

Elektronische Gesundheitskarte und Telematikinfrastruktur

# Spezifikation TI-Messenger-Dienst

Version: 1.1.1  
Revision: 872746  
Stand: 31.07.2023  
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
	16.08.2022		Möglichkeit einer Art Zugriffskontrolle für Org-Admin	gematik
1.1.1	31.07.2023		Einarbeitung TI-Messenger Maintenance 23.1 / VZD FHIR Maintenance_23.1	gematik

---

## Inhaltsverzeichnis

---

<b>1 Einordnung des Dokumentes.....</b>	<b>6</b>
1.1 Zielsetzung.....	6
1.2 Zielgruppe.....	6
1.3 Geltungsbereich.....	6
1.4 Abgrenzungen.....	7
1.5 Methodik.....	7
<b>2 Systemüberblick.....</b>	<b>9</b>
<b>3 Systemkontext.....</b>	<b>11</b>
3.1 Akteure und Rollen.....	11
3.1.1 Rolle: "User".....	11
3.1.2 Rolle: "User-HBA".....	11
3.1.3 Rolle: "Org-Admin".....	12
3.2 Nachbarsysteme.....	14
3.3 Ausprägungen des Messenger-Services.....	15
3.3.1 Anwendungsbeispiel für eine Arztpraxis.....	15
3.3.2 Anwendungsbeispiel für ein Krankenhaus.....	17
3.3.3 Anwendungsbeispiel für Apotheken.....	18
3.3.4 Anwendungsbeispiel für einen Verband für HBA-Inhaber.....	19
3.4 TI-Messenger Föderation.....	19
3.5 Berechtigungskonzept.....	20
3.5.1 Client-Server Kommunikation.....	20
3.5.1.1 Berechtigungskonzept - Stufe 1.....	20
3.5.2 Server-Server Kommunikation.....	21
3.5.2.1 Berechtigungskonzept - Stufe 1.....	21
3.5.2.2 Berechtigungskonzept - Stufe 2.....	21
3.5.2.3 Berechtigungskonzept - Stufe 3.....	21
3.6 Verwendung der Token.....	21
<b>4 Systemzerlegung.....</b>	<b>25</b>
4.1 IDP-Dienst.....	26
4.2 VZD-FHIR-Directory.....	26
4.2.1 FHIR-Proxy.....	27
4.2.2 Auth-Service.....	28
4.2.3 OAuth.....	28
4.2.4 FHIR-Directory.....	28
4.3 TI-Messenger-Fachdienst.....	28
4.3.1 Registrierungs-Dienst.....	29
4.3.2 Push-Gateway.....	30
4.3.3 Messenger-Service.....	30
4.3.3.1 Messenger-Proxy.....	30
4.3.3.1.1 Client-Server Proxy.....	31

4.3.3.1.2 Server-Server Proxy.....	31
4.3.3.1.3 Weiterführende Vorgaben.....	32
4.3.3.2 Matrix-Homeserver.....	32
<b>4.4 TI-Messenger-Client.....</b>	<b>32</b>
<b>5 Übergreifende Festlegungen.....</b>	<b>34</b>
<b>5.1 Datenschutz und Sicherheit.....</b>	<b>34</b>
<b>5.2 Verwendete Standards.....</b>	<b>34</b>
5.2.1 Matrix.....	34
5.2.2 OpenID-Connect.....	35
5.2.3 FHIR.....	35
<b>5.3 Authentifizierung und Autorisierung.....</b>	<b>35</b>
5.3.1 Authentifizierung von Akteuren am Messenger-Service.....	35
5.3.2 Authentifizierung am VZD-FHIR-Directory.....	36
5.3.2.1 Registrierungs-Dienst.....	36
5.3.2.2 TI-Messenger-Client.....	36
5.3.3 Autorisierung am Messenger-Service.....	37
5.3.4 Autorisierung am VZD-FHIR-Directory.....	37
5.3.4.1 Registrierungs-Dienst.....	37
5.3.4.2 TI-Messenger-Client.....	37
<b>5.4 Rechtekonzept VZD-FHIR-Directory.....</b>	<b>37</b>
5.4.1 Lesezugriff.....	37
5.4.1.1 Registrierungs-Dienst.....	37
5.4.1.2 TI-Messenger-Clients.....	37
5.4.2 Schreibzugriff.....	38
5.4.2.1 Registrierungs-Dienst.....	38
5.4.2.2 TI-Messenger-Clients.....	38
<b>5.5 User Management.....</b>	<b>39</b>
<b>5.6 Funktionsaccounts.....</b>	<b>40</b>
5.6.1 Chatbot.....	41
<b>5.7 Test.....</b>	<b>43</b>
<b>5.8 Betrieb.....</b>	<b>44</b>
<b>6 Anwendungsfälle.....</b>	<b>46</b>
<b>6.1 AF - Authentisieren einer Organisation am TI-Messenger-Dienst.....</b>	<b>48</b>
<b>6.2 AF - Bereitstellung eines Messenger-Service für eine Organisation.....</b>	<b>52</b>
<b>6.3 AF - Organisationsressourcen im Verzeichnisdienst hinzufügen.....</b>	<b>55</b>
<b>6.4 AF - Anmeldung eines Akteurs am Messenger-Service.....</b>	<b>58</b>
<b>6.5 AF - Akteur (User-HBA) im Verzeichnisdienst hinzufügen.....</b>	<b>62</b>
<b>6.6 AF - Föderationszugehörigkeit eines Messenger-Service prüfen.....</b>	<b>65</b>
<b>6.7 AF - Einladung von Akteuren innerhalb einer Organisation.....</b>	<b>68</b>
<b>6.8 AF - Austausch von Events zwischen Akteuren innerhalb einer Organisation.....</b>	<b>71</b>
<b>6.9 AF - Einladung von Akteuren außerhalb einer Organisation.....</b>	<b>74</b>

6.10 AF - Austausch von Events zwischen Akteuren außerhalb einer Organisation.....	78
<b>7 Anhang A - Verzeichnisse.....</b>	<b>82</b>
7.1 Abkürzungen.....	82
7.2 Glossar.....	83
7.3 Abbildungsverzeichnis.....	83
7.4 Tabellenverzeichnis.....	85
7.5 Referenzierte Dokumente.....	86
7.5.1 Dokumente der gematik.....	86
7.5.2 Weitere Dokumente.....	86
<b>8 Anhang B - Abläufe.....</b>	<b>88</b>
8.1 Einträge im VZD-FHIR-Directory suchen.....	88
8.2 Aktualisierung der Föderationsliste.....	90
8.3 Stufen der Berechtigungsprüfung.....	93

---

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

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 die beschriebenen Produkttypen betreiben. 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 Anwendungsfalles wird in den jeweiligen Steckbriefen festgelegt, in denen jeweils der Anwendungsfall gelistet ist. Akzeptanzkriterien werden in der Regel nicht im Steckbrief gelistet.

### Hinweis auf offene Punkte

*Offener Punkt: Das Kapitel wird in einer späteren Version des Dokumentes ergänzt.*

---

## 2 Systemüberblick

---

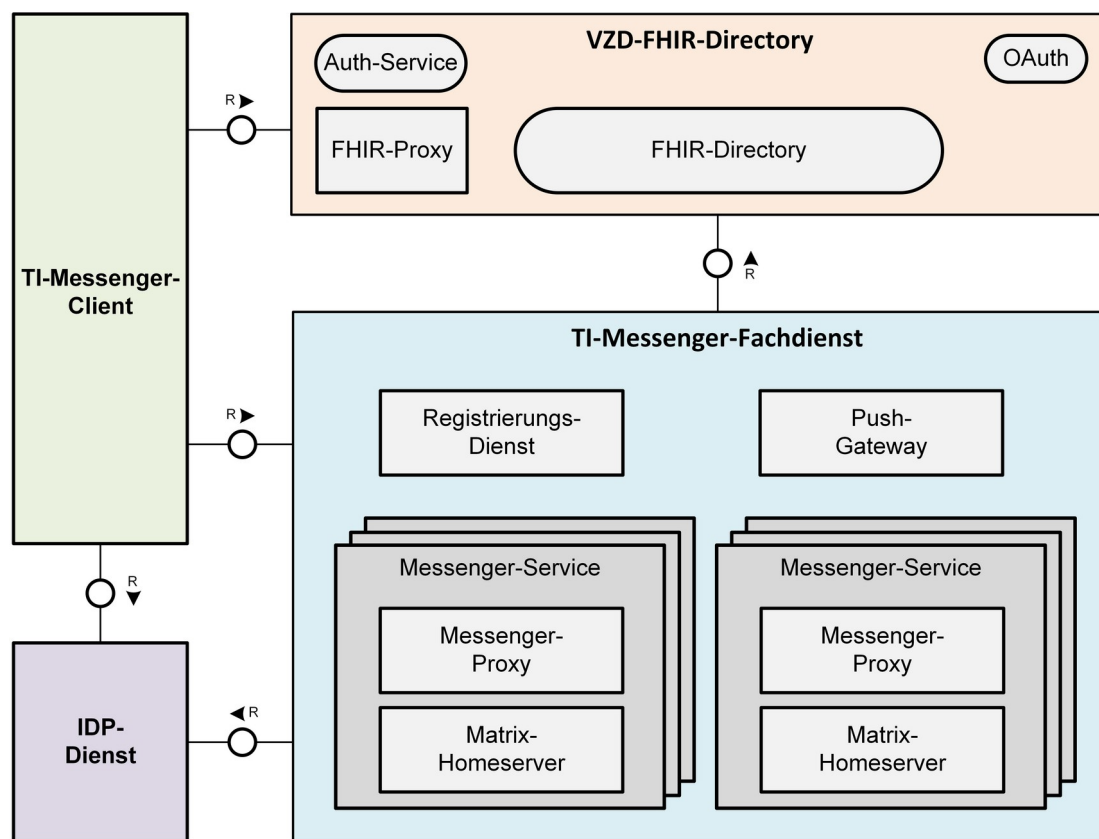
Der sichere Nachrichtenaustausch zwischen beteiligten Akteuren des deutschen Gesundheitswesens erfolgt über die von TI-Messenger-Anbietern bereitgestellten TI-Messenger-Fachdienste und TI-Messenger-Clients. Die Ad-Hoc Kommunikation zwischen den Akteuren findet hierbei über zugelassene TI-Messenger-Clients 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 (basierend auf dem Matrix-Protokoll) die jeweils für eine Organisation (SMC-B-Inhaber) des Gesundheitswesens bereitgestellt 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 eingesetzten Authentifizierungsmethoden nachnutzen. Dies ermöglicht eine nahtlose Integration in den Alltag. 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 verwendet werden. Messenger-Services KÖNNEN mit unterschiedlichen TI-Messenger-Clients verwendet werden. So ist es beispielsweise möglich, dass ein Arzt, der parallel in einer Klinik und in einer niedergelassenen Praxis tätig ist, durch beide Organisationen jeweils einen Messenger-Service zur Verfügung gestellt 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 zu werden, MUSS die jeweilige Domain eines Messenger-Services vom TI-Messenger-Anbieter durch den Registrierungs-Dienst des TI-Messenger-Fachdienstes im VZD-FHIR-Directory hinterlegt werden. Ist dies erfolgt, erhalten dessen Akteure Lesezugriff auf das VZD-FHIR-Directory und KÖNNEN je nach Berechtigung die Kommunikation mit Akteuren in anderen Organisationen starten. Die Kommunikation findet dabei Ende-zu-Ende-verschlüsselt zwischen den TI-Messenger-Clients der beteiligten Messenger-Services 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, MUSS der TI-Messenger-Fachdienst über ein Push-Gateway verfügen.

*Hinweis: Im Sinne des Matrix-Protokolls sind Enden Endgeräte - in der Matrix-Spezifikation als "devices" bezeichnet -, welche die Fähigkeit haben, die an sie gesendeten Daten erstmalig nach der vollständigen Übertragung zu entschlüsseln. Dabei ist zu beachten, dass mit "Endgeräten" dedizierte Client-Instanzen und nicht zwangsläufig physische Geräte gemeint sind, die eindeutig über ihre `device_ID` identifizierbar sind und von einem Client in dem Moment erzeugt werden, in dem dieser zur Anmeldung an einem Nutzerkonto verwendet wird. Damit sind ein oder mehrere Endgeräte einem Nutzerkonto, das selbst durch eine kryptographische Identität gekennzeichnet ist, untergeordnet und befähigen den Nutzer überhaupt erst zum Empfang und Versand Ende-zu-Ende-verschlüsselter Daten. Erst nach der Entschlüsselung der Daten können diese von einem Nutzer gelesen und von den von ihm eingesetzten Systemen wie beispielsweise einem Krankenhausinformationssystem dem Zweck entsprechend verarbeitet werden.*

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 Specification] spezifiziert ist. In den von der Matrix Foundation erstellten Spezifikationen ist sowohl die Client-Server-, die Server-Server-Kommunikation 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 Einschränkung des Nutzerkreises werden weitere Komponenten benötigt, welche in der jeweiligen durch die gematik veröffentlichten Spezifikation beschrieben werden.

---

## 3 Systemkontext

---

### 3.1 Akteure und Rollen

Im Kontext des TI-Messenger-Dienstes werden verschiedene Akteure und Rollen 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. Im Folgenden werden diese Rollen weiter beschrieben.

#### 3.1.1 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.

#### 3.1.2 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.

### 3.1.3 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 oder durch das KIM-Verfahren authentifiziert haben (siehe Anwendungsfall AF\_10103 - Authentifizieren 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 erfolgreichen 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
Leistungserbringer (z. B. Ärzte, Zahnärzte, Apotheker, psychologische Psychotherapeuten, Pflegepersonal, Hebammen, Mitarbeiter einer Kasse) im Sinne SGB V	HBA	VZD-FHIR-Directory über den zentralen IDP-Dienst	User-HBA
	Authentifizierungsverfahren der Organisation + 2. Faktor	Messenger-Service	User
	Admin-Account Credentials + 2. Faktor	Registrierungs-Dienst	Org-Admin
Mitarbeiter einer	Authentifizierungsverfahren der	Messenger-	User

Organisation im Gesundheitswesen, die keine Leistungserbringer im Sinne SGB V sind.	Organisation + 2. Faktor	Service	
	Admin-Account Credentials + 2. Faktor	Registrierungs-Dienst	Org-Admin
Beauftragter Administrator eines TI-Messenger-Anbieters	Admin-Account Credentials + 2. Faktor	Registrierungs-Dienst	Org-Admin
Chatbot	Authentifizierungsverfahren der Organisation	Messenger-Service	User

#### Hinweis:

- Bei den in der Tabelle genannten Nutzerszenarien mit der 2-Faktor-Authentifizierung MUSS der TI-Messenger Anbieter sicherstellen, dass die Sicherheitsempfehlungen des Bundesamt für Sicherheit in der Informationstechnik (BSI) gemäß [BSI 2-Faktor] berücksichtigt werden. Hierbei MUSS zur Resilienz gegen Angriffe aus der Ferne ein Verfahren gewählt werden, das mindestens mit "mittel" bewertet ist.
- Versicherte DÜRFEN aktuell NICHT als Akteure auf einem Messenger-Service eingetragen werden. Für die Nutzung eines Messenger-Service sind nur Akteure zugelassen, die durch ein bestehendes Vertragsverhältnis der jeweiligen Organisation zugeordnet werden können oder 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.

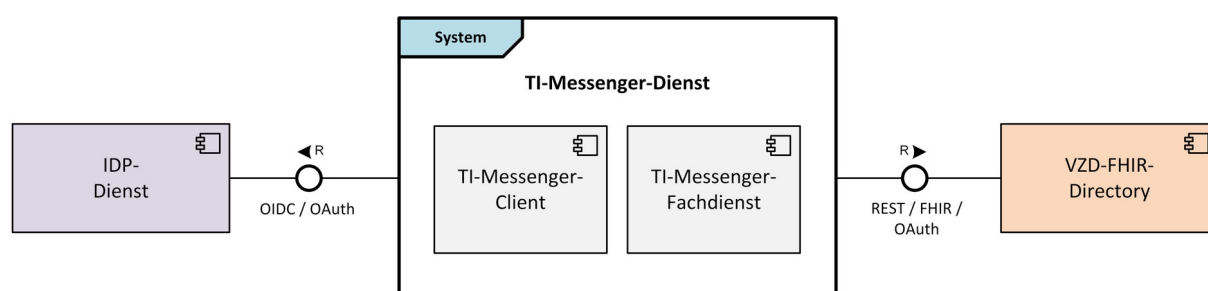
**Tabelle 2: Kommunikationsmatrix**

Org-Admin	User	User-HBA	Kommunikationsart
<b>Ausgehende Kommunikation an:</b>			
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 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-Dienstes zur Authentifizierung eines Akteurs sowie Schnittstellen des VZD-FHIR-Directory, um z. B. FHIR-Ressourcen zu finden oder zu ändern.

## 3.3 Ausprägungen des Messenger-Services

Der Messenger-Service ist eine Teilkomponente des TI-Messenger-Fachdienstes und wird durch den jeweiligen Anbieter für Organisationen bereitgestellt. Der Messenger-Service besteht aus einem Matrix-Homeserver (basierend auf dem Matrix-Protokoll) und einem Messenger-Proxy der sicherstellt, dass eine Kommunikation mit anderen Messenger-Services, als Teil des TI-Messenger-Dienstes, nur innerhalb der gemeinsamen TI-Föderation erfolgt. Die Messenger-Services KÖNNEN den Akteuren unterschiedliche

Authentifizierungsverfahren anbieten, bei denen der Besitz einer SMC-B oder eines HBAs nicht vorausgesetzt wird. Messenger-Services MÜSSEN immer Organisationen bzw. Verbänden zugeordnet sein, die über die Kontrolle 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 Akteure bereitgestellt werden. Die Organisation und der von ihr gewählte TI-Messenger-Anbieter vereinbaren das zur Anwendung kommende Authentifizierungsverfahren bilateral und stimmen sich über die technische Realisierung der dafür notwendigen Anbindung ab. Möglich ist beispielsweise die Nachnutzung eines in der Organisation betriebenen Active Directory (AD/LDAP) oder eines geeigneten Single-Sign-On-Verfahrens (SSO). Der Anbieter MUSS sicherstellen, dass die Organisation die Kontrolle über die jeweiligen Authentifizierungsmechanismen besitzt und die Möglichkeit erhält eine notwendige Löschung oder Sperrung eines Nutzer-Accounts sicherzustellen.

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

### 3.3.1 Anwendungsbeispiel für eine Arztpraxis

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 authentisiert seine Organisation unter Verwendung der SMC-B bei einem Registrierungs-Dienst eines 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. Zusätzlich kann der Akteur in der Rolle "Org-Admin" Akteure für seine Organisation auf den Matrix-Homeserver einrichten (z. B. MFA, Ärzte). Die angelegten Akteure melden sich am Messenger-Service an und können den TI-Messenger in der Rolle "User" direkt nutzen.

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 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 (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. Somit haben sie zusätzlich die Möglichkeit andere, auf dem VZD-FHIR-Directory hinterlegte, HBA-Inhaber (Rolle "User-HBA") in einen Chatraum einzuladen oder für diese erreichbar zu werden.

## **3.3.2 Anwendungsbeispiel für ein Krankenhaus**

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 Nutzereinträge 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 dem Registrierungs-Dienst eines TI-Messenger-Anbieters. Der Registrierungs-Dienst verifiziert die verwendete SMC-B der Organisation. Bei Erfolg stellt 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. Dieser Service wird *on-premise* im Krankenhaus bereitgestellt. Der Messenger-Service verwendet bei der Registrierung der Akteure am Matrix-Homeserver das bestehende Authentifizierungsverfahren des Krankenhauses (z. B. Active Directory). Die Akteure des Krankenhauses können anschließend mit den bestehenden Anmeldedaten den TI-Messenger-Dienst nahtlos verwenden, auch ohne im Besitz eines HBAs (Pflege, Therapeuten) zu sein.

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.

### **3.3.3 Anwendungsbeispiel für Apotheken**

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 betreffendem 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 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 die Apotheke, der in einem Rechenzentrum bereitgestellt wird. Für die Authentifizierung der Akteure am Messenger-Service wird der zuständige IDP-Dienst der Apotheken verwendet, so dass die dort hinterlegten Akteure der Apotheken sich am TI-Messenger mittels OpenID-Connect anmelden können.

Die Apotheke wird als Organisation für andere Akteure des TI-Messengers erreichbar, indem ein Akteur in der Rolle "Org-Admin" MXIDs von Akteuren seiner Apotheke im Organisationsverzeichnis auf dem VZD-FHIR-Directory einrichtet. Akteure der Apotheke im Besitz eines HBAs (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 die Möglichkeit andere, auf dem VZD-FHIR-Directory hinterlegte, HBA-Inhaber (Rolle "User-HBA") in einen Chatraum einzuladen oder für diese erreichbar zu werden.

### 3.3.4 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. Damit können sie andere, auf dem VZD-FHIR-Directory hinterlegte, HBA-Inhaber (Rolle "User-HBA") in einen Chatraum einladen oder für diese erreichbar werden.

## 3.4 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 3.4- TI-Messenger Föderation beschrieben, dient die TI-Messenger-Föderation dazu, nicht zugelassene Matrix-Homeserver aus 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 notwendig.

Das Rechtekonzept basiert auf einer mehrstufigen Prüfung. Mit Hilfe des Berechtigungskonzeptes wird nachgewiesen, ob ein Akteur berechtigt ist, innerhalb der TI-Messenger-Föderation mit einem anderen Akteur zu interagieren. Die Art der Prüfung ist abhängig davon, ob es sich um eine Client-Server oder Server-Server Kommunikation handelt. Das Berechtigungskonzept wird im Folgenden näher beschrieben.

## 3.5.1 Client-Server Kommunikation

### 3.5.1.1 Berechtigungskonzept - Stufe 1

In dieser Stufe MUSS bei der Client-Server Kommunikation geprüft werden, ob die in der Anfrage enthaltenen Matrix-Domains zugehörig zur TI-Föderation sind. Hierbei MUSS der Messenger-Proxy bei jedem Invite-Event prüfen, ob die in der Anfrage vom TI-Messenger-Client enthaltenen Matrix-Domains der Einzuladenden in der Föderationsliste enthalten sind. Ist dies der Fall, MUSS die Anfrage durch den Messenger-Proxy 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 des Einladenden prüft dieser, ob der eingeladene Akteur der gleichen Organisation angehört. Stellt der Matrix-Homeserver im Rahmen der obigen Prüfung fest, dass der eingeladene Akteur nicht zu seiner Domain gehört, wird das Invite-Event an den Messenger-Proxy des Matrix-Homeservers des einzuladenden Akteurs gerichtet, wobei die Regeln der Server-Server Kommunikation durchzuführen sind.

## 3.5.2 Server-Server Kommunikation

### 3.5.2.1 Berechtigungskonzept - Stufe 1

In der 1. Stufe der Server-Server Kommunikation MUSS der Messenger-Proxy für alle Events eine Prüfung durchführen, die feststellt, ob die im Event enthaltenen Matrix-Domains zur TI-Föderation gehören. Zur Prüfung der Föderationszugehörigkeit MUSS der Messenger-Proxy im Authorization-Header die im Attribut "origin" enthaltene Domain (bei eingehender Kommunikation) und die im Attribut "destination" enthaltene Domain (bei ausgehender Kommunikation) gegen die Domains in der Föderationsliste prüfen. Bei erfolgreicher Prüfung erfolgt dann die Weiterverarbeitung gemäß der Stufe 2.

### 3.5.2.2 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.

### 3.5.2.3 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.

### 3.6 Verwendung der Token

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

**Tabelle 3: Arten von Token**

Token	ausgestellt vom	Beschreibung
ID_TOKEN	zentralen IDP-Dienst	<p>Dieses Token wird auf Basis von SmartCard-Identitäten vom zentralen IDP-Dienst ausgestellt und beinhaltet die zugehörigen Identitätsdaten (TelematikID, ProfessionOID etc.).</p> <p>Der Registrierungs-Dienst nutzt dieses Token, um die enthaltene ProfessionOID auf einen gültigen Institutionstypen für eine SMC-B zu prüfen und im Rahmen einer Messenger-Service Bestellung die enthaltene TelematikID in die Föderationsliste einzutragen.</p> <p>Das VZD-FHIR-Directory nutzt dieses Token, um zu ermitteln für welche Ressource (identifiziert durch die TelematikID) ein owner-accesstoken ausgestellt wird.</p>
Matrix-ACCESS_TOKEN	Matrix-Homeserver	<p>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.</p> <p>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.</p>
Matrix-OpenID-Token	Matrix-Homeserver	<p>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.</p>

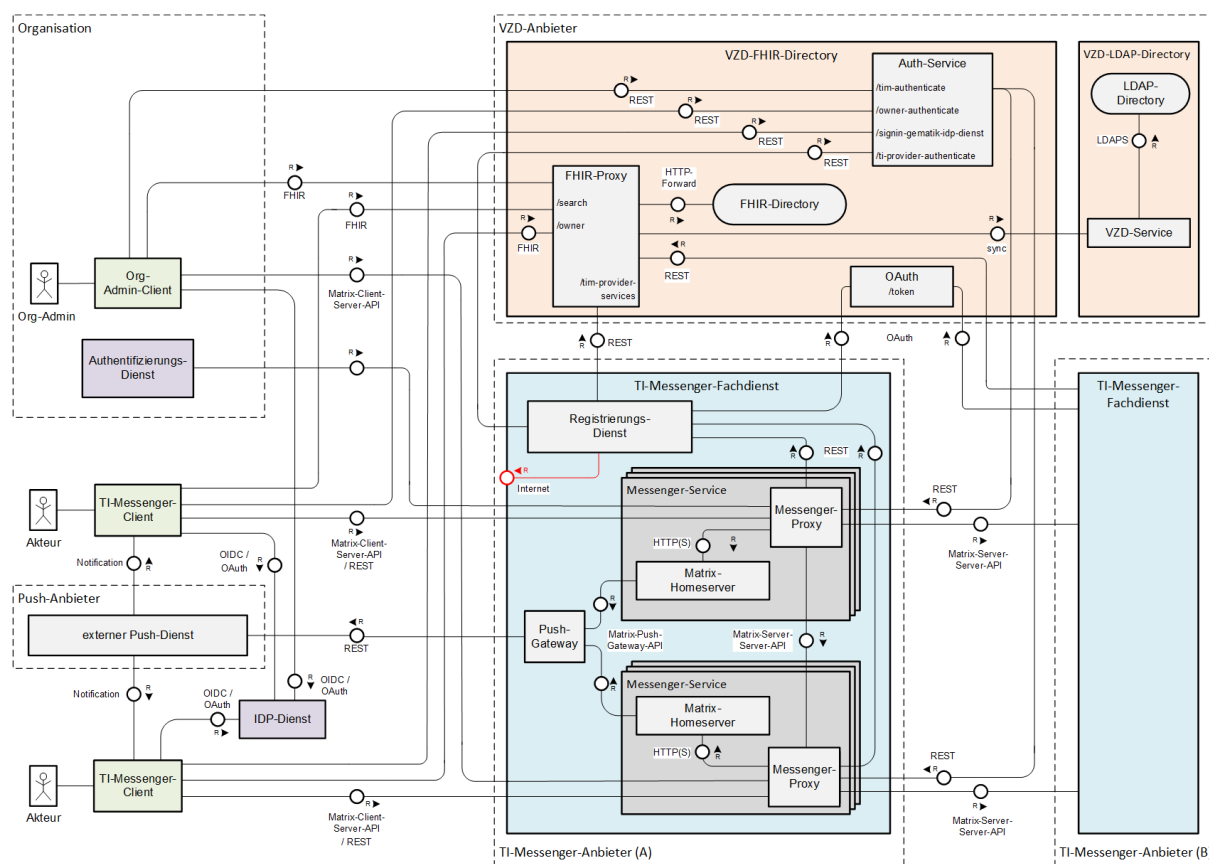
		<p>Das Matrix-OpenID-Token wird für die Verifizierung eines Messenger-Services sowie für das Suchen von FHIR-Ressourcen im VZD-FHIR-Directory benötigt. Hierfür wird das Matrix-OpenID-Token im Auth-Service des Verzeichnisdienstes gegen ein search-accesstoken ersetzt, welches am FHIR-Proxy für die weitere 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.</p>
RegService-OpenID-Token	Registrierungs-Dienst	<p>Bei dem RegService-OpenID-Token handelt es sich um ein JSON-Web-Token, welches von einem Registrierungs-Dienst bei Bedarf für einen Akteur in der Rolle "Org-Admin" ausgestellt wird.</p> <p>Das RegService-OpenID-Token wird für die Bearbeitung der FHIR-Ressourcen im VZD-FHIR-Directory benötigt. Hierfür wird das RegService-OpenID-Token im Auth-Service des Verzeichnisdienstes gegen ein owner-accesstoken ersetzt, welches am FHIR-Proxy für die weitere Verarbeitung benötigt wird.</p>
ti-provider-accesstoken / provider-accesstoken	OAuth / Auth-Service des VZD-FHIR-Directory	<p>Das ti-provider-accesstoken wird dem Registrierungs-Dienst durch den OAuth-Service und das provider-accesstoken durch den Auth-Service des VZD-FHIR-Directory bereitgestellt.</p> <p>Ein provider-accesstoken wird z. B. benötigt, wenn der Registrierungs-Dienst eines TI-Messenger-Fachdienstes, nach der Bereitstellung eines neuen Messenger-Service für eine Organisation, einen neuen Förderationslisteneintrag für diese Organisation anlegt oder der Registrierungs-Dienst eine Förderationsliste vom FHIR-Proxy abfragen möchte. Hierfür übergibt der Registrierungs-Dienst im ersten Schritt vereinbarte Client-Credentials an den OAuth-Service des VZD-FHIR-Directory und erhält nach der erfolgreichen Prüfung dieser Credentials das ti-provider-accesstoken. Das ti-provider-accesstoken wird anschließend an den Auth-Service des VZD-FHIR-Directory übergeben und bei erfolgreicher Prüfung durch das VZD-FHIR-Directory wird ein provider-accesstoken ausgestellt.</p>
search-accesstoken	Auth-Service des VZD-FHIR-Directory	<p>Das search-accesstoken wird einem berechtigten Akteur durch den Auth-Service des VZD-FHIR-Directory bereitgestellt.</p>

		<p>Dieses wird für die Suche im VZD-FHIR-Directory benötigt und stellt sicher, dass nur berechnigte 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.</p>
owner-accesstoken	Auth-Service des VZD-FHIR-Directory	<p>Das owner-accesstoken wird einem berechtigten Akteur durch den Auth-Service des VZD-FHIR-Directory bereitgestellt.</p> <p>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 den zentralen 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.</p>

## 4 Systemzerlegung

Wie bereits im Kapitel 2- Systemüberblick dargestellt sind bei der Umsetzung der Funktionalitäten des TI-Messenger-Dienstes mehrere Komponenten beteiligt, die durch verschiedene Anbieter bereitgestellt werden. 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. Weitere mögliche Formulierungen sind "zuständiger IDP", "zuständiger IDP-Dienst" oder "ein IDP-Dienst". 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 der Begriff IDP-Dienst verwendet, der in der ersten Ausbaustufe den zentralen IDP-Dienst meint.

## 4.2 VZD-FHIR-Directory

Beim VZD-FHIR-Directory handelt es sich um einen zentralen Verzeichnisdienst 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 3.6- 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-Directory 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.

### 4.2.1 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.

### 4.2.2 Auth-Service

Die Teilkomponente Auth-Service stellt den TI-Messenger-Clients sowie dem Registrierungs-Dienst eines TI-Messenger Fachdienstes die für den Aufruf der FHIR-

Schnittstellen am FHIR-Proxy benötigten access-token aus. Hierbei werden die folgenden REST-Schnittstellen:

- /tim-authenticate,
- /owner-authenticate,
- /signin-gematik-idp-dienst und
- /ti-provider-authenticate

verwendet. Die Schnittstelle /tim-authenticate erwartet ein Matrix-OpenID-Token, wohingegen bei der Schnittstelle /owner-authenticate das von einem Registrierungs-Dienst ausgestellte RegService-OpenID-Token übergeben werden muss. Alternativ KANN eine Authentisierung mittels Smartcard am zentralen IDP-Dienst der gematik durchgeführt werden und der erhaltene AuthorizationCode an die Schnittstelle /signin-gematik-idp-dienst übergeben werden. Die Schnittstelle /ti-provider-authenticate erwartet ein ti-provider-accesstoken, welches zuvor vom OAuth-Service des VZD-FHIR-Directories ausgestellt wurde.

## 4.2.3 OAuth

Die Teilkomponente OAuth stellt dem Registrierungs-Dienst über den /token-Endpunkt ein für den OAuth2 Client Credentials Flow temporäres ti-provider-accesstoken aus. Bevor der Registrierungs-Dienst den /token-Endpunkt am OAuth-Service aufrufen kann MUSS sich der TI-Messenger-Anbieter zuvor beim VZD-Anbieter Client-Credentials beantragen, die bei Aufruf des Endpunktes mit übergeben werden MÜSSEN.

## 4.2.4 FHIR-Directory

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

## 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 die in der TI-Föderation gelisteten TI-Messenger-Fachdienste übermittelt. Es MUSS sichergestellt werden, dass die Organisation die Akteure jederzeit identifizieren kann und das die Organisationen Akteure jederzeit aus dem TI-Messenger-Dienst ausschließen können. Daher MUSS die Kontrolle über die Identitäten bei der Organisation liegen. Hierbei ist eine Delegation, 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.*

## 4.3.1 Registrierungs-Dienst

Der Registrierungs-Dienst ist eine Komponente, die vom Hersteller des TI-Messenger-Fachdienstes umgesetzt werden MUSS. Durch 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 SOLL automatisch erfolgen. Ebenfalls KANN über den Registrierungs-Dienst das Accounting durchgeführt werden. Dies wird von der gematik nicht normativ festgelegt.

Um einen benutzerfreundlichen Onboarding-Prozess zu gewährleisten MUSS der Registrierungs-Dienst die Bereitstellung eines Messenger-Service über ein Frontend ermöglichen (im Folgenden auch als Frontend des Registrierungs-Dienstes bezeichnet). Hierfür MUSS sich die Organisation gegenüber dem Registrierungs-Dienst authentifizieren. Die Authentifizierung KANN hierbei entweder über OpenID Connect oder über eine bestehende KIM-Adresse der Organisation erfolgen. Bei der Authentifizierung via OpenID Connect wird ein durch den zentralen IDP-Dienst ausgestelltes ID\_TOKEN am Registrierungs-Dienst validiert. Bei der Authentifizierung mittels bestehender KIM-Adresse der Organisation wird durch den Registrierungs-Dienst eine KIM-Nachricht an die Organisation gesendet und durch Bestätigung einer in der KIM-Nachricht enthaltenen URL, die Organisation verifiziert. Nach der erfolgreichen Authentisierung einer Organisation wird für einen 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-Services für seine Organisation zu registrieren. Dazu MUSS das Frontend des Registrierungs-Dienstes beim zentralen IDP-Dienst registriert sein. Vor dem Anlegen eines neuen Messenger-Service MUSS der Registrierungs-Dienst prüfen, ob der beantragte Domain-Name verfügbar ist und diesen zur TI-Messenger Föderation hinzufügen.

Neben der Registrierung neuer Messenger-Services, dient der Registrierungs-Dienst als Middleware zwischen TI-Messenger-Services und dem VZD-FHIR-Directory und speichert eine aktuelle Liste aller verifizierten Domains (Föderationsliste), damit diese von den Messenger-Proxies des TI-Messenger-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). Zusätzlich stellt der Registrierungs-Dienst ID\_TOKEN (RegService-OpenID-Token) aus, die für die Berechtigung zur Änderung von Organisations-Einträgen im VZD-FHIR-Directory verwendet werden.

## 4.3.2 Push-Gateway

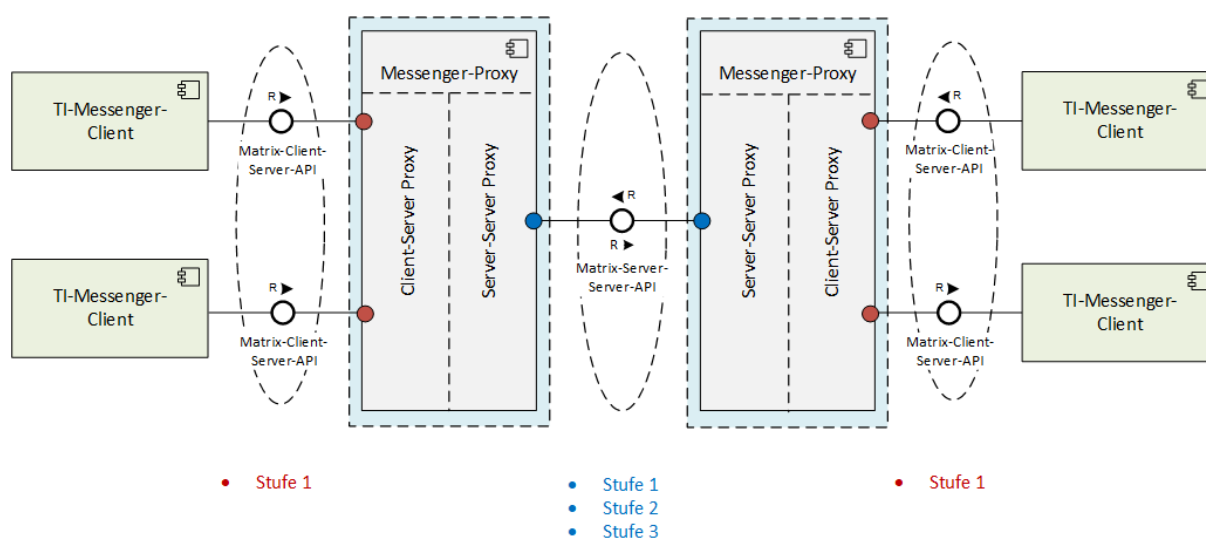
Jeder Anbieter eines TI-Messenger-Fachdienstes MUSS ein Push-Gateway bereitstellen, um seinen registrierten Akteuren den Eingang neuer Nachrichten zu signalisieren. Das Push-Gateway ist gemäß der Matrix-Foundation-Spezifikation [Push Gateway API] zu implementieren. Dieses leitet die Benachrichtigung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

### 4.3.3 Messenger-Service

Ein Messenger-Service besteht aus einem Messenger-Proxy 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. 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.

#### 4.3.3.1 Messenger-Proxy

Der Messenger-Proxy als Prüfinstanz aller eingehenden sowie ausgehenden 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 Prüfregele 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**

##### 4.3.3.1.1 Client-Server Proxy

In der Funktion als Client-Server Proxy prüft der Messenger-Proxy eingehende Invite- und createRoom-Events der TI-Messenger-Clients (in der Abbildung rot dargestellt) und fungiert so als Reverse-Proxy (siehe die im Kapitel 2- Systemüberblick dargestellte Abbildung als Überblick bzw. Kapitel 4- Systemzerlegung für eine Detailansicht). Bei jedem Invite-Event MUSS der Messenger-Proxy prüfen, ob die in der Anfrage enthaltenen Matrix-Domains zur TI-Föderation gehören (siehe Kapitel 3.5.1- Client-Server Kommunikation - Stufe 1 sowie Kapitel 8.3- Stufen der

Berechtigungsprüfung). Nach erfolgreicher Prüfung wird das Event an den Matrix-Homeserver des Einladenden weitergeleitet. Der Matrix-Homeserver prüft daraufhin, ob die beteiligten Akteure auf demselben Matrix-Homeserver registriert sind. Ist dies nicht der Fall, wird das Invite-Event an den zuständigen Messenger-Proxy des Einzuladenden gerichtet, wobei die Regeln der Server-Server Kommunikation durchzuführen sind.

Ebenfalls MUSS der Messenger-Proxy jedes createRoom-Event prüfen. Hierbei MUSS der Messenger-Proxy prüfen, ob das im Event enthaltene Attribut "invite" mit maximal einem Element befüllt ist. Ist dies nicht der Fall, dann MUSS der Messenger-Proxy die Verbindung mit einer Fehlernachricht ablehnen.

### 4.3.3.1.2 Server-Server Proxy

In der Funktion als Server-Server Proxy prüft der Messenger-Proxy alle ausgehenden sowie eingehenden Events. Damit fungiert der Server-Server Proxy sowohl als Forward als auch als Reverse-Proxy. Im Gegensatz zum Client-Server Proxy prüft der Server-Server Proxy bei jedem Event die Domainzugehörigkeit. Somit kann ausgeschlossen werden, dass mit einem nicht mehr zur Föderation gehörenden Messenger-Service kommuniziert werden kann. In der Funktion als Server-Server Proxy MÜSSEN alle Stufen gemäß Kapitel 3.5.2- Server-Server Kommunikation des Berechtigungskonzeptes 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. Darüber hinaus MUSS der Server-Server Proxy auch weitere legitime Anfragen zulassen, die über das Berechtigungskonzept hinausgehen. Beispielweise Anfragen vom VZD-FHIR-Directory an einen Matrix-Homeserver, damit dieser ein zu prüfendes Matrix-OpenID-Token verifizieren kann.

### 4.3.3.1.3 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 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.

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

### 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 Akteure sowie weitere Nutzerinteraktionen (z. B. Starten neuer Räume etc.) statt.

## 4.4 TI-Messenger-Client

Ein TI-Messenger-Client ist eine mobile oder stationäre Anwendung. Diese basiert auf der von der Matrix-Foundation definierten Spezifikation und ermöglicht die Ad-hoc-Kommunikation von Akteuren 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.

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.

---

## 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 Anforderungen, die in den jeweiligen Dokumenten in eigenen Kapiteln untergebracht sind, funktionsbezogenen 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

#### 5.2.1 Matrix

Für den TI-Messenger-Dienst wird das offene Kommunikationsprotokoll der Matrix-Foundation verwendet. Im Rahmen der Spezifikation wird das Server-Server- (gemäß [Server-Server API]) und das Client-Server-Protokoll (gemäß [Client-Server API]) nachgenutzt. Für die Kommunikation der Matrix-Homeserver in der Föderation wird die API gemäß [Server-Server API] verwendet. Der TI-Messenger-Client setzt bei der Kommunikation mit den 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.

Das Matrix-Protokoll erlaubt während der Erstellung eines Chatraumes einen eigene Raumtyp (*Custom Room Type*) für diesen mit Hilfe einer Typinitialisierung im `/createRoom` Endpunkt zu definieren, um spezielle Raumeigenschaften (*Room State*) für diesen *Custom Room Type* zu verwenden. Außerdem erlaubt das Matrix-Protokoll die Eigenschaften eines Chatraumes mit *State Events* zu erweitern bzw. zu ändern. Typische *State Events*, die ein *Room State* definieren und die durch das Matrix-Protokoll definiert sind, sind zum Beispiel `m.room.name` oder `m.room.topic`. Das Matrix-Protokoll erlaubt auch benutzerdefinierte *State Events* (*Custom State Events*) zu verwenden. In der vorliegenden Spezifikation werden bereits erste *Custom Room Types* sowie *Custom State Events* mit von der gematik definierten *Event Types* und *Event Content* definiert. Dies ermöglicht im Kontext des TI-Messengers, eine spezifischere und damit strukturiere und gerichtete Kommunikation durchzuführen, als es mit Standard Matrix-Chaträumen möglich wäre. Konkret werden Definitionen für den Fallbezug (Referenzierung von Behandlungsfällen im medizinischen Versorgungskontext) von Chats sowie für die interne und intersektorale Kommunikation eingeführt. Für die fallbezogene sowie die föderierte und intersektoraler Kommunikation ist es vorgesehen im *Event Content* eines *Custom*

State Events definierte FHIR-Objekte als Payload zu hinterlegen.

*Hinweis: In der vorliegenden Spezifikation wird die produktive Verwendung der Custom Room Types und Custom State Events aktuell nicht gefordert, da die notwendigen Vorbedingungen für den produktiven Einsatz seitens des Matrix-Protokolls noch nicht vollständig erfüllt sind.*

## 5.2.2 OpenID-Connect

Das VZD-FHIR-Directory, der Registrierungs-Dienst sowie die TI-Messenger-Clients nutzen im Rahmen der Authentifizierung ID\_TOKEN in Form eines JSON-Web-Token (JWT) gemäß [OpenID].

## 5.2.3 FHIR

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

## 5.3 Authentifizierung und Autorisierung

### 5.3.1 Authentifizierung von Akteuren am Messenger-Service

Für die Authentifizierung von 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 ihre eigenen Identitätsserver (IDP-Dienst) zu verwenden. Die Abstimmung, welches Authentifizierungsverfahren verwendet wird, trifft die Organisation mit dem jeweiligen TI-Messenger-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.

### 5.3.2 Authentifizierung am VZD-FHIR-Directory

Die Authentifizierung für den Lese- und Schreibzugriff auf das FHIR-Directory erfolgt mit Hilfe von Identitätstoken. Die jeweilige Überprüfung der Identitätstoken erfolgt am FHIR-Proxy des VZD-FHIR-Directory. Die Authentifizierung der Komponenten Registrierungs-Dienst und TI-Messenger-Client wird im Folgenden weiter beschrieben.

### 5.3.2.1 Registrierungs-Dienst

Die Authentifizierung des Registrierungs-Dienstes für die Nutzung der Schnittstelle `I_VZD_TIM_Provider_Services` am VZD-FHIR-Directory erfolgt mittels OAuth am `OAuth/Auth-Service` des VZD-FHIR-Directory. Nach erfolgreicher Authentifizierung mit vereinbarten Client-Credentials wird dem Registrierungs-Dienst ein `provider-accesstoken` ausgestellt.

Die Client Credentials erhält der TI-Messenger Anbieter, indem er einen Service des TI-ITSM-Systems zur Beantragung der Credentials nutzt. Die Beantragung der Credentials dient auch dazu, ein Vertrauensverhältnis zwischen dem Registrierungs-Dienst und dem VZD-FHIR-Directory herzustellen, da der Registrierungs-Dienst `RegService-OpenID-Token` ausstellt, die für die Berechtigung zur Änderung von Organisations-Einträgen im FHIR-Directory verwendet werden. Das Vertrauen zwischen dem VZD-FHIR-Directory und den Registrierungs-Diensten der TI-Messenger Anbieter wird hergestellt, indem der TI-Messenger Anbieter das Signatur-Zertifikats, das für die Signatur des `RegService-OpenID-Tokens` verwendet wird, bei der Beantragung der Client Credentials übergibt und somit bei der Token-Prüfung vom VZD-FHIR-Directory berücksichtigt werden kann. Das Signatur-Zertifikat erhält der TI-Messenger Anbieter mittels eines TI-ITSM-Service `Requests` zur Beantragung von TI-Komponenten-PKI-Zertifikaten (`C.FD.Sig` mit Anwendungskennzeichen `oid_tim`). Ein `RegService-OpenID-Token` mit der `TelematikID` der Organisation wird nach erfolgreichem Login eines Akteurs in der Rolle "Org-Admin" der Organisation ausgestellt.

### 5.3.2.2 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.

### 5.3.3 Autorisierung am Messenger-Service

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

## **5.3.4 Autorisierung am VZD-FHIR-Directory**

### **5.3.4.1 Registrierungs-Dienst**

Für den Schreibzugriff des Registrierungs-Dienstes autorisiert dieser sich gegenüber dem FHIR-Proxy des VZD-FHIR-Directory mit einem provider-accesstoken, welches vom Auth-Service des VZD FHIR-Directory ausgestellt wurde.

### **5.3.4.2 TI-Messenger-Client**

Für den Lesezugriff autorisieren sich TI-Messenger-Clients gegenüber dem FHIR-Proxy des VZD-FHIR-Directory mit einem search-accesstoken, welches vom Auth-Service des VZD FHIR-Directory ausgestellt wurde. Für den Schreibzugriff nutzen TI-Messenger-Clients das owner-accesstoken, welches vom Auth-Service des VZD FHIR-Directory ausgestellt wurde.

## **5.4 Rechtekonzept VZD-FHIR-Directory**

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

### **5.4.1 Lesezugriff**

#### **5.4.1.1 Registrierungs-Dienst**

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

#### **5.4.1.2 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**

#### **5.4.2.1 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.

### 5.4.2.2 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**

Rolle	Identität	FHIR-Ressource	Beschreibung
Org-Admin	SMC-B (stellvertretend durch einen RegService-OpenID-Token)	HealthcareService	Ein Akteur in der Rolle "Org-Admin" kann mit Hilfe eines TI-Messenger-Clients mit Administrationsfunktion und nach Authentisierung mit einem RegService-OpenID-Token, FHIR-Ressourcen im Namen der Organisation im Organisationsverzeichnis des VZD-FHIR-Directory bearbeiten, um zum Beispiel einen neuen Endpunkt unterhalb eines <i>HealthcareService</i> zu hinterlegen. Das RegService-OpenID-Token erhält der Akteur in der Rolle "Org-Admin" nach erfolgreicher Anmeldung am Registrierungs-Dienst durch Aufruf der vom Anbieter bereitgestellten Schnittstelle <i>I_requestToken</i> .
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 <i>PractitionerRole</i> um einen Endpunkt im Personenverzeichnis zu erweitern, um für andere Leistungserbringer anschreibbar zu werden oder um andere Leistungserbringer anzuschreiben.

## 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 am Matrix-Homeserver registriert. Bei der Erstellung des Nutzer-Accounts wird die MXID 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 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**

<b>Rolle</b>	<b>Client</b>	<b>Administration</b>	<b>Wo</b>
Org-Admin	TI-Messenger Client mit Administrationsfunktionen (Org-Admin-Client)	<ul style="list-style-type: none"> <li>Nutzer-Account anlegen</li> <li>Nutzer-Account verwalten</li> </ul>	Matrix-Homeserver (User Directory)
		<ul style="list-style-type: none"> <li>HealthcareService-Ressource anlegen</li> <li>Endpoint einer HealthcareService-Ressource anlegen</li> <li>Endpoint einer HealthcareService-Ressource verwalten</li> </ul>	VZD-FHIR-Directory (Organisationsverzeichnis)
User	TI-Messenger Client	<ul style="list-style-type: none"> <li>Nutzer-Account anlegen</li> </ul>	Matrix-Homeserver (User Directory)
User - HBA	TI-Messenger Client	<ul style="list-style-type: none"> <li>Endpoint einer PractitionerRole-Ressource anlegen</li> <li>Endpoint einer</li> </ul>	VZD-FHIR-Directory (Personenverzeichnis)

		PractitionerRole- Ressource verwalten	
--	--	--	--

## 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 "payloadTyp: *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 im URI Format eines Chatbots oder eines Akteurs (der stellvertretend für die Organisation eintritt) in das "address" Attribut der Endpoint Ressource hinterlegt. 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.

### 5.6.1 Chatbot

Chatbots sind spezielle Akteure (siehe Kapitel 3.1- Akteure und Rollen), die stellvertretend für eine Struktur einer Organisation von einem die Kommunikation initiiierenden 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	Empfang_Kardiologie (Chatbot)

			@MXID_02:<domain>.de	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:

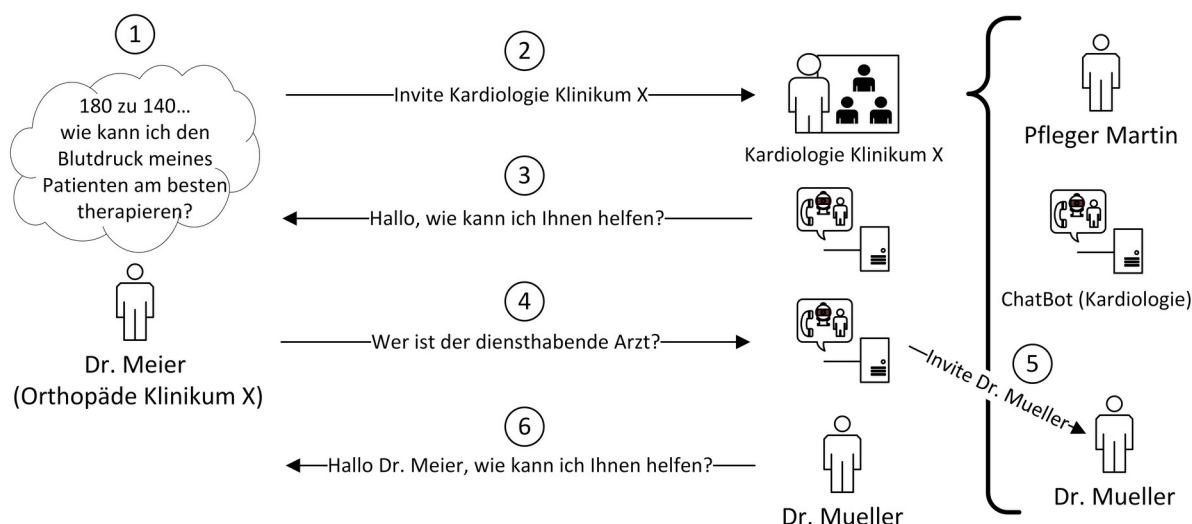
- Der Akteur in der Rolle "Org-Admin" legt einen Funktionsaccount (organisationsbezogene MXID) als einen *Endpoint* des gewünschten *HealthcareService* der Organisation an und ordnet dieser MXID einen Chatbot zu
- Der Akteur in der Rolle "Org-Admin" weist zuständige Akteure der Organisation (personenbezogene 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**

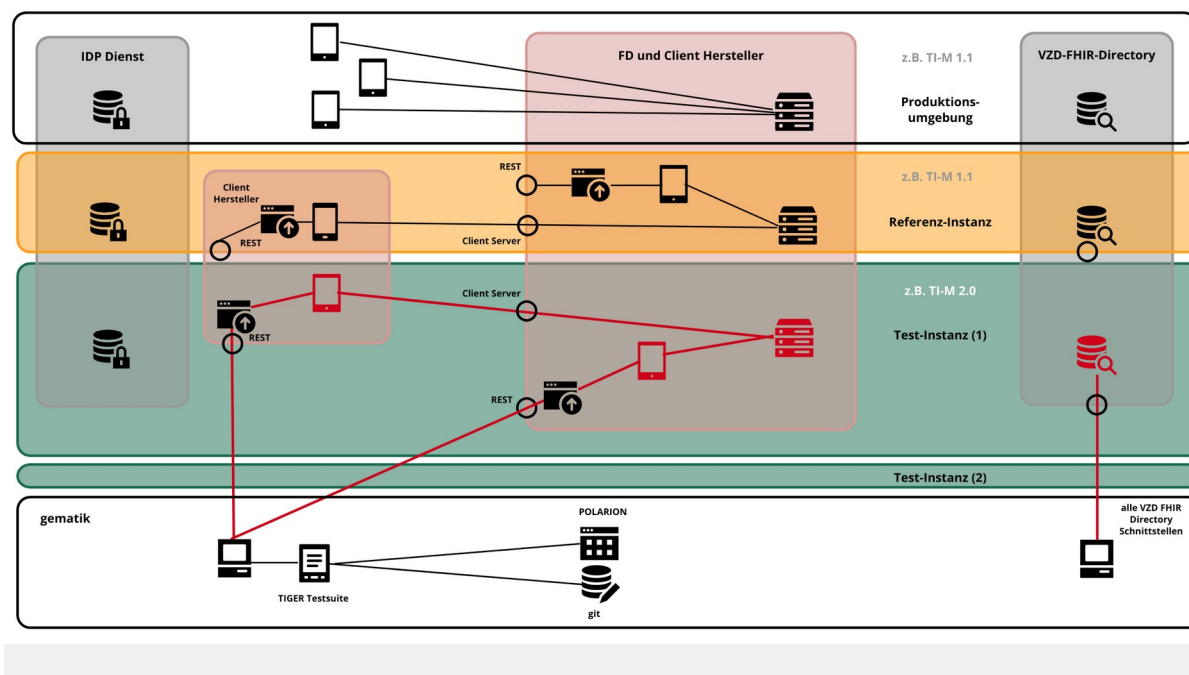
## 5.7 Test

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**

*Hinweis: Grundsätzlich ist es möglich, eine CC-Zertifizierung für das Gesamtprodukt oder Produktbestandteile durchzuführen und damit andere Testtypen und -arten, die die sicherheitstechnische Eignung prüfen sowie Produktgutachten zu ersetzen.*

## 5.8 Betrieb

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

- TI-Messenger-Fachdienst(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.

### A\_23658 - Produktnachweise im Rahmen der kontrollierten Inbetriebnahme

Das Produkt MUSS die Vorgaben zur Funktionalität, Sicherheit und Interoperabilität entsprechend des jeweiligen Produkttypsteckbriefs in der Produktivumgebung erfüllen. Die Nachweise dafür MÜSSEN entsprechend und im Rahmen des Konzepts zur kontrollierten Inbetriebnahme erbracht werden.

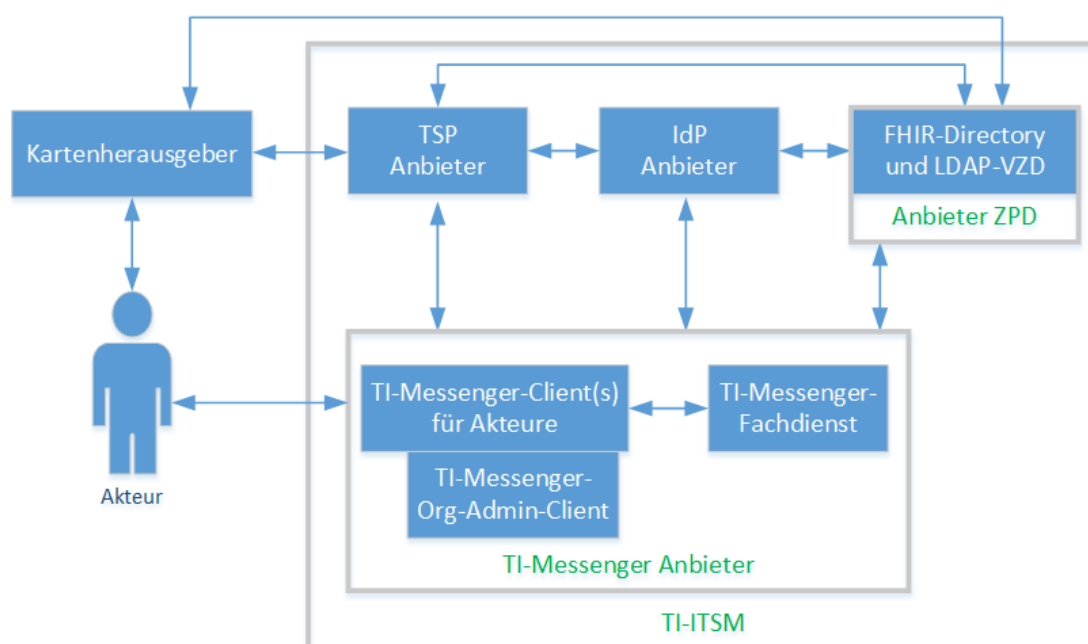
**[<=]**

*Hinweis: Die Anforderung [A\_22658] ist eine Ergänzung für die Produktivumgebung und ersetzt nicht die vorgelagerten Prüfverfahren der Produkte in der Referenzumgebung.*

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 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.



**Abbildung 7: Ausschnitt - TI-Messenger-Anbieter im TI-ITSM**

*Hinweis: Die Abbildung bildet die organisatorischen Kommunikationsbeziehungen im Vordergrund des TI-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.*

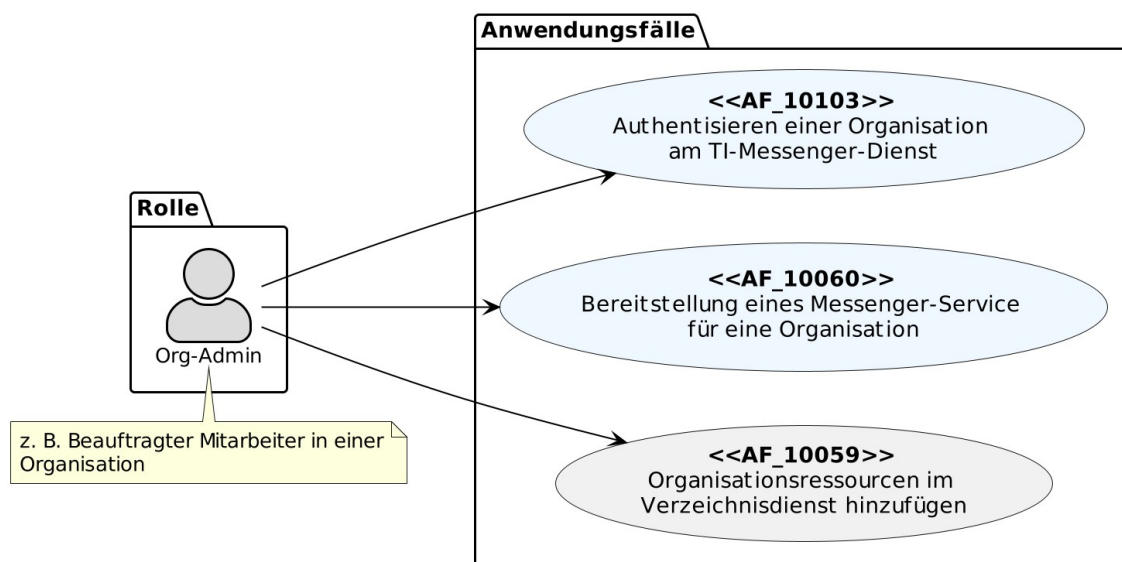
## 6 Anwendungsfälle

Die nachfolgend beschriebenen Anwendungsfälle sind spezifisch für den TI-Messenger-Dienst und weichen daher teilweise von der Matrix-Client-Server-API ab. Das gleiche gilt für die auf dem Matrix-Server-Server-Protokoll ([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.



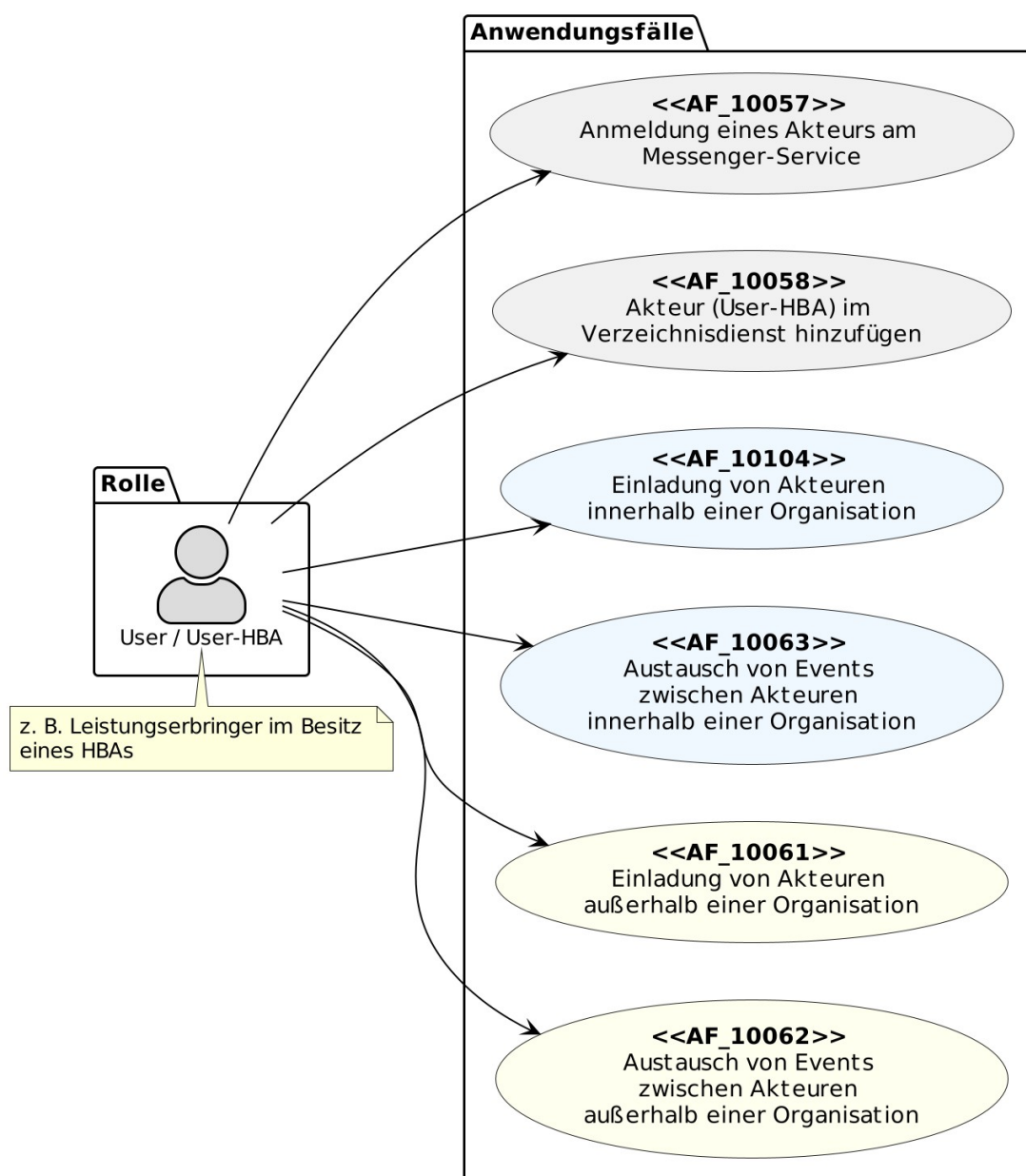
**Abbildung 8: Org-Admin - Übersicht Anwendungsfälle**

Der Anwendungsfall AF\_10060 - Bereitstellung eines 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.

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 einem 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\_10103-01 - 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". Durch die Authentifizierung MUSS der Besitz einer gültigen SMC-B nachgewiesen werden, da nur Organisationen des Gesundheitswesens berechtigt sind einen Messenger-Service zu erhalten. Als Nachweis MUSS eins der folgenden Verfahren verwendet werden.











Für die Verifizierung der Organisation MUSS

- Verfahren 1: bei der Authentisierung am zentralen IDP-Dienst eine freigeschaltete SMC-B verwendet werden oder
- Verfahren 2: eine KIM-Nachricht an die Adresse der Organisation mit der freigeschalteten SMC-B gesendet werden.

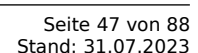
Als Nachweis zur Prüfung auf eine gültige Organisation MUSS der Registrierungs-Dienst in beiden Verfahren prüfen, ob die `ProfessionOID` zu einer Organisation des Gesundheitswesens gehört. Bei erfolgreicher Verifizierung der Organisation wird ein Administrator-Account für die Organisation am Registrierungs-Dienst 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_10103	Authentisieren einer Organisation am TI-Messenger-Dienst
Akteur	Beauftragter Mitarbeiter einer Organisation in der Rolle "Org-Admin"
Auslöser	Eine Organisation des deutschen Gesundheitswesens möchte am TI-Messenger-Dienst teilnehmen und benötigt die Berechtigung einen Messenger-Service zu registrieren
Komponenten	<ul style="list-style-type: none"> <li>• Frontend des Registrierungs-Dienstes,</li> </ul>

	<ul style="list-style-type: none"> <li>• Authenticator (Optional bei Verfahren 2),</li> <li>• Konnektor,</li> <li>• eHealth Kartenterminal mit gesteckter SMC-B,</li> <li>• Registrierungs-Dienst,</li> <li>• zentraler IDP-Dienst (Optional bei Verfahren 2)</li> <li>• KIM-Clientmodul und Mailclient (Optional bei Verfahren 1)</li> </ul>
Vorbedingung	<ol style="list-style-type: none"> <li>1. Der Akteur kann über ein Frontend des Registrierungs-Dienstes für die Kommunikation auf den Registrierungs-Dienst zugreifen.</li> <li>2. Verifizierung der Organisation: <ul style="list-style-type: none"> <li>• Verfahren 1: Der Akteur kann den Authenticator verwenden sowie das verwendete Frontend des Registrierungs-Dienstes, welches beim zentralen IDP-Dienst registriert ist.</li> <li>• Verfahren 2: Der Anbieter des TI-Messenger verfügt über eine SMC-B Org und eine KIM-Adresse sowie ein eHealth Kartenterminal und einen Konnektor mit TI-Zugang. Der Akteur verfügt über eine SMC-B und eine KIM-Adresse sowie ein eHealth Kartenterminal und einen Konnektor mit TI-Zugang.</li> </ul> </li> <li>3. Die im eHealth Kartenterminal gesteckte SMC-B ist freigeschaltet.</li> </ol>
Eingangsdaten	Identität der Organisation, SMC-B, Alternativ KIM-Adresse
Ergebnis	Die Organisation wurde am Registrierungs-Dienst des TI-Messenger-Fachdienstes verifiziert
Ausgangsdaten	Admin-Account, Status
Akzeptanzkriterien	  ML-128757,   ML-128759,   ML-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.



**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\_10060-01 - Bereitstellung eines Messenger-Service für eine Organisation**

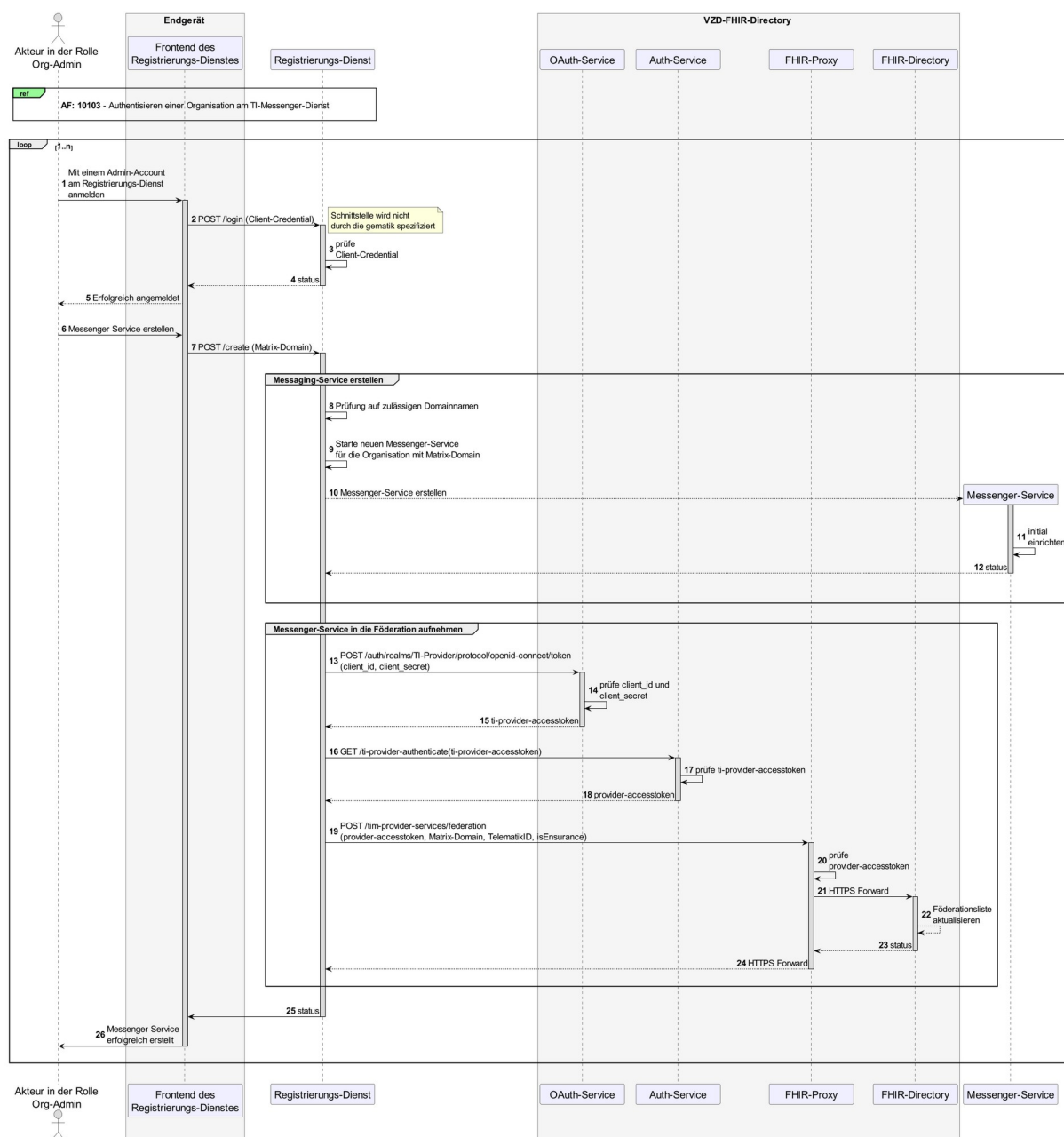
Mit diesem Anwendungsfall wird einer zuvor am Registrierungs-Dienst authentifizierten Organisation ein Messenger-Service für diese Organisation durch einen Akteur in der Rolle "Org-Admin" bereitgestellt. Die Beantragung zur Bereitstellung eines Messenger-Service wird durch den Akteur in der Rolle "Org-Admin" 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 Gesundheitswesens möchte am TI-Messenger-Dienst teilnehmen und benötigt die Bereitstellung eines oder mehrerer Messenger-Services
Komponenten	<ul style="list-style-type: none"> <li>• Frontend des Registrierungs-Dienstes,</li> <li>• Registrierungs-Dienst,</li> <li>• VZD-FHIR-Directory,</li> <li>• Messenger-Service.</li> </ul>
Vorbedingung	<ol style="list-style-type: none"> <li>1. Es besteht ein Vertragsverhältnis mit einem TI-Messenger-Anbieter.</li> <li>2. Der Akteur verfügt über ein Frontend des Registrierungs-Dienstes für die Kommunikation mit dem Registrierungs-Dienst.</li> <li>3. Das verwendete Frontend des Registrierungs-Dienstes ist beim zentralen IDP-Dienst registriert.</li> <li>4. Die Organisation ist erfolgreich beim Registrierungs-Dienst authentifiziert und ein Admin-Account ist vorhanden.</li> <li>5. Der Registrierungs-Dienst kann sich beim VZD-FHIR-Directory Server für Schreibzugriffe mit OAuth2 authentisieren.</li> </ol>
Eingangsdaten	Admin-Account, Identität der Organisation (SMC-B)
Ergebnis	<ol style="list-style-type: none"> <li>1. Der Messenger-Service für die Organisation wurde erstellt.</li> <li>2. Die Matrix-Domain des neuen Messenger-Services wurde als Endpunkt im VZD-FHIR-Directory eingetragen und in die Föderation aufgenommen.</li> </ol>
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 - Authentifizieren 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\_10059-01 - 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 *Endpoint*-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 (siehe [gemSpec\_VZD\_FHIR\_Directory]).

**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	<ul style="list-style-type: none"> <li>• TI-Messenger-Client (mit erweiterter Org-Admin Funktionalität),</li> <li>• TI-Messenger Registrierungs-Dienst,</li> <li>• Auth-Service,</li> <li>• FHIR-Proxy,</li> <li>• FHIR-Directory.</li> </ul>
Vorbedingungen	1. Für die Organisation wurde ein Messenger-Service bereitgestellt und es existiert ein Eintrag der Organisation im FHIR-Directory.

	<ol style="list-style-type: none"> <li>Der Administrator der Organisation verfügt über einen TI-Messenger-Client (mit erweiterter Org-Admin Funktionalität).</li> <li>Es existiert eine Vertrauensbeziehung zwischen dem TI-Messenger Registrierungs-Dienst und dem VZD-FHIR-Directory (Übergabe des Zertifikates)</li> <li>Der Administrator der Organisation wurde vom Registrierungs-Dienst authentifiziert.</li> </ol>
Eingangsdaten	Org-Admin-Credentials, zweiter Faktor (*), FHIR-Organisations-Ressourcen
Ergebnis	FHIR-Organisations-Ressourcen aktualisiert, Status
Ausgangsdaten	Aktualisierte VZD-FHIR-Directory-Datensätze
Akzeptanzkriterien	 ML-123626,  ML-132586,  ML-138468

(\*) Hinweis: Hinsichtlich des in der Tabelle unter "Eingangsdaten" genannten Zweitfaktors **MÜSSEN** die Sicherheitsempfehlungen des Bundesamt für Sicherheit in der Informationstechnik (BSI) gemäß [BSI 2-Faktor] berücksichtigt werden. Hierbei **MUSS** zur Resilienz gegen Angriffe aus der Ferne ein Verfahren gewählt werden, das mindestens mit "mittel" bewertet ist.

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.

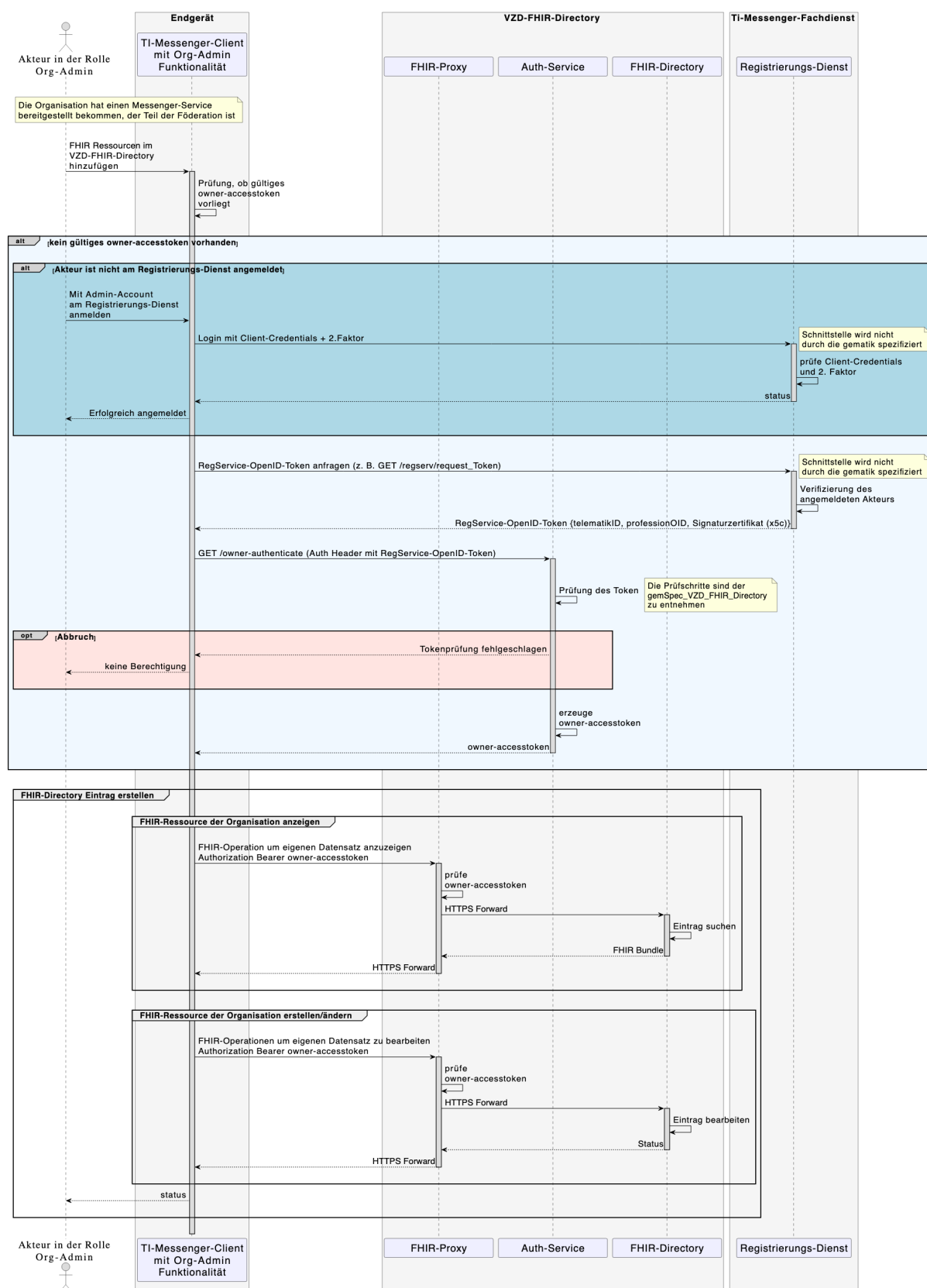


Abbildung 12: Laufzeitsicht - Organisationsressourcen im Verzeichnisdienst hinzufügen

[&lt;=]

## Akzeptanzkriterien für den Anwendungsfall: Organisationsressourcen im Verzeichnisdienst hinzufügen (AF\_10059)

### 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.

[<=]

### ML-138468 - AF\_10059 - Organisationsressourcen im VZD-FHIR-Directory hinzufügen

Nach erfolgreicher Authentisierung am Registrierungs-Dienst als Administrator einer Organisation kann der Akteur in der Rolle "Org-Admin" sich einen RegService-OpenID-Token ausstellen lassen und diesen gegen einen owner-accesstoken beim VZD-FHIR-Directory eintauschen. Mit dem owner-accesstoken kann der Akteur die MXID eines Akteurs seiner Organisation unterhalb der *HealthcareService*-Ressourcen in einen *Endpoint* eintragen oder neue *HealthcareService*-Ressourcen für die Organisation anlegen. Der Akteur in der Rolle "Org-Admin" wird über den Erfolg der Operation informiert.

[<=]

## 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 beispielsweise 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.

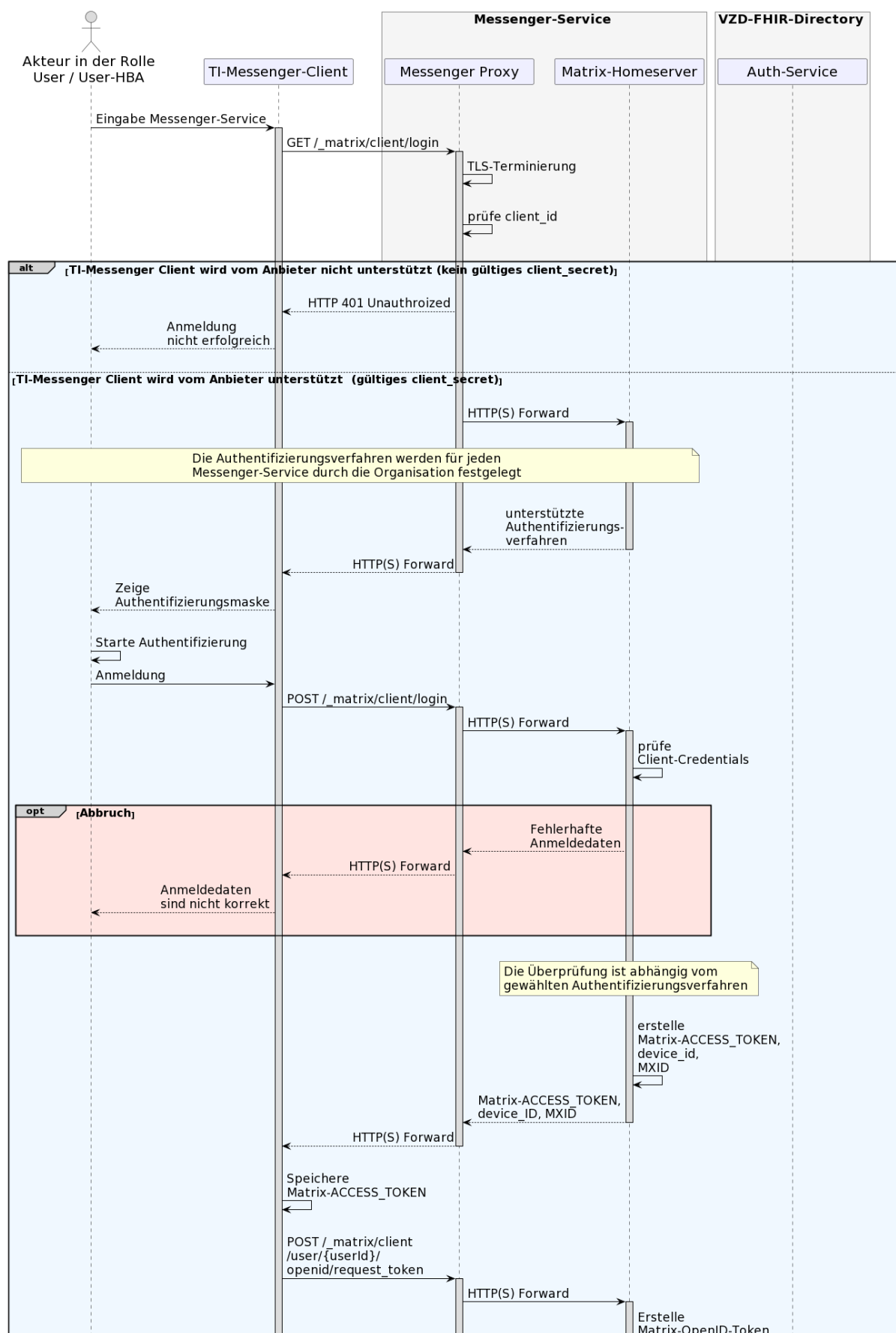
**Tabelle 11: AF - Anmeldung eines Akteurs am Messenger-Service**

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	<ul style="list-style-type: none"> <li>TI-Messenger-Client,</li> </ul>

	<ul style="list-style-type: none"> <li>• Messenger-Proxy,</li> <li>• Messenger-Homeserver,</li> <li>• FHIR-Proxy,</li> <li>• FHIR-Directory.</li> </ul>
Vorbedingungen	<ol style="list-style-type: none"> <li>1. Der Akteur verfügt über einen vom Anbieter unterstützen TI-Messenger-Client.</li> <li>2. Der Akteur kennt die URL des Messenger-Services oder die URL ist bereits in seinem TI-Messenger-Client konfiguriert.</li> <li>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.</li> <li>4. Der verwendete Matrix-Homeserver ist in die Föderation integriert (valider Messenger-Service).</li> </ol>
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

[&lt;=]

**Akzeptanzkriterien für den Anwendungsfall: Anmeldung eines Akteurs am Messenger-Service (AF\_10057)****ML-123571 - AF\_10057 - Akteur kann sich erfolgreich an einem gültigen Messenger-Service anmelden**

Ein Akteur hat sich erfolgreich an einem gültigen Messenger-Service angemeldet und mit einem zugelassenen Authentifizierungsverfahren erfolgreich authentisiert. Es MUSS sichergestellt werden, dass die Anmeldung an Messenger-Services, die nicht Teil der Föderation sind, nicht möglich ist.

[&lt;=]

**ML-123576 - AF\_10057 - Der Messenger-Service stellt dem TI-Messenger-Client ein Access-Token aus**

Nach erfolgreicher Anmeldung hat der Messenger-Service dem TI-Messenger-Client ein Matrix-ACCESS\_TOKEN ausgestellt.

[&lt;=]

**ML-123575 - AF\_10057 - Speicherung Access-Token durch TI-Messenger-Client**

Der TI-Messenger-Client speichert das ihm übergebene Matrix-ACCESS\_TOKEN zur Verwendung in den folgenden Anwendungsfällen.

[&lt;=]

**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.

[&lt;=]

**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.[<=]

**6.5 AF - Akteur (User-HBA) im Verzeichnisdienst hinzufügen****AF\_10058-01 - Akteur (User-HBA) im Verzeichnisdienst hinzufügen**

Mit diesem Anwendungsfall wird ein Akteur in der Rolle "User-HBA" für andere Akteure anderer Messenger-Services auffindbar und erreichbar. Dafür werden FHIR-Ressourcen mit ihrer jeweiligen MXID im Personenverzeichnis (*PractitionerRole*) des VZD-FHIR-Directory hinterlegt. Zusätzlich besteht die Möglichkeit die Sichtbarkeit für andere Akteure einzuschränken. Dieser 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 Akteur in der Rolle "User-HBA" während des Anmeldevorgangs durch den TI-Messenger-Client gefragt, ob dieser im Besitz eines HBAs ist.

**Tabelle 12: AF - Akteur (User-HBA) im Verzeichnisdienst hinzufügen**

AF_10058	Akteur (User-HBA) im Verzeichnisdienst hinzufügen
----------	---

Akteur	Leistungserbringer, Mitarbeiter einer Organisation im Gesundheitswesen in der Rolle "User-HBA"
Auslöser	Ein Akteur in der Rolle "User-HBA" möchte sich im Personenverzeichnis erreichbar machen, indem er seine MXID im seinen Practitioner-Datensatz im VZD-FHIR-Directory hinterlegt.
Komponenten	<ul style="list-style-type: none"> <li>• TI-Messenger-Client,</li> <li>• Authenticator,</li> <li>• zentraler IDP-Dienst,</li> <li>• FHIR-Proxy,</li> <li>• Auth-Service,</li> <li>• FHIR-Directory .</li> </ul>
Vorbedingungen	<ol style="list-style-type: none"> <li>1. Der Akteur ist bei einem gültigen Messenger-Service angemeldet.</li> <li>2. Der Akteur verfügt über einen zugelassenen TI-Messenger-Client.</li> <li>3. Das VZD-FHIR-Directory ist beim zentralen IDP-Dienst registriert.</li> <li>4. Der Akteur kann sich am zentralen IDP-Dienst authentisieren.</li> </ol>
Eingangsdaten	HBA, FHIR-Practitioner-Ressourcen
Ergebnis	FHIR-Practitioner-Ressourcen aktualisiert, Status
Ausgangsdaten	aktualisierter Practitioner-Datensatz
Akzeptanzkriterien	  ML-123612,   ML-123611,   ML-132588

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.

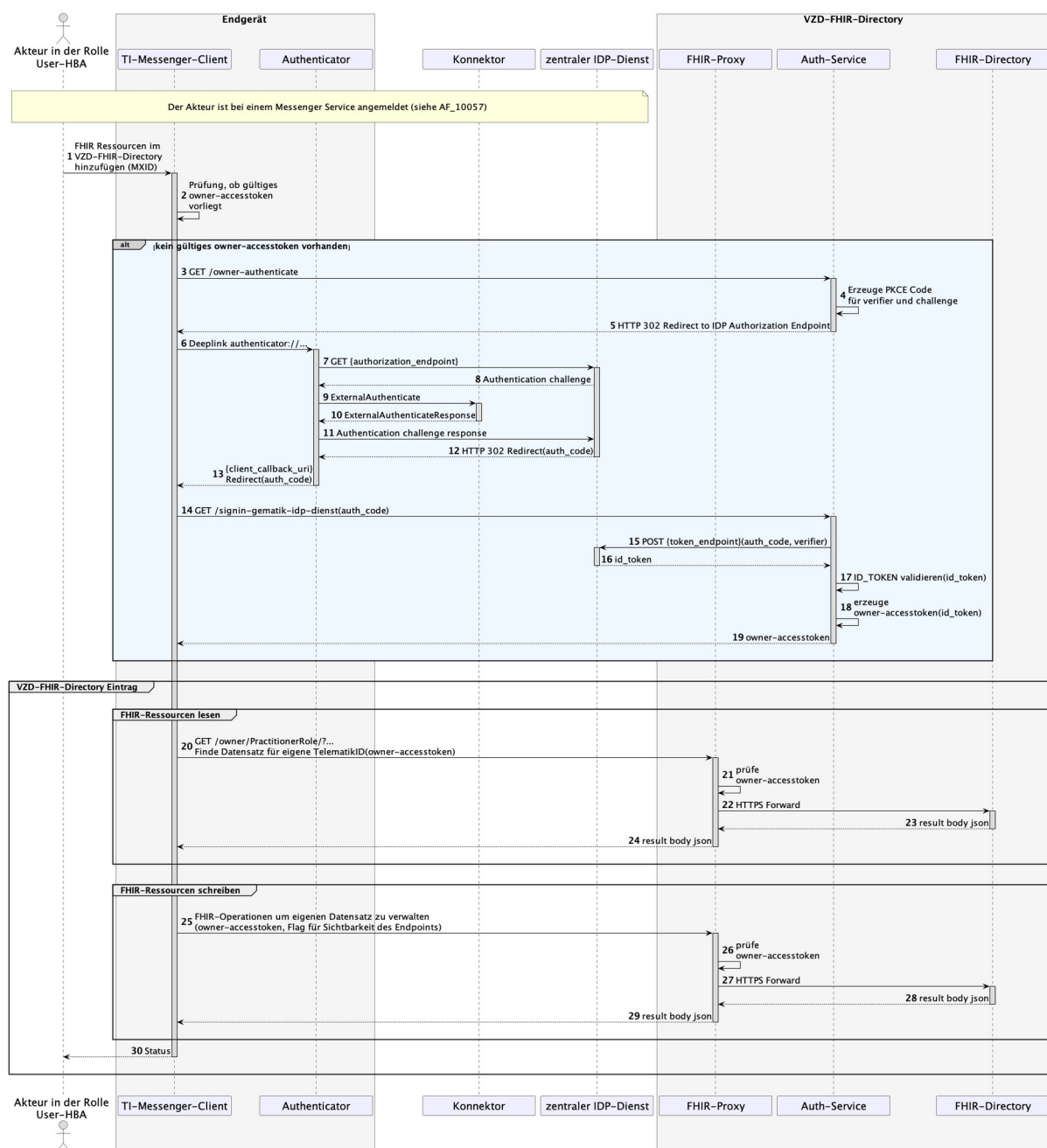


Abbildung 14: Laufzeitsicht - Akteur (User-HBA) im Verzeichnisdienst hinzufügen

[<=]

## Akzeptanzkriterien für den Anwendungsfall: Akteur (User-HBA) im Verzeichnisdienst hinzufügen (AF\_10058)

### ML-123612 - AF\_10058 - Akteur als Practitioner hinzufügen

Die MXID wurde in den Practitioner-FHIR-Datensatz eingefügt und der Akteur über den Erfolg informiert.

[<=]

**ML-123611 - AF\_10058 - MXID-Eintrag nur für eigenen Practitioner-FHIR-Datensatz**

Der Akteur in der Rolle "User-HBA" darf nur die eigene FHIR-Ressourcen 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.[<=]

## 6.6 AF - Föderationszugehörigkeit eines Messenger-Service prüfen

**AF\_10064-01 - Föderationszugehörigkeit eines Messenger-Service prüfen**

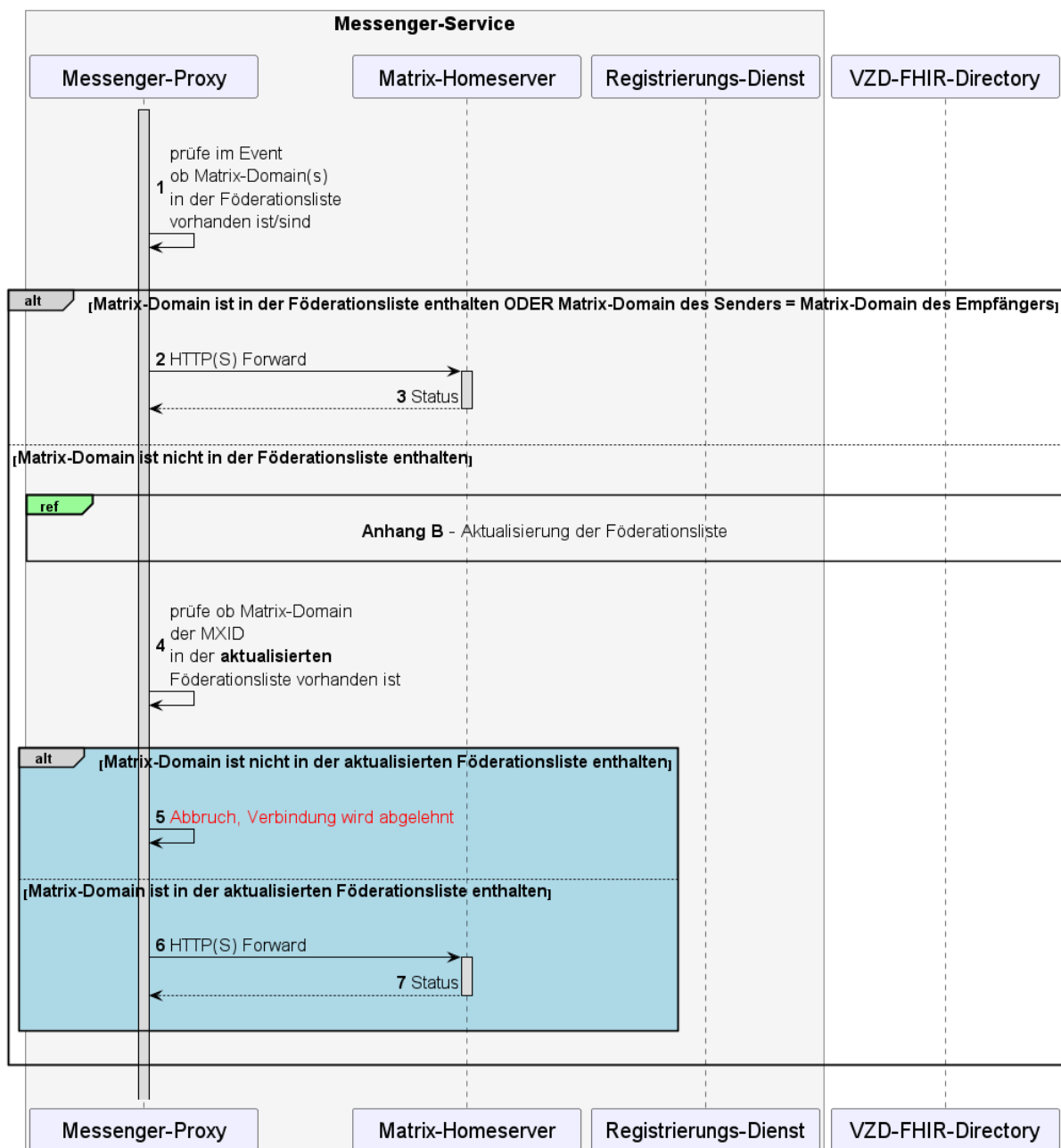
Dieser Anwendungsfall prüft gemäß der im Kapitel 3.5-

Berechtigungskonzept festgelegten Kriterien für die Stufe 1 der Client-Server und Server-Server Kommunikation, ob ein Messenger-Service zugehörig zur TI-Messenger-Föderation ist und gilt für alle Anwendungsfälle, welche die Matrix-Domain eines 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 8.2- Aktualisierung der Föderationsliste beschrieben.

**Tabelle 13: Föderationszugehörigkeit eines Messenger-Service prüfen**

AF_10064	Föderationszugehörigkeit eines Messenger-Service prüfen
Akteur	-
Auslöser	Der Messenger-Proxy empfängt oder sendet ein Matrix-Event und MUSS die im Request enthaltenen MXIDs auf Domain-Zugehörigkeit zur TI-Messenger-Föderation prüfen.
Komponenten	<ul style="list-style-type: none"> <li>• Messenger-Proxy,</li> <li>• Matrix-Homeserver.</li> </ul>
Vorbedingungen	keine
Eingangsdaten	Matrix-Event
Ergebnis	Der Messenger-Proxy ermittelt mittels der Föderationsliste, ob die Matrix-Domain des anderen Messenger-Service Teil der TI-Messenger-Föderation ist.
Ausgangsdaten	Status vom Matrix-Homeserver und Weiterleitung
Akzeptanzkriterien	 ML-123672,  ML-123891,  ML-132589,  ML-137902

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 8.2- Aktualisierung der Föderationsliste hinreichend beschrieben.



**Abbildung 15: Laufzeitsicht - Föderationszugehörigkeit eines Messenger-Service prüfen [≤]**

#### Akzeptanzkriterien für den Anwendungsfall: Föderationszugehörigkeit eines Messenger-Service 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-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 Messenger-Service Teil der Föderationsliste ist.

[<=]

**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.

[<=]

**ML-137902 - AF\_10064 - Aktualität - Föderationsliste Messenger-Proxy**

Es MUSS sichergestellt werden, dass die Föderationsliste vom Messenger-Proxy aktuell ist. Dafür MUSS der Messenger-Proxy in einem festen Intervall von einmal pro Stunde eine aktuelle Liste beim Registrierungs-Dienst anfordern.

[<=]





## 6.7 AF - Einladung von Akteuren innerhalb einer Organisation

**AF\_10104-01 - 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 gemäß Kapitel 3.5- Berechtigungskonzept der Client-Server Kommunikation, ob die im Invite-Event enthaltenen Matrix-Domains Teil der TI-Föderation sind. Ist dies der Fall erfolgt die Weiterleitung an den Matrix-Homeserver des Einladenden. 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 für die externe Zustellung 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	<ul style="list-style-type: none"> <li>TI-Messenger Client A + B,</li> </ul>

	<ul style="list-style-type: none"> <li>• Messenger-Proxy,</li> <li>• Matrix-Homeserver,</li> <li>• Push-Gateway.</li> </ul>
Vorbedingungen	<ol style="list-style-type: none"> <li>1. Die Akteure sind am selben Messenger-Service angemeldet.</li> <li>2. Jeder Akteur hat einen zugelassenen TI-Messenger-Client.</li> <li>3. Ein Chatraum wurde durch den Einladenden eingerichtet.</li> </ol>
Eingangsdaten	Invite-Event
Ergebnis	<p>Akteur A und Akteur B sind beide in einem gemeinsamen Chatraum.</p> <p>Optional erfolgt eine Benachrichtigung an Akteur B über die Einladung in den Chatraum.</p>
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. Daher wird in diesem Anwendungsbeispiel ein `/_matrix/client/v3/rooms/{roomId}/invite` Event am Messenger-Proxy geprüft. 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.

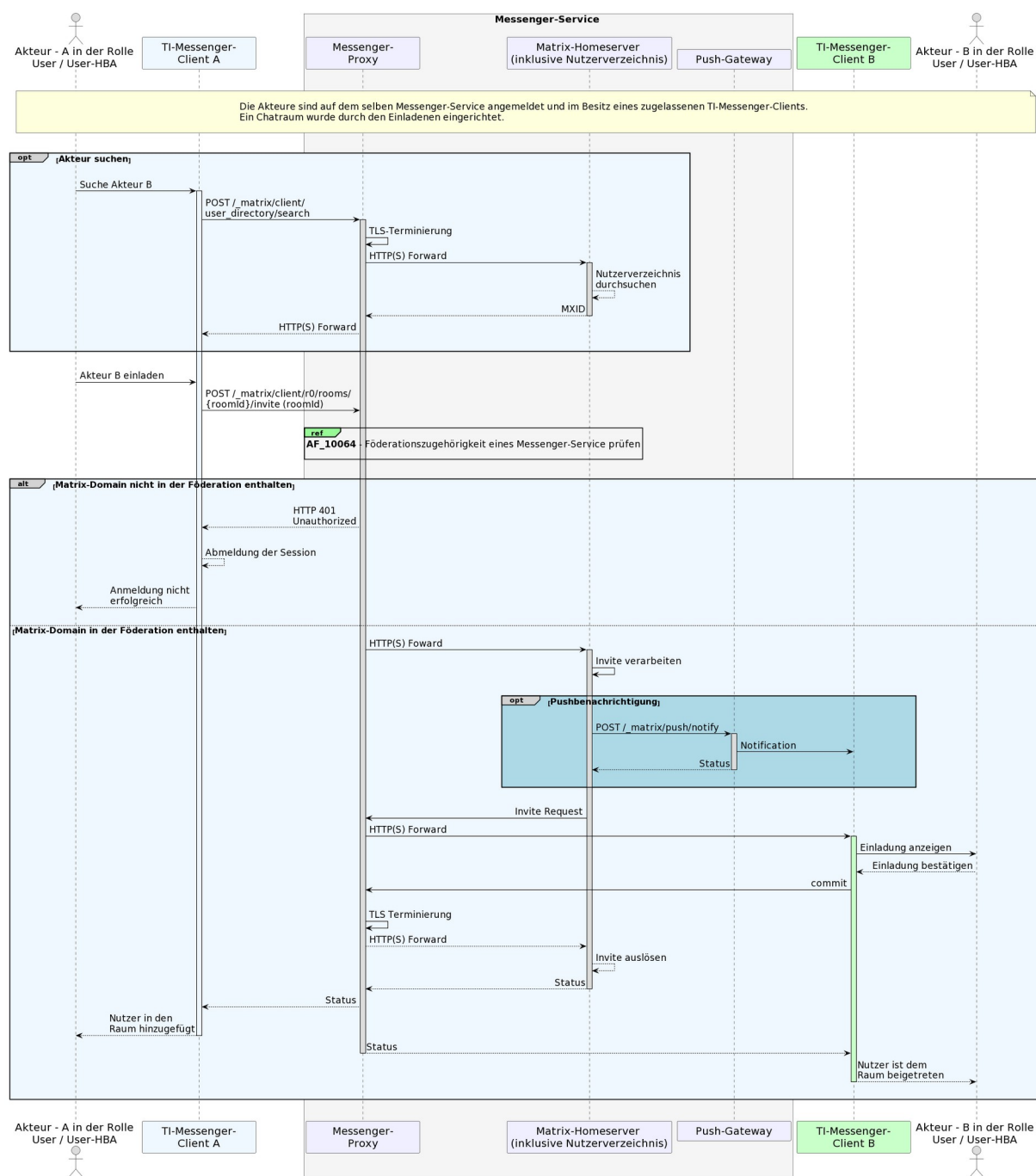


Abbildung 16: Einladung von Akteuren innerhalb einer Organisation

[&lt;=]

## Akzeptanzkriterien für den Anwendungsfall: 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 Akteure eines Matrix-Homeservers an.

[&lt;=]

### ML-129415 - AF\_10104 - Messenger-Proxy prüft TI-Föderationszugehörigkeit

Der Messenger-Proxy lehnt den Invite-Event ab, wenn die Matrix-Domain nicht zur TI-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.[<=]

## **6.8 AF - Austausch von Events zwischen Akteuren innerhalb einer Organisation**

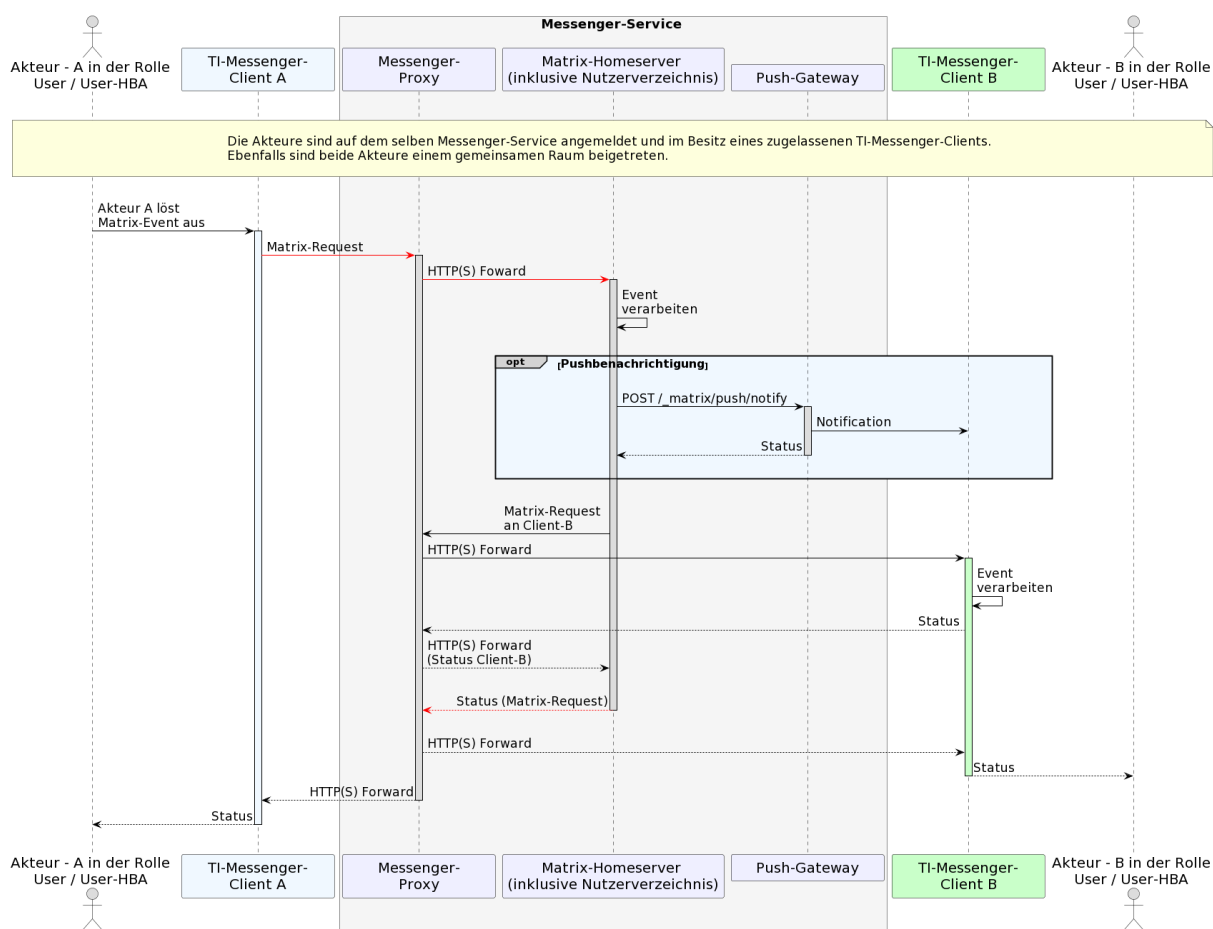
### **AF\_10063 - Austausch von Events zwischen Akteuren innerhalb einer Organisation**

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 (Events) auszuführen.

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	<ul style="list-style-type: none"> <li>• TI-Messenger Client A + B,</li> <li>• Messenger-Proxy,</li> <li>• Matrix-Homeserver,</li> <li>• Push-Gateway.</li> </ul>
Vorbedingungen	<ol style="list-style-type: none"> <li>1. Die Akteure sind am selben Messenger-Service angemeldet.</li> <li>2. Jeder Akteur hat einen zugelassenen TI-Messenger-Client.</li> <li>3. Die Teilnehmer sind einem gemeinsamen Raum beigetreten.</li> </ol>
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 um eine **vereinfachte Laufzeitansicht** 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 TI-Messenger-Client A an TI-Messenger-Client B wurde vom Matrix-Homeserver erfolgreich verarbeitet.

[<=]

#### 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-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\_10061-01 - Einladung von Akteuren außerhalb einer Organisation

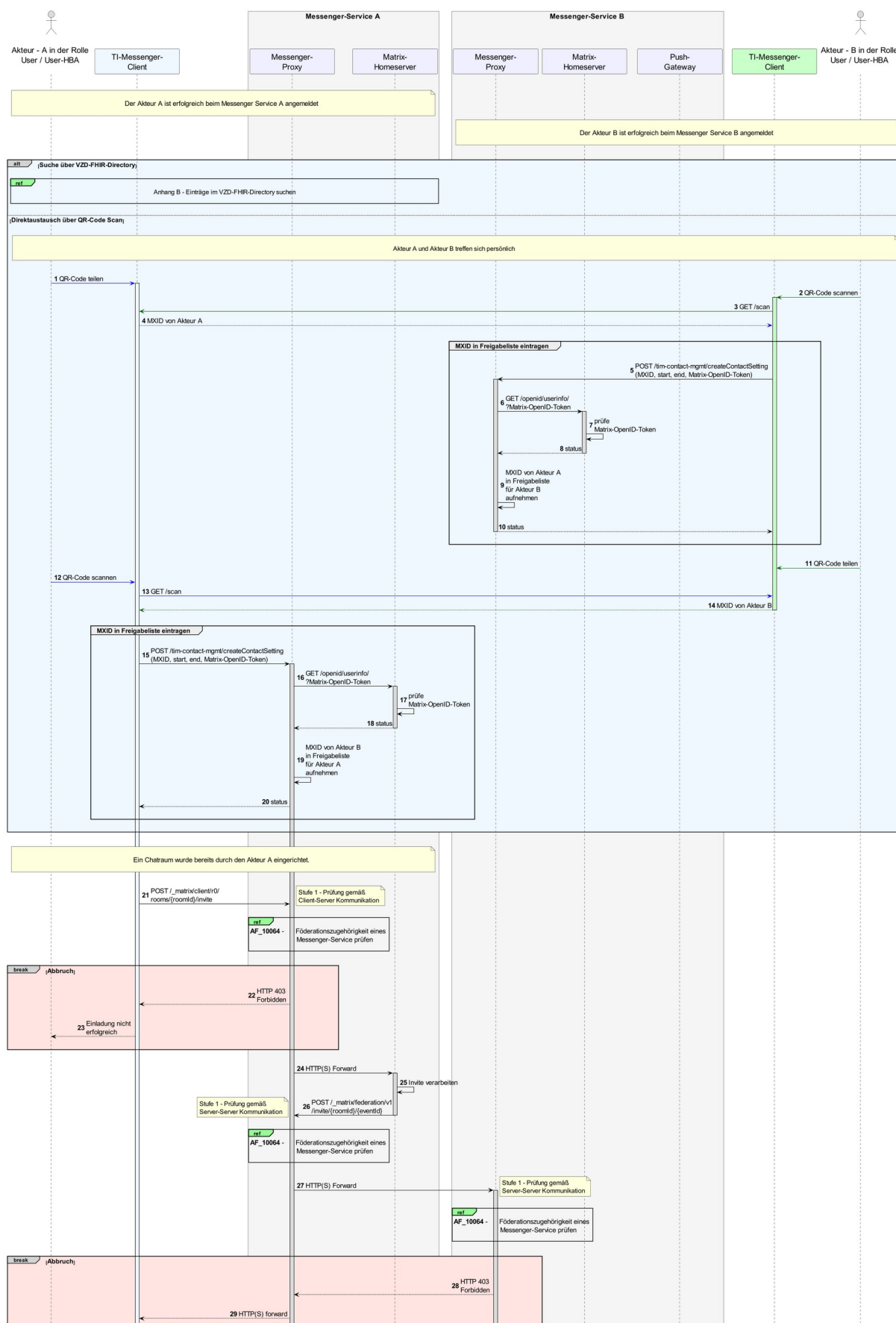
In diesem Anwendungsfall wird ein Akteur außerhalb einer Organisation eingeladen. Für die Suche von Akteuren außerhalb der Organisation KANN das VZD-FHIR-Directory verwendet werden. Ist die MXID des gesuchten Akteurs dort nicht vorhanden MUSS es die Möglichkeit geben, die Kontaktaufnahme auch auf andere Wege zu ermöglichen. Es MUSS mindestens die Kontaktaufnahme mit Hilfe eines QR-Code Scans angeboten werden. Weitere Optionen zur Eingabe der MXID (z. B. manuelle Eingabe) sind zulässig. Im Gegensatz zu einer Einladung von Akteuren innerhalb einer Organisation (siehe AF\_10104 - Einladung von Akteuren innerhalb einer Organisation), prüft in diesem Anwendungsfall der Messenger-Proxy zusätzlich die im Kapitel 3.5- Berechtigungskonzept festgelegten Kriterien der Server-Server Kommunikation (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	<ul style="list-style-type: none"> <li>• TI-Messenger Client A + B,</li> <li>• Messenger-Proxy A + B,</li> <li>• Matrix-Homeserver A + B,</li> <li>• VZD-FHIR-Directory,</li> <li>• Push-Gateway B.</li> </ul>
Vorbedingungen	<ol style="list-style-type: none"> <li>1. Die Akteure verfügen über einen zugelassenen TI-Messenger-Client.</li> <li>2. Die Akteure kennen die URL ihres Messenger-Service oder die URL ist bereits in ihren TI-Messenger-Clients konfiguriert.</li> <li>3. Die Akteure sind am Messenger-Services angemeldet</li> <li>4. Die verwendeten Messenger-Services sind Bestandteile der TI-Messenger-Föderation.</li> </ol>
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-132864,  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 eine eventuell notwendige Aktualisierung der Föderationsliste vom eigenem Registrierungs-Dienst zu zeigen. Der Abruf der Föderationsliste ist im Anhang 8.2- Aktualisierung der Föderationsliste hinreichend beschrieben. Die einzelnen Prüfschritte die der Messenger-Proxy für die festgelegten Kriterien (Stufe 2 - 3) der Server-Server Kommunikation durchführt, sind im Anhang 8.3- Stufen der Berechtigungsprüfung zu finden. Für die vereinfachte Darstellung wird vorausgesetzt, dass die TI-Messenger-Clients der beteiligten Akteure online sind. In dieser Laufzeitansicht lädt der Akteur A den Akteur B unmittelbar in einem gemeinsamen Chatraum ein.



## Abbildung 18: Laufzeitsicht - Einladung von Akteuren außerhalb einer Organisation

[<=]

### Akzeptanzkriterien für den Anwendungsfall: 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-123663 - AF\_10061 - Akteure sind dem Chatraum beigetreten**

Alle Chat Parteien sind erfolgreich im Chatraum vorhanden.

[<=]

#### **ML-132864 - AF\_10061 - Berechtigungsprüfung aller Stufen**

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

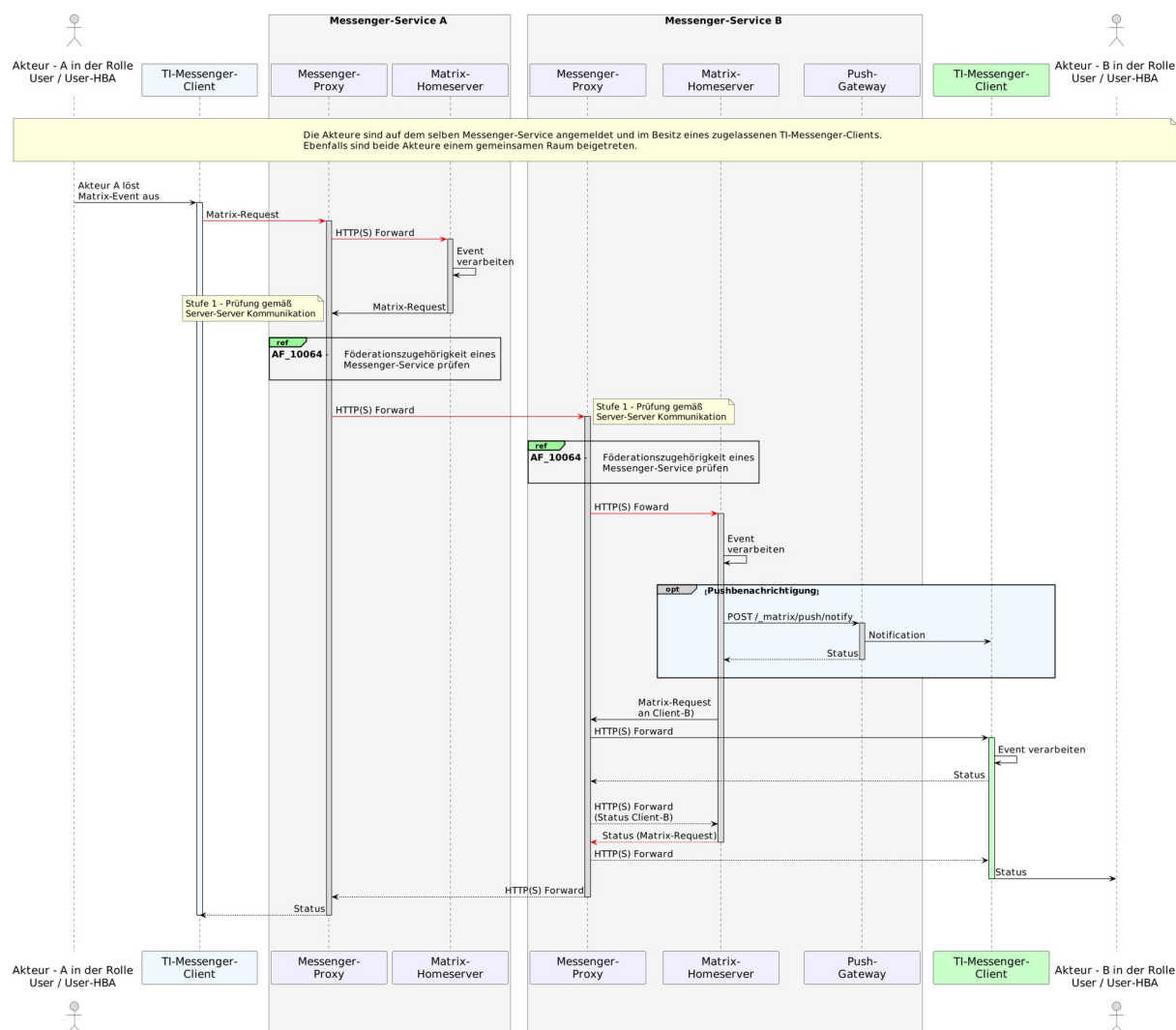
### **AF\_10062-01 - Austausch von Events zwischen Akteuren außerhalb einer Organisation**

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 Akteure voraus. Die Prüfung auf Domainzugehörigkeit findet jedoch bei jedem Event der Server-Server Kommunikation statt. In diesem Anwendungsfall sind die beteiligten Akteure in einem gemeinsamen Chatraum und auf unterschiedlichen Messenger-Services verteilt.

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

AF_10062	Austausch von Events zwischen Akteuren außerhalb einer Organisation
Akteur	Leistungserbringer, Mitarbeiter einer Organisation im Gesundheitswesen in der Rolle "User / User-HBA"
Auslöser	Alle Matrix-Events die zwischen Messenger-Services unterschiedlicher Organisationen ausgeführt werden.
Komponenten	<ul style="list-style-type: none"> <li>• TI-Messenger-Client A + B,</li> <li>• Messenger-Proxy A + B,</li> <li>• Matrix-Homeserver A + B,</li> <li>• Push-Gateway B.</li> </ul>
Vorbedingungen	<ol style="list-style-type: none"> <li>1. Beide Akteure sind Teilnehmer eines gemeinsamen Raumes.</li> <li>2. Die Messenger Proxies verfügen über eine aktuelle Föderationsliste.</li> </ol>
Eingangsdaten	Matrix-Event
Ergebnis	Matrix-Event wurde erfolgreich verarbeitet
Ausgangsdaten	Abhängig vom Matrix-Event, Status
Akzeptanzkriterien	 ML-123665,  ML-123666,  ML-123667,  ML-123668,  ML-132593

In der Laufzeitsicht sind die Interaktionen zwischen den Komponenten, die durch den Anwendungsfall genutzt werden, dargestellt. Hierbei handelt es um eine **vereinfachte Laufzeitsicht** 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 - Austausch von Events zwischen Akteuren außerhalb einer Organisation**

[<=]

### Akzeptanzkriterien für den Anwendungsfall: 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.

[<=]

### **ML-132593 - AF\_10062 - 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.

[<=]

---

## 7 Anhang A - Verzeichnisse

---

### 7.1 Abkürzungen

Kürzel	Erläuterung
AD	Active Directory
AF	Anwendungsfall
AZPD	Anbieter zentrale Plattformdienste
FHIR	Fast Healthcare Interoperable Resources
HBA	Heilberufsausweis
HTTP	Hypertext Transfer Protocol
IDP	Identity Provider
JSON	JavaScript Object Notation
JWT	JSON Web Token
LDAP	Lightweight Directory Access Protocol
LE	Leistungserbringer
MXID	Matrix-User-ID
OAuth	Open Authorization
PTA	Pharmazeutisch-technischer Assistent
REST	Representational State Transfer
SMC-B	Institutionenkarte (Security Module Card Typ B)
SMC-B ORG	<a href="#">Security Module Card für Organisationen</a>
SPOC	Single Point of Contact

SSO	Single Sign-on
TI	Telematikinfrastruktur
TI-ITSM	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 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

Abbildung 1: Komponenten der TI-Messenger-Architektur (vereinfachte Darstellung).....	10
Abbildung 2: Benachbarten Produkttypen des TI-Messenger-Dienstes.....	14
Abbildung 3: Komponenten der TI-Messenger-Architektur und deren Schnittstellen.....	25
Abbildung 4: Darstellung der Berechtigungsprüfung am Messenger-Proxy.....	31
Abbildung 5: Beispiel einer Interaktion mit einem Chatbot.....	43
Abbildung 6: TI-Messenger-Dienst Instanzen.....	44
Abbildung 7: Ausschnitt - TI-Messenger-Anbieter im TI-ITSM.....	45
Abbildung 8: Org-Admin - Übersicht Anwendungsfälle.....	46
Abbildung 9: User / User HBA - Übersicht Anwendungsfälle .....	47
Abbildung 10: Laufzeitsicht - Authentisieren einer Organisation am TI-Messenger-Dienst	52
Abbildung 11: Laufzeitsicht - Bereitstellung eines Messenger-Service für eine Organisation .....	54

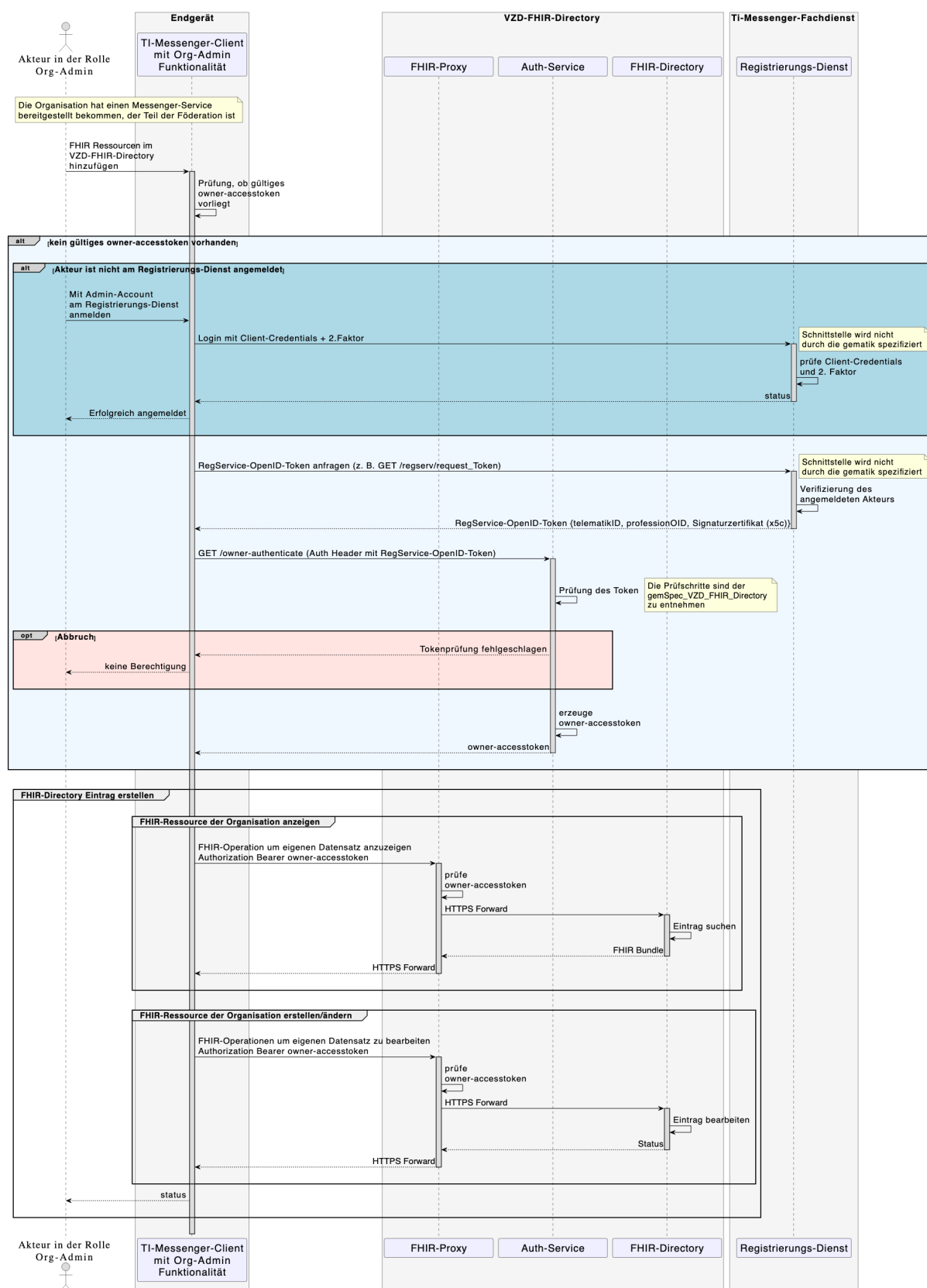


Abbildung 12: Laufzeitsicht - Organisationsressourcen im Verzeichnisdienst hinzufügen..... 57

Abbildung 13: Laufzeitsicht - Anmeldung eines Akteurs am Messenger-Service.....	62
Abbildung 14: Laufzeitsicht - Akteur (User-HBA) im Verzeichnisdienst hinzufügen.....	64
Abbildung 15: Laufzeitsicht - Föderationszugehörigkeit eines Messenger-Service prüfen	67
Abbildung 16: Einladung von Akteuren innerhalb einer Organisation.....	70
Abbildung 17: Laufzeitsicht - Austausch von Events zwischen Akteuren innerhalb einer Organisation.....	73
Abbildung 18: Laufzeitsicht - Einladung von Akteuren außerhalb einer Organisation.....	78
Abbildung 19: Laufzeitsicht - Austausch von Events zwischen Akteuren außerhalb einer Organisation.....	80
Abbildung 20: Laufzeitansicht - Einträge im VZD-FHIR-Directory suchen.....	89
Abbildung 21 Laufzeitansicht - Aktualisierung der Föderationsliste.....	92
Abbildung 22 Provider authentifizieren und Föderationsliste abrufen.....	92
Abbildung 23 Signatur der Föderationsliste prüfen.....	93
Abbildung 24: Laufzeitansicht - Stufen der Berechtigungsprüfung.....	94

## 7.4 Tabellenverzeichnis

Tabelle 1 Akteure und Rollen.....	12
Tabelle 2: Kommunikationsmatrix.....	13
Tabelle 3: Arten von Token.....	22
Tabelle 4: Verzeichnistypen - Rechtekonzept.....	27
Tabelle 5: Schreibzugriff - VZD-FHIR-Ressourcen.....	38
Tabelle 6: Überblick der Benutzerverwaltung in Abhängigkeit der Rolle.....	39
Tabelle 7: Beispiel für Funktionsaccounts.....	41
Tabelle 8: Tabelle : AF - Authentisieren einer Organisation am TI-Messenger-Dienst.....	48
Tabelle 9: AF - Bereitstellung eines Messenger-Service für eine Organisation.....	53
Tabelle 10: AF - Organisationsressourcen im Verzeichnisdienst hinzufügen.....	55
Tabelle 11: AF - Anmeldung eines Akteurs am Messenger-Service.....	58
Tabelle 12: AF - Akteur (User-HBA) im Verzeichnisdienst hinzufügen.....	63
Tabelle 13: Föderationszugehörigkeit eines Messenger-Service prüfen.....	66
Tabelle 14: Einladung von Akteuren innerhalb einer Organisation.....	68
Tabelle 15: Austausch von Events zwischen Akteuren innerhalb einer Organisation.....	72
Tabelle 16 AF - Einladung von Akteuren außerhalb einer Organisation.....	75
Tabelle 17: AF - Austausch von Events zwischen Akteuren außerhalb einer Organisation	79

## 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
[api-messenger]	gematik: api-ti-messenger <a href="https://github.com/gematik/api-ti-messenger/">https://github.com/gematik/api-ti-messenger/</a>
[api-vzd]	gematik: Verzeichnisdienst der Telematikinfrastruktur <a href="https://github.com/gematik/api-vzd">https://github.com/gematik/api-vzd</a>
[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
[BSI 2-Faktor]	BSI 2-Faktor Authentisierung für mehr Datensicherheit <a href="https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Zwei-Faktor-Authentisierung/Bewertung-2FA-Verfahren/bewertung-2fa-verfahren_node.html">https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Zwei-Faktor-Authentisierung/Bewertung-2FA-Verfahren/bewertung-2fa-verfahren_node.html</a>
[Client-Server API]	Matrix Foundation: Matrix Specification - Client-Server API <a href="https://spec.matrix.org/v1.3/client-server-api/">https://spec.matrix.org/v1.3/client-server-api/</a>
[FHIR]	HL7 FHIR Dokumentation <a href="https://www.hl7.org/fhir/documentation.html">https://www.hl7.org/fhir/documentation.html</a>

[gematik Authenticator]	gematik Authenticator <a href="https://cloud.gematik.de/index.php/s/23ebxa75z3s7zGt?path=%2Fv2.1.0">https://cloud.gematik.de/index.php/s/23ebxa75z3s7zGt?path=%2Fv2.1.0</a>
[Matrix Bots]	Matrix Bot Implementierungen <a href="https://matrix.org/bots/">https://matrix.org/bots/</a>
[Matrix Specification]	Matrix Foundation: Matrix Specification <a href="https://spec.matrix.org/v1.3/">https://spec.matrix.org/v1.3/</a>
[OpenID]	OpenID Foundation <a href="https://openid.net/developers/specs/">https://openid.net/developers/specs/</a>
[Push Gateway API]	Matrix Foundation: Matrix Specification - Push Gateway API <a href="https://spec.matrix.org/v1.3/push-gateway-api/">https://spec.matrix.org/v1.3/push-gateway-api/</a>
[RFC 8225]	IETF <a href="https://datatracker.ietf.org/doc/html/rfc8225">https://datatracker.ietf.org/doc/html/rfc8225</a>
[Server-Server API]	Matrix Foundation: Matrix Specification - Server-Server API <a href="https://spec.matrix.org/v1.3/server-server-api/">https://spec.matrix.org/v1.3/server-server-api/</a>

---

## 8 Anhang B - Abläufe

---

### 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. Für die Prüfung des Matrix-OpenID-Tokens MUSS der Zugriff auf den Endpunkt `/_matrix/federation/v1/openid/userinfo` ermöglicht werden.

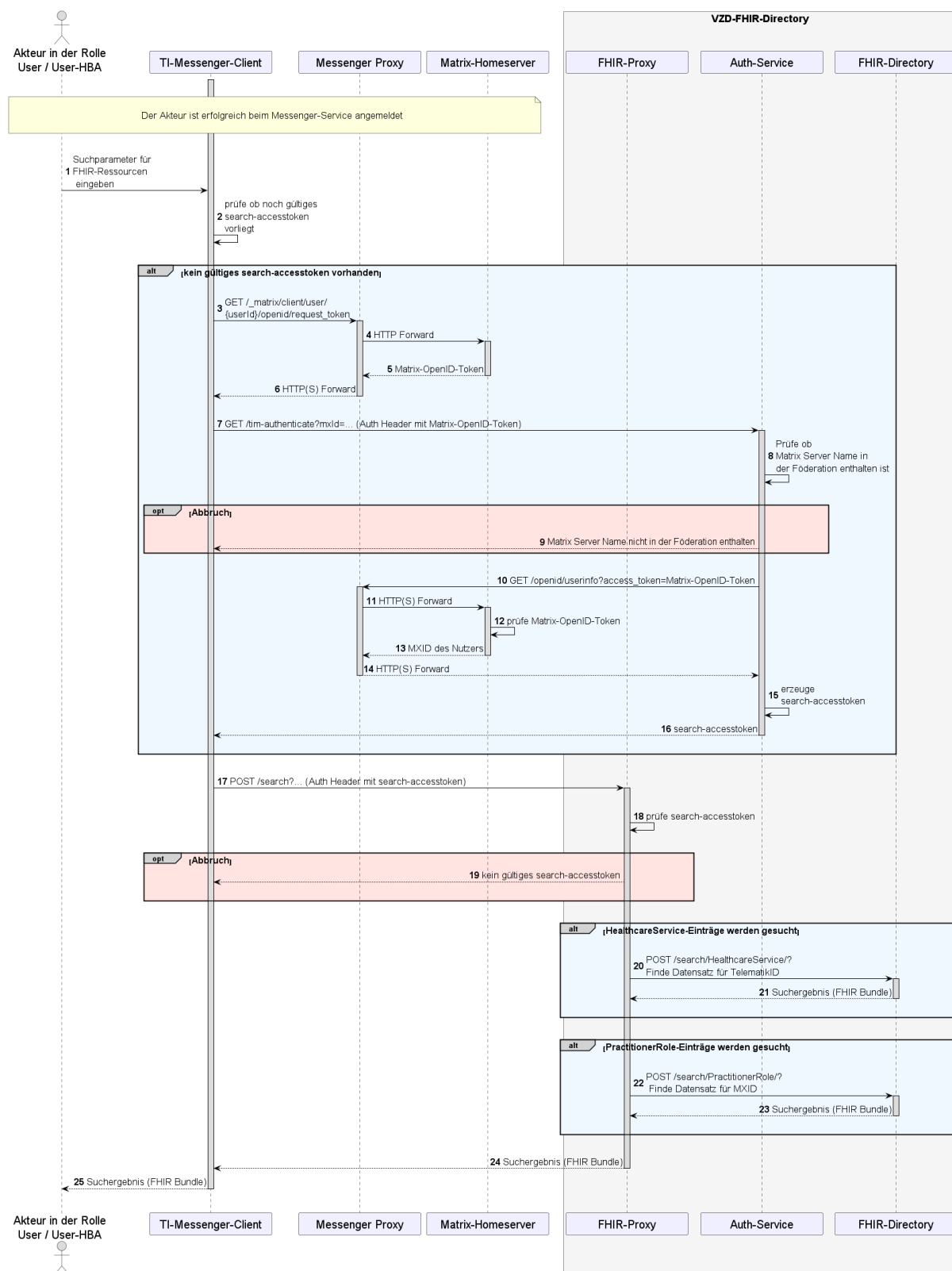


Abbildung 20: Laufzeitansicht - Einträge im VZD-FHIR-Directory suchen

## 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. 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 der Registrierungs-Dienst die Aktualität der durch ihn ausgelieferten Liste sicherstellen, indem er die von ihm gespeicherte Version der Föderationsliste im Bedarfsfall mit einer aktuelleren Version, die vom FHIR-Proxy bezogen wurde, überschreibt. 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.

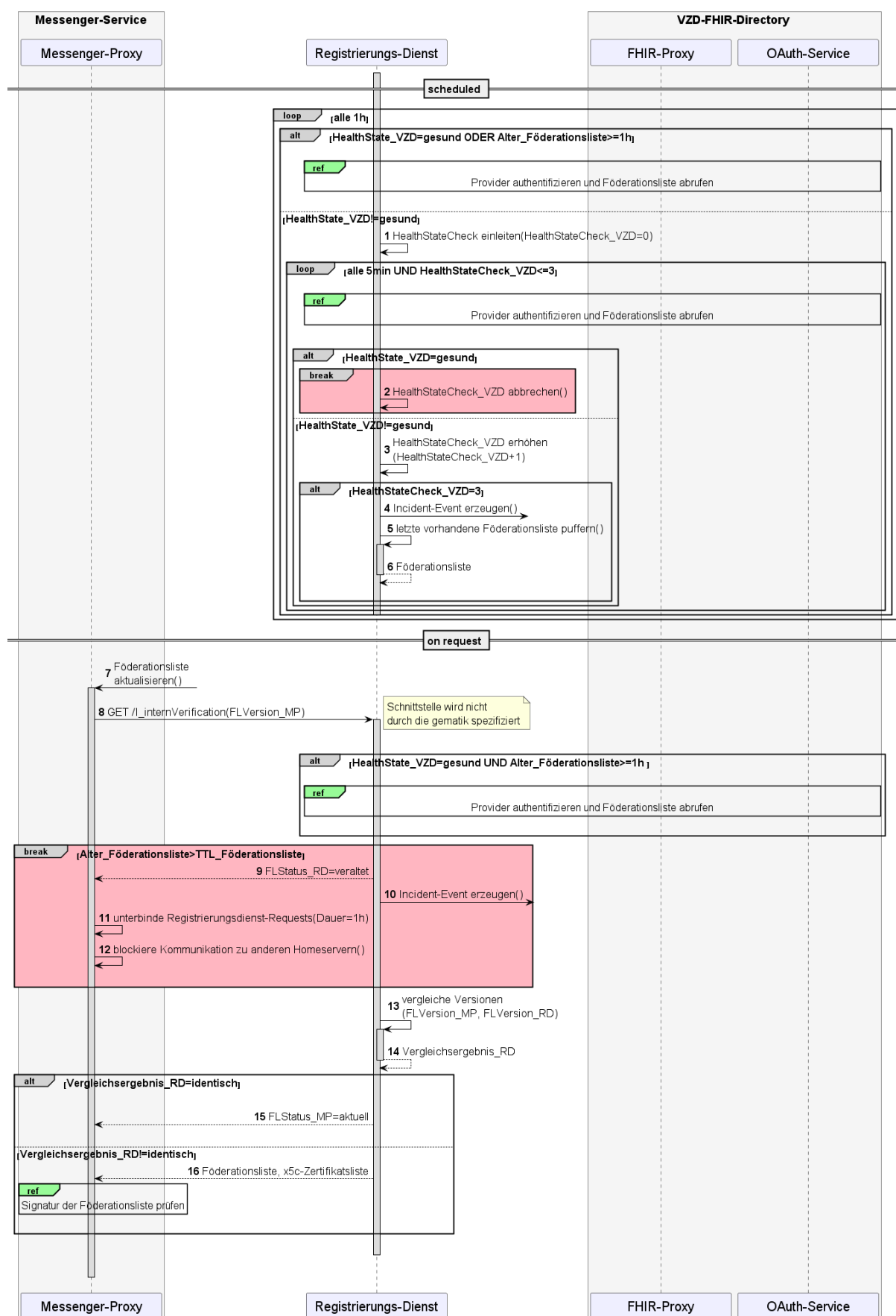


Abbildung 21 Laufzeitansicht - Aktualisierung der Föderationsliste

Das in der Abbildung "Laufzeitansicht - Aktualisierung der Föderationsliste" referenzierte Sequenzdiagramm "Provider authentifizieren und Föderationsliste abrufen":

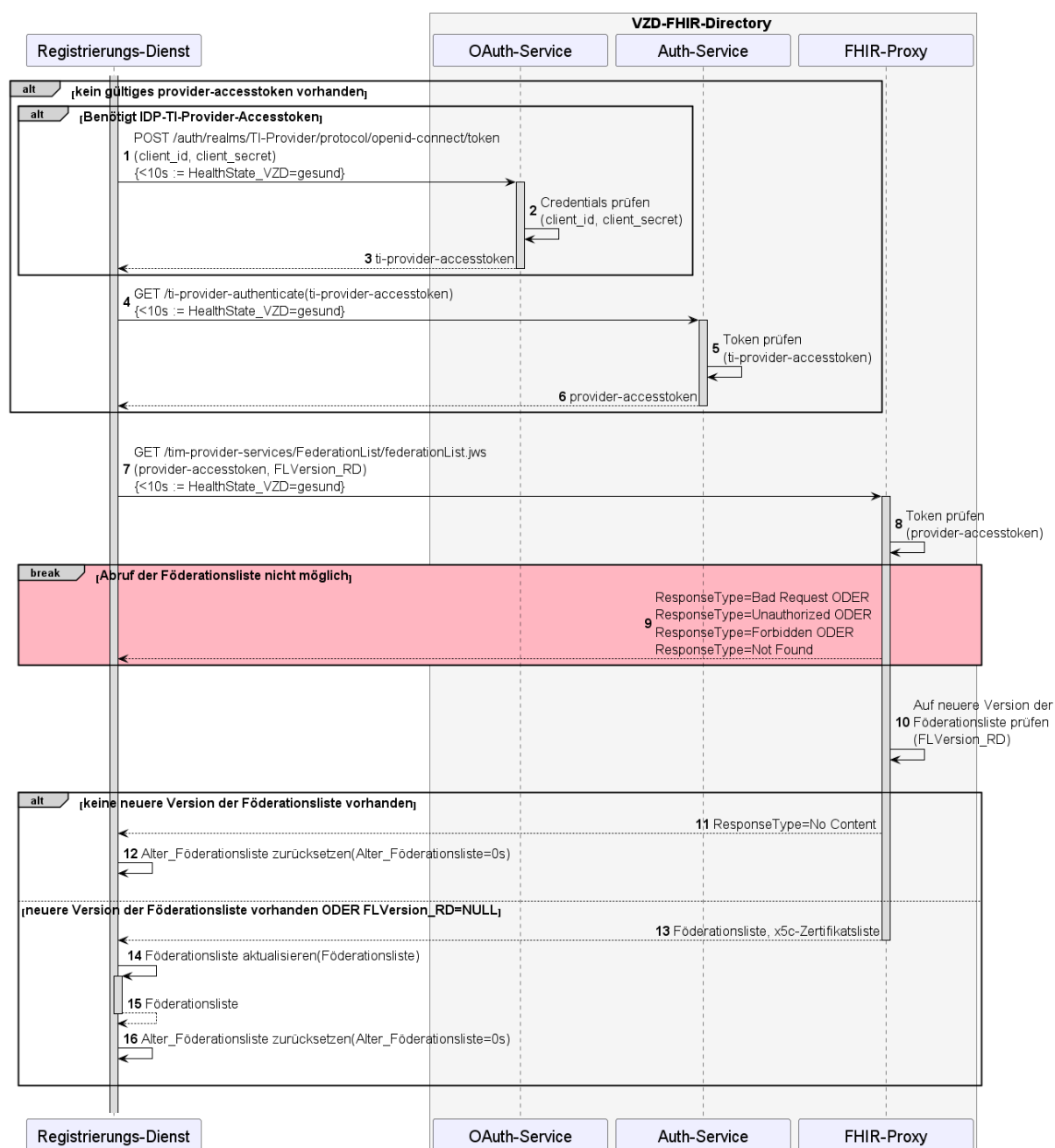


Abbildung 22 Provider authentifizieren und Föderationsliste abrufen

Das in der Abbildung "Laufzeitansicht - Aktualisierung der Föderationsliste" referenzierte Sequenzdiagramm "Signatur der Föderationsliste prüfen":

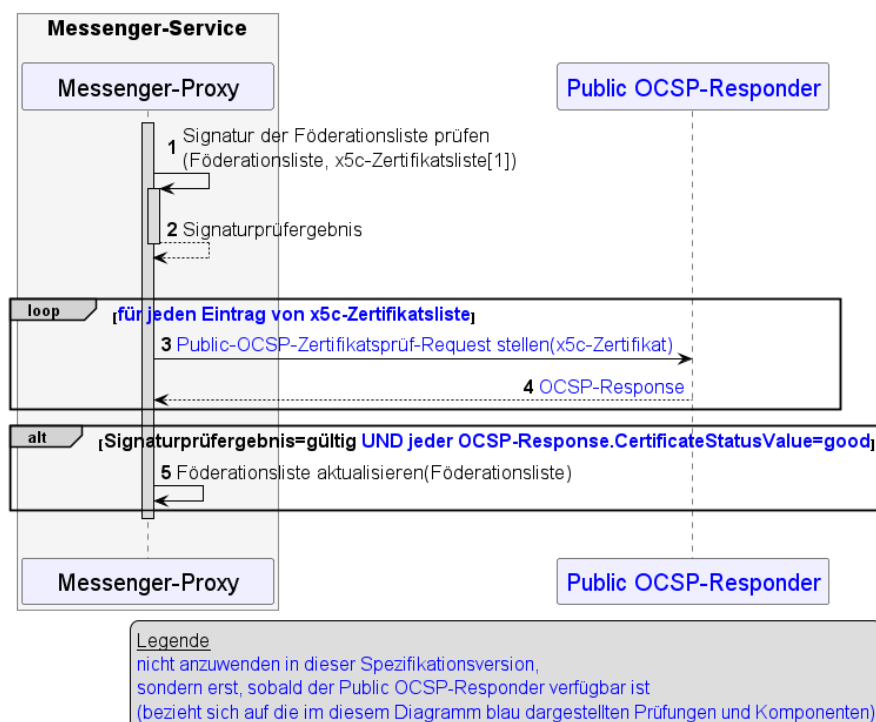


Abbildung 23 Signatur der Föderationsliste prüfen

### 8.3 Stufen der Berechtigungsprüfung

Die folgende Abbildung beschreibt, wie die Berechtigungsprüfung eingehender und ausgehender Matrix-Events am Messenger-Proxy erfolgen MUSS. Das Berechtigungskonzept basiert auf einer dreistufigen Prüfung, die in den Kapiteln [3.5.1- Client-Server Kommunikation](#) und [3.5.2- Server-Server Kommunikation](#) beschrieben sind. Es wird auf die Erwähnung notwendiger Authentifizierungen an dieser Stelle verzichtet.

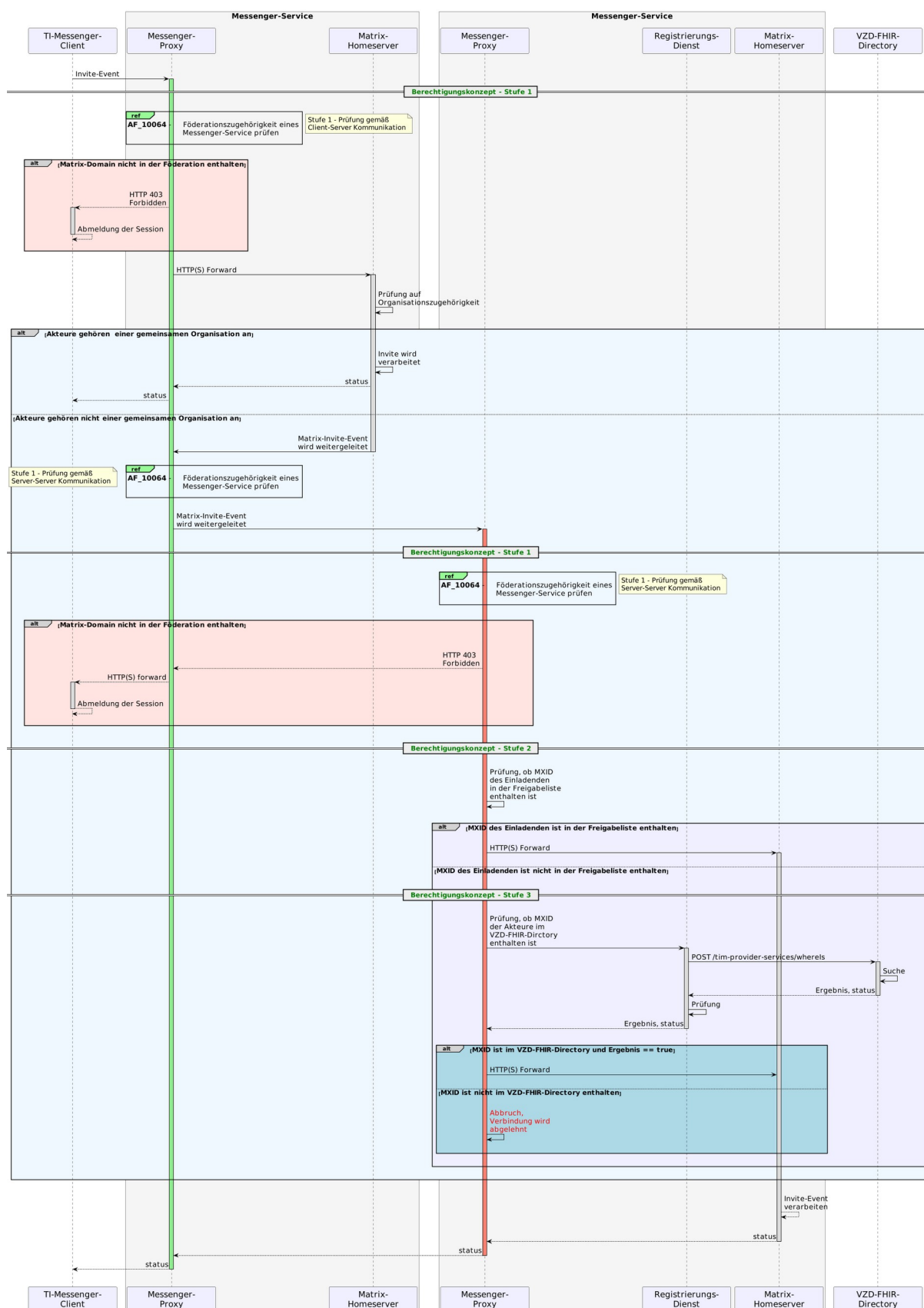


Abbildung 24: Laufzeitansicht - Stufen der Berechtigungsprüfung