**Elektronische Gesundheitskarte und Telematikinfrastruktur**

# Spezifikation
# TI-Messenger-Dienst

| | |
|---|---|
| Version: | 1.0.0 |
| Revision: | 408178 |
| Stand: | 01.10.2021 |
| Status: | freigegeben |
| Klassifizierung: | öffentlich |
| Referenzierung: | gemSpec_TI-Messenger-Dienst |

# Dokumentinformationen

### Änderungen zur Vorversion

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

### Dokumentenhistorie

| **Version** | Stand | Kap./ Seite | Grund der Änderung, besondere Hinweise | Bearbeitung |
|---|---|---|---|---|
| 1.0.0 | 01.10.2021 | | Erstversion des Dokumentes | gematik |
| | | | | |
| | | | | |

# Inhaltsverzeichnis

# 1 Einordnung des Dokumentes

## 1.1 Zielsetzung

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

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 Schutzrechtsinhabern einzuholen. Die gematik GmbH übernimmt insofern keinerlei Gewährleistungen.*

## 1.4 Abgrenzungen

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

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

Die vollständige Anforderungslage für den TI-Messenger-Dienst ergibt sich aus mehreren Spezifikationsdokumenten. Diese sind in den einzelnen Produkt- und Anbietertypsteckbriefen des TI-Messengers verzeichnet.

## 1.5 Methodik

Die Spezifikation ist im Stil einer RFC-Spezifikation verfasst. Dies bedeutet:

- **Der gesamte Text in der Spezifikation ist sowohl für den Hersteller des Produktes TI-Messenger-Dienst als auch für den betreibenden Anbieter entsprechend [gemKPT_Betr] verbindlich zu betrachten und gilt als Zulassungskriterium beim Produkt und Anbieter.**
- Die Verbindlichkeit SOLL durch die dem RFC 2119 [RFC2119] entsprechenden, in Großbuchstaben geschriebenen deutschen Schlüsselworte MUSS, DARF NICHT, SOLL, SOLL NICHT, KANN gekennzeichnet werden.
- Da in dem Beispielsatz „Eine leere Liste DARF NICHT ein Element besitzen.“ die Phrase „DARF NICHT“ semantisch irreführend wäre (wenn nicht ein, dann vielleicht zwei?), wird in diesem Dokument stattdessen „Eine leere Liste DARF KEIN Element besitzen.“ verwendet.
- Die Schlüsselworte KÖNNEN außerdem um Pronomen in Großbuchstaben ergänzt werden, wenn dies den Sprachfluss verbessert oder die Semantik verdeutlicht.

Anwendungsfälle und Akzeptanzkriterien als Ausdruck normativer Festlegungen werden als Grundlage für Erlangung der Zulassung durch Tests geprüft und nachgewiesen. Sie besitzen eine eindeutige, permanente ID, welche als Referenz verwendet werden SOLL. Die Tests werden gegen eine von der gematik gestellte Referenz-Implementierung durchgeführt.

Anwendungsfälle und Akzeptanzkriterien werden im Dokument wie folgt dargestellt:
**<ID> - <Titel des Anwendungsfalles / Akzeptanzkriteriums>**

Text / Beschreibung
[<=]

Die einzelnen Elemente beschreiben:

- **ID**: einen eindeutigen Identifier.
  - Bei einem Anwendungsfall besteht der Identifier aus der Zeichenfolge 'AF_' gefolgt von einer Zahl,
  - Der Identifier eines Akzeptanzkriterium wird von System vergeben, z.B. die Zeichenfolge 'ML_' gefolgt von einer Zahl
- **Titel des Anwendungsfalles / Akzeptanzkriteriums**: Ein Titel, welcher zusammenfassend den Inhalt beschreibt
- **Text / Beschreibung**: Ausführliche Beschreibung des Inhalts. Kann neben Text Tabellen, Abbildungen und Modelle enthalten

Dabei umfasst der Anwendungsfall bzw. das Akzeptanzkriterium sämtliche zwischen ID und Textmarke [<=] angeführten Inhalte.

Der für die Erlangung einer Zulassung notwendige Nachweis der Erfüllung des Anwendungsfalls wird in den jeweiligen Steckbriefen festgelegt, in denen jeweils der Anwendungsfall gelistet ist. Akzeptanzkriterien werden in der Regel nicht im Steckbrief gelistet.

**Hinweis auf offene Punkte**

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

# 2 Systemüberblick

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

Messenger-Services werden immer für eine Organisation des Gesundheitswesens bereitgestellt und unterscheiden sich lediglich in der Art des verwendeten Authentifizierungsverfahrens. Dies ermöglicht eine nahtlose Integration in den Alltag, da bestehende sichere Authentifizierungsverfahren nachgenutzt werden können. Nutzer, 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. Nutzer die zugehörig zu einer Organisation agieren, KÖNNEN den durch diese Organisation bereitgestellten Messenger-Service nutzen und die innerhalb dieser Organisation verwendeten Authentifizierungsmethoden verwenden. Es ist für Nutzer möglich verschiedene TI-Messenger-Clients unterschiedlicher Organisationen zu nutzen (Beispiel: Ärztin ist in einer Klinik und in einer niedergelassenen Praxis tätig und bekommt von beiden Organisationen einen TI-Messenger-Service zur Verfügung gestellt). Messenger-Services werden durch TI-Messenger-Anbieter dezentral für Organisationen (SMC-B Inhaber) bereitgestellt, die über das Matrix-Protokoll Nachrichten austauschen.

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 in dem 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 Nutzern 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:

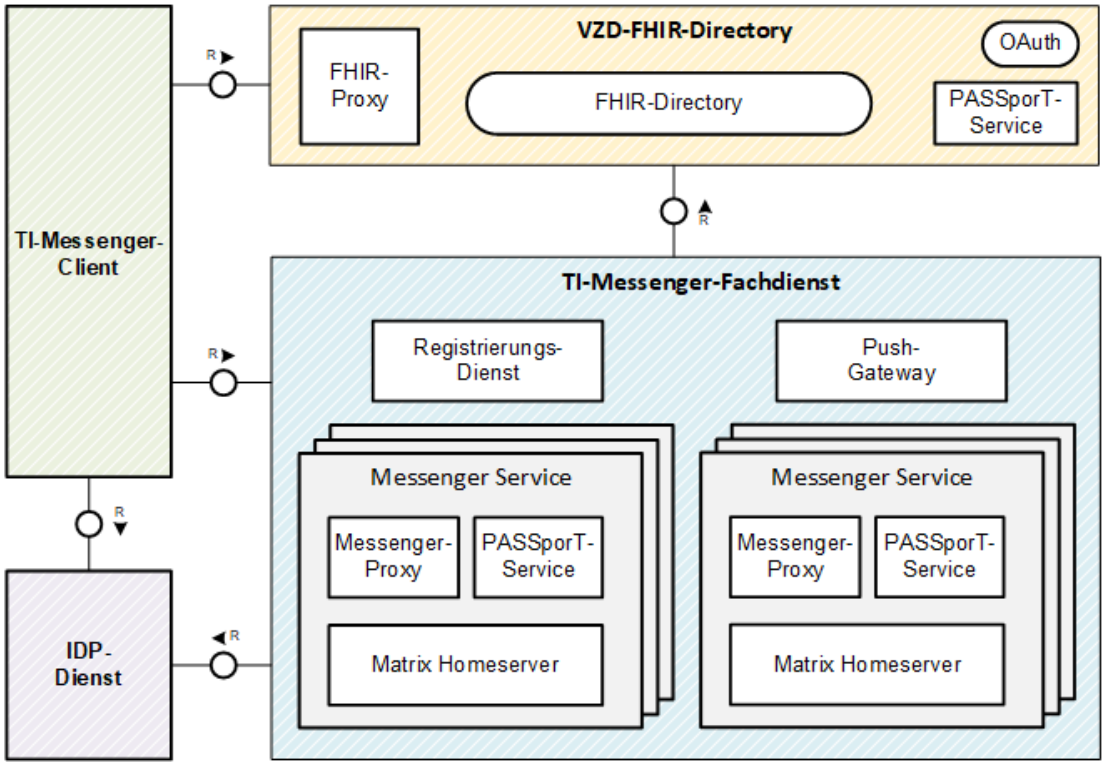


**Abbildung 1: Komponenten der TI-Messenger-Architektur (vereinfachte Darstellung)**

Der TI-Messenger-Dienst basiert auf dem offenen Kommunikationsprotokoll Matrix, das bereits von der Matrix Foundation gemäß [Matrix Foundation] 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 Sicherstellung der föderalen und dezentralen Struktur des TI-Messenger-Dienstes und zur Kontrolle des Nutzerkreises werden weitere Komponenten benötigt, welche in der jeweiligen 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 (z. B. Zahnärzte, Apotheker, psychologische Psychotherapeuten) | User-HBA | Ein LE im Besitz eines HBAs kann<br>• sich am Smartcard-IDP authentisieren<br>• sich am Messenger-Service anmelden<br>• seine MXID auf dem VZD-FHIR Server hinterlegen und sich damit sektorübergreifend erreichbar machen<br>• den TI-Messenger-Dienst nutzen<br>  • Kommunikationen innerhalb seiner Organisation aufbauen und entgegennehmen<br>  • Kommunikationen mit anderen Organisationen aufbauen<br>  • Kommunikationen mit LEs aufbauen und entgegennehmen, die ebenfalls mit HBA authentisiert und somit für ihn auf dem VZD-FHIR-Server auffindbar sind<br>  • *Direct Messaging [Direct Messaging] mit allen Teilnehmern der TI-Messenger-Dienste<br>  • **Group Messaging [Group Messaging] mit allen Teilnehmern der TI-Messenger-Dienste<br>• im Namen der Organisation Kommunikation empfangen |

| | | |
|---|---|---|
| | Org-Admin | Ein LE im Besitz eines HBAs und einer SMC-B kann<br>• sich am Smartcard-IDP authentisieren<br>• einen Messenger-Service für seine Organisation (korrespondierend zu seiner SMC-B) anlegen<br>• seine Organisation auf dem VZD-FHIR Server administrieren und damit sektorübergreifend erreichbar machen<br>• die User dieses Messenger-Services administrieren<br>• Homeserver-Konfigurationen vornehmen |
| Mitarbeiter einer Organisation im Gesundheitswesen (z. B. Pflegepersonal, Hebammen, Arzt im Krankenhaus, Mitarbeiter einer Kasse ) | User | Ein Mitarbeiter einer Organisation im Gesundheitswesen kann<br>• sich gegenüber dem Messenger-Service authentisieren<br>• sich am Messenger-Service anmelden<br>• den TI-Messenger-Dienst nutzen<br>  • Kommunikationen innerhalb seiner Organisation aufbauen und entgegennehmen<br>  • Kommunikationen mit anderen Organisationen aufbauen<br>  • Direct Messaging [Direct Messaging] mit allen Teilnehmern der TI-Messenger-Dienste<br>  • Group Messaging [Group Messaging] mit allen Teilnehmern der TI-Messenger-Dienste<br>• im Namen der Organisation Kommunikation empfangen |
| | Org-Admin | Ein Mitarbeiter einer Organisation im Gesundheitswesen mit Zugriff auf eine SMC-B<br>• sich am Smartcard-IDP authentisieren |

| | | |
|---|---|---|
| | | • einen Messenger-Service für seine Organisation (korrespondierend zu seiner SMC-B) anlegen<br>• seine Organisation auf dem VZD-FHIR Server administrieren und damit sektorübergreifend erreichbar machen<br>• die User dieses Messenger-Services administrieren<br>• Homeserver-Konfigurationen vornehmen |
| TI-Messenger-Anbieter | Org-Admin | Ein TI-Messenger-Anbieter kann, auf Wunsch des LEs im Besitz einer SMC-B<br>• einen Messenger-Service für die Organisation (korrespondierend zur SMC-B des LEs) anlegen<br>• diese Organisation auf dem VZD-FHIR Server administrieren und damit sektorübergreifend erreichbar machen<br>• die User dieses Messenger-Services administrieren<br>• Homeserver-Konfigurationen für LEs vornehmen |

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

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

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

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

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

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

Mitarbeiter einer Organisation im Gesundheitswesen in der Rolle *User* KÖNNEN zunächst nur Akteuren schreiben, die ihrer Organisation zugeordnet sind. Um mit Mitarbeitern

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

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

Versicherte DÜRFEN aktuell NICHT als Nutzer auf einem Messenger-Service eingetragen werden. Für die Nutzung eines Messenger-Service sind nur Nutzer zugelassen die durch ein bestehendes Vertragsverhältnis mit der jeweiligen Organisation zugeordnet werden können. Ein Nutzer-Account MUSS einer juristischen Person eindeutig zugeordnet sein. Das Teilen von Passwörtern oder Zugangsdaten für die gleichzeitige Nutzung eines Accounts ist nicht erlaubt.

## 3.2 Nachbarsysteme

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

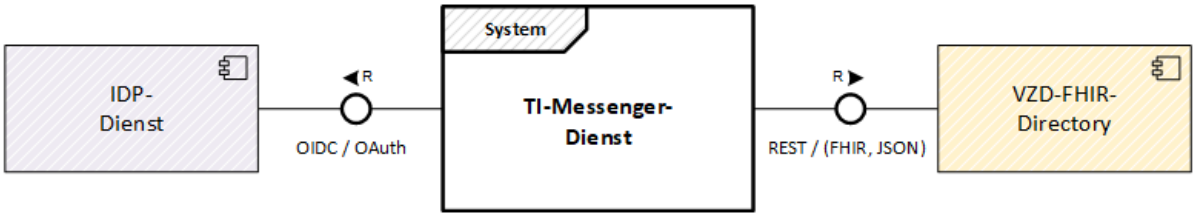


**Abbildung 2: Benachbarten Produkttypen des TI-Messenger-Dienstes**

Der TI-Messenger-Dienst nutzt die Schnittstellen vom Smartcard IDP-Dienst der gematik zur Authentifizierung von Akteuren sowie Schnittstellen des gesondert spezifizierten VZD-FHIR-Directory um z. B. Nutzer und deren MXIDs 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 Föderation mit anderen Messenger-Services als Teil des TI-Messenger-Dienstes erfolgt. Bei diesen zusätzlichen Komponenten handelt es sich jeweils um einen Messenger-Proxy und einen PASSporT-Service. Die Messenger-Services KÖNNEN den Nutzern aufgrund der Vielzahl an verschiedenen Akteuren unterschiedliche Authentifizierungsverfahren anbieten, bei denen der Besitz einer SMC-B oder eines HBA nicht vorausgesetzt werden kann. Messenger-

Services MÜSSEN immer Organisationen zugeordnet werden, die über die Kontrolle der verbundenen Authentifizierungsverfahren verfügen.

Abhängig vom jeweiligen Messenger-Service gibt es verschiedene Abläufe bei der Anmeldung an einem TI-Messenger-Fachdienst. Dabei können diverse Authentifizierungsmechanismen durch eine Organisation für Ihre Nutzer bereitgestellt werden. Die Organisation und der von ihr gewählte TI-Messenger-Anbieter vereinbaren den Authentifizierungsmechanismus 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 Nutzerlöschung oder Sperrung sicherzustellen.

Zum besseren Verständnis werden im Folgenden vier Anwendungsbeispiele dargestellt:

### 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 einen 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 Nutzer einer Arztpraxis (z. B. MFA, Ärzte). Die angelegten Nutzer melden sich am Messenger-Service an und können den TI-Messenger in der Roller *User* direkt nutzen.

Die Arztpraxis wird als Organisation für Nutzer anderer Organisationen des TI-Messenger-Dienstes erreichbar. Dazu KANN ein Akteur in der Rolle Org-Admin Kontaktpunkte auf dem VZD-FHIR-Directory einrichten. Nutzer der Arztpraxis im Besitz eines HBAs KÖNNEN zusätzlich im TI-Messenger-Client mittels HBA authentisieren und so die eigene MXID als Practitioner-Eintrag auf dem VZD-FHIR-Directory hinterlegen. Damit können die Nutzer andere hinterlegte HBA-Inhaber per Direct/Group-Messaging erreichen, oder für diese erreichbar werden

### Anwendungsbeispiel Krankenhaus

Ein Krankenhaus registriert sich mittels SMC-B bei einem 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 Nutzer 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 Nutzer des TI-Messenger-Dienstes erreichbar. Dazu KANN ein Akteur in der Rolle Org-Admin Kontaktpunkte auf dem VZD-FHIR-Directory einrichten. Nutzer des Krankenhauses im Besitz eines HBAs KÖNNEN zusätzlich mittels des TI-Messenger-Clients die eigene MXID als Practitioner-Eintrag auf dem VZD-FHIR-Directory hinterlegen (Rolle = *User-HBA*). Damit können die Nutzer andere hinterlegte HBA-Inhaber per Direct/Group-Messaging erreichen, oder für diese erreichbar werden.

### Anwendungsbeispiel Apotheke

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 Nutzer 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 Nutzer des TI-Messengers erreichbar, indem ein Akteur in der Rolle *Org-Admin* Kontaktpunkte auf dem VZD-FHIR-Directory einrichtet. Nutzer der Apotheke im Besitz eines HBAs 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 hinterlegte HBA-Inhaber per Direct-Messaging zu erreichen oder für diese erreichbar zu werden.

### Anwendungsbeispiel Verbände

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

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

Im Folgenden wird noch einmal 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 | • Start der Kommunikation mit anderen Organisationen<br>• Start der Kommunikation mit Nutzern in der Rolle *User* und *User-HBA* innerhalb einer Organisation<br>• Start der Kommunikation mit Nutzern in der Rolle *User* und *User-HBA* anderer Messenger-Services durch Scan eines QR-Codes | • Kommunikationsanfragen durch Nutzer in der Rolle *User* und *User-HBA* innerhalb einer Organisation<br>• Kommunikationsanfragen durch Nutzer in der Rolle *User* und *User-HBA* anderer Messenger-Services durch Scan eines QR-Codes<br>• Kommunikationsanfragen durch Nutzer in der Rolle *User* und *User-HBA* anderer Messenger-Services als Ansprechpartner der Organisation. Die MXID wurde |

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

## 3.4 Nutzung von Personal Assertion Token (PASSporT)

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

PASSporT durch den Messenger-Server erfolgt analog zum PASSporT-Service des VZD-FHIR-Directory.

## 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. Es existieren die folgenden für eine Authentisierung benötigten Token:

- ID_TOKEN und ACCESS_TOKEN ausgestellt vom Smartcard IDP-Dienst
- Matrix-ACCESS_TOKEN ausgestellt von den Matrix-Homeservern
- Matrix-OpenID-Token ausgestellt vom Matrix-Homeserver

### ID_TOKEN (Smartcard IDP-Dienst)

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

### ACCESS_TOKEN (Smartcard IDP-Dienst)

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

### Matrix-ACCESS_TOKEN (Matrix-Homeserver)

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

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

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

# 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:

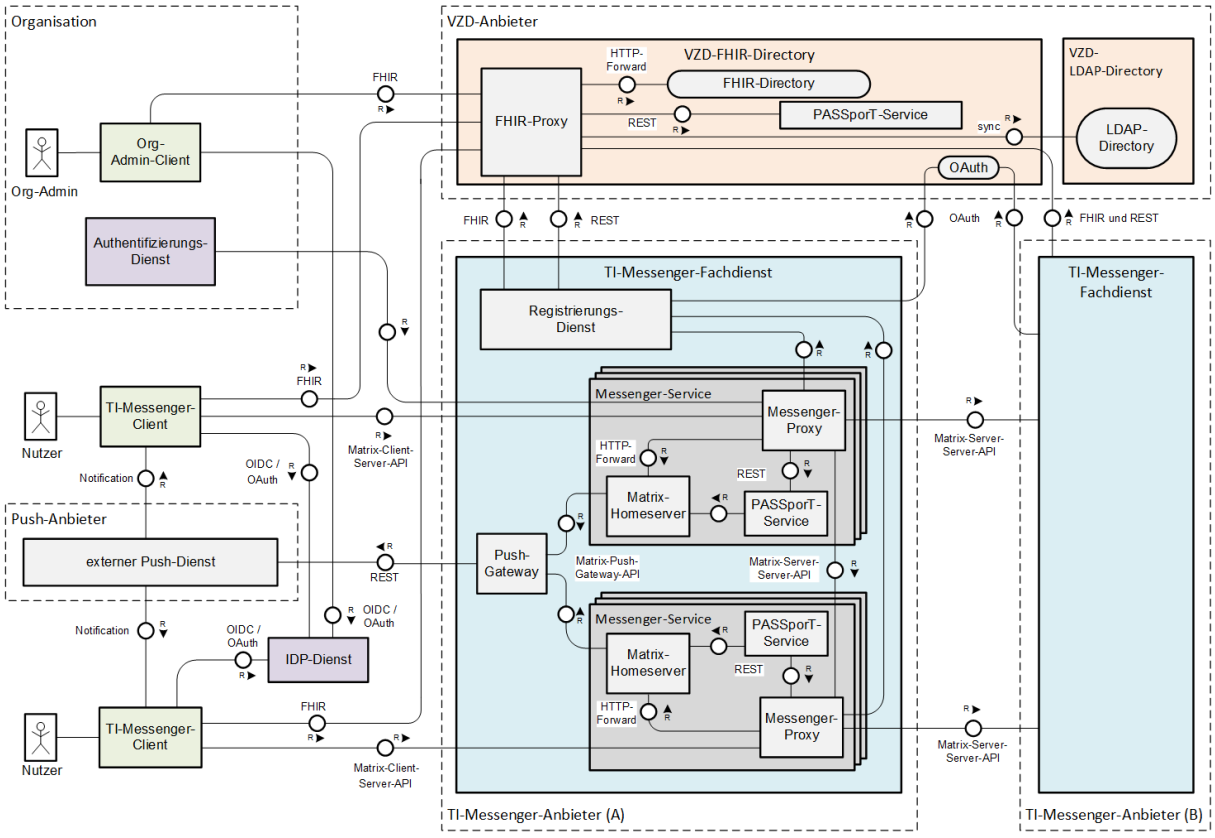


**Abbildung 3: Komponenten der TI-Messenger-Architektur und deren Schnittstellen**

## 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 Nutzer jederzeit identifizieren kann und das die Organisationen Nutzer jederzeit aus dem TI-Messenger-Dienst ausschließen können. Daher MUSS die Kontrolle über die Identitäten

bei der Organisation liegen. Hierbei ist eine Delegierung, z.B. an einen Dienstleister zulässig. Jeder Anbieter, der einen TI-Messenger-Fachdienst bereitstellt, MUSS einen Registrierungs-Dienst, ein Push-Gateway sowie einen oder mehrere Messenger-Services betreiben. Im Folgenden werden die einzelnen Komponenten weiter beschrieben.

### 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 den durch den Smartcard IDP-Dienst ausgestellten ACCESS_TOKEN und ID_TOKEN validieren und einen dezentralen Messenger-Service starten. Dazu MUSS das Frontend des Registrierungs-Dienstes am 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-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 Nutzern den Eingang neuer Nachrichten zu signalisieren. Das Push-Gateway ist gemäß der Matrix-Foundation-Spezifikation [Matrix-PushGW] 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 gemäß der Spezifikation der Matrix Foundation. 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 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. Durch eine Anfrage bei jedem `Transaction-Event` an den Registrierungs-Dienst erfolgt die Prüfung auf Zugehörigkeit zur TI-Messenger Föderation. Die Komponente Messenger-Proxy MUSS für jeden Messenger-Service separat bereitgestellt werden.

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

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

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

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

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

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

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

## 4.2 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 ermöglicht die Ad-hoc-Kommunikation

im TI-Messenger-Dienst. Die Akteure KÖNNEN über entsprechende Suchanfragen im VZD-FHIR-Directory durch den TI-Messenger-Client gesucht werden. Der TI-Messenger-Client basiert auf der von der Matrix-Foundation definierten Spezifikation.

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

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

## 4.3 VZD-FHIR-Directory

Beim VZD-FHIR-Directory handelt es sich um einen zentralen Verzeichnisdient, der die deutschlandweite Nutzersuche des TI-Messenger-Dienstes ermöglicht. Das VZD-FHIR-Directory basiert auf dem FHIR-Standard zum Austausch 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.

### 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 Kommunikationsablauf für den Zugriff auf das VZD-FHIR-Directory durch den TI-Messenger-Client ist in [gemSpec_VZD_FHIR_Directory#6.2] beschrieben.

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

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

### OAuth

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

# 5 Übergreifende Festlegungen

## 5.1 Datenschutz und Sicherheit

Der TI-Messenger 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 gemäß [Matrix Foundation] verwendet. Im Rahmen der Spezifikation wird daher das Server-Server- und das Client-Server-Protokoll gemäß [Matrix Foundation] nachgenutzt. Für die Kommunikation der Matrix-Homeserver in der Föderation wird somit die API gemäß Matrix-Server-Server-Protokoll verwendet. Der TI-Messenger-Client setzt bei der Kommunikation mit den TI-Messenger-Matrix-Homeservern die API des Matrix-Client-Server-Protokolls um. 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 ein ID- und ACCESS_TOKEN für Nutzer in Form eines JSON-Web-Token (JWT) gemäß [OpenID] aus.

### FHIR

Der TI-Messenger-Client nutzt die Schnittstellen des VZD-FHIR-Directorys gemäß dem FHIR-Standard [FHIR] mit einer RESTful API.

### PASSporT

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

## 5.3 Authentifizierung und Autorisierung

### 5.3.1 Authentifizierung von Nutzern

Für die Authentifizierung von Nutzern, also 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 eigene 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 (*I*n 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 Schreibzugriff der Nutzer 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 Leistungserbringer oder Akteur in der Rolle *Org-Admin* KANN mittels des ACCESS_TOKEN die MXID als `Telecom` Eintrag der Practitioner-Ressource oder Organisations-Ressource zuordnen. Diese Zuordnung verifiziert die MXID des Leistungserbringers, oder macht die jeweilige Organisationsressource anschreibbar durch Nutzer anderer Organisationen.

### 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 Nutzer 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 TIPractitioner-Einträge im VZD-FHIR-Directory*" beschrieben. Eine Erläuterung zu dem Rechtekonzept des VZD-FHIR-Directoy findet sich in dieser Spezifikation im Kapitel "*Rechtekonzept VZD-FHIR-Directory*".

## 5.4 Föderation

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

Um allen berechtigten Akteuren des deutschen Gesundheitswesens 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 beschreiben, wie der Schreib- und Lesezugriff durch die TI-Messenger-Clients des TI-Messenger-Fachdienstes auf dem VZD-FHIR-Directory erfolgt.

### 5.5.1 Schreibzugriffe für TI-Messenger-Fachdienste

Die TI-Messenger-Fachdienste erhalten die Möglichkeit, mittels ihres Registrierungs-Dienstes die bereits bestehende Föderation um weitere Messenger-Services zu erweitern. Die Autorisierung am VZD-FHIR-Directory des Registrierungs-Dienstes 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

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

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

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

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

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

### 5.5.3 Lesezugriff für TI-Messenger-Clients

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

Es gilt:

- die Sichtbarkeit auf die Organisations-Ressourcen KANN für andere Organisationen oder Practitioners eingeschränkt werden und
- die Sichtbarkeit auf Practitoner-Ressourcen ist nur möglich, wenn der Nutzer 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 können, werden in diesem Konzept nicht aufgeführt. Stattdessen wird auf die Matrix-Client-Server-API verwiesen ([Matrix Foundation#Client_Server]). Die nachfolgend beschriebenen Anwendungsfälle sind spezifisch für den TI-Messenger und weichen daher teilweise von der Matrix-Client-Server-API ab. Das gleich gilt für die auf dem Matrix-Server-Server-Protokoll ([Matrix Foundation#Server_Server]) basierenden Anwendungsfälle.

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

## 6.1 AF - Anmeldung eines Nutzers an Messenger-Service

**AF_10057 - Anmeldung eines Nutzers am Messenger-Service**
Mit diesem Anwendungsfall meldet sich ein Nutzer als Person an einem Messenger-Service an. Die Anmeldung erfolgt durch den Nutzer mit einem TI-Messenger-Client und einem Authentifizierungsverfahren, das vom Messenger-Service unterstützt wird. Der TI-Messenger-Client präsentiert dem Nutzer eine Liste aller unterstützten Messenger-Services. Ebenfalls ist es möglich, dass der Nutzer die Domain eines Messenger-Service direkt eingibt, um sich an diesen zu authentifizieren. Nach erfolgreicher Anmeldung erhält der TI-Messenger-Client ein Matrix-ACCESS_TOKEN (`AuthZ`) vom Matrix-Homeserver, das für die spätere Autorisierungen genutzt wird. Das Matrix-ACCESS_TOKEN ist mit dem TI-Messenger-Client des Nutzers über die `device_id` verknüpft.

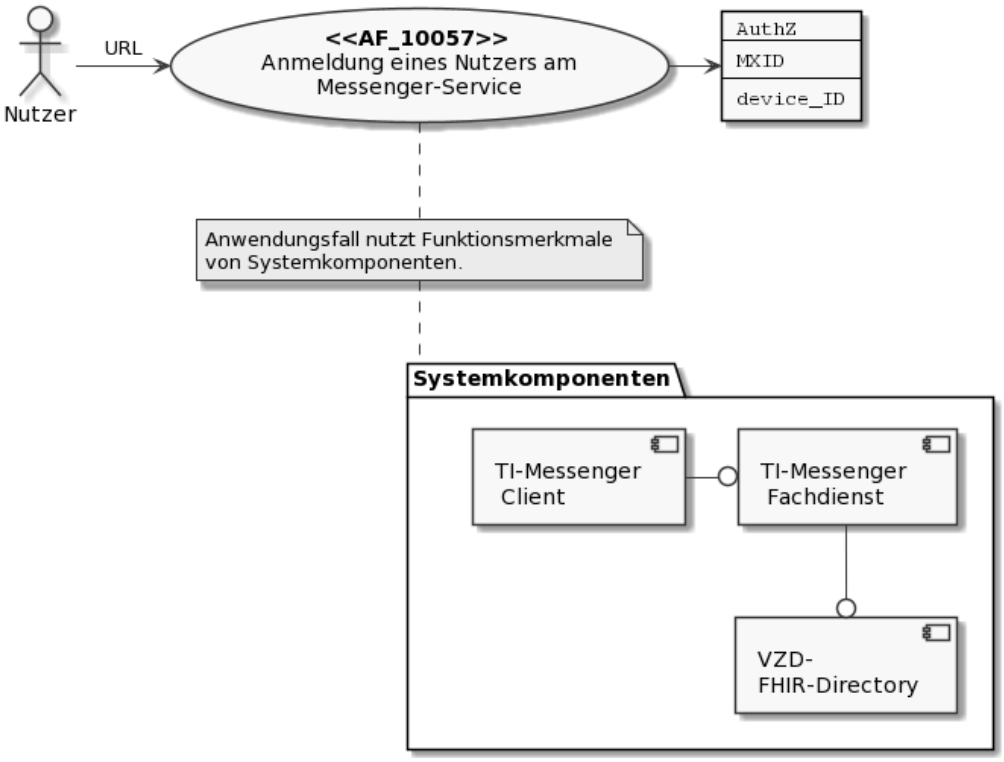


**Abbildung 4: Systemkomponenten des AF - Anmeldung eines Nutzers am Messenger-Service**

**Tabelle 3: AF - Anmeldung eines Nutzers am Messenger-Service**

| **AF_10057** | **Anmeldung eines Nutzers am Messenger-Service** |
|---|---|
| Akteur | Nutzer |
| Auslöser | Nutzer möchte sich mit TI-Messenger-Client bei einem Messenger-Service anmelden |
| Komponenten | TI-Messenger-Client,<br>Messenger-Service,<br>VZD-FHIR-Directory |
| Vorbedingungen | 1. Der Nutzer verfügt über einen TI-Messenger-Client<br>2. Der Nutzer kennt die URL des Messenger-Services oder die URL ist bereits in seinem Client konfiguriert.<br>3. Der Nutzer kann sich durch ein beim Matrix-Homeserver unterstütztes Authentisierungsverfahren identifizieren.<br>4. Der verwendete Matrix-Homeserver unterstützt vereinbarte Authentisierungsverfahren.<br>5. Der verwendete Matrix-Homeserver ist in die Föderation integriert. |

| | |
|---|---|
| Eingangsdaten | URL des Matrix-Homeservers |
| Ergebnis | TI-Messenger Account erzeugt |
| Ausgangsdaten | `Matrix-ACCESS_TOKEN, MXID, device_id` |
| Akzeptanzkriterien | ML-123571, ML-123576 , ML-123575 |

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

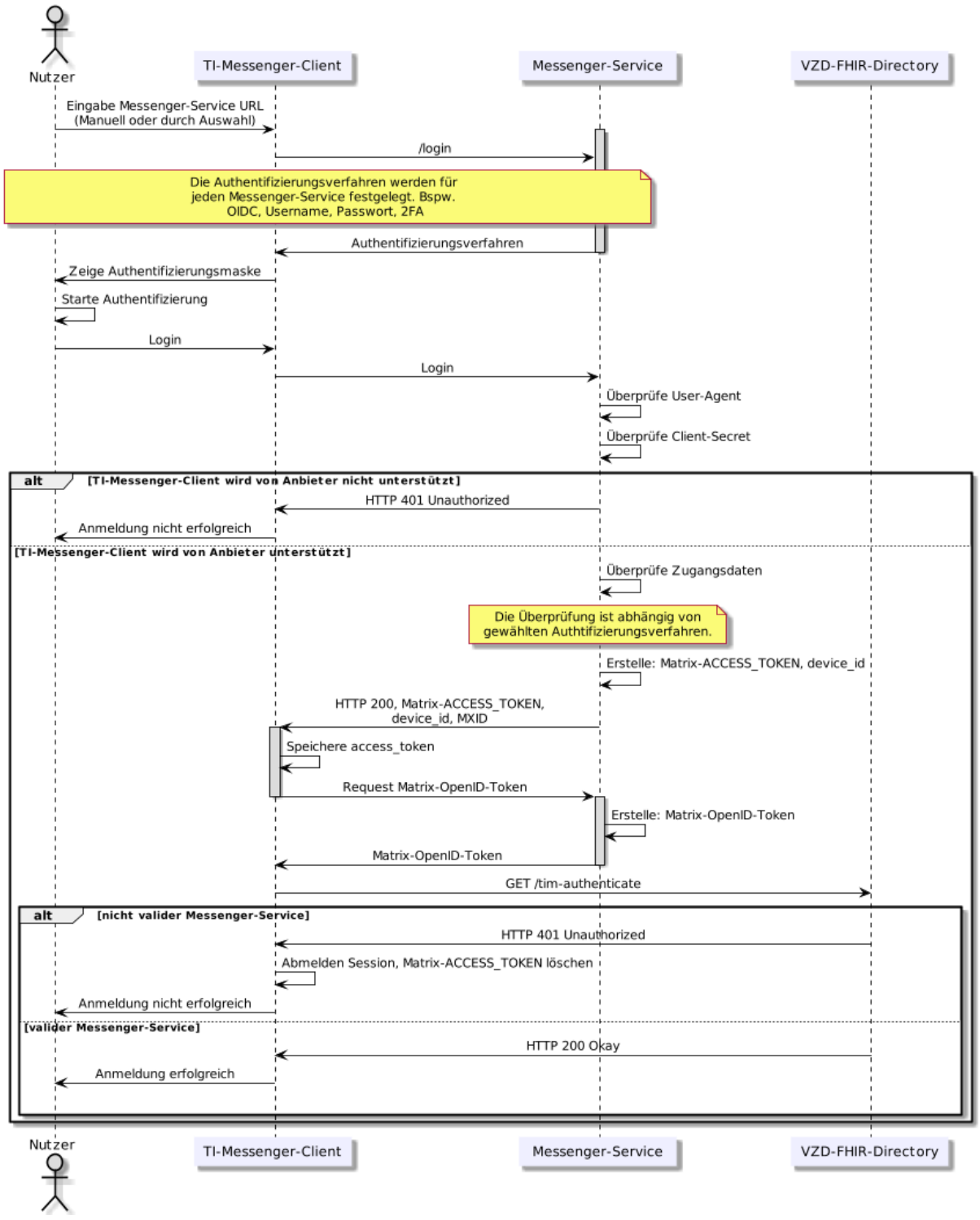


**Abbildung 5: Laufzeitsicht - Anmeldung eines Nutzers am Messenger-Service**

**[<=]**

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

**ML-123571 - AF_10057 - Nutzer kann sich erfolgreich an einem gültigen Messenger-Service anmelden**
Ein Nutzer kann sich erfolgreich an einem gültigen Messenger-Service anmelden, wenn er sich mit einem zugelassenen Authentisierungsverfahren 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**
Bei der erfolgreichen Anmeldung stellt der Messenger-Service dem TI-Messenger-Client ein Access Token aus.
**[<=]**

**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.**[<=]**

## 6.2 AF - Leistungserbringer als Practitioner hinzufügen

**AF_10058 - Leistungserbringer als Practitioner hinzufügen**
Mit diesem Anwendungsfall trägt ein Leistungserbringer mit HBA seine MXID in seinen Practitioner-Datensatz auf dem VZD-FHIR-Directory ein. Danach hat der Leistungserbringer die Möglichkeit, mit anderen verifizierten LE in Kontakt zu treten und ist für andere verifizierte LE über das VZD-FHIR-Directory erreichbar. Dieser Flow SOLL direkt mit dem initialen Anmeldevorgang kombiniert werden. Hierfür wird der LE während des Onboardings durch den TI-Messenger-Client gefragt, ob es sich bei dem Nutzer um einen Leistungserbringer mit Zugriff auf HBA handelt. Zusätzlich KANN der LE angeben, ob er andere LE über das VZD-FHIR-Directory finden möchte und ob eine Sichtbarkeit gegenüber anderen LE gewünscht ist.

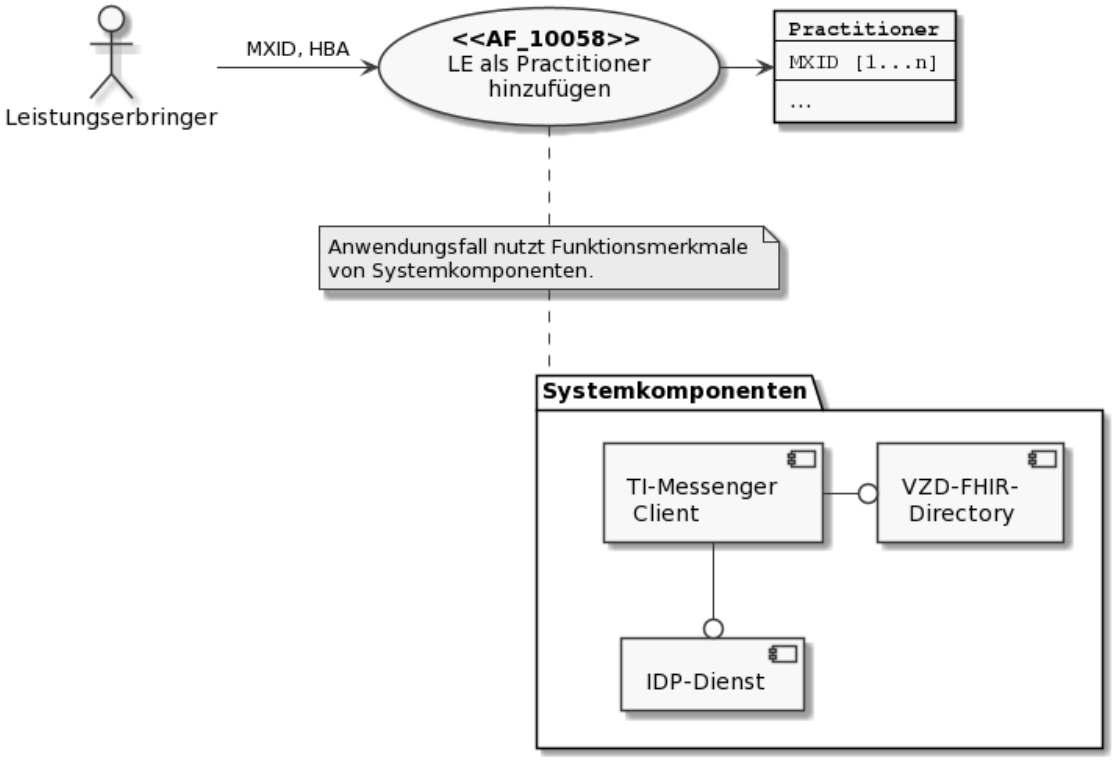


**Abbildung 6: Systemkomponenten des AF - Leistungserbringer als Practitioner hinzufügen**

**Tabelle 4: AF - Leistungserbringer als Practitioner hinzufügen**

| **AF_10058** | **Leistungserbringer als Practitioner hinzufügen** |
|---|---|
| Akteur | Leistungserbringer |
| Auslöser | Leistungserbringer möchte seinen Practitioner-Datensatz auf dem VZD-FHIR-Directory aktualisieren |
| Komponenten | TI-Messenger-Client,<br>IDP-Dienst,<br>VZD-FHIR-Directory |
| Vorbedingungen | 1. Der LE verfügt über einen TI-Messenger-Client<br>2. Der LE ist beim Smartcard IDP-Dienst der TI registriert.<br>3. Der LE ist als Nutzer im Messenger-Service angemeldet (AF_10057).<br>4. Das VZD-FHIR-Directory ist beim Smartcard IDP-Dienst registriert.<br>5. Der verwendete Matrix-Homeserver ist in die Föderation integriert.<br>6. Der LE kann sich am (Practitioner) Smartcard IDP-Dienst authentisieren. |

| | |
|---|---|
| Eingangsdaten | MXID des Leistungserbringers, HBA |
| Ergebnis | MXID im Practitioner-Datensatz des Nutzers auf dem FHIR-Server eingetragen, (gemäß [gemSpec_VZD_FHIR_Directory]) |
| 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. Für das zu benutzende Authentifizierungsverfahren gilt die Spezifikation gemäß OpenID-Connect.
Das Verfahren OIDC wird im Anhang B beschrieben.

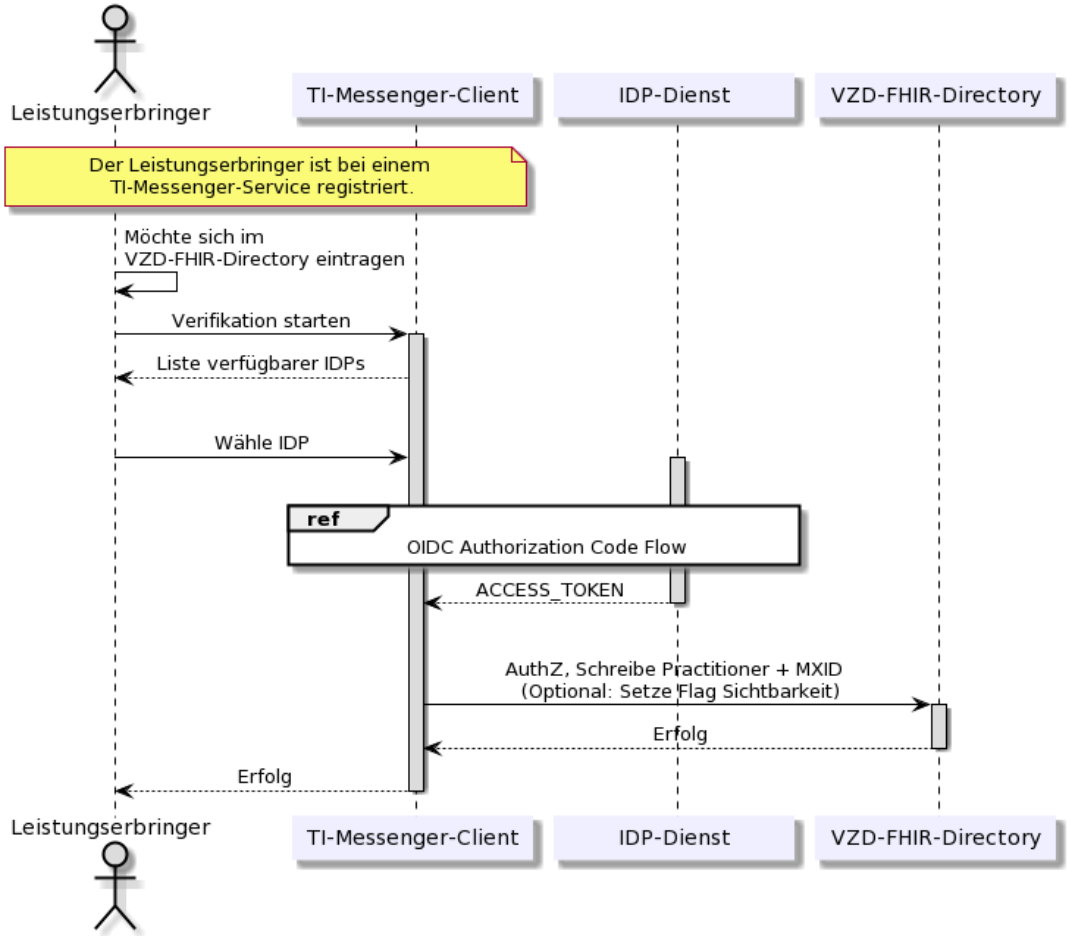


**Abbildung 7: Laufzeitsicht - LE als Practitioner hinzufügen**

**[<=]**

**Akzeptanzkriterien für den Anwendungsfall: LE als Practitioner hinzufügen (AF_10058)**

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

**ML-123611 - AF_10058 - MXID-Eintrag nur für eigenen Practitioner-FHIR-Datensatz**
Der Leistungserbringer darf nur eigene FHIR-Ressourcen (AF_10037 - gemSpec_VZD_FHIR_Directory) ändern.
**[<=]**

## 6.3 AF - Messenger-Service bereitstellen

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

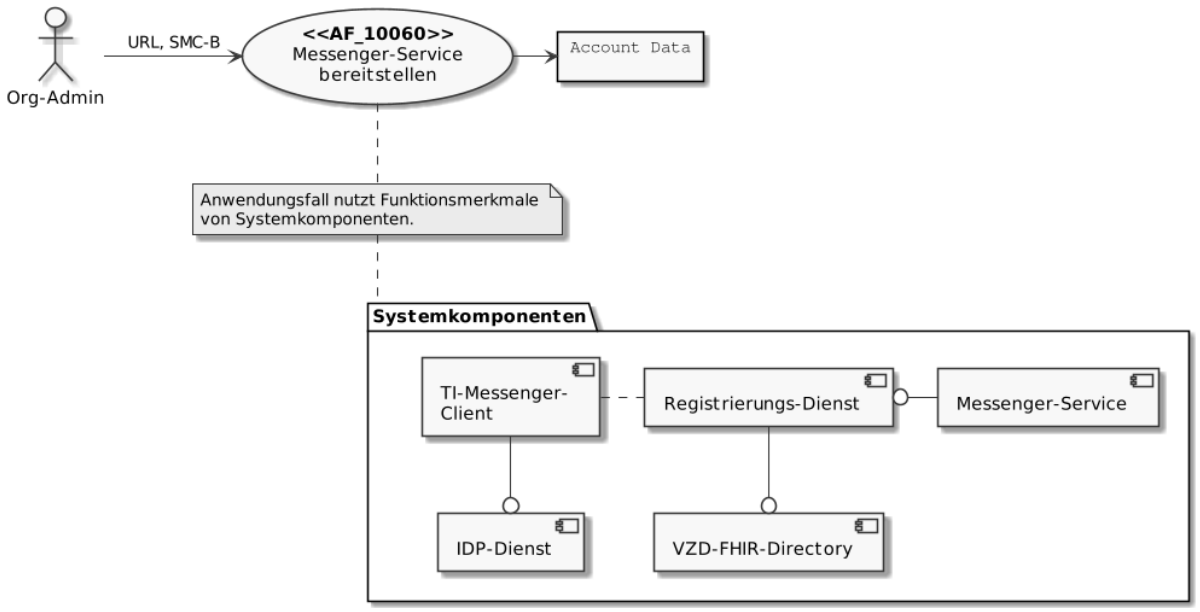


**Abbildung 8: Systemkomponenten des AF - Messenger-Service bereitstellen**

**Tabelle 5: AF - Messenger-Service bereitstellen**

| **AF_10060** | **Messenger-Service bereitstellen** |
|---|---|
| Akteur | Beauftragter Mitarbeiter der Organisation (z. B. *Org-Admin*) |
| Auslöser | Eine Organisation des deutschen Gesundheitswesen möchte am TI Messenger Dienst teilnehmen und benötigt die Bereitstellung eins Messenger-Service |
| Komponenten | TI-Messenger-Client<br>IDP-Dienst<br>Registrierungs-Dienst<br>VZD-FHIR-Directory<br>Messenger-Service |
| Vorbedingung | 1. Der Nutzer verfügt über ein Frontend (innerhalb oder außerhalb eines TI-Messenger-Clients) für die Kommunikation mit dem Registrierungs-Dienst<br>2. Das verwendete Frontend des Registrierungs-Dienst ist beim Smartcard IDP-Dienst registriert.<br>3. Der verwendete Registrierungs-Dienst kann sich beim VZD-FHIR-Directory Server für Schreibzugriffe authentifizieren. |
| Eingangsdaten | Identität der Organisation, SMC-B |

| | |
|---|---|
| Ergebnis | 1. Die Domain des neuen Messenger-Services wurde als Endpunkt im VZD-FHIR-Server eingetragen.<br>2. Der Messenger-Service für die Organisation wurde erstellt.<br>3. Für den beauftragten Mitarbeiter der Organisation (*Org-Admin*) wurde ein Account auf dem Messenger-Service mit Administrationsrechten erstellt. |
| Ausgangsdaten | Messenger-Service der Organisation, Account-Daten |
| Akzeptanzkriterien | ML-123648 , ML-123649 , ML-123650 , ML-123651 |

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

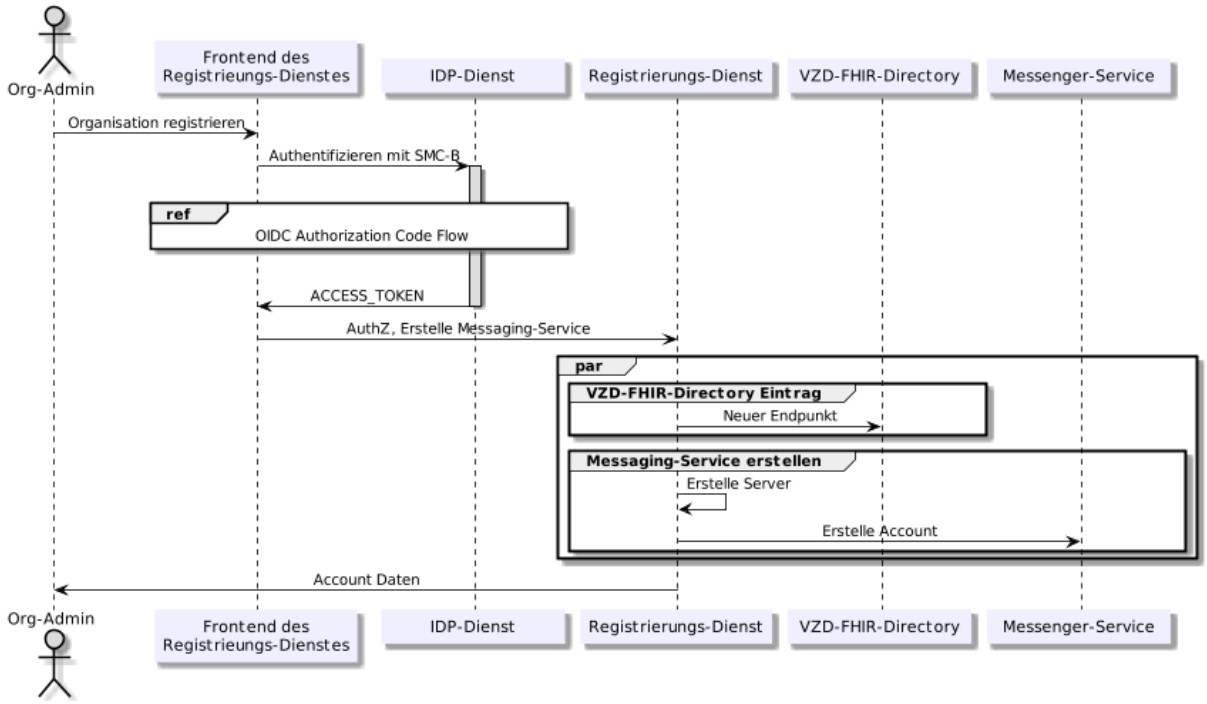


**Abbildung 9: Laufzeitsicht - Messenger-Service automatisch bereitstellen**

**[<=]**

### Akzeptanzkriterien für den Anwendungsfall: Messenger-Service - bereitstellen (AF_10060)

### ML-123648 - AF_10060 - Messenger-Service bereitstellen nur als Nutzer Rolle Org-Admin

Nur ein Nutzer in der Rolle *Org-Admin* darf einen Messenger-Service automatisch bereitstellen. Es ist eine SMC-B- Karte für die Erstellung notwendig.
**[<=]**

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

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

**ML-123651 - AF_10060 - Org-Admin Administrator Account vorhanden**
Der Nutzer in der Rolle *Org-Admin* der Organisation hat einen Administrator-Account auf dem Messenger-Service seiner Organisation.
**[<=]**

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

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

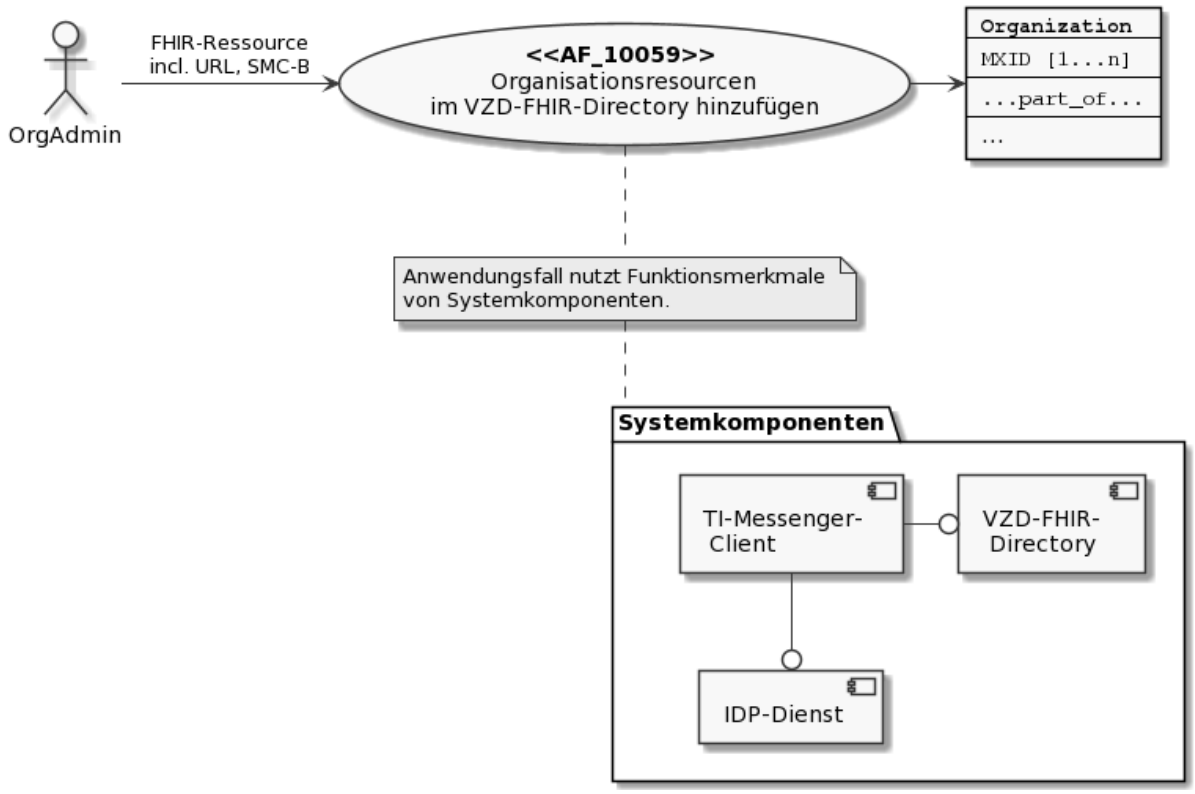


**Abbildung 10: Systemkomponenten des AF - Organisationsressourcen im VZD-FHIR-Directory hinzufügen**

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

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

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

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

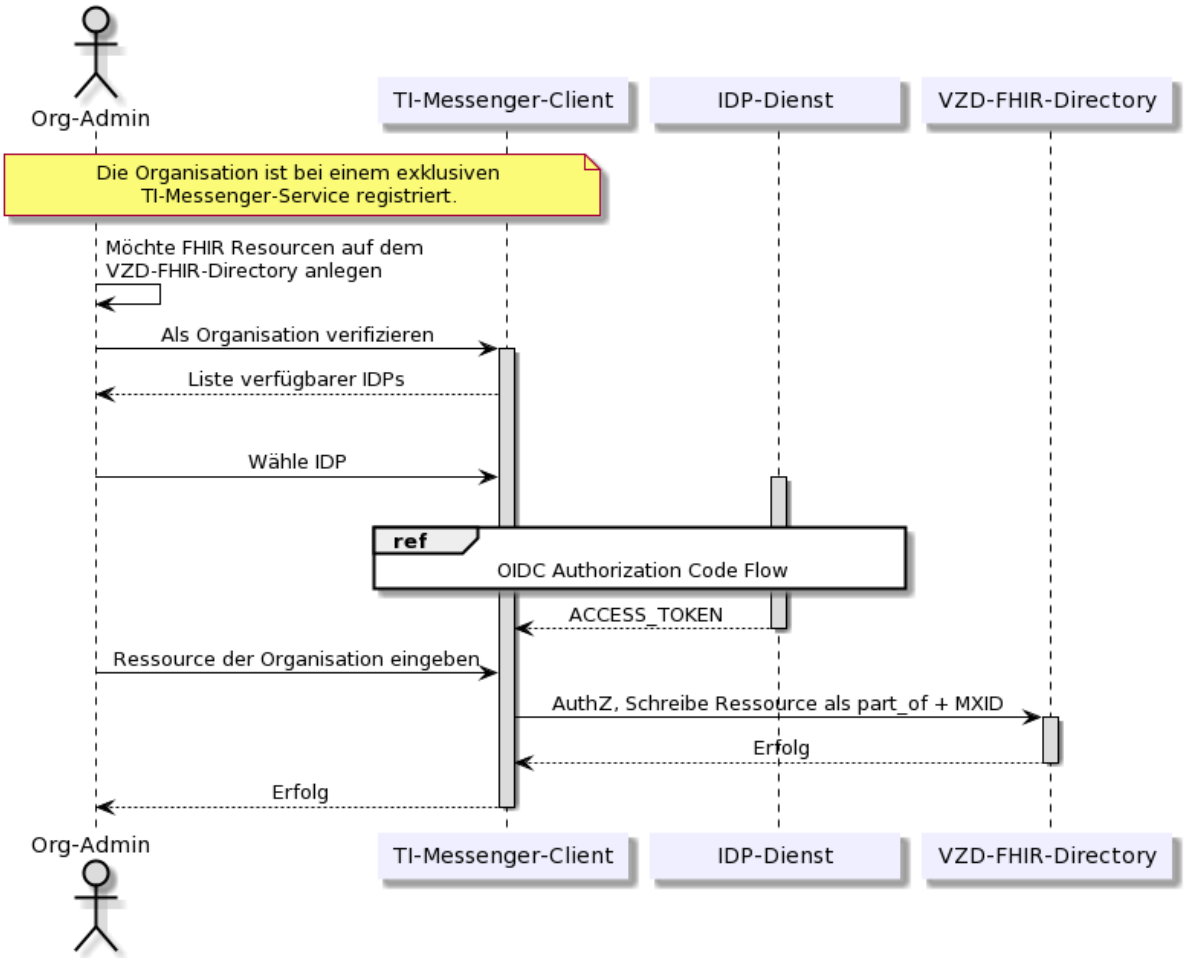


**Abbildung 11: Laufzeitsicht - Organisations-Ressourcen im VZD-FHIR-Directory hinzufügen**

**[<=]**

### Akzeptanzkriterien für den Anwendungsfall: Organisationsressourcen im VZD-FHIR-Directory hinzufügen (AF_10059)

#### ML-123627 - AF_10059 - Organisations-Ressourcen im VZD-FHIR-Directory hinzufügen

Nach erfolgreicher Authentisierung an einem zugelassenen IDP-Dienst als Administrator einer Organisation kann der Nutzer in der Rolle *Org-Admin* die Matrix User URI (MXID) in den FHIR-Organization-Datensatz eintragen und Unterstrukturen für die Organisation anlegen. Der Nutzer in der Rolle *Org-Admin* wird über den Erfolg der Operation informiert.

**[<=]**

#### ML-123626 - AF_10059 - Änderungen nur für eigene Organization-FHIR-Datensätze

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

**[<=]**

## 6.5 AF - TI-Messenger Remote Invite

**AF_10061 - TI-Messenger Remote Invite**
Nutzer haben die Möglichkeit innerhalb der Föderation des deutschen Gesundheitswesens zwischen Messenger-Services-Chatnachrichten und andere durch die Matrix-Spezifikation festgelegte Aktionen auszuführen. Dafür MUSS ein Chatraum zwischen den entsprechenden Parteien entstehen. Dieser Ablauf zeigt, wie ein Chatraum zwischen den Parteien entsteht.

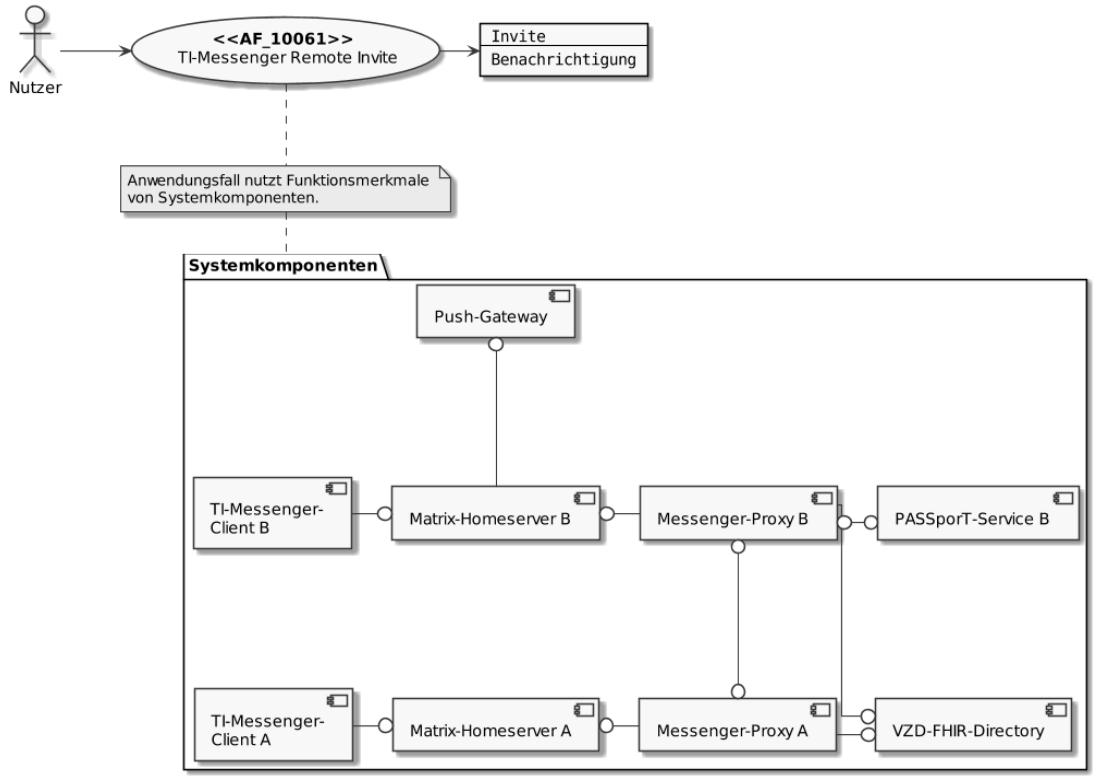


**Abbildung 12: Systemkomponenten des AF - TI-Messenger Remote Invite**

**Tabelle 7 AF - TI-Messenger Remote Invite**

| **AF_10061** | **TI-Messenger Remote Invite** |
|---|---|
| Akteur | Nutzer A, Nutzer B |
| Auslöser | Nutzer A möchte mit Nutzer B einen gemeinsamen Chatraum einrichten |
| Komponenten | TI-Messenger Client<br>Matrix-Homeserver<br>VZD-FHIR-Directory<br>PASSporT-Service<br>Push-Gateway |
| Vorbedingungen | 1. Die Nutzer verfügen über einen TI-Messenger-Client<br>2. Die Nutzer kennen die URL ihres Matrix-Homeservers oder die URL ist bereits in ihren Clients konfiguriert.<br>3. Die Nutzer sind am Messenger-Services angemeldet (AF_10057)<br>4. Die verwendeten Matrix-Homeserver sind in die Föderation integriert. |
| Eingangsdaten | beabsichtigter Nachrichtenaustausch |
| Ergebnis | Nutzer A und Nutzer B sind beide in einem gemeinsamen Chatraum.<br>Optional erfolgt eine Benachrichtigung von Nutzer B über die Einladung in den Chatraum. |
| Ausgangsdaten | keine |
| Akzeptanzkriterien | ML-123654 , ML-123659 , ML-123660 , ML-123661 , ML-123663 |

*Hinweis: Es handelt sich hierbei um eine **vereinfachte Laufzeitansicht**. Bei der Laufzeitansicht wurde nicht betrachtet, dass die Verbindung zwischen TI-Messenger-Client und Matrix-Homeserver über den Messenger-Proxy läuft. Ebenfalls wurde für eine vereinfachte Darstellung darauf verzichtet, dass der Messenger-Proxy die Föderationsliste bei dem Registrierungs-Dienst abruft, welcher die Liste beim VZD-FHIR-Directory abruft und zur Verfügung stellt. Der Abruf der Föderationsliste ist in AF 6.8 - Check remote domain hinreichend beschrieben.*

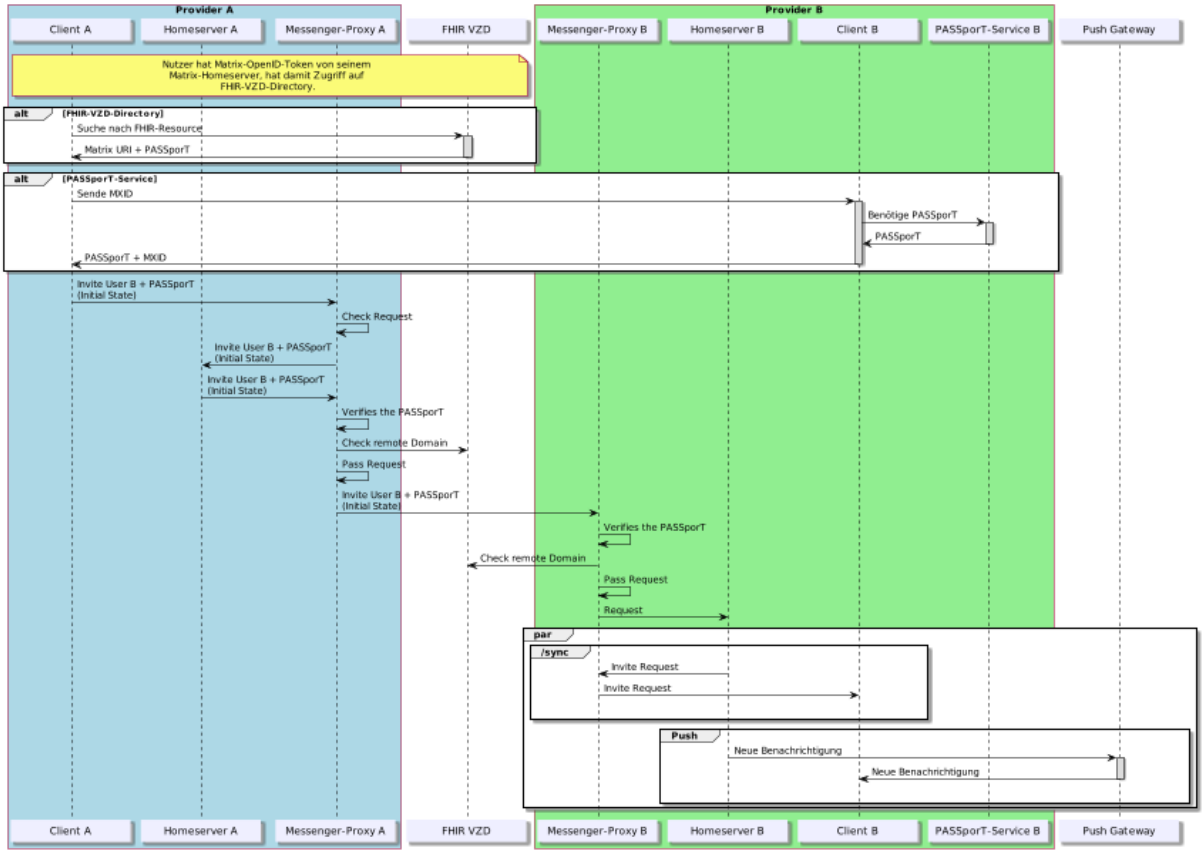


**Abbildung 13: Laufzeitsicht - TI-Messenger Remote Invite**

**[<=]**

### Akzeptanzkriterien für den Anwendungsfall: TI-Messenger Remote Invite (AF_10061)

#### ML-123654 - AF_10061 - Suche im VZD-FHIR-Directory

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

**[<=]**

#### ML-123659 - AF_10061 - PASSporT Übergabe

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

**[<=]**

#### ML-123660 - AF_10061 - Invite nur mit PASSporT

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

**[<=]**

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

**ML-123661 - AF_10061 - Messenger-Proxy prüft PASSporT auf Gültigkeit**
Der Messenger-Proxy lehnt das Invite bei ungültigem PASSporT ab.
**[<=]**

**ML-123663 - AF_10061 - Nutzer sind dem Chatraum beigetreten**
Alle Chat Parteien sind erfolgreich im Chatraum vorhanden.
**[<=]**

## 6.6 AF - Message senden (Remote)

**AF_10062 - Message senden (Remote)**
Dieser Anwendungsfall setzt ein erfolgreiches Invite eines oder mehrerer beteiligter Nutzer voraus und führt den eigentlichen Nachrichtenaustausch durch. Die beteiligten Nutzer sind mit TI-Messenger-Clients Mitglied des Chatraumes und auf unterschiedlichen Messenger-Services verteilt.

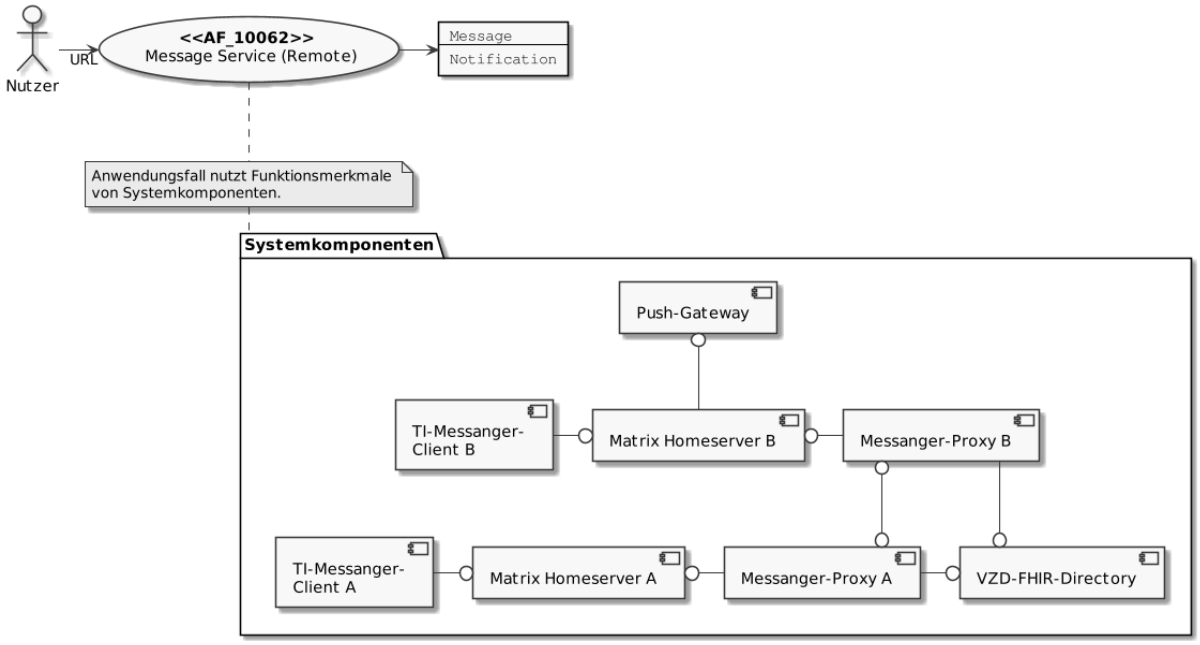


**Abbildung 14: Systemkomponenten des AF - Message senden (Remote)**

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

| AF_10062 | Message senden (Remote) |
|---|---|
| Akteur | Nutzer A, Nutzer B |
| Auslöser | Nutzer A möchte eine Chatnachricht an Nutzer B (föderierter Matrix-Homeserver) versenden |
| Komponenten | TI-Messenger-Client A + B<br>Matrix-Homeserver A + B<br>Messenger-Proxy A + B<br>Registrierungs-Dienst<br>VZD-FHIR-Directory<br>Push-Gateway |
| Vorbedingungen | 1. Beide Nutzer sind Mitglied eines gemeinsamen Raumes.<br>2. Es liegt eine aktualisierte Föderationsliste vor.<br>3. Die Messenger-Proxys überprüfen die Remote-Domain (siehe AF 6.8) |
| Eingangsdaten | Chatnachricht |
| Ergebnis | Nutzer B erhält Chatnachricht von Nutzer A; optional erfolgt eine Benachrichtigung von Nutzer B über eine neue Nachricht |
| Ausgangsdaten | Chatnachricht erreicht Nutzer B |
| Akzeptanzkriterien | ML-123665 , ML-123666 , ML-123667 , ML-123668 |

*Hinweis: Es handelt sich hierbei um eine **vereinfachte Laufzeitansicht**. Bei der Laufzeitansicht wurde nicht betrachtet, dass die Verbindung zwischen TI-Messenger-Client und Matrix-Homeserver über den Messenger-Proxy läuft. Ebenfalls wurde für eine vereinfachte Darstellung darauf verzichtet, dass der Messenger-Proxy die Föderationsliste bei dem Registrierungs-Dienst abruft, welcher die Liste beim VZD-FHIR-Directory abruft und zur Verfügung stellt. Der Abruf der Föderationsliste ist in AF 6.8 - Check remote domain hinreichend beschrieben.*

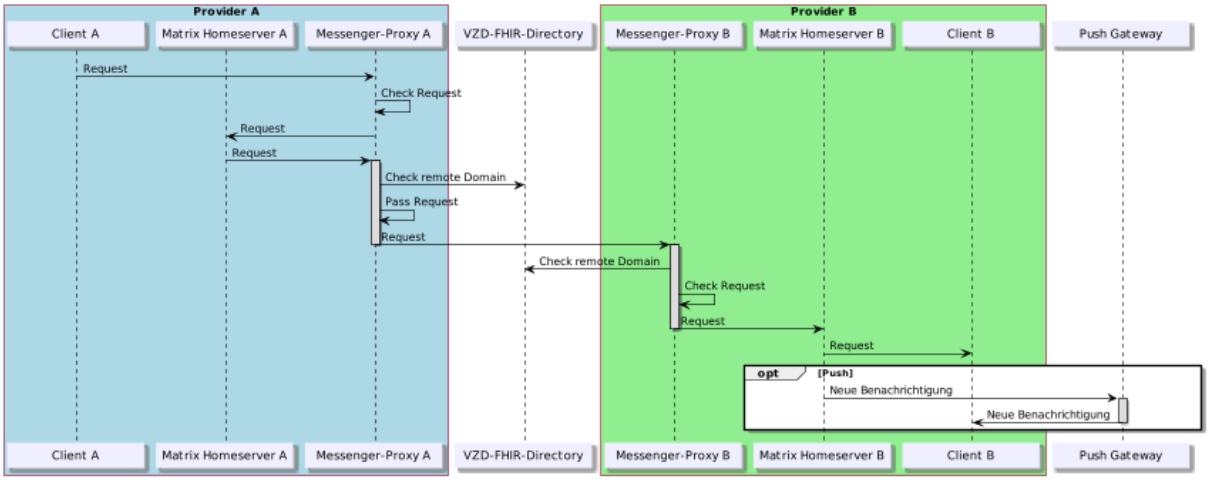


**Abbildung 15: Laufzeitsicht - Message senden (Remote)**

**[<=]**

### Akzeptanzkriterien für den Anwendungsfall: Message senden (AF_10062)

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

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

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

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

## 6.7 AF - Messenger-Service (Lokal)

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

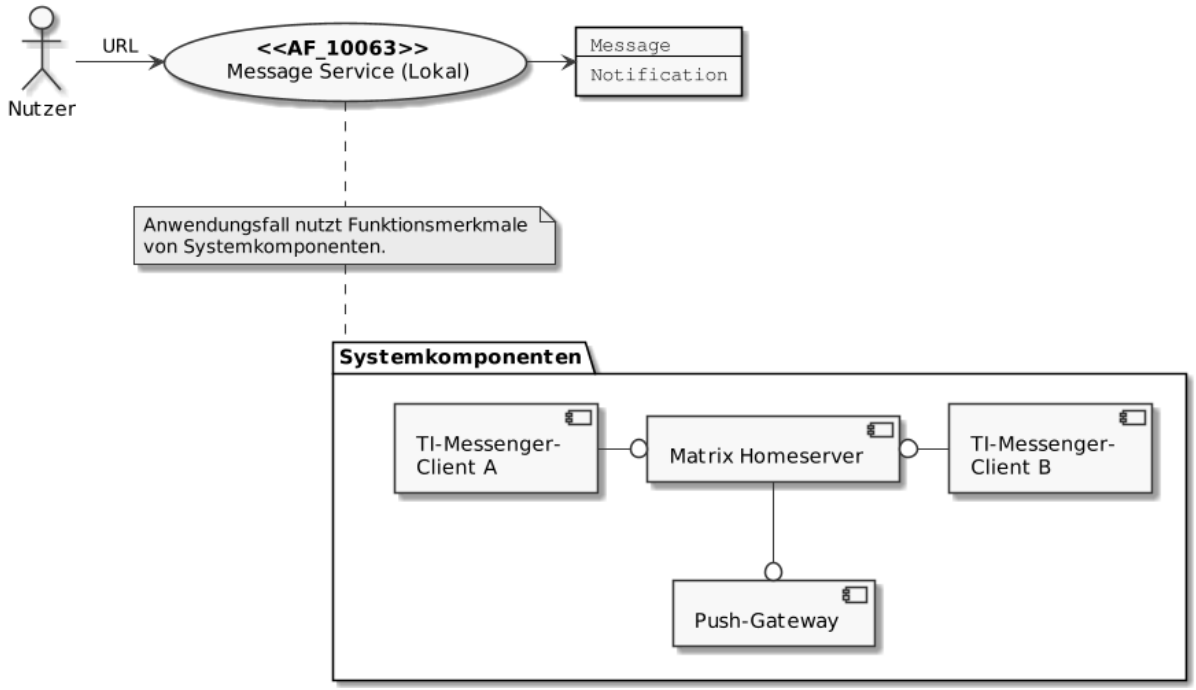


**Abbildung 16: Systemkomponenten des AF - Messenger-Service (Lokal)**

**Tabelle 9 Messenger-Service (Lokal)**

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

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

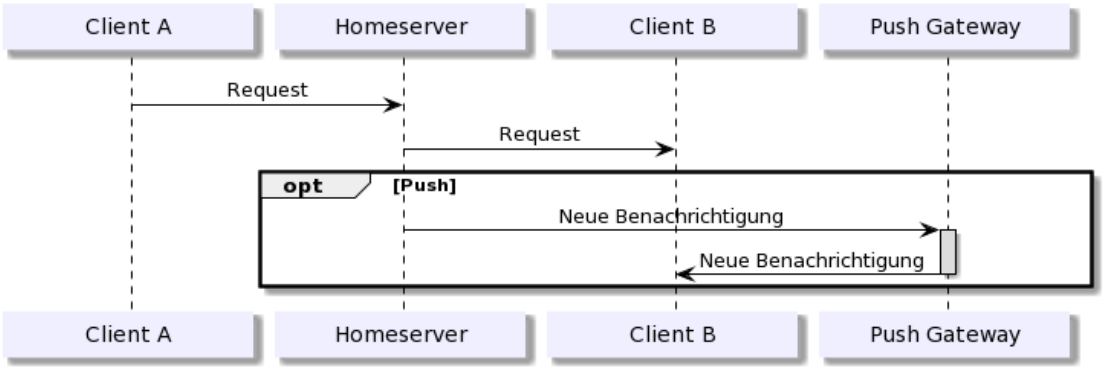


**Abbildung 17: Laufzeitsicht - Messenger Service (Lokal)**

**[<=]**

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

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

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

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

## 6.8 AF - Check remote Domain

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

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

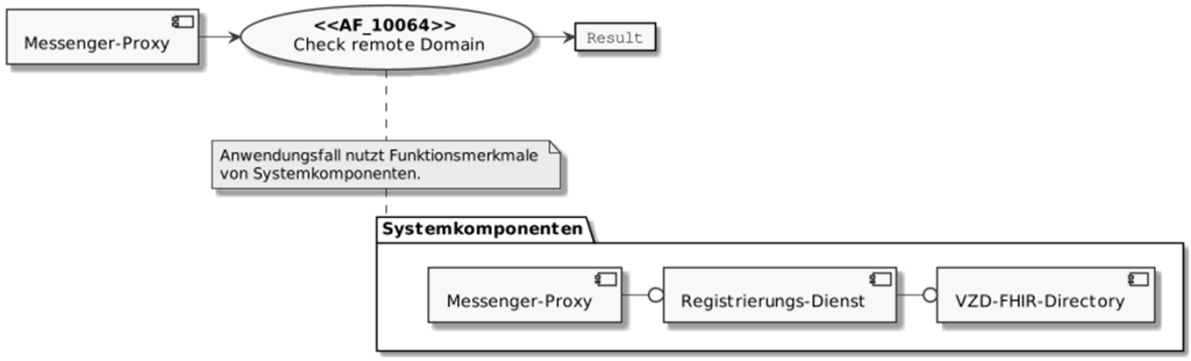


**Abbildung 18: Systemkomponenten des AF - Check remote Domain**

**Tabelle 10 Check remote Domain**

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

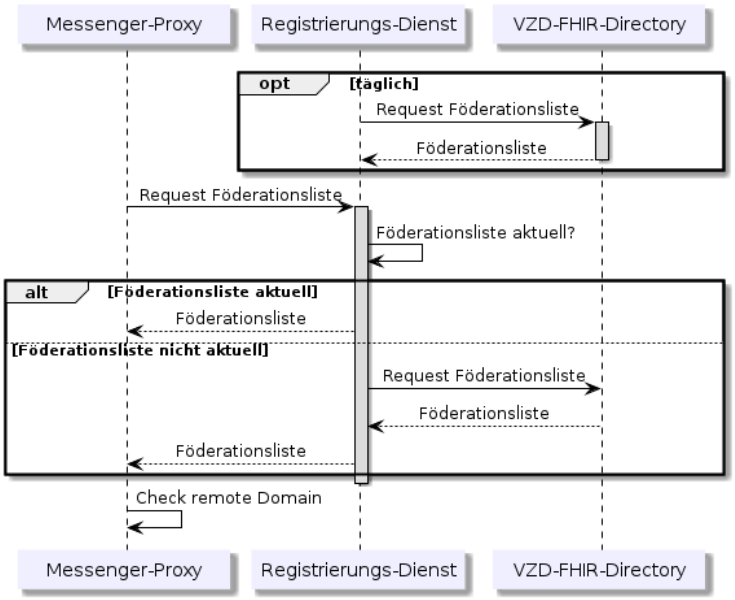


**Abbildung 19: Laufzeitsicht - Ablauf Check remote Domain**

**[<=]**

### Akzeptanzkriterien für den Anwendungsfall: Check remote Domain (AF_10064)

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

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

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

# 7 Anhang A – Verzeichnisse

## 7.1 Abkürzungen

| Kürzel | Erläuterung |
|---|---|
| AD | Active Directory |
| AF | Anwendungsfall |
| APN | 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 | Hyptertext 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-Nutzers (Matrix-User-ID) |
| on-premise | das Produkt wird auf eigener oder gemieteter Hardware betrieben |
| Third-Party | Drittanbieter, der Zusatzleistungen oder Komponenten beisteuert |

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

## 7.3 Abbildungsverzeichnis

## 7.4 Tabellenverzeichnis



## 7.5 Referenzierte Dokumente

### 7.5.1 Dokumente der gematik

Die nachfolgende Tabelle enthält die Bezeichnung der in dem vorliegenden Dokument referenzierten Dokumente der gematik zur Telematikinfrastruktur. Der mit der vorliegenden Version korrelierende Entwicklungsstand dieser Konzepte und Spezifikationen wird pro Release in einer Dokumentenlandkarte definiert; Version und

Stand der referenzierten Dokumente sind daher in der nachfolgenden Tabelle nicht aufgeführt. Deren zu diesem Dokument jeweils gültige Versionsnummern sind in der aktuellen, von der gematik veröffentlichten Dokumentenlandkarte enthalten, in der die vorliegende Version aufgeführt wird.

| [Quelle] | Herausgeber: Titel |
|---|---|
| [gemKPT_TI_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 |
|---|---|
| [Direct Messaging] | Matrix Foundation<br>https://matrix.org/docs/spec/client_server/r0.6.1 |
| [Matrix Foundation] | Matrix Foundation<br>https://matrix.org/docs/spec/ |
| [Nutzer Token] | Matrix Foundation<br>https://matrix.org/docs/spec/client_server/r0.6.1 |
| [Matrix-PushGW] | Matrix Foundation<br>https://matrix.org/docs/spec/push_gateway/r0.1.1 |
| [MatrixSpecProposal] | Matrix Foundation<br>https://spec.matrix.org/unstable/proposals/ |
| [RFC 8225] | IETF<br>https://datatracker.ietf.org/doc/html/rfc8225 |
| [OpenID] | OpenID Foundation<br>https://openid.net/developers/specs/ |
| [FHIR] | HL7 FHIR Dokumentation<br>https://www.hl7.org/fhir/documentation.html |

# 8 Anhang B - Abläufe

## 8.1 OIDC - Authorization Code Flow