

## Elektronische Gesundheitskarte und Telematikinfrastruktur

# Spezifikation TI-Messenger-Dienst

Version: 1.0.5  
Revision: 453509  
Stand: 14.04.2022  
Status: in Bearbeitung  
Klassifizierung: öffentlich\_Entwurf  
Referenzierung: gemSpec\_TI-Messenger-Dienst

## Dokumentinformationen

*Beim vorliegenden Dokument handelt es sich um einen Entwurf in Vorbereitung auf zukünftige normative Festlegungen und soll als Grundlage für spätere Zulassungs- und Bestätigungsverfahren dienen. Die gematik versendet diesen Entwurf mit dem Ziel, dass sich Interessierte vorab einen Überblick zur Weiterentwicklung der Telematikinfrastruktur verschaffen können.*

*Die gematik übernimmt keine Gewähr für Aktualität, Richtigkeit und Vollständigkeit dieses Entwurfs. Die gematik behält sich das Recht vor, ohne vorherige Ankündigung Änderungen oder Ergänzungen vorzunehmen oder von den Regelungen insgesamt oder teilweise Abstand zu nehmen.*

### 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
1.0.5	14.04.2022		Arbeitsstand zur Information	gematik

## Inhaltsverzeichnis

1	Einordnung des Dokumentes	4
1.1	Zielsetzung	4
1.2	Zielgruppe	4
1.3	Geltungsbereich	4
1.4	Abgrenzungen	4
1.5	Methodik	5
2	Systemüberblick	6
3	Systemkontext	7
3.1	Akteure und Rollen	7
3.2	Nachbarsysteme	9
3.3	Ausprägungen des Messenger-Service	9
3.4	Nutzung von Personal Assertion Token (PASSporT)	11
3.5	Verwendung der Token	12
4	Systemzerlegung	13
4.1	TI-Messenger-Fachdienst	14
4.1.1	Registrierungs-Dienst	14
4.1.2	Push-Gateway	14
4.1.3	Messenger-Service	15
4.1.3.1	Messenger-Proxy	15
4.1.3.1.1	Server-Server Proxy	15
4.1.3.1.2	Client-Server Proxy	15
4.1.3.2	PASSporT-Service des Messenger-Service	15
4.1.3.3	Matrix-Homeserver	16
4.2	TI-Messenger-Client	16
4.3	VZD-FHIR-Directory	16
5	Übergreifende Festlegungen	17
5.1	Datenschutz und Sicherheit	17
5.2	Verwendete Standards	17
5.3	Authentifizierung und Autorisierung	18

5.3.1	Authentifizierung von Akteuren	18
5.3.2	Autorisierung am Messenger-Service	19
5.3.3	Autorisierung am FHIR-Proxy	19
5.4	Föderation	19
5.5	Rechtekonzept VZD-FHIR-Directory	19
5.5.1	Schreibzugriffe für den Registrierungs-Dienst	19
5.5.2	Schreibzugriff für TI-Messenger-Clients	20
5.5.3	Lesezugriff für TI-Messenger-Clients	20
5.6	Betrieb	20
6	Anwendungsfälle	21
6.1	AF - Authentisieren einer Organisation am TI-Messenger-Dienst	22
6.2	AF - Bereitstellung eines Messenger-Service für eine Organisation	25
6.3	AF - Organisationsressourcen im Verzeichnisdienst hinzufügen	28
6.4	AF - Anmeldung eines Akteurs am Messenger-Service	30
6.5	AF - Akteur (User-HBA) im Verzeichnisdienst hinzufügen	32
6.6	AF - Föderationszugehörigkeit eines Messenger-Service prüfen	35
6.7	AF - Einladung von Akteuren innerhalb eines Messenger-Service	36
6.8	AF - Austausch von Events innerhalb eines Messenger-Service	39
6.9	AF - Einladung von Akteuren anderer Messenger-Services	41
6.10	AF - Austausch von Events zwischen anderen Messenger-Services	43
7	Anhang A – Verzeichnisse	46
7.1	Abkürzungen	46
7.2	Glossar	47
7.3	Abbildungsverzeichnis	47
7.4	Tabellenverzeichnis	47
7.5	Referenzierte Dokumente	48
7.5.1	Dokumente der gematik	48
7.5.2	Weitere Dokumente	48
8	Anhang B - Abläufe	49
8.1	Einträge im VZD-FHIR-Directory suchen	49
8.2	Aktualisierung der Föderationsliste	51

## 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 Kassenorganisationen werden in der zweiten Ausbaustufe des TI-Messengers Berücksichtigung finden und daher im vorliegenden Dokument nicht weiter betrachtet.

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

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

### 1.2 Zielgruppe

Das Dokument richtet sich zum Zwecke der Realisierung an Hersteller von Produkttypen des TI-Messengers sowie an Anbieter, welche einen oder mehrere dieser Produkttypen betreiben [gemKPT\_Betr]. Alle Hersteller und Anbieter von TI-Anwendungen, deren Schnittstellen einen der Produkttypen des TI-Messengers nutzen, oder Daten mit den Produkttypen des TI-Messengers austauschen oder solche Daten verarbeiten, müssen dieses Dokument ebenso berücksichtigen.

### 1.3 Geltungsbereich

Dieses Dokument enthält normative Festlegungen zur Telematikinfrastruktur des deutschen Gesundheitswesens. Der Gültigkeitszeitraum der vorliegenden Version und deren Anwendung in Zulassungs- oder Abnahmeverfahren wird durch die gematik GmbH in gesonderten Dokumenten (z. B. gemPTV\_ATV\_Festlegungen, Produkttypsteckbrief, Anbietertypsteckbrief, u.a.) oder Webplattformen (z. B. gitHub, u.a.) festgelegt und bekanntgegeben.

### Schutzrechts-/Patentrechtshinweis

*Die nachfolgende Spezifikation ist von der gematik allein unter technischen Gesichtspunkten erstellt worden. Im Einzelfall kann nicht ausgeschlossen werden, dass die Implementierung der Spezifikation in technische Schutzrechte Dritter eingreift. Es ist allein Sache des Anbieters oder Herstellers, durch geeignete Maßnahmen dafür Sorge zu tragen, dass von ihm aufgrund der Spezifikation angebotene Produkte und/oder Leistungen nicht gegen Schutzrechte Dritter verstoßen und sich ggf. die erforderlichen Erlaubnisse/Lizenzen von den betroffenen Schutzrechtinhabern 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

## Mainline

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 TI-Messenger-Dienst des deutschen Gesundheitswesens wird durch TI-Messenger-Anbieter betrieben. Dabei werden von jedem Anbieter die benötigten Produkttypen bereitgestellt. Für den Nachrichtenaustausch wird von den beteiligten Akteuren ein TI-Messenger-Client verwendet. Hierbei findet die sichere Ad-hoc-Kommunikation zwischen den Akteuren über die TI-Messenger-Clients und die vom TI-Messenger-Anbieter bereitgestellten Messenger-Fachdienste statt.

Messenger-Services werden jeweils für eine Organisation des Gesundheitswesens bereitgestellt und unterscheiden sich lediglich in der Art des verwendeten Authentifizierungsverfahrens. Akteure die zugehörig zu einer Organisation agieren, KÖNNEN den durch diese Organisation bereitgestellten Messenger-Service nutzen und die innerhalb dieser Organisation bereits verwendeten Authentifizierungsmethoden nutzen. Dies ermöglicht eine nahtlose Integration in den Alltag, da bestehende sichere Authentifizierungsverfahren nachgenutzt werden können. Akteure, die nicht zugehörig zu einer Organisation agieren, KÖNNEN Messenger-Services von Verbänden nutzen, falls diese durch einen Verband für ihre Mitglieder zur Verfügung gestellt werden. Hierbei kann das bestehende Authentifizierungsverfahren des Verbandes nachgenutzt werden. Messenger-Services KÖNNEN mit verschiedenen Messenger-Clients verwendet werden. So ist es beispielsweise möglich, dass eine Ärztin, die in einer Klinik und in einer niedergelassenen Praxis tätig ist, durch beide Organisationen jeweils einen TI-Messenger-Service mit jeweiligen TI-Messenger-Clients zur Verfügung gestellt bekommt. Messenger-Services werden durch TI-Messenger-Anbieter jeweils in separaten Umgebungen für Organisationen (SMC-B-Inhaber) bereitgestellt, die über das Matrix-Protokoll Nachrichten austauschen.

Um Teil der Föderation des TI-Messenger-Dienstes des deutschen Gesundheitswesens zu werden, MUSS die jeweilige Domain eines Messenger-Services vom Anbieter durch einen Registrierungs-Dienst im VZD-FHIR-Directory hinterlegt werden. Ist dies erfolgt, erhalten dessen Nutzer Lesezugriff auf das VZD-FHIR-Directory und KÖNNEN je nach Berechtigung die Kommunikation mit Akteuren in anderen Organisationen und/oder Leistungserbringern starten. Die Kommunikation findet dabei Ende-zu-Ende-verschlüsselt zwischen den jeweiligen beteiligten Messenger-Services und TI-Messenger-Clients statt. Um die beteiligten Akteure über den Eingang neuer Nachrichten zu informieren, MÜSSEN die TI-Messenger-Fachdienst-Anbieter ein Push-Gateway betreiben.

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

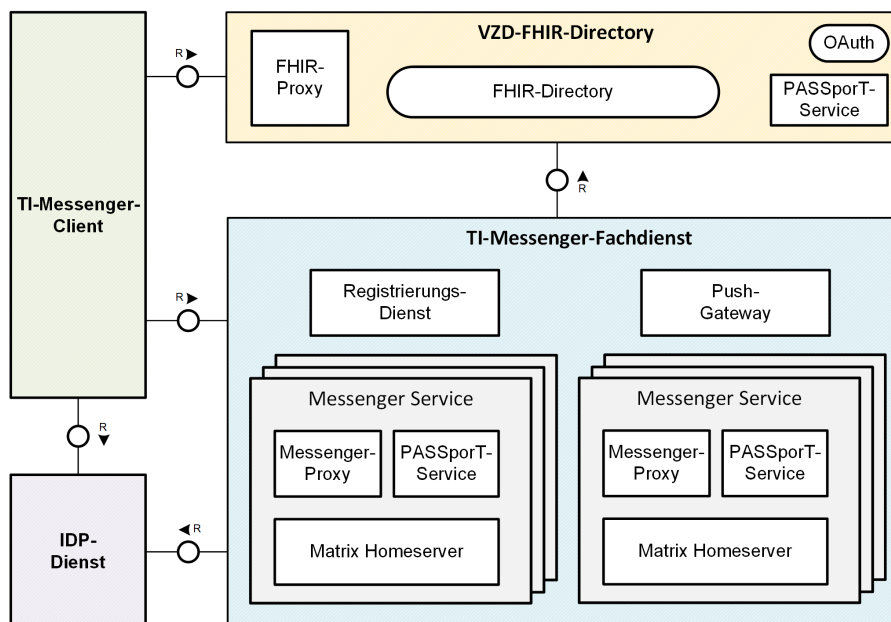


Abbildung 1: Komponenten der TI-Messenger-Architektur (vereinfachte Darstellung)

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 und auch die API des Matrix-Push-Gateways beschrieben. Für die

## Mainline

Sicherstellung der föderalen und dezentralen Struktur des TI-Messenger-Dienstes und zur Kontrolle des Nutzerkreises werden weitere Komponenten benötigt, welche in der jeweiligen durch die gematik veröffentlichten Spezifikation dieser Komponenten beschrieben werden. Die Komponenten sind so ausgelegt, dass diese der Matrix Spezifikation entsprechen und somit die Funktionen des TI-Messengers mit der Funktionalität der Matrix Spezifikation weiterentwickelt werden können.

### 3 Systemkontext

#### 3.1 Akteure und Rollen

Im Kontext des TI-Messenger-Dienstes werden verschiedene Akteure und Rollen betrachtet. Abhängig von dem verwendeten Authentifizierungsverfahren ergeben sich unterschiedliche Rollen, die ein Akteur einnehmen kann. Diese sind in der Tabelle "Akteure und Rollen" beschrieben.

Tabelle 1: Akteure und Rollen

Akteur	Rolle	Beschreibung und Berechtigungen
Leistungserbringer im Besitz eines HBAs und/oder einer SMC-B (z. B. Zahnärzte, Apotheker, psychologische Psychotherapeuten)	User-HBA	<p>Ein LE im Besitz eines HBAs kann</p> <ul style="list-style-type: none"> <li>sich am Smartcard-IDP authentisieren</li> <li>sich am Messenger-Service anmelden</li> <li>seine MXID auf dem VZD-FHIR Server hinterlegen und sich damit sektorübergreifend erreichbar machen</li> <li>den TI-Messenger-Dienst nutzen <ul style="list-style-type: none"> <li>Kommunikationen innerhalb seiner Organisation aufbauen und entgegennehmen</li> <li>Kommunikationen mit anderen Organisationen aufbauen</li> <li>Kommunikationen mit LEs aufbauen und entgegennehmen, die ebenfalls mit HBA authentisiert und somit für ihn auf dem VZD-FHIR-Server auffindbar sind</li> <li>*Direct Messaging gemäß [Client-Server API#Direct Messaging] mit allen Teilnehmern der TI-Messenger-Dienste</li> <li>**Group Messaging [Group Messaging] mit allen Teilnehmern der TI-Messenger-Dienste</li> </ul> </li> <li>im Namen der Organisation Kommunikation empfangen</li> </ul>
	Org-Admin	<p>Ein LE im Besitz eines HBAs und einer SMC-B kann</p> <ul style="list-style-type: none"> <li>sich am Smartcard-IDP authentisieren</li> <li>einen Messenger-Service für seine Organisation (korrespondierend zu seiner SMC-B) anlegen</li> <li>seine Organisation auf dem VZD-FHIR Server administrieren und damit sektorübergreifend erreichbar machen</li> <li>die User dieses Messenger-Services administrieren</li> <li>Homeserver-Konfigurationen vornehmen</li> </ul>
Mitarbeiter einer Organisation im	User	Ein Mitarbeiter einer Organisation im Gesundheitswesen kann

## Mainline

Gesundheitswesen (z. B. Pflegepersonal, Hebammen, Arzt im Krankenhaus, Mitarbeiter einer Kasse)		<ul style="list-style-type: none"> <li>• sich gegenüber dem Messenger-Service authentisieren</li> <li>• sich am Messenger-Service anmelden</li> <li>• den TI-Messenger-Dienst nutzen <ul style="list-style-type: none"> <li>• Kommunikationen innerhalb seiner Organisation aufbauen und entgegennehmen</li> <li>• Kommunikationen mit anderen Organisationen aufbauen</li> <li>• *Direct Messaging gemäß [Client-Server API#Direct Messaging] mit allen Teilnehmern der TI-Messenger-Dienste</li> <li>• **Group Messaging [Group Messaging] mit allen Teilnehmern der TI-Messenger-Dienste</li> </ul> </li> <li>• im Namen der Organisation Kommunikation empfangen</li> </ul>
	Org-Admin	<p>Ein Mitarbeiter einer Organisation im Gesundheitswesen mit Zugriff auf eine SMC-B kann</p> <ul style="list-style-type: none"> <li>• sich am Smartcard-IDP authentisieren</li> <li>• einen Messenger-Service für seine Organisation (korrespondierend zu seiner SMC-B) anlegen</li> <li>• seine Organisation auf dem VZD-FHIR Server administrieren und damit sektorübergreifend erreichbar machen</li> <li>• die User dieses Messenger-Services administrieren</li> <li>• Homeserver-Konfigurationen vornehmen</li> </ul>
Beauftragter Administrator eines TI-Messenger-Anbieters	Org-Admin	<p>Ein TI-Messenger-Anbieter kann, auf Wunsch des LEs im Besitz einer SMC-B</p> <ul style="list-style-type: none"> <li>• einen Messenger-Service für die Organisation (korrespondierend zur SMC-B des LEs) anlegen</li> <li>• diese Organisation auf dem VZD-FHIR Server administrieren und damit sektorübergreifend erreichbar machen</li> <li>• die User dieses Messenger-Services administrieren</li> <li>• Homeserver-Konfigurationen für LE vornehmen</li> </ul>

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

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

Ein Akteur ist eine Person, die mit einem TI-Messenger-Fachdienst interagiert. Diese Interaktion wird durch einen Anwendungsfall ausgelöst. Im Folgenden werden die Akteure mit ihren jeweiligen Rollen ausführlich beschrieben.

Ein Akteure in der Rolle *User-HBA* (Leistungserbringer im Besitz eines HBAs) KÖNNEN ihre MXID im VZD-FHIR-Directory hinterlegen, um für andere Leistungserbringer, die ebenfalls die eigene MXID auf dem VZD-FHIR-Directory hinterlegt haben, auffindbar zu sein.

Akteure in der Rolle *User* hinterlegen keine MXID auf dem VZD-FHIR-Directory. Dieser kann daher lediglich als Mitarbeiter einer Organisation gefunden werden oder Chatnachrichten im Namen seiner Organisation empfangen. Um mit Akteuren außerhalb einer Organisation kommunizieren zu können, MUSS zwischen den Akteuren ein gültiges PASSporT ausgetauscht werden. Dieser wird je nach Anwendungsfall entweder vom PASSporT-Service des VZD-FHIR-Directory



## Mainline

oder dem jeweiligen Messenger-Service bereitgestellt.

Ein Akteur in der Rolle *Org-Admin* benötigt den Zugriff auf eine SMC-B in seiner Organisation, um im VZD-FHIR-Directory Einträge zu erstellen und zu administrieren. Ein Leistungserbringer im Besitz eines HBAs und Mitarbeiter einer Organisation im Gesundheitswesen KANN Zugriff auf eine SMC-B der Organisation erhalten und somit die Rolle *Org-Admin* einnehmen. Für die Rolle *Org-Admin* besteht die Notwendigkeit, einen Administrator einzusetzen, welcher für Themen der Informationssicherheit geschult und sensibilisiert wurde. Ein TI-Messenger Anbieter KANN im Auftrag einer Organisation einen Administrator mit der Rolle *Org-Admin* beauftragen und die in der Tabelle "Akteure und Rollen" beschriebenen Services anbieten.

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. Ein Account MUSS einer juristischen Person eindeutig zugeordnet sein. Das Teilen von Passwörtern oder Zugangsdaten für die gleichzeitige Nutzung eines Accounts ist nicht erlaubt.

### 3.2 Nachbarsysteme

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

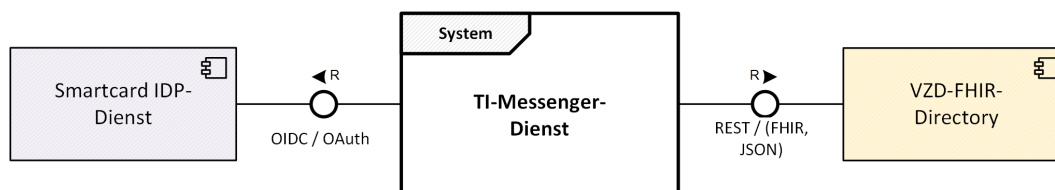


Abbildung 2 Benachbarten Produkttypen des TI-Messenger-Dienstes

Der TI-Messenger-Client des TI-Messenger-Dienstes nutzt die Schnittstellen vom Smartcard IDP-Dienst der gematik zur Authentifizierung von Akteuren sowie Schnittstellen des gesondert spezifizierten VZD-FHIR-Directory, um z. B. FHIR-Ressourcen (z. B. practitioner und organization) und deren MXID zu finden.

### 3.3 Ausprägungen des Messenger-Service

Der Messenger-Service ist eine Teilkomponente des TI-Messenger-Fachdienstes und wird dezentral durch den jeweiligen Anbieter für Organisationen bereitgestellt. Der Messenger-Service besteht aus einem Matrix-Homeserver (basierend auf dem Matrix-Protokoll) und Komponenten die sicherstellen, dass eine Kommunikation mit anderen Messenger-Services als Teil des TI-Messenger-Dienstes **nur innerhalb der gemeinsamen Föderation** erfolgt. Bei diesen zusätzlichen Komponenten handelt es sich jeweils um einen Messenger-Proxy und einen PASSporT-Service. Die Messenger-Services KÖNNEN den Akteuren unterschiedliche Authentifizierungsverfahren anbieten, bei denen der Besitz einer SMC-B oder eines HBA nicht vorausgesetzt werden kann. Messenger-Services MÜSSEN immer Organisationen 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 Authentifizierung ab. Möglich ist beispielsweise die Nachnutzung eines in der Organisation betriebenen Active Directory Servers (AD/LDAP) oder eines geeigneten Single-Sign-On-Verfahrens (SSO). Der Anbieter MUSS sicherstellen, dass die Organisation die Kontrolle über die jeweiligen Authentifizierungsmechanismen besitzt, um eine mögliche Löschung oder Sperrung eines Accounts sicherzustellen.

Zum besseren Verständnis werden im Folgenden vier Anwendungsbeispiele erläutert:

### Anwendungsbeispiel Arztpraxis

Eine Arztpraxis registriert sich mittels SMC-B bei einem Registrierungs-Dienst eines Messenger-Anbieters. Der Anbieter stellt daraufhin der Arztpraxis einen Messenger-Service mit einem sicheren Authentifizierungsverfahren bereit. Durch die Dezentralität KANN dieser Service sowohl *on-premise*, als auch in einem Rechenzentrum installiert werden. Zusätzlich wird ein Account für einen Akteur in der Rolle *Org-Admin* durch den Messenger-Anbieter erstellt. Der *Org-Admin* meldet sich am Messenger-Service an und hinterlegt sämtliche Akteure einer Arztpraxis (z. B. MFA, Ärzte). Die angelegten Akteure melden sich am Messenger-Service an und können den TI-Messenger in der Rolle *User* direkt nutzen.

Die Arztpraxis wird als Organisation für Akteure anderer Organisationen des TI-Messenger-Dienstes erreichbar. Dazu KANN ein Akteur in der Rolle *Org-Admin* Kontaktpunkte auf dem VZD-FHIR-Directory einrichten. 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 auf dem VZD-FHIR-Directory hinterlegen. Somit haben sie die Möglichkeit andere, auf dem VZD-FHIR-Directory hinterlegte, HBA-Inhaber (Rolle *User-HBA*) in einen Chatraum einzuladen oder für diese erreichbar zu sein.

### Anwendungsbeispiel Krankenhaus

Ein Krankenhaus registriert sich mittels SMC-B bei dem Registrierungs-Dienst eines Messenger-Anbieters. Der Anbieter prüft die bereitgestellte SMC-B und stellt dem Krankenhaus einen Messenger-Service bereit. Durch die Dezentralität KANN dieser Service sowohl *on-premise*, als auch in einem Rechenzentrum installiert werden. Der Messenger-Service KANN das bestehende Authentifizierungsverfahren des Krankenhauses (z. B. Active Directory) nutzen. Die Akteure des Krankenhauses können mit den bestehenden Anmeldedaten den TI-Messenger nahtlos verwenden, auch ohne im Besitz eines HBAs (Pflege, Therapeuten, Ärzte ohne HBA = Rolle: *User*) zu sein.

Das Krankenhaus wird als Organisation für andere Akteure des TI-Messenger-Dienstes erreichbar. Dazu KANN ein Akteur in der Rolle *Org-Admin* Kontaktpunkte auf dem VZD-FHIR-Directory einrichten. Akteure des Krankenhauses im Besitz eines HBAs KÖNNEN zusätzlich mittels des TI-Messenger-Clients die eigene MXID als Practitioner-Eintrag auf dem VZD-FHIR-Directory hinterlegen (Rolle *User-HBA*). Somit haben sie die Möglichkeit andere, auf dem VZD-FHIR-Directory hinterlegte, HBA-Inhaber (Rolle *User-HBA*) in einen Chatraum einzuladen oder für diese erreichbar zu sein.

### Anwendungsbeispiel Apotheke

Der Anbieter stellt der Apotheke einen Messenger-Service bereit. Durch die Dezentralität KANN dieser Service sowohl *on-premise*, als auch in einem Rechenzentrum installiert werden. Der Messenger-Service wird mit dem bestehenden IDP-Dienst der Apotheken verwendet. Die dort hinterlegten Akteure der Apotheke können den TI-Messenger mittels OpenID-Connect verwenden auch ohne im Besitz eines HBA zu sein (z. B. PTA, angestellte Apotheker ohne HBA).

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

### Anwendungsbeispiel Verbände

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

Akteure des Verbandes im Besitz eines HBAs (Rolle *User-HBA*) KÖNNEN zusätzlich mittels des TI-Messenger-Clients die eigene MXID als Practitioner-Eintrag 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.

## Mainline

Im Folgenden wird die Kommunikation für eingehende und ausgehende Nachrichten aus der Nutzersicht in der Rolle *User* und *User-HBA* in einer Kommunikationsmatrix verdeutlicht.

Tabelle 2: Kommunikationsmatrix

Rolle	Ausgehende Kommunikation	Eingehende Kommunikation
User	<ul style="list-style-type: none"> <li>Start der Kommunikation mit anderen Organisationen</li> <li>Start der Kommunikation mit Akteuren in der Rolle <i>User</i> und <i>User-HBA</i> innerhalb einer Organisation</li> <li>Start der Kommunikation mit Akteuren in der Rolle <i>User</i> und <i>User-HBA</i> anderer Messenger-Services durch Scan eines QR-Codes</li> </ul>	<ul style="list-style-type: none"> <li>Kommunikationsanfragen durch Akteure in der Rolle <i>User</i> und <i>User-HBA</i> innerhalb einer Organisation</li> <li>Kommunikationsanfragen durch Akteure in der Rolle <i>User</i> und <i>User-HBA</i> anderer Messenger-Services durch Scan eines QR-Codes</li> <li>Kommunikationsanfragen durch Akteure in der Rolle <i>User</i> und <i>User-HBA</i> anderer Messenger-Services als Ansprechpartner der Organisation. Die MXID wurde durch einen Akteur in der Rolle <i>Org-Admin</i> der entsprechenden Ressource der Organisation auf dem VZD-FHIR-Directory hinterlegt</li> </ul>
User-HBA	<ul style="list-style-type: none"> <li>Start der Kommunikation mit anderen Organisationen</li> <li>Start der Kommunikation mit Akteuren in der Rolle <i>User</i> und <i>User-HBA</i> innerhalb einer Organisation</li> <li>Start der Kommunikation mit Akteuren in der Rolle <i>User</i> und <i>User-HBA</i> anderer Messenger-Services durch Scan eines QR-Codes</li> <li>Start der Kommunikation mit Akteuren in der Rolle <i>User-HBA</i> anderer Messenger-Services durch Suche eines Akteurs auf dem VZD-FHIR-Directory</li> </ul>	<ul style="list-style-type: none"> <li>Kommunikationsanfragen durch Akteure in der Rolle <i>User</i> und <i>User-HBA</i> innerhalb einer Organisation</li> <li>Kommunikationsanfragen durch Akteure in der Rolle <i>User</i> und <i>User-HBA</i> anderer Messenger-Services durch Scan eines QR-Codes</li> <li>Kommunikationsanfragen durch Akteure in der Rolle <i>User-HBA</i> anderer Messenger-Services durch Auffindbarkeit im VZD-FHIR-Directory</li> <li>Kommunikationsanfragen durch Akteure in der Rolle <i>User</i> und <i>User-HBA</i> anderer Messenger-Services als Ansprechpartner der Organisation. Die MXID wurde durch einen Akteur in der Rolle <i>Org-Admin</i> der entsprechenden Ressource der Organisation auf dem VZD-FHIR-Directory hinterlegt</li> </ul>

### 3.4 Nutzung von Personal Assertion Token (PASSporT)

Für die Etablierung eines Rechtekonzeptes innerhalb des TI-Messenger-Dienstes werden Personal Assertion Token (PASSporT) gemäß [RFC 8225#PASSporT: Personal Assertion Token] verwendet. Durch das PASSporT wird nachgewiesen, dass ein Akteur berechtigt ist, innerhalb der TI-Messenger-Föderation Aktionen mit anderen berechtigten Akteuren durchzuführen. Das PASSporT wird initial beim Eintritt in einem Chatraum benötigt. Ein ausgestelltes PASSporT MUSS den Anfragen an den Matrix-Homeserver hinzugefügt und durch den jeweiligen vorgeschalteten Messenger-Proxy (eingehende/ausgehende Kommunikation) ausgewertet werden. Bei einer erfolgreichen Prüfung wird die Anfrage an den Matrix-Homeserver weitergeleitet. Handelt es sich um kein gültiges PASSporT MUSS diese vom Messenger-Proxy abgelehnt werden.

Ein PASSporT wird entweder zentral durch den PASSporT-Service des VZD-FHIR-Directory, unmittelbar in Verbindung mit einer im VZD-FHIR-Directory ausgelösten Suche, oder durch den PASSporT-Service des Messenger-Service des eingeladenen Akteurs ausgestellt. Ein PASSporT wird durch den PASSporT-Service des VZD-FHIR-Directory ausgestellt, wenn für den Akteur eine MXID mit einem der TI-Messenger-Föderation zugehörigen Domain Part hinterlegt wurde. Die

## Mainline

Bereitstellung des PASSporT durch den PASSporT-Service des Messenger-Service erfolgt analog zum PASSporT-Service des VZD-FHIR-Directory und wird notwendig, wenn der eingeladene Akteur seine MXID nicht im VZD-FHIR-Directory hinterlegt hat. Bestandteil eines PASSporT ist sowohl die MXID des einladenden Akteurs, als auch die MXID des eingeladenen Akteurs.

### 3.5 Verwendung der Token

Für die Nutzung des TI-Messenger-Dienstes kommen unterschiedliche Arten von Token zum Einsatz und werden in verschiedenen Anwendungsfällen verwendet. Die folgenden für eine Authentisierung benötigten Token werden verwendet:

- ID\_TOKEN die auf Basis von SmartCard Identitäten vom zentralen IDP-Dienst ausgestellt werden,
- Matrix-ACCESS\_TOKEN die von den Matrix-Homeservern ausgestellt werden und
- Matrix-OpenID-Token die vom Matrix-Homeserver ausgestellt werden und,
- admin-accesstoken und,
- tim-search-accesstoken und,
- owner-accesstoken

#### ID\_TOKEN (zentraler IDP-Dienst)

Das vom zentralen IDP-Dienst ausgestellte ID\_TOKEN, wird vom Frontend des Registrierungs-Dienstes sowie den TI-Messenger-Clients verwendet, um sich gegenüber dem Registrierungs-Dienst oder dem Auth-Service des VZD-FHIR-Directory zu authentifizieren.

#### Matrix-ACCESS\_TOKEN (Matrix-Homeserver)

Nach der erfolgreichen initialen Registrierung oder 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. Mit dem Matrix-ACCESS\_TOKEN MUSS sich ein Akteur mit einem existierenden Matrix-Account, an seinem Matrix-Homeserver authentisieren. Dieses Token wird im lokalen Speicher des TI-Messenger-Clients sicher abgespeichert und MUSS bei jeder weiteren Interaktion mit seinem Matrix-Homeserver verwendet werden und ist an die Session des jeweiligen Clients gebunden.

#### Matrix-OpenID-Token (Matrix-Homeserver)

Bei dem Matrix-OpenID-Token handelt es sich um ein 3rd-Party-Token, welches von einem Matrix-Homeserver gemäß [Client-Server API#OpenID] bei Bedarf für einen Akteur ausgestellt wird. Im Kontext des TI-Messenger-Dienstes wird das 3rd-Party-Token als Matrix-OpenID-Token bezeichnet. Das Matrix-OpenID-Token wird für die Verifizierung eines Messenger-Services sowie für das Suchen von FHIR-Ressourcen im VZD-FHIR-Directory benötigt. Hierfür wird das Matrix-OpenID-Token im Auth-Service des Verzeichnisdienstes gegen ein tim-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 Matrix-Homeserver auf.

#### admin-accesstoken (OAuth des VZD-FHIR-Directory)

ToDo:

#### tim-search-accesstoken (Auth-Service des VZD-FHIR-Directory)

ToDo:

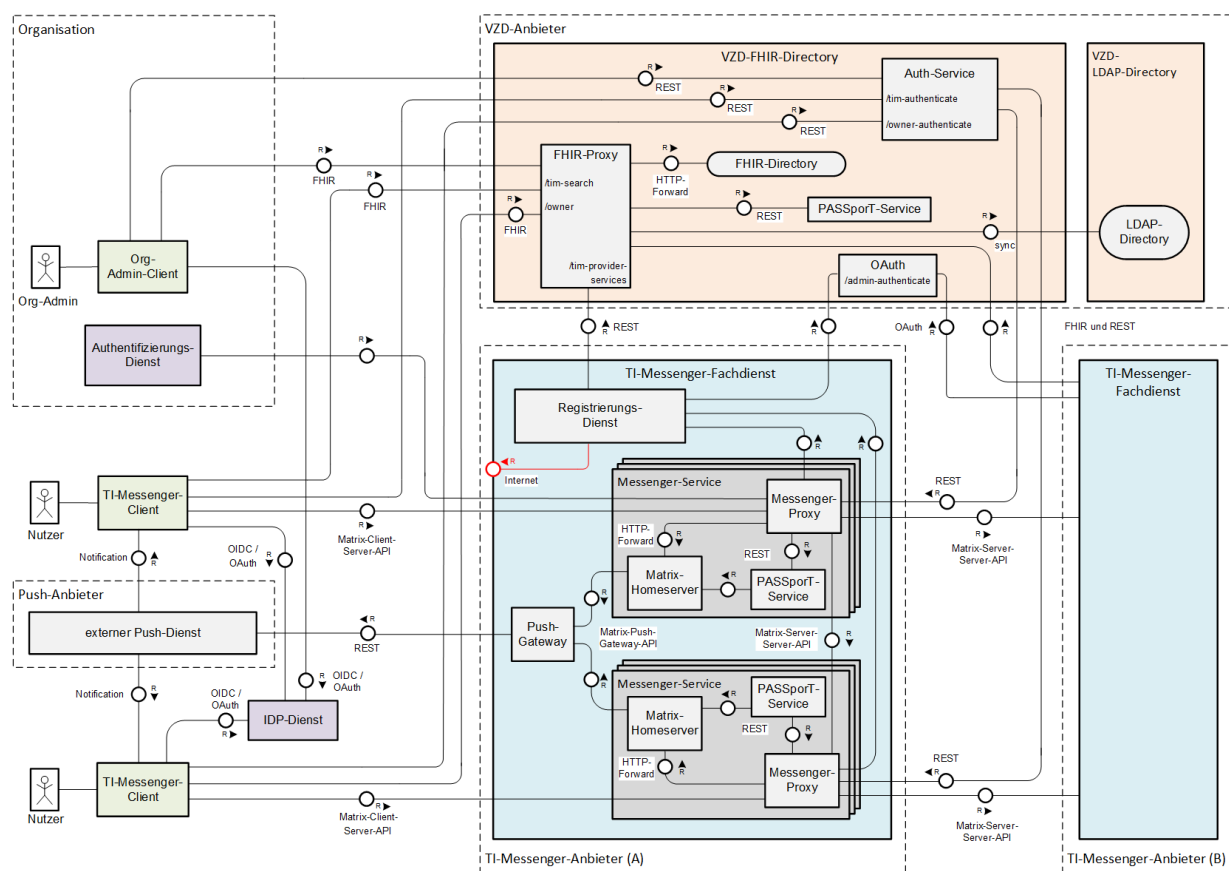
**owner-accesstoken (Auth-Service des VZD-FHIR-Directory)**

ToDo:

## 4 Systemzerlegung

Bei der Umsetzung der Funktionalitäten des TI-Messenger-Dienstes des deutschen Gesundheitswesens sind mehrere Komponenten beteiligt, die durch verschiedene Anbieter bereitgestellt werden können. Im Folgenden werden die jeweiligen beteiligten Komponenten des TI-Messenger-Dienstes 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**

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

Die in der Abbildung rot dargestellte Schnittstelle am Registrierungs-Dienst wird nicht durch die gematik normativ vorgegeben. Es bleibt dem TI-Messenger-Anbieter überlassen diese in geeigneter Form bereitzustellen.

#### 4.1 TI-Messenger-Fachdienst

Der TI-Messenger-Fachdienst ist die zentrale Komponente des TI-Messenger-Dienstes zur Ad-hoc-Kommunikation zwischen mehreren Akteuren. Für die Kommunikation mit den TI-Messenger-Clients stellt der Fachdienst alle notwendigen Schnittstellen bereit. Für eine fachdienstübergreifende Kommunikation werden alle Nachrichten an weitere Fachdienste übermittelt. Der Zugriff auf den TI-Messenger-Fachdienst ist durch unterschiedliche Authentifizierungsverfahren abgesichert und ist abhängig vom Messenger-Service, der verwendet wird. Es MUSS sichergestellt werden, dass die Organisation die Akteure jederzeit identifizieren kann und dass 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. Die Komponenten sind als logische Dienste zu verstehen, welche letztendlich die in der Spezifikation beschriebenen Funktionalitäten umsetzen müssen. Die tatsächliche Realisierung bzw. Trennung dieser Dienste darf variabel durch die Produkthersteller erfolgen, solange alle Anforderungen an die Funktionalität, Sicherheit und Interoperabilität stets erfüllt sind und eingehalten werden.

##### 4.1.1 Registrierungs-Dienst

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

Um einen interoperablen Onboarding-Prozess zu gewährleisten MUSS der Registrierungs-Dienst die Bereitstellung eines Messenger-Service über ein Frontend ermöglichen. So MUSS der Dienst bei einer neuen Registrierungsanfrage die durch den Smartcard IDP-Dienst ausgestellten ACCESS\_TOKEN und ID\_TOKEN validieren und einen dezentralen Messenger-Service starten. Dazu MUSS das Frontend des Registrierungs-Dienst beim Smartcard 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 in die TI-Messenger Föderation eintragen.

Neben der Registrierung neuer Messenger-Services, dient der Registrierungs-Dienst ebenfalls als Middleware zwischen TI-Messenger-Client und VZD-FHIR-Directory und speichert eine aktuelle Liste aller verifizierten Domains, damit diese von dem Messenger-Proxy abgerufen werden können. Für die Prüfung der Signatur der durch den PASSporT-Service im VZD-FHIR-Directory ausgestellten PASSporT wird das öffentliche Zertifikat des PASSporT-Service im Registrierungs-Dienst abgelegt. Die Messenger-Proxies aller Messenger-Services des TI-Messenger-Fachdienst-Anbieters MÜSSEN dieses Zertifikat am Registrierungs-Dienst für die Prüfung der vom PASSporT-Service im VZD-FHIR-Directory ausgestellten PASSporT nutzen.

##### 4.1.2 Push-Gateway

Jeder Anbieter eines TI-Messenger-Fachdienstes MUSS ein Push-Gateway bereitstellen, um seinen registrierten Akteure 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.

#### 4.1.3 Messenger-Service

Ein Messenger-Service besteht aus einem Messenger-Proxy, einem PASSporT-Service und einem Matrix-Homeserver der gemäß der Spezifikation der Matrix Foundation implementiert ist. Messenger-Services unterscheiden sich lediglich durch die jeweils unterstützten Authentifizierungsverfahren. Es ist notwendig, dass sich die Messenger-Services mit steigender Last skalieren lassen. Ein Messenger-Service wird immer einer Organisation des Gesundheitswesens zugeordnet. Näheres zur Absicherung der Komponenten der Messenger-Services findet sich in der Spezifikation des TI-Messenger-Fachdienstes [gemSpec\_TI-Messenger-FD].

##### 4.1.3.1 Messenger-Proxy

Der Messenger-Proxy als Prüfinstanz aller Request zum Messenger-Server ist sowohl für die Regelung der gemäß Matrix Server-Server-API und Matrix-Client-Server-API geltenden Aufrufe zuständig. Die hierbei jeweils notwendigen Prüfungen unterscheiden sich und werden im Folgenden beschrieben.

###### 4.1.3.1.1 Server-Server Proxy

Der Messenger-Proxy schließt nicht zur TI-Messenger Föderation gehörende Matrix-Homeserver aus. Für die Prüfung der Berechtigung hat der Messenger-Proxy Zugriff auf den Registrierungs-Dienst des zugehörigen TI-Messenger-Anbieters. Dieser stellt ihm eine täglich aktualisierte Föderationsliste zur Verfügung. Bei jedem Transaction-Event der Messenger-Server erfolgt damit die Prüfung auf Zugehörigkeit zur TI-Messenger-Föderation.

###### 4.1.3.1.2 Client-Server Proxy

Der Messenger-Proxy prüft, ob ein Akteur berechtigt ist eine Kommunikation mit anderen Akteuren aufzubauen (Invite-Request). Dazu benötigen Leistungserbringer und Mitarbeiter von Organisationen PASSporT, die vom VZD-FHIR-Directory, oder einem Messenger-Service ausgestellt werden. Diese PASSporT zeigen die Berechtigung zum Kommunikationsaufbau an. Findet die Kommunikation zwischen Akteuren auf einem gemeinsamen Messenger-Service statt muss dies der Messenger-Proxy erkennen, auf die Prüfung auf gültige PASSporT verzichten und nur die Zugehörigkeit zu Matrix-Domain dieses Messenger-Service beachten.

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 Arte der Umsetzung bleibt dem Anbieter überlassen.

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

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

##### 4.1.3.2 PASSporT-Service des Messenger-Service

Der PASSporT-Service des TI-Messenger-Fachdienstes wird verwendet, wenn Akteure, die nicht im VZD-FHIR-Directory gefunden werden, eine Kommunikation aufbauen möchten oder ein direkter Kontakt zwischen den Akteuren möglich ist. In diesem Fall wird kein PASSporT durch den VZD-FHIR-Directory PASSporT-Service ausgestellt. Dies MUSS dann durch den PASSporT-Service des TI-Messenger-Fachdienstes des einzuladenden Akteurs gemäß [gemSpec\_TI-Messenger-FD#5.2.3] bereitgestellt werden.



#### 4.1.3.3 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 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 (Starten neuer Räume etc.) statt. Der TI-Messenger Anbieter MUSS sicherstellen, dass folgende Matrix-Spec-Changes (MSCs) gemäß [MSC] zum Thema Push-Benachrichtigungen von dem Matrix-Homeserver unterstützt werden:

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

#### 4.2 TI-Messenger-Client

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

Der TI-Messenger-Anbieter MUSS mindestens einen mobilen und einen desktopfähigen TI-Messenger-Client anbieten. Welche Art des Clients angeboten wird, ist dem Anbieter überlassen. Ebenfalls MUSS der TI-Messenger-Client am Smart card IDP-Dienst registriert sein, damit mittels SMC-B oder HBA Änderungen am VZD-FHIR-Directory durch einen Akteur in der Rolle *Org-Admin* vorgenommen werden können.

Für die Realisierung von Anwendungsfällen, für die ausschließlich ein *Org-Admin* berechtigt, ist MUSS ein TI-Messenger-Anbieter einen TI-Messenger-Client anbieten der einen Akteur in der Rolle *Org-Admin* in die Lage versetzt die im Kapitel 6 dem Akteur *Org-Admin* zugeordneten Anwendungsfälle umzusetzen. Diese erweiterte Funktionalität kann in den TI-Messenger-Client integriert werden und in geeigneter Form für den *Org-Admin* freigegeben werden oder durch einen separaten Client bereitgestellt werden.

#### 4.3 VZD-FHIR-Directory

Beim VZD-FHIR-Directory handelt es sich um einen zentralen Verzeichnisdienst, der die deutschlandweite Suche von Akteuren des TI-Messenger-Dienstes ermöglicht. Das VZD-FHIR-Directory basiert auf dem FHIR-Standard zum Austausch von definierten Informationsobjekten. Das VZD-FHIR-Directory bietet eine FHIR-Schnittstelle zur Suche nach Leistungserbringern (*Practitioner*) und Organisationen an. Somit wird eine einfache Suche nach Akteuren, die an dem TI-Messenger teilnehmen, gewährleistet. Der Zugriff auf das VZD-FHIR-Directory ist mittels OAuth2 Client Credentials Flow gesichert. Ebenfalls ermöglicht das VZD-FHIR-Directory die sektorenübergreifende Kommunikation. Hierzu wird die Domain der Matrix-Homeserver durch einen Eintrag im VZD-FHIR-Directory registriert. Für die Nutzung des TI-Messenger-Dienstes bietet das zentrale VZD-FHIR-Directory einen FHIR-Proxy sowie einen PASSporT-Service an, die im Folgenden weiter beschrieben werden.

ToDo: Personenverzeichnis vs. Organisationsverzeichnis mit aufnehmen

#### FHIR-Proxy

Der FHIR-Proxy ist das zentrale Interface der TI-Messenger-Fachdienste zum VZD-FHIR-Directory. Der FHIR-Proxy leitet autorisierte Anfragen und Kommandos vom TI-Messenger-Client an das VZD-FHIR-Directory weiter. Die Komponente Registrierungs-Dienst benutzt den FHIR-Proxy ebenfalls für den Zugriff auf das VZD-FHIR-Directory. Der



## Mainline

Kommunikationsablauf für den Zugriff auf das VZD-FHIR-Directory durch den TI-Messenger-Client ist in [gemSpec\_VZD\_FHIR\_Directory#6.2] beschrieben.

ToDo: Auth Komponente zur Ausstellung von User-Token

### PASSporT-Service des VZD-FHIR-Directory

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

### OAuth

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

Für die Zugriff auf den OAuth-Server MUSS der TI-Messenger-Anbieter für seinen Registrierungsdienst beim VZD-Anbieter Client-Credentials beantragen. Die Beantragung erfolgt über einen Service-Request an [betrieb@gematik.de](mailto:betrieb@gematik.de) mit dem Betreff "VZD-FHIR-Directory (De-)/Registrierung" notwendig.

Weiterführende Informationen zum VZD-FHIR-Directory sind in [api-vzd] zu finden.

## 5 Übergreifende Festlegungen

### 5.1 Datenschutz und Sicherheit

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

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

### 5.2 Verwendete Standards

#### Matrix

Für den TI-Messenger-Dienst wird das offene Kommunikationsprotokoll der Matrix-Foundation 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 TI-Messenger-Matrix-Homeservern die API des Matrix-Client-Server-Protokolls um. Für die Benachrichtigung der Akteure über eingehende Nachrichten wird ein Push Gateway verwendet, welches gemäß [Push Gateway API] nachgenutzt wird. Bei der Kommunikation werden REST-Webservices über HTTPS (JSON-Objekte) aufgerufen.

#### OpenID-Connect

Das VZD-FHIR-Directory nutzt als Authorisierungsserver den Smartcard IDP-Dienst der TI. Hierfür stellt der IDP-Dienst

**Mainline**

ein ID\_TOKEN und ACCESS\_TOKEN für Akteure in Form eines JSON-Web-Token (JWT) gemäß [OpenID] aus.

**FHIR**

Der TI-Messenger-Client sowie der Registrierungs-Dienst des TI-Messenger-Fachdienstes nutzen die Schnittstellen des VZD-FHIR-Directories gemäß dem FHIR-Standard [FHIR] mit einer RESTful API.

**PASSporT**

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

**5.3 Authentifizierung und Autorisierung****5.3.1 Authentifizierung von Akteuren**

Für die Authentifizierung von Akteuren (z. B. Mitarbeiter in einer Organisation oder Leistungserbringer) 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-Fachdienst-Anbieter. Die Benutzerverwaltung erfolgt durch autorisierte Mitarbeiter in der jeweiligen Organisation (In der Rolle *Org-Admin*). Die verwendeten Authentifizierungsmethoden MÜSSEN unter der Kontrolle der jeweiligen Organisation sein.

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

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

Für die Authentifizierung von Leistungserbringern und Organisationen des Gesundheitswesens, die im Besitz einer SMC-B/HBA sind, wird der durch die gematik spezifizierte IDP-Dienst verwendet [gemSpec\_IDP\_Dienst]. Dazu MUSS der verwendete TI-Messenger-Client beim **Smartcard IDP-Dienst** registriert sein. Der Akteur in der Rolle *Org-Admin* KANN mittels des ACCESS\_TOKEN die MXID als **Telecom** Eintrag der Organisations-Ressource zuordnen. Diese Zuordnung macht die jeweilige Organisationsressource anschreibbar durch Akteure anderer Organisationen. Der Akteur in der Rolle *User-HBA* KANN mittels des ACCESS\_TOKEN die MXID als **Telecom** Eintrag der eigenen Practitioner-Ressource zuordnen. Diese Zuordnung verifiziert die MXID des Leistungserbringers, so dass dieser durch andere verifizierte Akteure (Rolle *User-HBA*) auf dem VZD-FHIR-Directory gefunden werden kann oder andere verifizierte Akteure in der Rolle *User-HBA* in Chaträume einladen kann.

### 5.3.2 Autorisierung am Messenger-Service

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

### 5.3.3 Autorisierung am FHIR-Proxy

TI-Messenger-Clients autorisieren sich gegenüber dem FHIR-Proxy des VZD-FHIR-Directory für lesenden Zugriff mittels Matrix-OpenID-Token, welches vom Matrix-Homeserver ausgestellt wird. Für schreibenden Zugriff nutzen TI-Messenger-Clients ein ACCESS\_TOKEN, welches durch den **Smartcard IDP-Dienst** ausgestellt wird. Der Ablauf der Autorisierung am FHIR-Proxy wird in der [gemSpec\_VZD\_FHIR\_Directory] im Anwendungsfall "**Nutzer sucht TIOrganization- und TIPractioner-Einträge im VZD-FHIR-Directory**" beschrieben. Eine Erläuterung zu dem Rechtekonzept des VZD-FHIR-Directory findet sich in dieser Spezifikation im Kapitel "**Rechtekonzept VZD-FHIR-Directory**".

## 5.4 Föderation

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

Um allen berechtigten Akteuren des deutschen Gesundheitswesens den Zugang zum TI-Messenger zu gewähren, MUSS ein Anbieter eines TI-Messenger-Fachdienstes für Leistungserbringerinstitutionen und/oder einer Organisation entsprechende Messenger-Services bereitstellen.

Um nicht zum TI-Messenger gehörende Matrix-Server ausschließen zu können, werden die TI-Messenger-Fachdienste in einer Föderation zusammengefasst. Voraussetzung für die Aufnahme in die Föderation ist der Betrieb eines Messenger-Proxies als Teil des Messenger-Services, der sicherstellen MUSS, dass nur zugelassene TI-Messenger-Fachdienste Zugang in die Föderation erhalten. Voraussetzung für die Aufnahme in die Föderation ist eine erfolgreiche Zulassung durch die gematik. Nach einer erfolgreichen Zulassung erhält der Registrierungs-Dienst des jeweiligen Fachdienstes die Möglichkeit die Domains des jeweiligen Messenger-Services der entsprechenden Organisation auf dem VZD-FHIR-Directory zuzuordnen.

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

## 5.5 Rechtekonzept VZD-FHIR-Directory

Im Folgenden Kapitel wird beschrieben, wie der Schreib- und Lesezugriff durch die TI-Messenger-Clients und dem Registrierungs-Dienst auf dem VZD-FHIR-Directory erfolgt.

### 5.5.1 Schreibzugriffe für den Registrierungs-Dienst

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

### 5.5.2 Schreibzugriff für TI-Messenger-Clients

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

#### Schreibzugriff für Akteure in der Rolle Org-Admin

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

#### Schreibzugriff für Akteure in der Rolle User-HBA

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

### 5.5.3 Lesezugriff für TI-Messenger-Clients

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

Es gilt:

- die Sichtbarkeit auf die Organisations-Ressourcen KANN für andere Organisationen oder Practitioners eingeschränkt werden und
- die Sichtbarkeit auf Practitioner-Ressourcen ist nur möglich, wenn der Akteur selbst mit der Matrix User URI (MXID) als Practitioner auf dem VZD hinterlegt ist und die Period gemäß [Spec\_VZD-FHIR\_Directory] gesetzt wurde.

## 5.6 Betrieb

Der TI-Messenger-Anbieter verantwortet im Betrieb folgende Produkte: TI-Messenger-Fachdienst und TI-Messenger-Client(s). Der TI-Messenger-Anbieter KANN auch mehrere TI-Messenger-Clients anbieten. Der tatsächliche Betrieb kann gemäß [gemKPT\_Betr#Anbieterkonstellationen] ausgelagert werden.

Der TI-Messenger-Anbieter MUSS seinen Nutzern und Organisationen einen Helpdesk entsprechend [gemKPT\_Betr] anbieten, welcher auch Störungen zu allen verantworteten TI-Messenger-Clients entgegen nimmt.

Der TI-Messenger-Anbieter ist gemäß Betriebskonzept [gemKPT\_Betr] ein Teilnehmer im TI-ITSM mit allen damit verbundenen Rechten und Pflichten.

Der TI-Messenger-Anbieter MUSS Referenzinstanzen des TI-Messenger-Fachdienstes bereitstellen und betreiben.

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

## 6 Anwendungsfälle

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

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

### Org-Admin

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

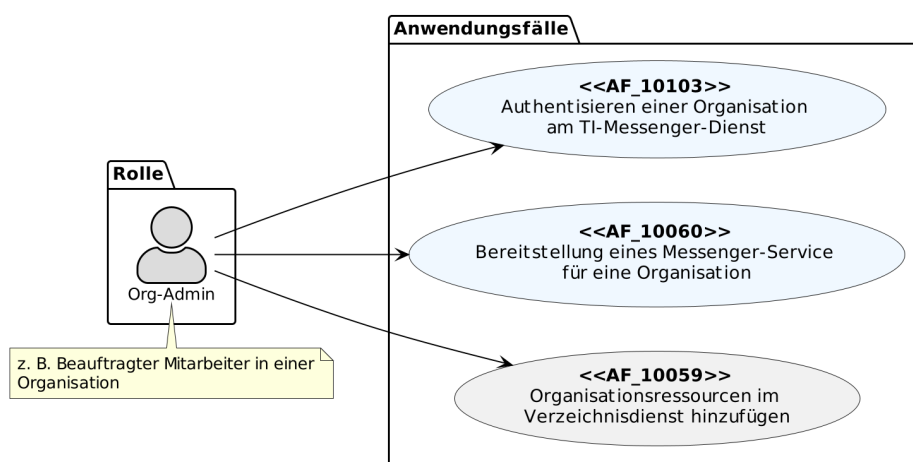


Abbildung 4 : Org-Admin - Übersicht Anwendungsfälle

Der Anwendungsfall "AF\_10060 - Bereitstellung eines Messenger Service für eine Organisation" setzt die erfolgreiche Authentifizierung der Organisation durch den Anwendungsfall AF\_10103 voraus. Werden durch eine Organisation mehrere Messenger-Services benötigt (z. B. im Krankenhausumfeld) KANN der Anwendungsfall mehrfach ausgeführt werden.

### User / User-HBA

Ein Akteur in der Rolle User / User-HBA MUSS ein berechtigter Mitarbeiter einer Organisation sein und als Nutzer des TI-Messenger-Dienstes die folgenden Anwendungsfälle auslösen können.

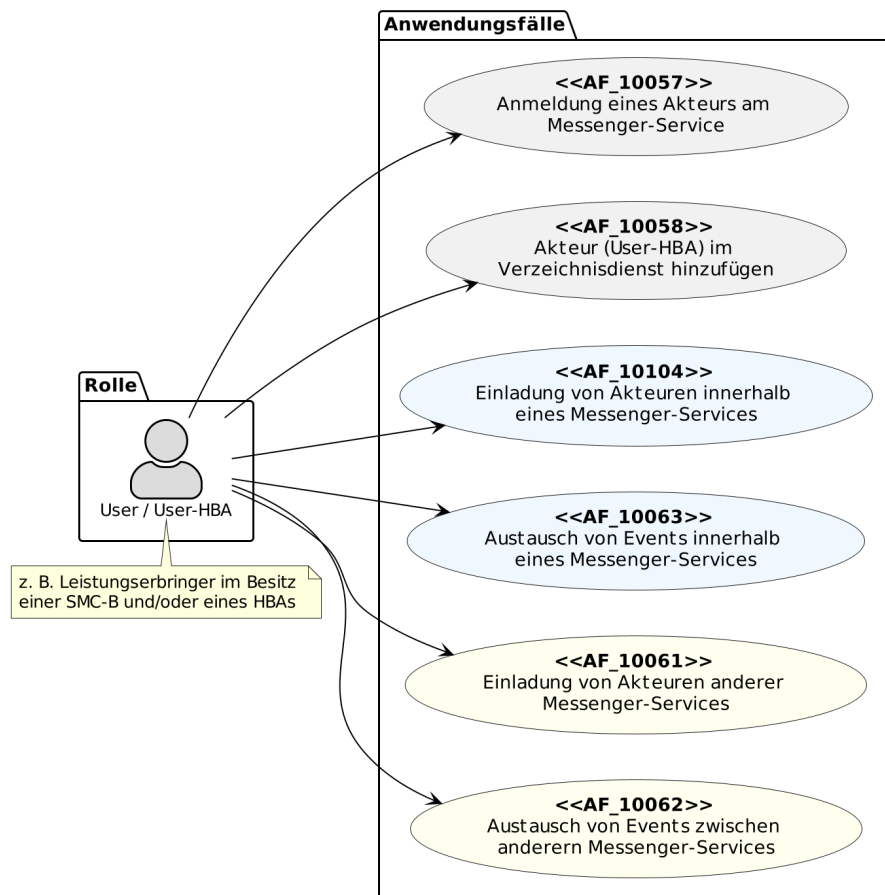


Abbildung 5 : User / User HBA - Übersicht Anwendungsfälle

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 Anwendungsfällen hingewiesen werden.




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

### AF\_10103 - Authentisieren einer Organisation am TI-Messenger-Dienst

Mit diesem Anwendungsfall authentisiert ein Akteur, in der Rolle Org-Admin, seine Organisation bei einem TI-Messenger Anbieter. Für die Authentisierung einer Organisation stellt der Messenger Fachdienst eine Schnittstelle an seinem Registrierungs-Dienst bereit. Diese wird über das Frontend des Registrierungs-Dienstes für die Authentisierung verwendet. Die Authentisierung der Organisation erfolgt individuell und nutzungsabhängig durch einen Akteur in der Rolle Org-Admin. Für die Verifizierung der Organisation MUSS bei der Authentisierung am IDP-Dienst eine freigeschaltete SMC-B verwendet werden. Als Nachweis zur Prüfung auf eine gültige Organisation MUSS der Registrierungs-Dienst die im ID\_TOKEN enthaltene ProfessionOID gegen der OID-Festlegung für Institutionen gemäß [gemSpec\_OID] prüfen. Bei erfolgreicher Verifizierung der Organisation wird ein Administrator-Account für die Organisation am Registrierungs-Dienst angelegt.

Dies ermöglicht es einem Administrator Messenger-Services zu registrieren und seiner Organisation am TI-Messenger-Dienst teilzunehmen.

Tabelle 3 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> <li>• Authenticator,</li> <li>• Konnektor,</li> <li>• eHealth Kartenterminal mit gesteckter SMC-B,</li> <li>• Registrierungs-Dienst,</li> <li>• IDP-Dienst</li> </ul>
Vorbedingung	<ol style="list-style-type: none"> <li>1. Der Akteur kann über ein Frontend für die Kommunikation auf den Registrierungs-Dienst zugreifen.</li> <li>2. Das verwendete Frontend des Registrierungs-Dienst ist bei einem zugelassenen IDP-Dienst registriert.</li> <li>3. Der Akteur kann den Authenticator des jeweiligen TI-Messenger-Anbieters verwenden.</li> <li>4. Die im eHealth Kartenterminal gesteckte SMC-B ist freigeschaltet.</li> </ol>
Eingangsdaten	Identität der Organisation, SMC-B
Ergebnis	Die Organisation wurde am Registrierungs-Dienst des TI-Messenger-Fachdienstes verifiziert
Ausgangsdaten	ID_TOKEN, Admin-Account
Akzeptanzkriterien	 ML-128757,  ML-128759,  ML-128758

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

## Mainline

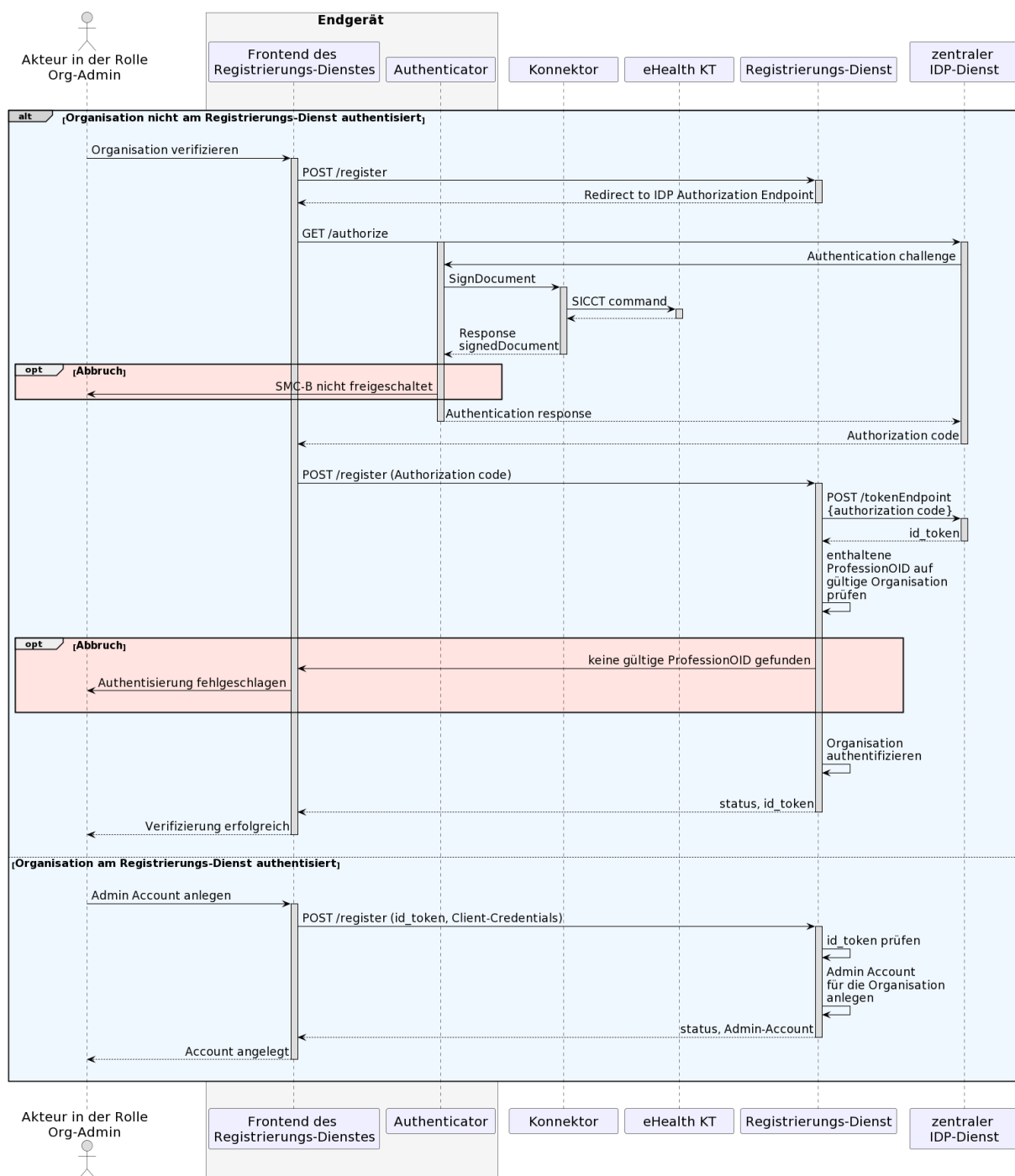


Abbildung 6 Laufzeitsicht - Authentisieren einer Organisation am TI-Messenger-Dienst

[&lt;=]

### Akzeptanzkriterien für den Anwendungsfall: Authentisieren einer Organisation am TI-Messenger-Dienst (AF\_10103)

#### ML-128757 - 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.

[&lt;=]



Mainline

**ML-128759 - Organisation wurde erfolgreich verifiziert**

Die Organisation wurde beim TI-Messenger-Fachdienst erfolgreich mit einer Identität einer Organisation des Gesundheitswesens verifiziert

[<= ]

**ML-128758 - ID-Token wurden ausgestellt und übergeben**

Das vom IDP-Dienst ausgestellte ID\_TOKEN ist gültig und liegen dem Frontend des Registrierungs-Dienstes vor.

[<= ]

**ML-129853 - Administrator Account angelegt**




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

**6.2 AF - Bereitstellung eines Messenger-Service für eine Organisation**

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

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

Tabelle 4: 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	Frontend des Registrierungs-Dienstes, Registrierungs-Dienst, VZD-FHIR-Directory, Messenger-Service
Vorbedingung	<ol style="list-style-type: none"> <li>1. Der Akteur verfügt über ein Frontend für die Kommunikation mit dem Registrierungs-Dienst.</li> <li>2. Das verwendete Frontend des Registrierungs-Dienst ist beim verwendeten IDP-Dienst registriert.</li> <li>3. Die Organisation ist erfolgreich beim Registrierungs-Dienst authentifiziert und ein Admin-Account ist vorhanden.</li> <li>4. 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
Akzeptanzkriterien	 ML-123648 ,  ML-123649 ,  ML-123650 , <input type="checkbox"/> ML-123651 - Missing cross-reference

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 Anwendungsfalles "AF\_10103 - Authentisieren einer Organisation am TI-Messenger-Dienst" vorausgesetzt. Die Komponente Messenger-Service für die Organisation wird im Verlauf des Anwendungsfalles zu einem späteren Zeitpunkt erstellt.

## Mainline

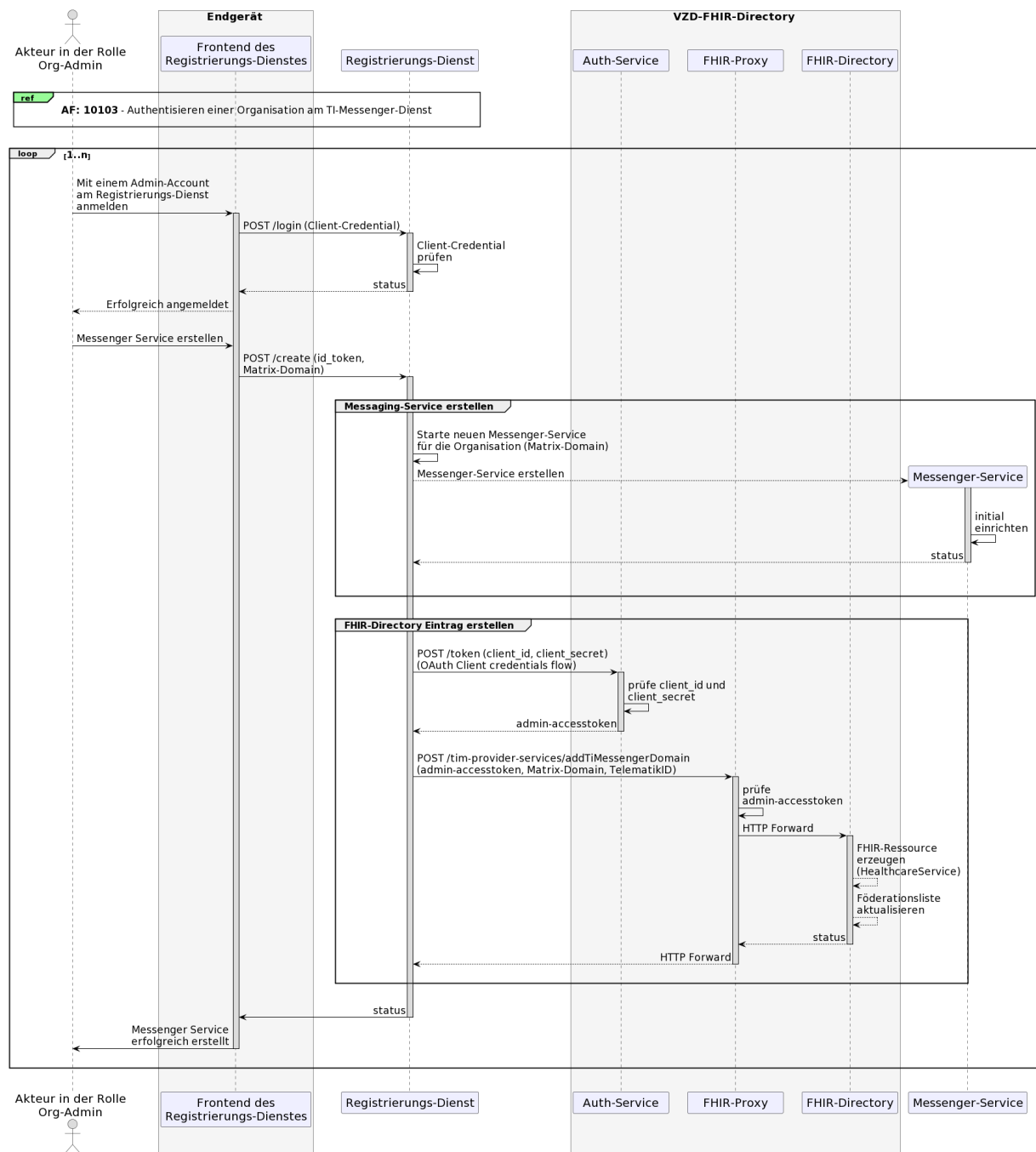


Abbildung 7: Laufzeitsicht - Bereitstellung eines Messenger-Service für eine Organisation

[&lt;= ]

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.

[&lt;= ]

**ML-123649 - AF\_10060 - Messenger-Service wurde erzeugt**

## Mainline

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



[<= ]

### 6.3 AF - Organisationsressourcen im Verzeichnisdienst hinzufügen

#### AF\_10059 - Organisationsressourcen im Verzeichnisdienst hinzufügen

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

Tabelle 5 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 und die MXIDs der Akteure der Organisation im VZD-FHIR-Directory hinterlegt werden.
Komponenten	TI-Messenger-Client (mit erweiterter Org-Admin Funktionalität), Authenticator des IDP-Dienst, IDP-Dienst, Auth-Service, FHIR-Proxy, FHIR-Directory
Vorbedingungen	<ol style="list-style-type: none"> <li>Für die Organisation wurde ein Messenger-Service bereitgestellt und eine FHIR-Ressource im VZD-FHIR-Directory erzeugt.</li> <li>Der Administrator der Organisation verfügt über einen TI-Messenger-Client (mit erweiterter Org-Admin Funktionalität).</li> <li>Das VZD-FHIR-Directory ist bei einem zugelassenen IDP-Dienst registriert.</li> <li>Der Administrator der Organisation kann sich an einem zugelassenen IDP-Dienst authentisieren.</li> </ol>
Eingangsdaten	SMC-B, FHIR-Organisations-Ressourcen
Ergebnis	FHIR-Organisations-Ressourcen aktualisiert
Ausgangsdaten	Aktualisierte VZD-FHIR-Directory-Datensätze
Akzeptanzkriterien	 ML-123626 ,  ML-123627

In der Laufzeitsicht sind die Interaktionen zwischen den Komponenten, die durch den Anwendungsfall genutzt werden, dargestellt. Hierbei handelt es sich um eine **vereinfachte Laufzeitsicht** in der zum Beispiel die TLS-Terminierung am FHIR-Proxy auf Grund der Übersichtlichkeit nicht berücksichtigt wurde.

## Mainline

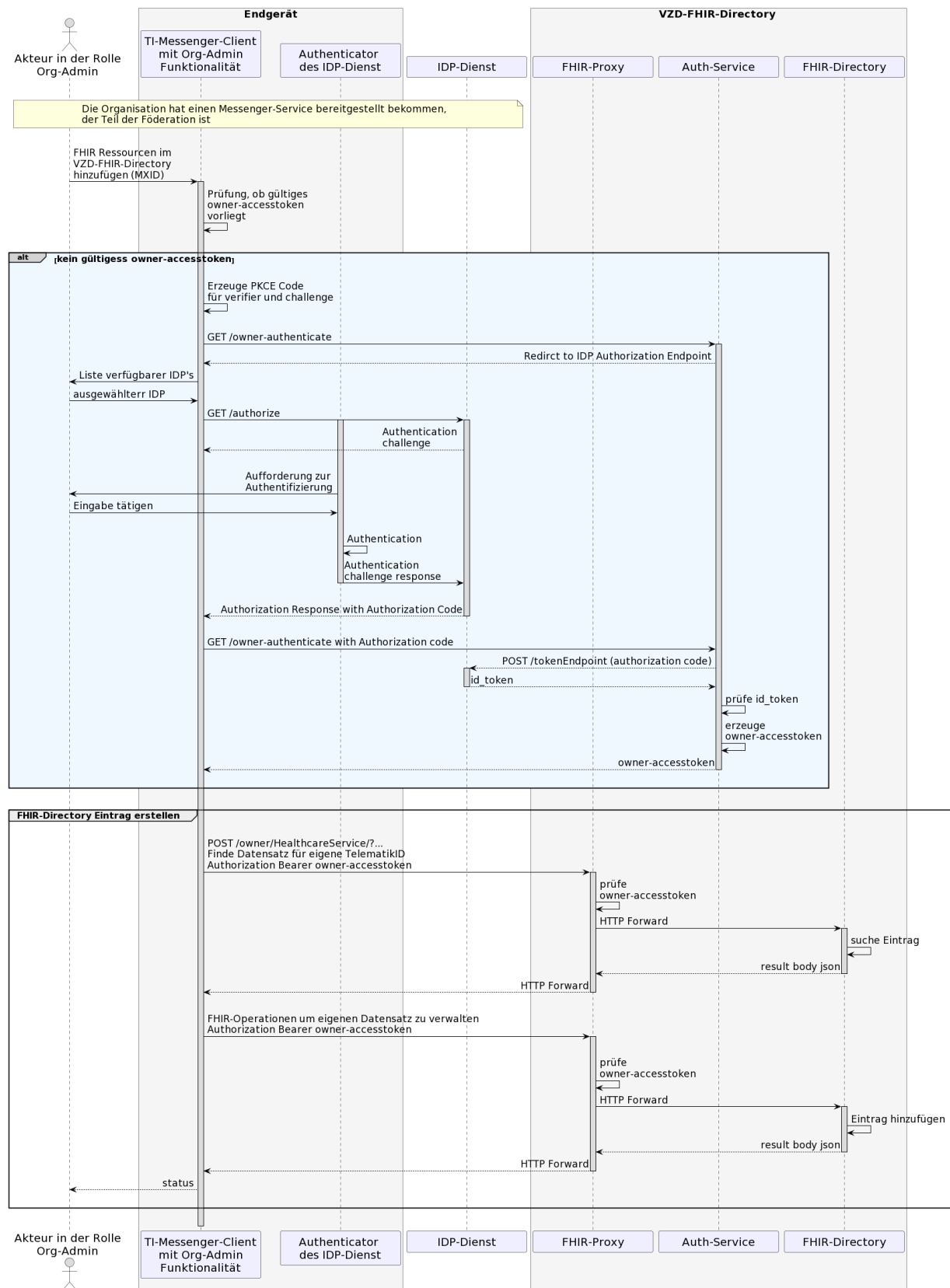


Abbildung 8: Laufzeitsicht - Organisationsressourcen im Verzeichnisdienst hinzufügen

[&lt;=]

Mainline

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

**ML-123627 - AF\_10059 - Organisationsressourcen im VZD-FHIR-Directory hinzufügen**

Nach erfolgreicher Authentisierung an einem zugelassenen IDP-Dienst als Administrator einer Organisation kann der Akteur in der Rolle Org-Admin die MXID eines Akteurs seiner Organisation in den FHIR-Organization-Datensatz eintragen und Unterstrukturen für die Organisation anlegen. Der Akteur in der Rolle Org-Admin wird über den Erfolg der Operation informiert.

[<= ]

**ML-123626 - AF\_10059 - Änderungen nur für eigene Organization-FHIR-Datensätze**

Der Akteur in der Rolle Org-Admin darf nur FHIR-Ressourcen seiner eigenen Organisation (inklusive der Unterstrukturen) ändern.

[<= ]

**6.4 AF - Anmeldung eines Akteurs am Messenger-Service**

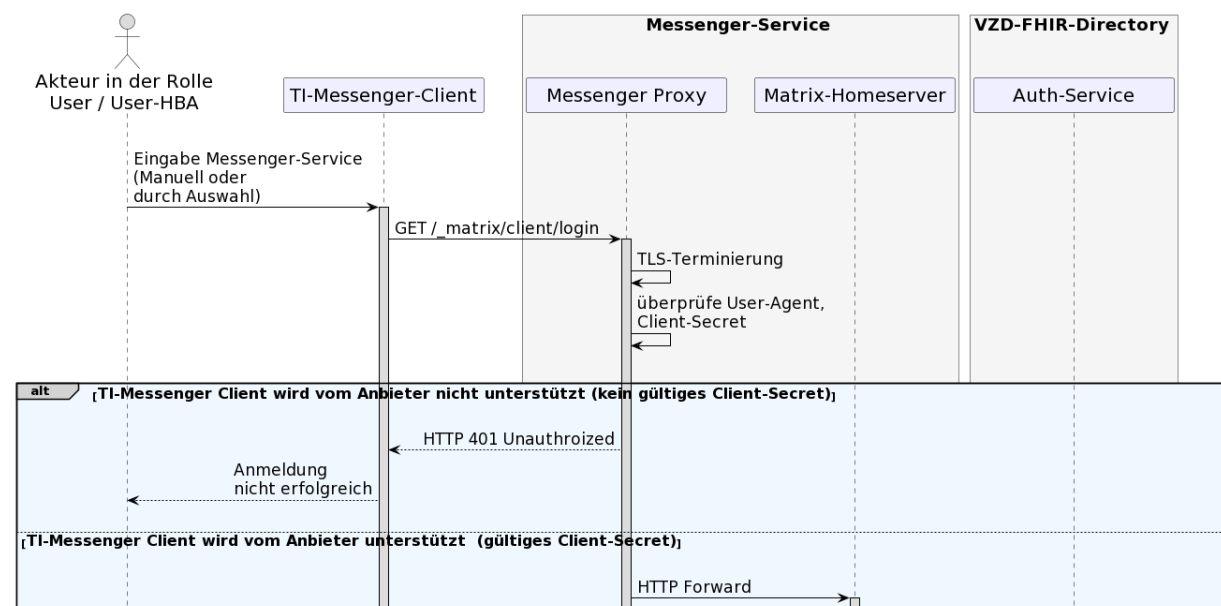
**AF\_10057 - Anmeldung eines Akteurs am Messenger-Service**

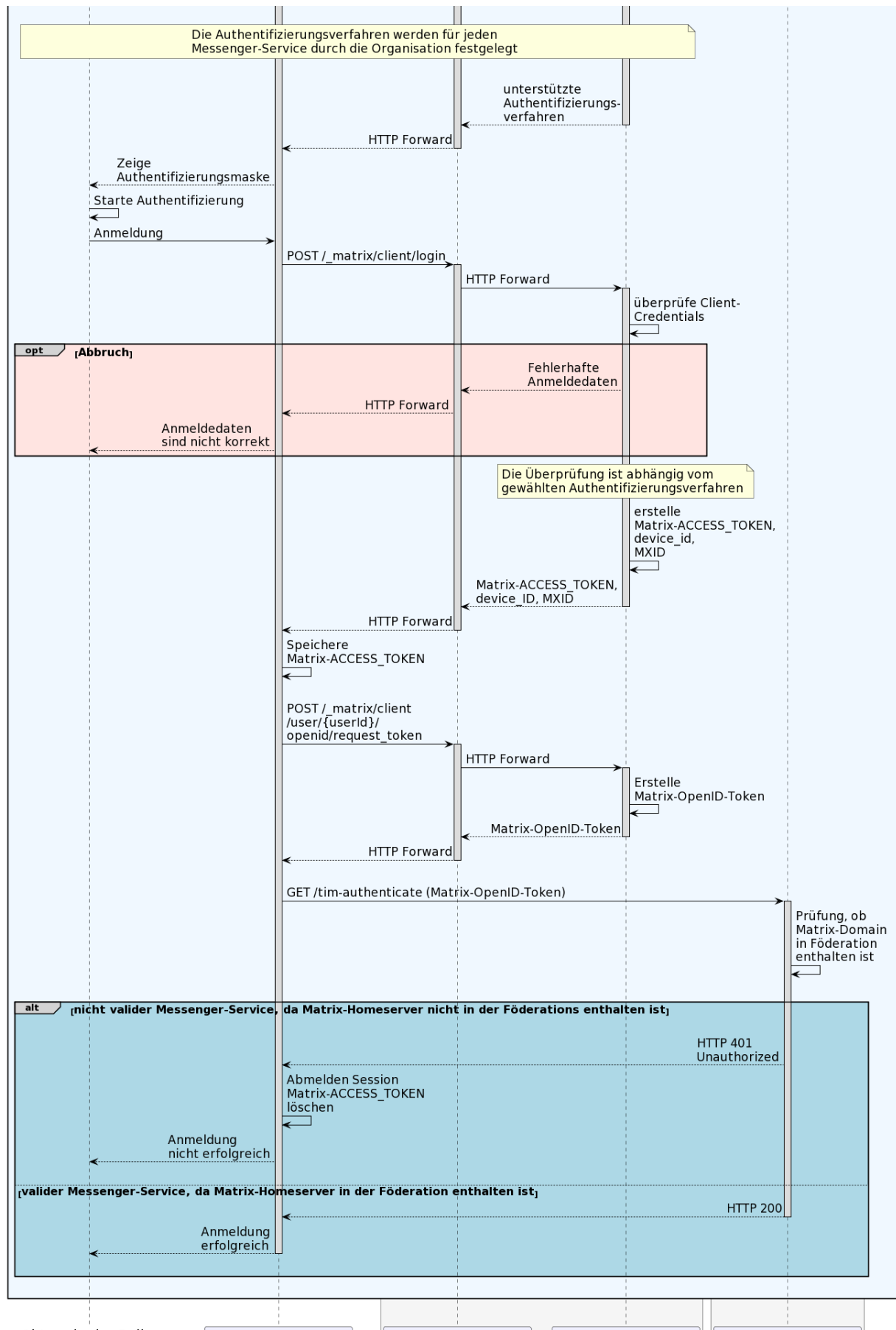
Mit diesem Anwendungsfall meldet sich ein Akteur an einem in der TI-Föderation zugelassenen Messenger-Service an und registriert seinen TI-Messenger-Client als Endgerät. Der TI-Messenger-Client KANN dem Akteur eine Liste aller vom TI-Messenger-Client unterstützten Messenger-Services anzeigen. Wird durch den TI-Messenger-Client keine Liste der unterstützten Messenger-Services angezeigt, so MUSS der Akteur die Domain des gewünschten Messenger-Services direkt im Client eingeben können. 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 6: AF - Anmeldung eines Akteurs am Messenger-Service

AF_10057	Anmeldung eines Akteurs am Messenger-Service
Akteur	Leistungserbringer, Mitarbeiter einer Organisation im Gesundheitswesen in der Rolle User / User-HBA
Auslöser	Ein Akteur möchte sich mit seinem TI-Messenger-Client bei einem Messenger-Service anmelden.
Komponenten	TI-Messenger-Client, Messenger-Proxy, Messenger-Homeserver, FHIR-Proxy, FHIR-Dirctory
Vorbedingungen	<ol style="list-style-type: none"> <li>Der Akteur verfügt über einen vom Anbieter unterstützten TI-Messenger-Client.</li> <li>Der Akteur kennt die URL des Messenger-Services oder die URL ist bereits in seinem TI-Messenger-Client konfiguriert.</li> <li>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>Der verwendete Matrix-Homeserver ist in die Föderation integriert (valider Messenger-Service).</li> </ol>
Eingangsdaten	URL des Matrix-Homeservers
Ergebnis	Ein TI-Messenger Account für einen Akteur in der Rolle User / User-HBA wurde erzeugt.
Ausgangsdaten	Matrix-ACCESS_TOKEN, MXID, device_id, Matrix-OpenID-Token
Akzeptanzkriterien	ML-123571, ML-123576, ML-123575

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.







## Mainline



Abbildung 9: Laufzeitsicht - Anmeldung eines Akteurs am Messenger-Service

[<= ]

### 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.

[<= ]

#### 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 Access Token ausgestellt.

[<= ]

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

Der TI-Messenger-Client speichert das ihm übergebene Access Token zur Verwendung in den folgenden Anwendungsfällen. [<= ]

#### ML-129870 - 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.



[<= ]

### 6.5 AF - Akteur (User-HBA) im Verzeichnisdienst hinzufügen

#### AF\_10058 - 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) 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 7: 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	TI-Messenger-Client, Authenticator des IDP-Dienst, IDP-Dienst, FHIR-Proxy, Auth-Service, FHIR-Directory
Vorbedingungen	<ol style="list-style-type: none"> <li>1. Der Akteur ist bei einem gültigen Messenger-Service angemeldet (siehe AF_10057).</li> <li>2. Der Akteur verfügt über einen zugelassenen TI-Messenger-Client.</li> <li>3. Das VZD-FHIR-Directory ist bei einem IDP-Dienst registriert.</li> <li>4. Der Akteur kann sich am IDP-Dienst authentisieren.</li> </ol>
Eingangsdaten	HBA, FHIR-Practitioner-Ressourcen
Ergebnis	FHIR-Practitioner-Ressourcen aktualisiert
Ausgangsdaten	aktualisierter Practitioner-Datensatz
Akzeptanzkriterien	 ML-123611,  ML-123612

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.

## Mainline

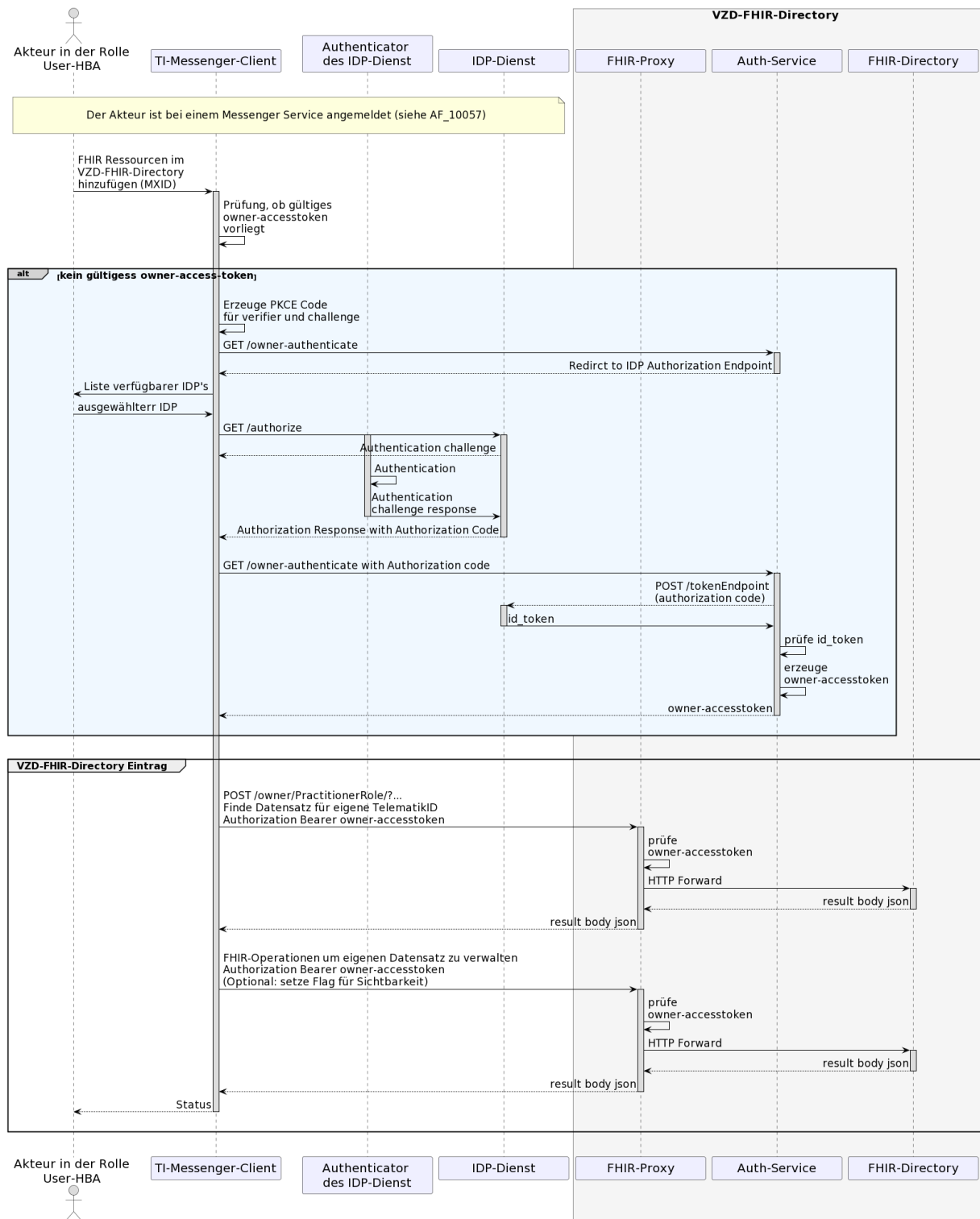


Abbildung 10: Laufzeitsicht - Akteur (User-HBA) im Verzeichnisdienst hinzufügen

[&lt;= ]

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

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

## Mainline

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.

[<= ]

### 6.6 AF - Föderationszugehörigkeit eines Messenger-Service prüfen

#### AF\_10064 - Föderationszugehörigkeit eines Messenger-Service prüfen

Dieser Anwendungsfall prüft, ob ein Messenger-Service zugehörig zur TI-Messenger-Föderation ist und gilt für alle Anwendungsfälle, welche die Remote-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 B "Aktualisierung der Föderationsliste" beschrieben.

Tabelle 8 Föderationszugehörigkeit eines Messenger-Service prüfen

AF_10064	Föderationszugehörigkeit eines Messenger-Service prüfen
Akteur	-
Auslöser	Der Messenger-Proxy empfängt einen Matrix-Request und MUSS die im Request enthaltenen MXIDs auf Domain-Zugehörigkeit zur TI-Messenger-Föderation prüfen.
Komponenten	Messenger-Proxy, Matrix-Homeserver
Vorbedingungen	keine
Eingangsdaten	Matrix-Event
Ergebnis	Der Messenger-Proxy ermittelt mittels der Föderationsliste, ob die Remote-Domain des Messenger-Service Teil der TI-Messenger-Föderation ist.
Ausgangsdaten	Status vom Matrix-Homeserver und Weiterleitung
Akzeptanzkriterien	 ML-123672 ,  ML-123891 ,  ML-123893

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.

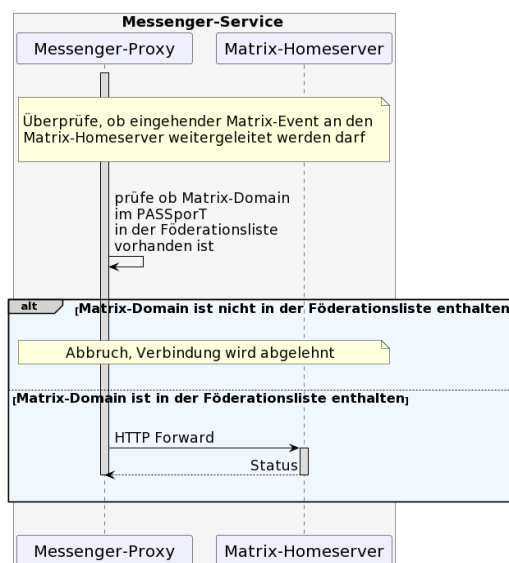


Abbildung 11: Laufzeitsicht - Föderationszugehörigkeit eines Messenger-Service prüfen

[&lt;= ]

**Akzeptanzkriterien für den Anwendungsfall: Föderationszugehörigkeit eines Messenger-Service prüfen (AF\_1006 4)**

#### 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.

[&lt;= ]

#### ML-123893 - Aktualität - Föderationsliste Messenger-Proxy

Es MUSS sichergestellt werden, dass die Föderationsliste des Messenger-Proxy aktuell ist. Dafür MUSS der Messenger-Proxy mindestens einmal täglich eine aktuelle Liste bei dem Registrierungs-Dienst anfordern.

[&lt;= ]

#### ML-123891 - Remote-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 Remote-Domain Teil der Föderationsliste ist.



[&lt;= ]

### 6.7 AF - Einladung von Akteuren innerhalb eines Messenger-Service

#### AF\_10104 - Einladung von Akteuren innerhalb eines Messenger-Service

In diesem Anwendungsfall wird ein Akteur eines gemeinsamen Messenger-Service in einen Raum eingeladen um Aktionen auszuführen. Für die Suche von Akteuren innerhalb eines Messenger-Service durchsucht ein TI-Messenger-Client das Nutzerverzeichnis des gemeinsamen Matrix-Homeserver. In diesem Anwendungsfall prüft der Messenger-Proxy lediglich, ob die Sender- und Empfänger-Domain zu der Organisation gehören. Die Überprüfung eines PASSporT wird in diesem Anwendungsfall nicht benötigt.

Tabelle 9 Einladung von Akteuren innerhalb eines Messenger-Service

AF_10104	Einladung von Akteuren innerhalb eines Messenger-Service
Akteur	Leistungserbringer, Mitarbeiter einer Organisation im Gesundheitswesen in der Rolle User / User-HBA
Auslöser	Akteur A möchte Akteur B in einen gemeinsamen Raum einladen.
Komponenten	TI-Messenger Client A + B, Messenger-Proxy, Matrix-Homeserver, Push-Gateway
Vorbedingungen	<ol style="list-style-type: none"> <li>Die Akteure sind am selben Messenger-Service angemeldet</li> <li>Jeder Akteur hat einen zugelassenen TI-Messenger-Client</li> <li>Ein Chatraum wurde durch den Einladenden eingerichtet</li> </ol>
Eingangsdaten	Matrix Invite-Request
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	keine
Akzeptanzkriterien	 ML-129415,  ML-129414

In der Laufzeitsicht sind die Interaktionen zwischen den Komponenten, die durch den Anwendungsfall genutzt werden, dargestellt. Der für die zukünftige Kommunikation genutzte Chatraum wurde durch den Einladenden Akteur bereits erstellt. Die folgende Darstellung zeigt lediglich die Einladung zwischen zwei Akteuren. Weitere Akteure können unabhängig von dieser Laufzeitsicht eingeladen werden (Hinweis: Group-Messaging).

## Mainline

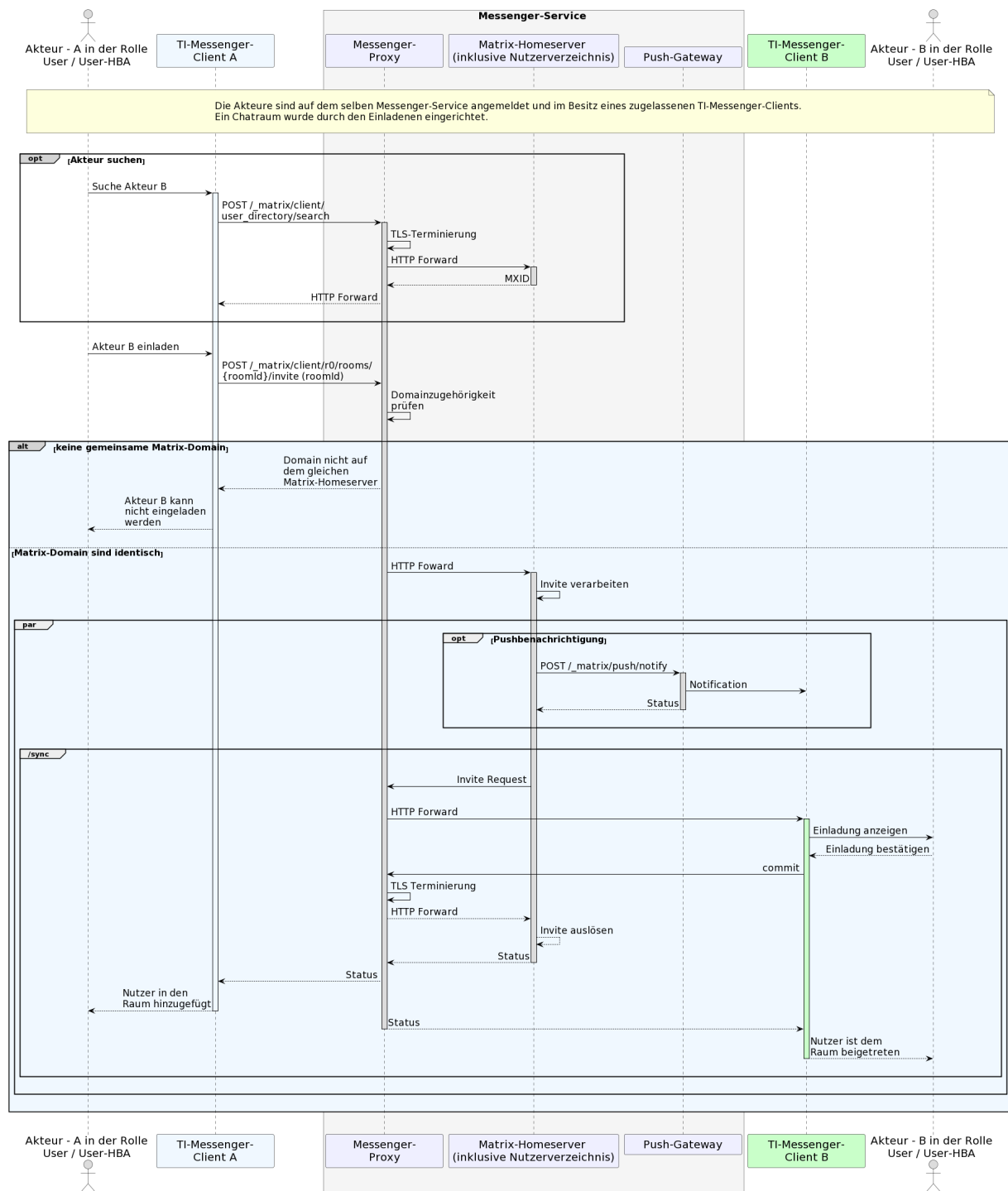


Abbildung 12 Einladung von Akteuren innerhalb eines Messenger-Service

[&lt;= ]

### Akzeptanzkriterien für den Anwendungsfall: Einladung von Akteuren innerhalb eines Messenger-Service (AF\_10104)

#### ML-123896 - Matrix-Homeserver nach Akteuren durchsuchen

Der TI-Messenger-Client zeigt eine Liste aller Akteure eines Matrix-Homeservers an.

[&lt;= ]

## Mainline

**ML-129415 - Messenger-Proxy prüft Domainzugehörigkeit**

Der Messenger-Proxy lehnt den Invite-Request ab, wenn die Domain der beteiligten Akteuren nicht zu seiner Domain gehören.

[<= ]

**ML-129414 - Akteure sind dem Chatraum beigetreten**

Alle Chat Parteien sind erfolgreich im Chatraum vorhanden.

[<= ]

**6.8 AF - Austausch von Events innerhalb eines Messenger-Service****AF\_10063 - Austausch von Events innerhalb eines Messenger-Service**

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 10 Austausch von Events innerhalb eines Messenger-Service*

AF_10063	Austausch von Events innerhalb eines Messenger-Service
Akteur	Leistungserbringer, Mitarbeiter einer Organisation im Gesundheitswesen in der Rolle User / User-HBA
Auslöser	Alle Matrix-Events die innerhalb eines Messenger-Service ausgeführt werden
Komponenten	TI-Messenger Client A + B, Matrix-Proxy, Matrix-Homeserver, Push-Gateway
Vorbedingungen	<ol style="list-style-type: none"> <li>Die Akteure sind am selben Messenger-Service angemeldet.</li> <li>Jeder Akteur hat einen zugelassenen TI-Messenger-Client.</li> <li>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-123896

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.



## Mainline

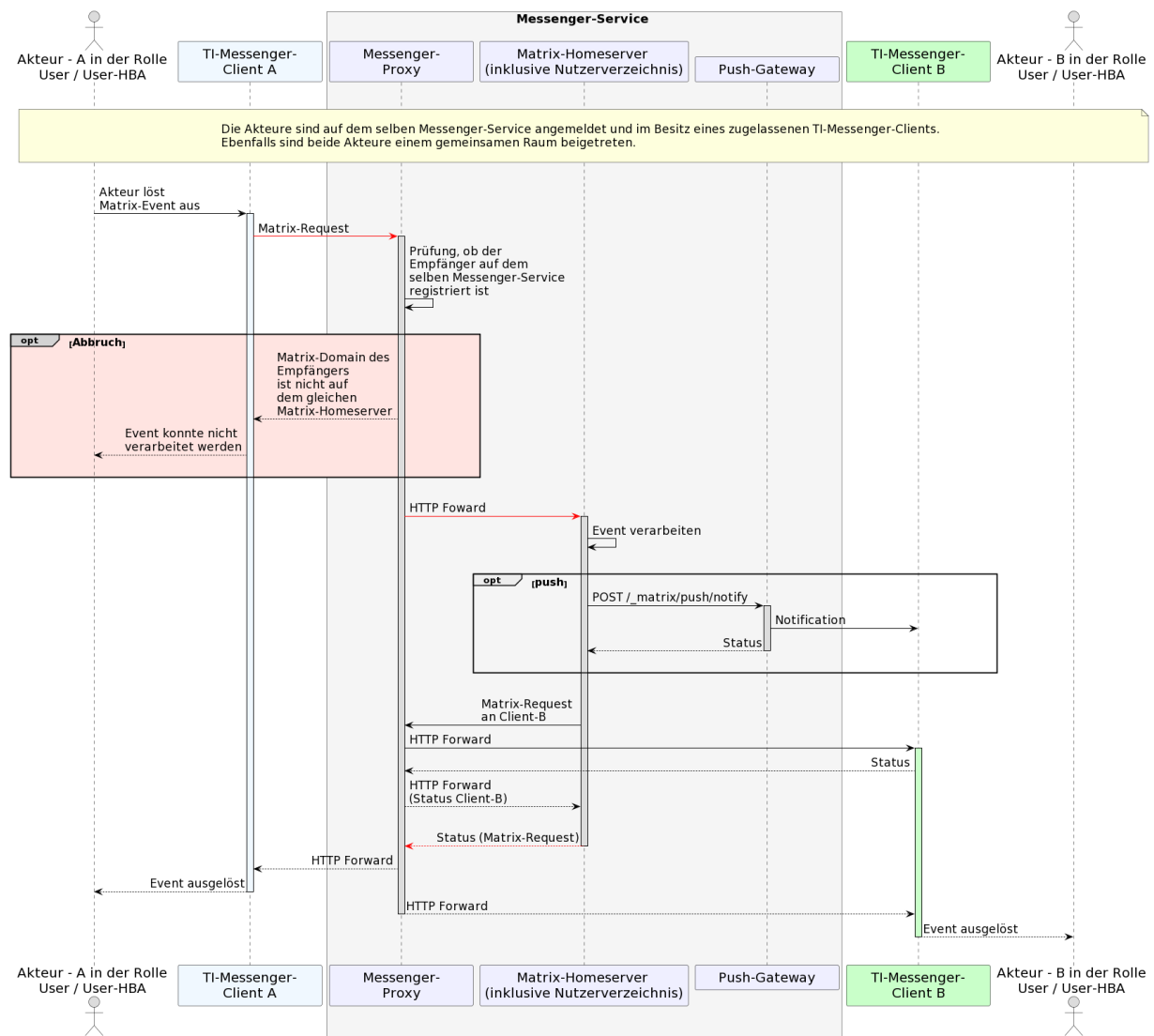


Abbildung 13: Laufzeitsicht - Austausch von Events innerhalb eines Messenger-Service

[&lt;= ]

### Akzeptanzkriterien für den Anwendungsfall: Austausch von Events innerhalb eines Messenger-Service (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.

[&lt;= ]

#### 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.






[&lt;= ]

## 6.9 AF - Einladung von Akteuren anderer Messenger-Services

### AF\_10061 - Einladung von Akteuren anderer Messenger-Services

In diesem Anwendungsfall wird ein Akteur eines anderen Messenger-Service innerhalb der TI-Messenger-Föderation eingeladen. Für die Suche von Akteuren auf anderen Messenger-Services KANN das VZD-FHIR-Directory verwendet werden. Das hierbei für die Einladung benötigte PASSporT wird in diesem Fall vom VZD-FHIR-Directory bereitgestellt. Weiterhin ist es möglich sich ein PASSporT vom Messenger-Service des einzuladenden Akteurs ausstellen zu lassen. Im Gegensatz zu einer Einladung von Akteuren auf einen gemeinsamen Messenger-Service (siehe AF\_10063), prüft in diesem Anwendungsfall der Messenger-Proxy das Vorhandensein eines PASSporT.

Tabelle 11 AF - Einladung von Akteuren anderer Messenger-Services

AF_10061	Einladung von Akteuren anderer Messenger-Services
Akteur	Leistungserbringer, Mitarbeiter einer Organisation im Gesundheitswesen in der Rolle User / User-HBA
Auslöser	Akteur A möchte mit Akteur B eines anderen Messenger-Service einen gemeinsamen Chatraum einrichten.
Komponenten	TI-Messenger Client A + B, Messenger-Proxy A + B, Matrix-Homeserver A + B, VZD-FHIR-Directory, PASSporT-Service B, Push-Gateway B
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 (siehe AF_10057)</li> <li>4. Die verwendeten Messenger-Services sind Bestandteile der TI-Messenger-Föderation.</li> </ol>
Eingangsdaten	Matrix Invite-Request
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	keine
Akzeptanzkriterien	 ML-123654 ,  ML-123659 ,  ML-123660 ,  ML-123661 ,  ML-123663

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 in dem Anwendungsfall "AF\_10064 - Föderationszugehörigkeit eines Messenger-Service prüfen" hinreichend beschrieben.

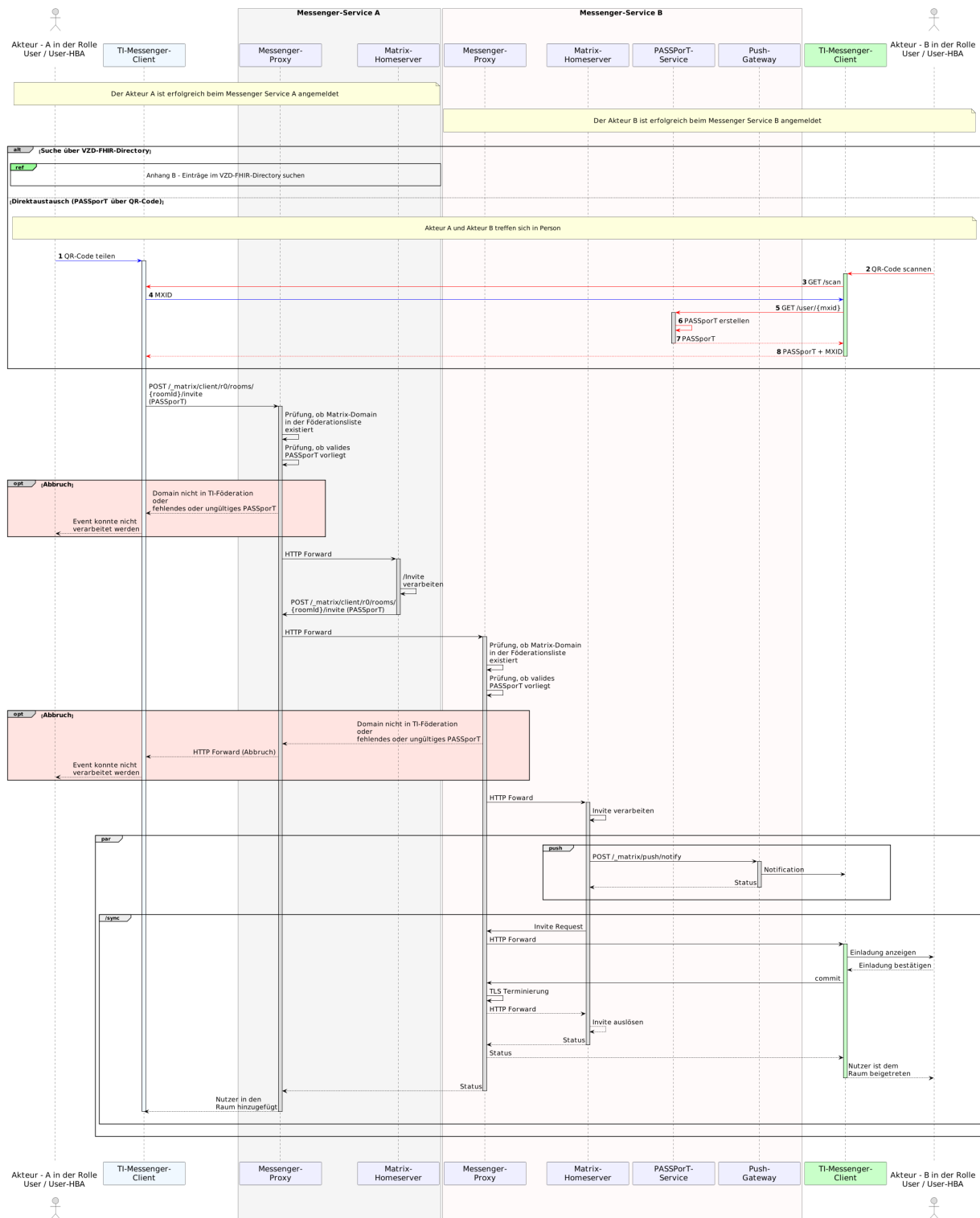


Abbildung 14: Laufzeitsicht - Einladung von Akteuren anderer Messenger-Services

[&lt;=]

## Akzeptanzkriterien für den Anwendungsfall: Einladung von Akteuren anderer Messenger-Services (AF\_10061)

### ML-123654 - AF\_10061 - Suche im VZD-FHIR-Directory

Ein Messenger-Client kann erfolgreich im VZD-FHIR-Directory nach einem Chatpartner suchen.

## Mainline

[&lt;= ]

**ML-123659 - AF\_10061 - PASSporT Übergabe**

PASSporT wurde erfolgreich an den Messenger-Proxy übergeben, enthält alle benötigten Informationen und ist auswertbar.

[&lt;= ]

**ML-123660 - AF\_10061 - Invite nur mit PASSporT**

Im Invite Request steht das PASSporT an der richtigen Stelle und kann vom Messenger-Proxy ausgewertet werden.

[&lt;= ]

Ein Beispiel für einen Invite-Request ist im Dokument [gemSpec\_TI-Messenger-FD] im Kapitel "*Messenger Proxy*" zu finden.

**ML-123661 - AF\_10061 - Messenger-Proxy prüft PASSporT auf Gültigkeit**

Der Messenger-Proxy lehnt das Invite bei ungültigem PASSporT ab.

[&lt;= ]

**ML-123663 - AF\_10061 - Akteure sind dem Chatraum beigetreten**

Alle Chat Parteien sind erfolgreich im Chatraum vorhanden.

[&lt;= ]

**6.10 AF - Austausch von Events zwischen anderen Messenger-Services****AF\_10062 - Austausch von Events zwischen anderen Messenger-Services**

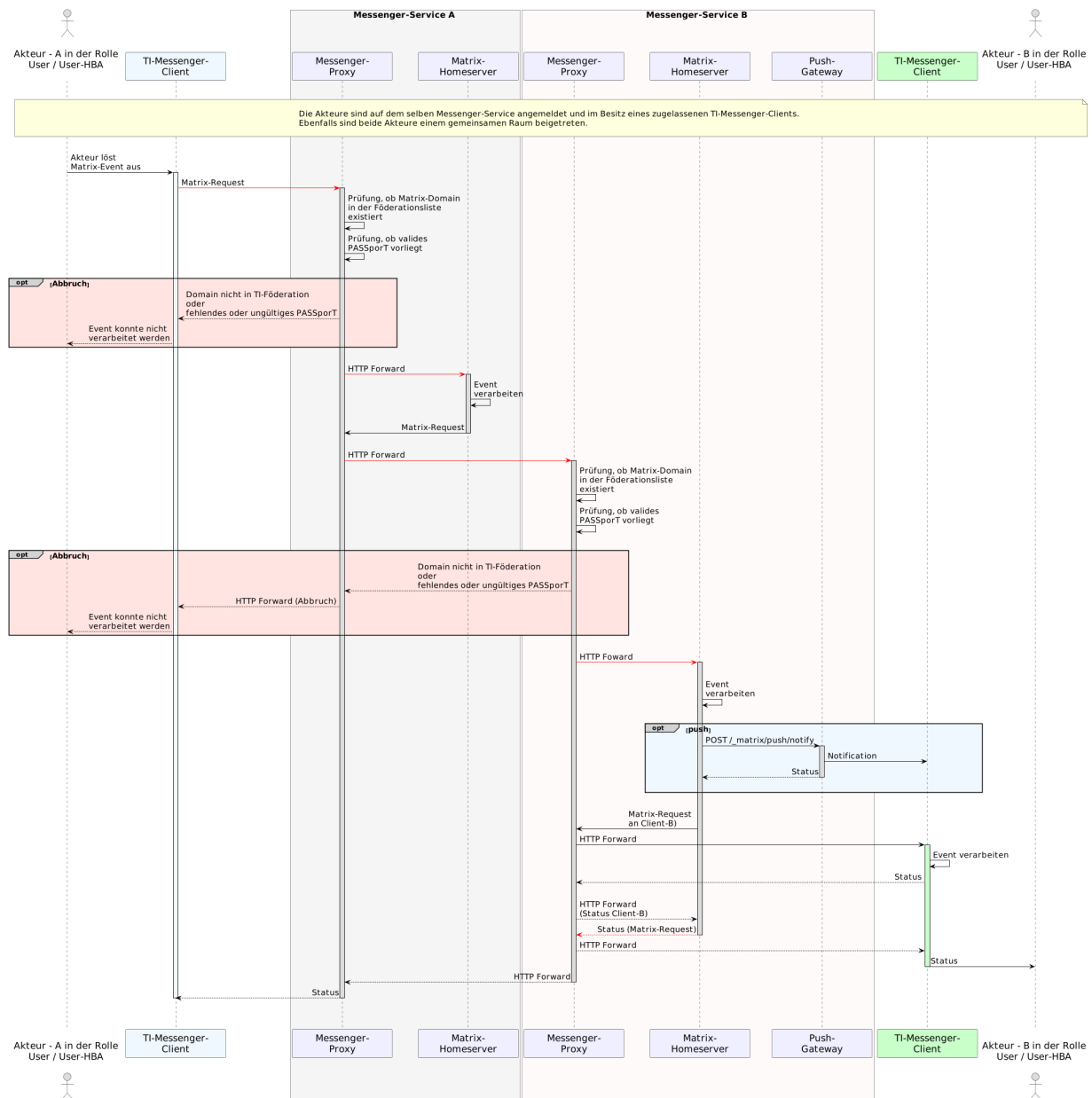
In diesem Anwendungsfall können Akteure welche sich in einem gemeinsamen Raum befinden Nachrichten austauschen und andere durch die Matrix-Spezifikation festgelegte Aktionen ausführen. Dieser Anwendungsfall setzt ein erfolgreiches Matrix Invite-Request eines oder mehrerer beteiligter Akteure voraus. In diesem Anwendungsfall sind die beteiligten Akteure in einem gemeinsamen Chatraum und auf unterschiedlichen Messenger-Services verteilt. Die in der Abbildung rot dargestellten Linien symbolisieren den Kommunikationsverlauf des auslösenden Matrix-Request.

Tabelle 12 AF - Austausch von Events zwischen anderen Messenger-Services

AF_10062	Austausch von Events zwischen anderen Messenger-Services
Akteur	Leistungserbringer, Mitarbeiter einer Organisation im Gesundheitswesen in der Rolle User / User-HBA
Auslöser	Alle Events die zwischen Messenger-Services ausgeführt werden.
Komponenten	TI-Messenger-Client A + B, Messenger-Proxy A + B, Matrix-Homeserver A + B, Push-Gateway B
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> <li>3. Die Messenger-Proxys überprüfen die Zugehörigkeit der beteiligten Messenger-Services (siehe AF_10064)</li> </ol>
Eingangsdaten	Matrix-Event
Ergebnis	Matrix-Event wurde erfolgreich verarbeitet
Ausgangsdaten	Abhängig vom Matrix-Event
Akzeptanzkriterien	 <a href="#">ML-123665</a> ,  <a href="#">ML-123666</a> ,  <a href="#">ML-123667</a> ,  <a href="#">ML-123668</a>

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 AF\_10064 - Föderationszugehörigkeit eines Messenger-Service prüfen verwiesen.

## Mainline



[&lt;= ]

### Akzeptanzkriterien für den Anwendungsfall: Austausch von Nachrichten zwischen Messenger-Services (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.

[&lt;= ]

#### 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.

[&lt;= ]

#### ML-123667 - AF\_10062 - Auslösen einer Notifikation

Der Matrix-Homeserver des Empfängers löst eine Benachrichtigung des Messenger-Clients über sein Push-Gateway aus.

[&lt;= ]

**ML-123668 - AF\_10062 - Nachricht wird angezeigt**

Die Nachricht wird dem Empfänger im gemeinsamen Raum angezeigt.

[&lt;= ]

**7 Anhang A – Verzeichnisse****7.1 Abkürzungen**

Kürzel	Erläuterung
AD	Active Directory
AF	Anwendungsfall
APN	Apple Push Notification Service
AuthZ	Authorization
BSI	Bundesamt für Sicherheit in der Informationstechnik
FCM	Firebase Cloud Messaging
FHIR	Fast Healthcare Interoperable Resources
HBA	Heilberufsausweis
HTTP	Hypertext Transfer Protocol
IDP-Dienst	Identity Provider
JSON	JavaScript Object Notation
JWT	JSON Web Token
KV	Kassenärztliche Vereinigung
LDAP	Lightweight Directory Access Protocol
LE	Leistungserbringer
MSC	Matrix Spec Change
OAuth	Open Authorization
OIDC	OpenID Connect
PASSporT	Personal Assertion Token
REST	Representational State Transfer
SMC-B	Institutionenkarte (Security Module Card Typ B)
SSO	Single Sign-on
TI	Telematikinfrastruktur
UIA	User Interactive Authorization Flow
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)

Abbildung 2 Benachbarten Produkttypen des TI-Messenger-Dienstes

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

Abbildung 4 : Org-Admin - Übersicht Anwendungsfälle

Abbildung 5 : User / User HBA - Übersicht Anwendungsfälle

Abbildung 6 Laufzeitsicht - Authentisieren einer Organisation am TI-Messenger-Dienst

Abbildung 7: Laufzeitsicht - Bereitstellung eines Messenger-Service für eine Organisation

Abbildung 8: Laufzeitsicht - Organisationsressourcen im Verzeichnisdienst hinzufügen

Abbildung 9: Laufzeitsicht - Anmeldung eines Akteurs am Messenger-Service

Abbildung 10: Laufzeitsicht - Akteur (User-HBA) im Verzeichnisdienst hinzufügen

Abbildung 11: Laufzeitsicht - Föderationszugehörigkeit eines Messenger-Service prüfen

Abbildung 12 Einladung von Akteuren innerhalb eines Messenger-Service

Abbildung 13: Laufzeitsicht - Austausch von Events innerhalb eines Messenger-Service

Abbildung 14: Laufzeitsicht - Einladung von Akteuren anderer Messenger-Services

Abbildung 15: Laufzeitsicht - Austausch von Events zwischen anderen Messenger-Services

## 7.4 Tabellenverzeichnis

Tabelle 1: Akteure und Rollen

Tabelle 2: Kommunikationsmatrix

Tabelle 3 Tabelle : AF - Authentisieren einer Organisation am TI-Messenger-Dienst

Tabelle 4: AF - Bereitstellung eines Messenger-Service für eine Organisation

Tabelle 5 AF - Organisationsressourcen im Verzeichnisdienst hinzufügen

Tabelle 6: AF - Anmeldung eines Akteurs am Messenger-Service

Tabelle 7: AF - Akteur (User-HBA) im Verzeichnisdienst hinzufügen

Tabelle 8 Föderationszugehörigkeit eines Messenger-Service prüfen

Tabelle 9 Einladung von Akteuren innerhalb eines Messenger-Service

Tabelle 10 Austausch von Events innerhalb eines Messenger-Service

Tabelle 11 AF - Einladung von Akteuren anderer Messenger-Services

Tabelle 12 AF - Austausch von Events zwischen anderen Messenger-Services

## 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-vzd]	gematik: <a href="https://github.com/gematik/api-vzd">https://github.com/gematik/api-vzd</a>
[gemKPT_TI_Messenger]	gematik: Konzeptpapier TI-Messenger
[gemKPT_Betr]	gematik: Betriebskonzept Online-Produktivbetrieb
[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

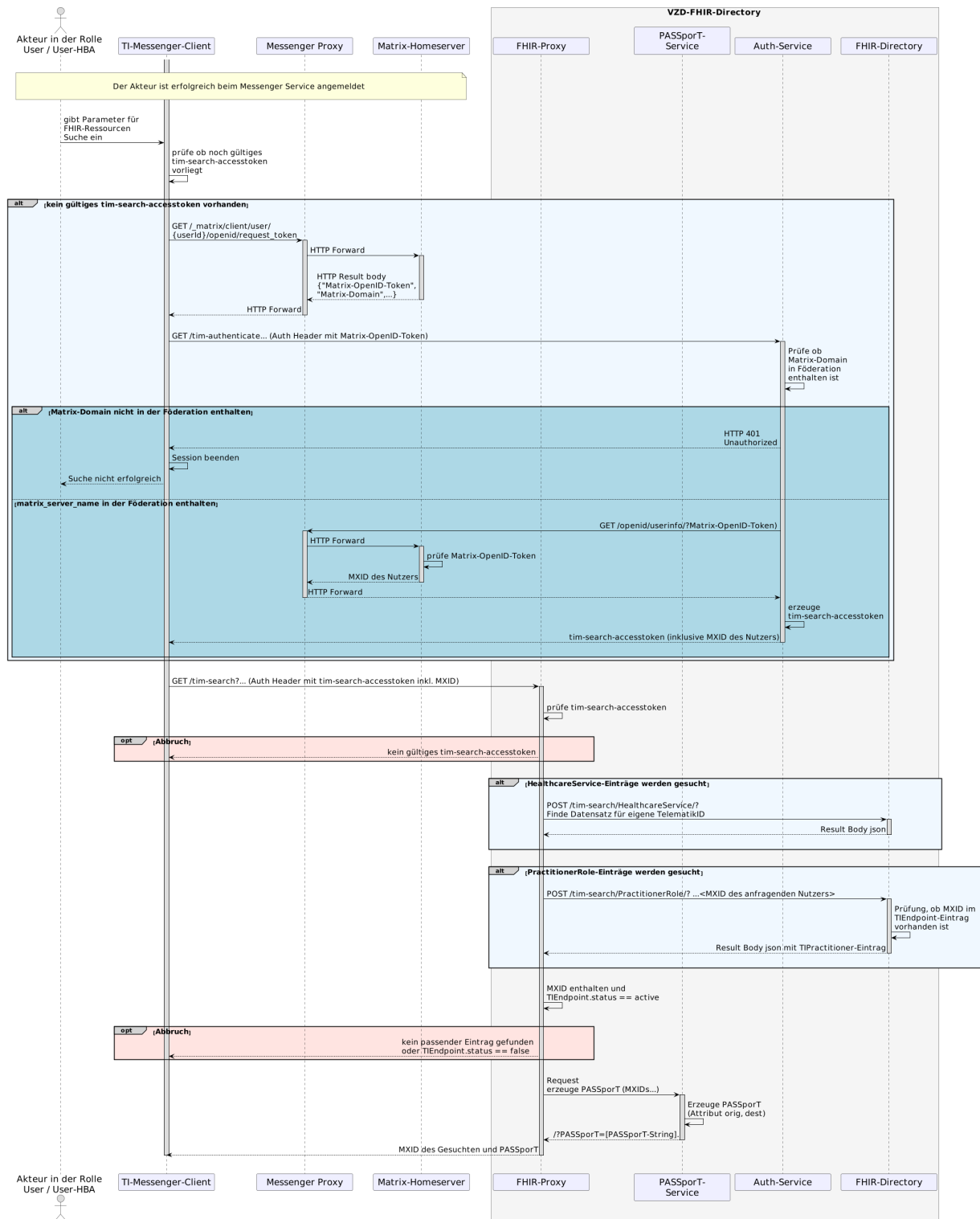
### 7.5.2 Weitere Dokumente

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[Client-Server API]	Matrix Foundation: Matrix Specification - Client-Server API <a href="https://spec.matrix.org/v1.2/client-server-api/">https://spec.matrix.org/v1.2/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>
[Matrix Specification]	Matrix Foundation: Matrix Specification <a href="https://spec.matrix.org/v1.2/">https://spec.matrix.org/v1.2/</a>
[MSC]	Matrix Foundation: Matrix Specification - Spec Change Proposals <a href="https://spec.matrix.org/v1.2/proposals/">https://spec.matrix.org/v1.2/proposals/</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/v1.2/push-gateway-api/">https://spec.matrix.org/v1.2/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/v1.2/server-server-api/">https://spec.matrix.org/v1.2/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.



## 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-Fachdienst anfragen. Hierbei sollte die Anfrage einer neuer Liste nicht zu selten passieren (mindestens einmal am Tag). Hierbei überprüft der Registrierungs-Dienst die Aktualität der Version seiner Föderationsliste beim FHIR-Proxy des VZD-FHIR-Directory. 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. Die Struktur dieser Föderationsliste ist in [gemSpec\_VZD\_FHIR\_Directory] beschrieben.

