dies setzt eine erfolgreiche Anmeldung des Akteurs an einem Messenger-Service voraus. Der dargestellte Ablauf zeigt alle prinzipiell notwendigen Kommunikationsbeziehungen. Weitergehende Informationen zum Ablauf sind in der [gemSpec_VZD_FHIR_Directory] zu finden.

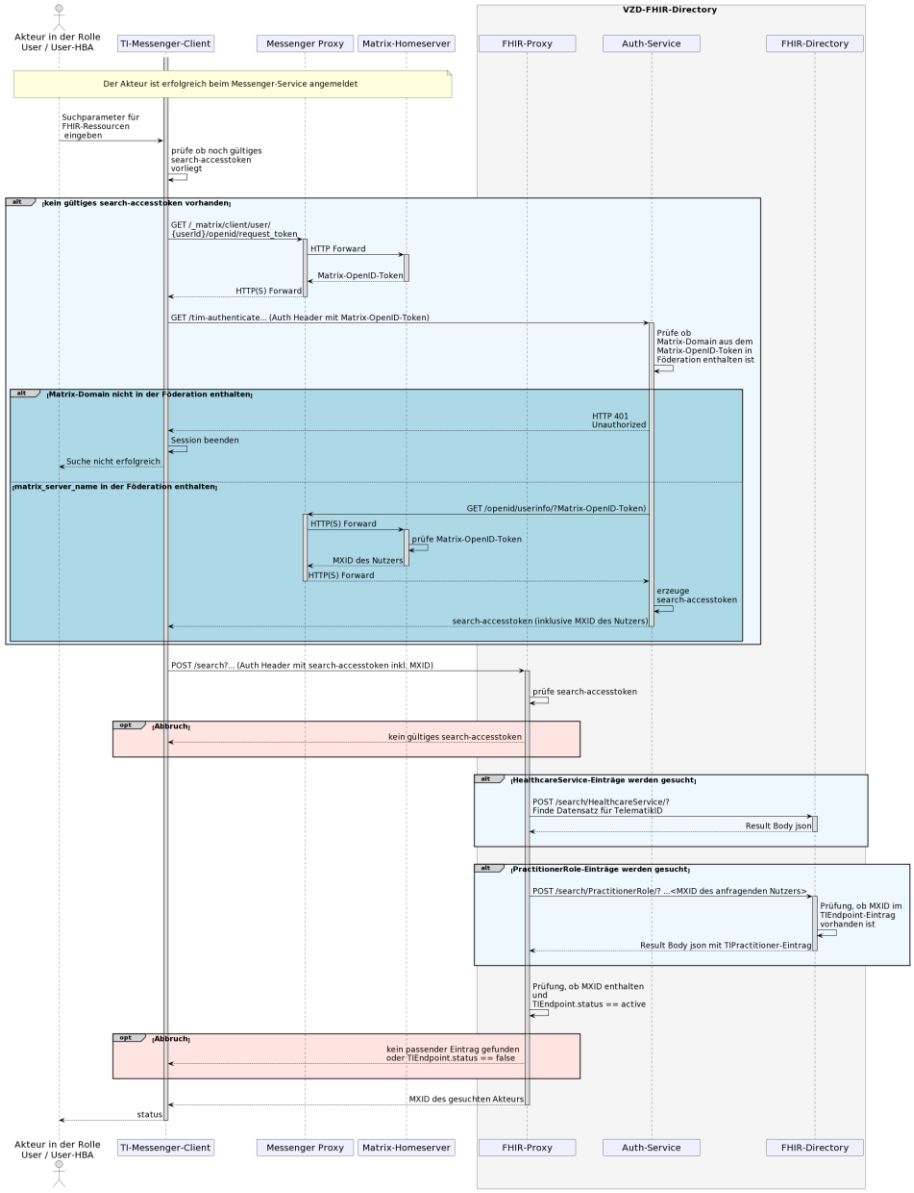


Abbildung 20: Laufzeitansicht - Einträge im VZD-FHIR-Directory suchen

8.2 Aktualisierung der Föderationsliste

Die folgende Abbildung beschreibt, wie der Messenger-Proxy seine lokal vorgehaltene Föderationsliste aktualisiert. Für die Aktualisierung der Föderationsliste MUSS der Messenger-Proxy diese beim Registrierungs-Dienst seines TI-Messenger-Fachdienstes anfragen. Die Häufigkeit der Anfrage einer neuen Liste wird durch den Anbieter festgelegt, Ziel sollte eine möglichst aktuelle Föderationsliste sein (mindestens jedoch einmal am Tag). Hierbei übergibt der Messenger-Proxy die durch ihn gespeicherte Version der Föderationsliste im Aufruf an den Registrierungs-Dienst. Bei Übereinstimmung der Version wird für den Messenger-Proxy keine neue Föderationsliste durch den Registrierungs-Dienst bereitgestellt. Ist die Version größer als die vom Messenger-Proxy übergebene, dann wird durch den Registrierungs-Dienst eine aktualisierte Föderationsliste zur Verfügung gestellt. Bei jeder Anfrage eines Messenger-Proxys beim Registrierungs-Dienst nach einer aktuellen Föderationsliste MUSS auch der Registrierungs-Dienst die Aktualität beim FHIR-Proxy prüfen indem er die von ihm gespeicherte Version der Föderationsliste beim Aufruf am FHIR-Proxy übergibt. Ein Download der Föderationsliste ist nur notwendig, wenn eine neuere Version auf dem FHIR-Proxy existiert. Die Struktur der Föderationsliste ist in [gemSpec_VZD_FHIR_Directory] beschrieben. Nach dem Abruf der Föderationsliste vom Registrierungs-Dienst, durch den Messenger Proxy, MUSS dieser die Signatur der Föderationsliste prüfen.

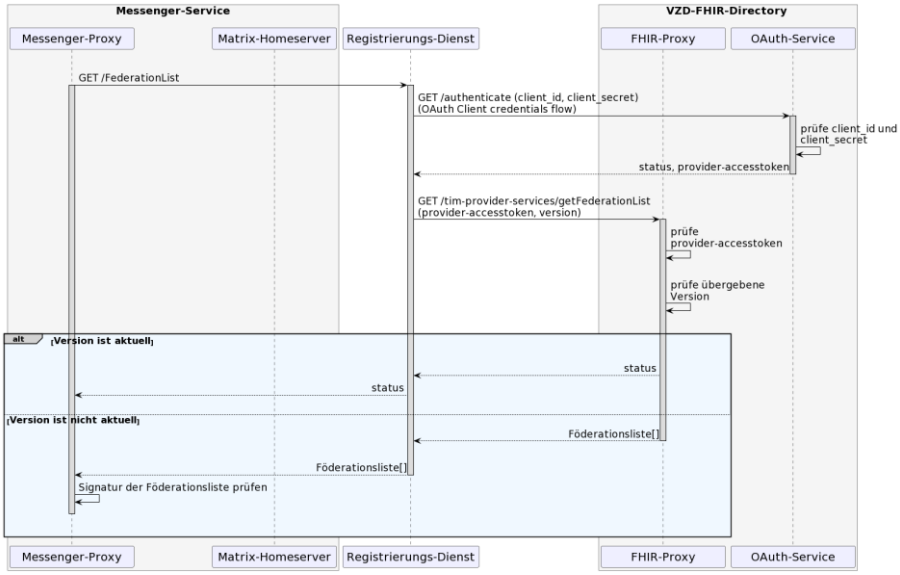


Abbildung 21: Laufzeitansicht - Aktualisierung der Föderationsliste

8.3 Stufen der Berechtigungsprüfung

Die folgende Abbildung beschreibt, wie die Berechtigungsprüfung eingehender Matrix-Anfragen am Messenger-Proxy erfolgen MUSS. Das Berechtigungskonzept basiert auf einer dreistufigen Prüfung, die in Kapitel "*Berechtigungskonzept*" beschrieben ist. Es wird auf die Erwähnung notwendiger Authentifizierungen an dieser Stelle verzichtet.

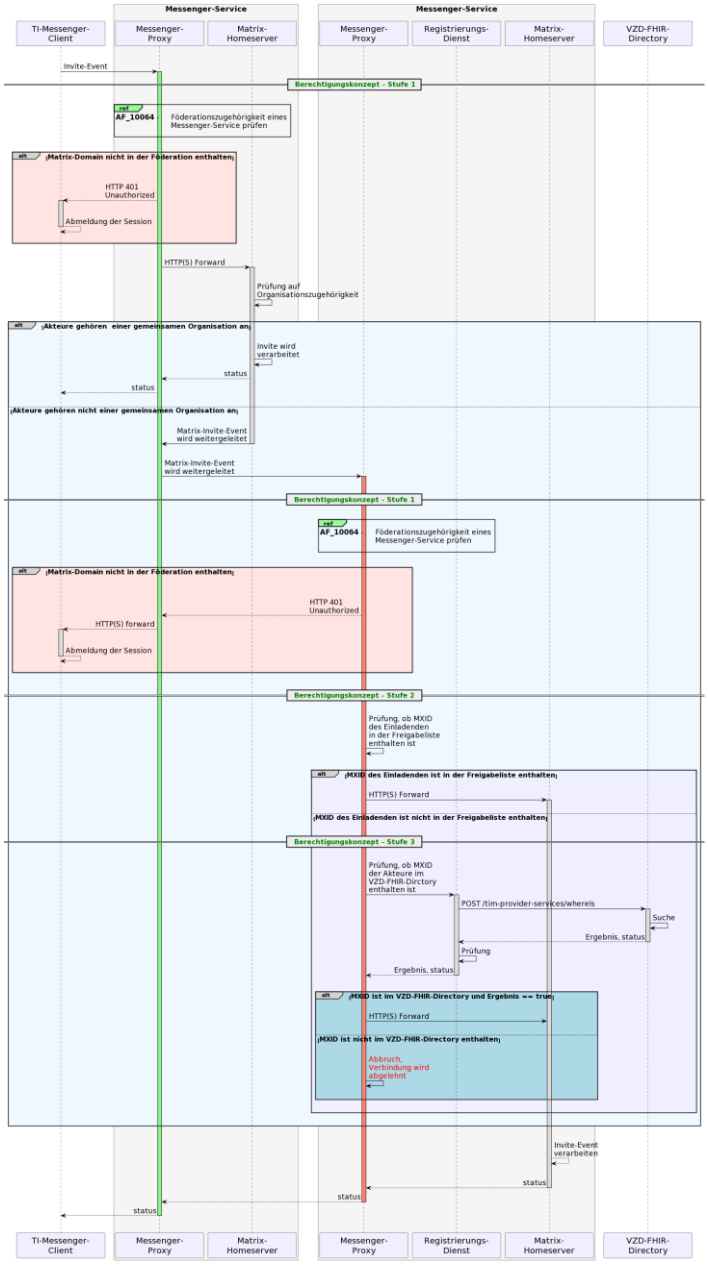


Abbildung 22: Laufzeitansicht - Stufen der Berechtigungsprüfung