**Elektronische Gesundheitskarte und Telematikinfrastruktur**

# Spezifikation
# TI-Messenger-Fachdienst

| | |
|---|---|
| Version: | 1.0.0 |
| Revision: | 408198 |
| Stand: | 01.10.2021 |
| Status: | freigegeben |
| Klassifizierung: | öffentlich |
| Referenzierung: | gemSpec_TI-Messenger-FD |

# Dokumentinformationen

### Änderungen zur Vorversion

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

### Dokumentenhistorie

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

# 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.

Die vorliegende Spezifikation definiert die Anforderungen zu Herstellung, Test und Betrieb des Produkttyps TI-Messenger-Fachdienst. Der Fachdienst ermöglicht die sichere Ad-hoc-Kommunikation zwischen Teilnehmern. Aus den Kommunikationsbeziehungen mit dem TI-Messenger-Client und dem VZD-FHIR-Directory resultieren vom TI-Messenger-Fachdienst anzubietende Schnittstellen, die in diesem Dokument normativ beschrieben werden. Vom TI-Messenger-Fachdienst genutzte Schnittstellen liegen zumeist in anderen Verantwortungsbereichen (z. B. IDP-Dienst). Diese werden in der entsprechenden Produkttypspezifikation definiert.

## 1.2 Zielgruppe

Das Dokument richtet sich zwecks der Realisierung an Hersteller des Produkttypen Fachdienst TI-Messenger sowie an Anbieter, welche diesen Produkttypen betreiben [gemKPT_Betr]. Alle Hersteller und Anbieter von TI-Anwendungen, die Schnittstellen der Komponente nutzen, oder Daten mit dem Produkttypen Fachdienst TI-Messenger austauschen oder solche Daten verarbeiten, müssen dieses Dokument ebenso berücksichtigen.

## 1.3 Geltungsbereich

Dieses Dokument enthält normative Festlegungen zur Telematikinfrastruktur des deutschen Gesundheitswesens. Der Gültigkeitszeitraum der vorliegenden Version und deren Anwendung in Zulassungs- oder Abnahmeverfahren wird durch die gematik GmbH in gesonderten Dokumenten (z. B. gemPTV_ATV_Festlegungen, 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

Spezifiziert werden in dem Dokument die von dem Produkttyp bereitgestellten (angebotenen) Schnittstellen. Benutzte Schnittstellen werden hingegen in der Spezifikation desjenigen Produkttypen beschrieben, der diese Schnittstelle bereitstellt. Auf die entsprechenden Dokumente wird referenziert (siehe auch Anhang, Kapitel 6.5-Referenzierte Dokumente).

Die vollständige Anforderungslage für den Produkttyp ergibt sich aus weiteren Konzept- und Spezifikationsdokumenten, diese sind in dem Produkttypsteckbrief des Produkttyps TI-Messenger verzeichnet.

## 1.5 Methodik

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

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

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

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

Die einzelnen Elemente beschreiben:

- **ID**: einen eindeutigen Identifier.

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

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

Der für die Erlangung einer Zulassung notwendige Nachweis der Erfüllung des 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-Fachdienst ermöglicht eine sichere Kommunikation verschiedener Teilnehmer im deutschen Gesundheitswesen. Der TI-Messenger-Fachdienst basiert auf dem offenen und dezentralen Kommunikationsprotokoll Matrix. Dabei stellt der Matrix Standard RESTful-APIs für die sichere Übertragung von JSON-Objekten zwischen Matrix-Clients und weiteren Diensten bereit. Die sichere Kommunikation zwischen den einzelnen Akteuren findet in verschlüsselter Form in Räumen auf den beteiligten Matrix-Homeservern statt.

Der TI-Messenger-Fachdienst besteht aus dezentralen und zentralen Teilkomponenten, die ein Anbieter bereitstellen MUSS. Bei den dezentralen Teilkomponenten handelt es sich um die Messenger-Services. Die Messenger-Services beinhalten jeweils Matrix-Homeserver und Komponenten, welche dafür sorgen, dass eine Föderation der Matrix-Homeserver nur zwischen verifizierten Domains stattfindet. Diese werden in der Spezifikation als Messenger-Proxy und PASSporT-Service bezeichnet. Messenger-Services werden für einzelne Organisationen (z. B. Leistungserbringerinstitutionen, Verbände) bereitgestellt und erlauben die Nutzung durch alle Nutzer einer Organisation. Weiterhin KÖNNEN Messenger-Services durch Organisationen bereitgestellt werden, die nur für Leistungserbringer nutzbar sind. Diese unterscheiden sich technisch nicht von anderen Messenger-Services. Einzig die zugeordnete Organisation bietet ein für Leistungserbringer Authentifizierungsverfahren an.

Die Kommunikation zwischen einem TI-Messenger-Client und einem TI-Messenger-Fachdienst erfolgt über die Messenger-Proxies der Messenger-Services. Hier findet zunächst die TLS-Terminierung der Verbindungen von den TI-Messenger-Clients statt. Der Messenger-Proxy kontrolliert die Föderation durch Abfragen am Registrierungs-Dienst. Hierbei wird geprüft, ob die beteiligten Matrix-Homeserver registrierte Mitglieder der Föderation sind und ein Teilnehmer berechtigt ist, Requests auf dem Homeserver auszulösen.

Neben den dezentralen Messenger-Services besteht der TI-Messenger-Fachdienst aus einem zentralen Registrierungs-Dienst sowie einem zentralen Push-Gateway. Über den Registrierungs-Dienst bekommt der Anbieter die Möglichkeit die Domainnamen der von ihm bereitgestellten Messenger-Services in das zentrale VZD-FHIR-Directory einzutragen, Messenger-Services automatisiert Organisationen zur Verfügung zu stellen und Domainabfragen vorzunehmen. Das Push-Gateway dient zur Übertragung von Benachrichtigungen (Notifications) an die jeweiligen TI-Messenger-Clients um den Eingang einer neuen Nachricht zu signalisieren. Für die Authentisierung von Nutzern des TI-Messenger kommen unterschiedliche Verfahren zur Anwendung. Beispielhaft soll auf die Möglichkeit der Verwendung eines IDP-Dienstes verwiesen werden.

Die folgende Abbildung zeigt einen Systemüberblick aller am TI-Messenger beteiligten Teilkomponenten in vereinfachter Form.

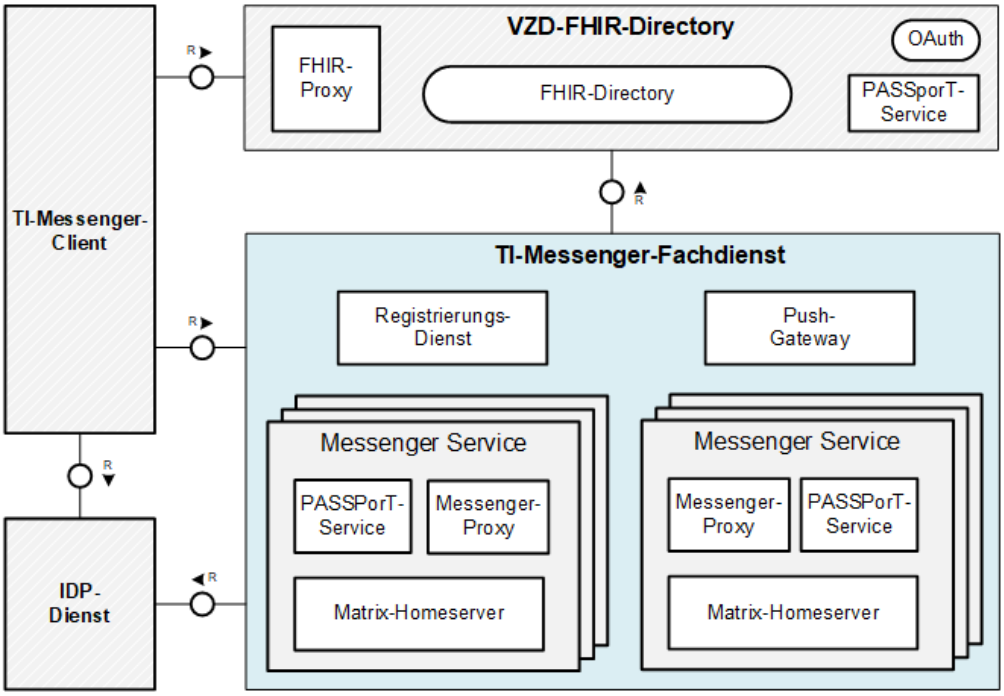


**Abbildung 1: Systemüberblick (Vereinfachte Darstellung)**

# 3 Systemkontext

Der folgende Abschnitt setzt den TI-Messenger-Fachdienst in den Systemkontext des TI-Messenger-Dienstes.

## 3.1 Nachbarsysteme

Für den Betrieb des TI-Messenger-Fachdienstes werden weitere Systeme benötigt. Dazu gehört der Smartcard-IDP-Dienst der gematik und das VZD-FHIR-Directory. Die Abbildung *Systemüberblick* aus Kapitel 2 zeigt deren Beziehung zum TI-Messenger-Fachdienst.

Der Smartcard-IDP-Dienst stellt allen berechtigten Teilnehmern ID_TOKEN (AuthN) sowie ACCESS_TOKEN (AuthZ), gemäß des OpenID Foundation [OpenID] spezifizierten Protokolls, zur Verfügung. Mit den ausgestellten Token erfolgt die notwendige Authentisierung der TI-Messenger-Nutzer bei der initialen Registrierung eines Messenger-Service für eine Organisation, oder für schreibenden Zugriff auf das VZD-FHIR-Directory mittels TI-Messenger-Client. Dazu ist es notwendig das der TI-Messenger-Client und das Frontend des Registrierungs-Dienstes sich bei dem Smartcard IDP-Dienst registriert. Damit ist sichergestellt das Änderungen an den VZD-FHIR-Directory Einträgen durch den TI-Messenger-Client möglich sind.

Das zentrale VZD-FHIR-Directory bildet ein Verzeichnis aller TI-Messenger-Fachdienste, Organisationen und Leistungserbringer und bietet die Möglichkeit der Suche von Teilnehmern anhand konfigurierter Merkmale. Der TI-Messenger-Fachdienst trägt bei erfolgreicher Aufnahme in die Föderation im VZD-FHIR-Directory (in die Organisationsressource) seine Matrix-Domain ein. Das VZD-FHIR-Directory vertraut den Matrix-Homerservern der jeweiligen Messenger-Services, wenn die Domain des Messenger-Service erfolgreich in das VZD-FHIR-Directory eingetragen wurde.

## 3.2 Messenger-Services

Durch TI-Messenger-Anbieter werden Messenger-Services jeweils für eine Organisation des Gesundheitswesens (z. B. Arztpraxis, Krankenhaus, Apotheke, Verband, etc.) bereitgestellt. Die Bereitstellung erfolgt durch den Registrierungs-Dienst eines TI-Messenger-Anbieters dezentral und kann *on-premise* oder innerhalb von Rechenzentren stattfinden. Jeder Messenger-Service MUSS einer Organisation zugeordnet sein. Die Messenger-Services unterscheiden sich nur in den jeweils verwendeten Authentifizierungsverfahren. Diese werden durch die jeweilige Organisation festgelegt und bereitgestellt. Die jeweilige Organisation MUSS die Kontrolle über die Benutzerverwaltung haben, um zu jedem Zeitpunkt Nutzer aus dem TI-Messenger ausschließen zu können. Dabei MÜSSEN Nutzer vom Messenger-Service gelöscht/gesperrt werden, wenn der Nutzer innerhalb der Nutzerverwaltung gelöscht/gesperrt wurde.

**Authentifizierungsverfahren**

Messenger-Services können je nach Art der Organisation verschiedene Authentifizierungsverfahren anbieten. Sind bereits Systeme wie Active-Directory oder LDAP innerhalb einer Organisation verfügbar, können diese entsprechend genutzt

werden, indem der Matrix-Homeserver bei diesen registriert wird. Sind keine Authentifizierungsverfahren vorhanden (z. B. innerhalb einer Arztpraxis) KÖNNEN TI-Messenger-Anbieter entsprechende Authentifizierungsverfahren zur Verfügung stellen. Diese erlauben einen Login für Nutzer (z. B. Benutzername/Passwort und einen zweiten Faktor) und können auch von weiteren Systemen nachgenutzt werden. Die nachfolgende Abbildung verdeutlicht das Authentifizieren von Nutzern an einen Messenger-Service.

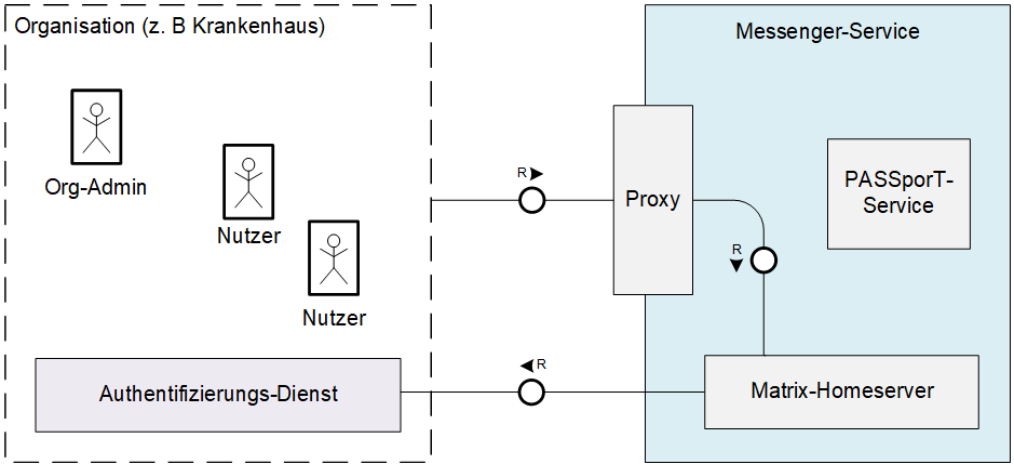


**Abbildung 2: Beispiel - Authentifizierung von Nutzern einer Organisation**

# 4 Übergreifende Festlegungen

## 4.1 Datenschutz und Sicherheit

**ML-123614 - Verbot von Organisationsaccounts für Versicherte**
Der Anbieter MUSS sicherstellen, dass organisationsbasierte TI-Messenger-Accounts nicht an Versicherte vergeben werden. Er MUSS sicherstellen, dass nur Accounts an Personen vergeben werden, mit denen ein Beschäftigungsverhältnis besteht. Hierzu ist eine organisatorische Lösung ausreichend.
**[<=]**

**ML-123618 - PUSH-Benachrichtigungen**
TI-Messenger-Anbieter MÜSSEN dafür sorgen, dass diese Gateways externe PUSH-Dienste datenschutzkonform nutzen. Hierzu wurden folgende Kriterien definiert, die in jedem Fall beachtet werden MÜSSEN:

- PUSH-Benachrichtigungen dürfen erst nach expliziter Zustimmung der Nutzer erfolgen (Opt-In).
- Alle PUSH-Nachrichteninhalte, auf die der PUSH-Anbieter nicht zugreifen können muss, MÜSSEN verschlüsselt werden.
- PUSH-Nachrichten MÜSSEN vor dem Versenden um einen Zufallswert von 0-10 Sekunden verzögert werden um Timingbasierte Profilbildung zu erschweren.
- Wo möglich, MÜSSEN PUSH-Anbieter gewählt werden, die eine Wahrung der Betroffenenrechte für personenbezogene Informationen ermöglichen.
- Wenn ein Zielclient gerade aktiv ist, soll dieser selbsttätig auf einkommende Nachrichten lauschen und nicht per PUSH benachrichtigt werden.
- PUSH-Nachrichten dürfen keine Nachrichteninhalte enthalten, ihre Funktion besteht lediglich darin Clientsysteme zu informieren, dass Nachrichten abrufbar sind und eine Synchronisierung mit dem Homeserver nötig ist. Es DARF nur die Room-ID und Event-ID enthalten sein.

**[<=]**

Für Details der Verschlüsselung und enthaltene personenbezogene Daten siehe [MSC 3013].

**ML-123615 - Flächendeckende Verwendung von TLS**
Betreiber und Hersteller MÜSSEN sicherstellen, dass sämtliche Verbindungen zwischen Komponenten des TI-Messengers mittels TLS kommunizieren, sofern diese Kommunikation die Grenzen einer virtuellen/physischen Maschine überschreitet. Hierzu MUSS mindestens serverseitig authentizitätsgeschütztes TLS verwendet werden. Sofern kein beidseitiges TLS verwendet wird, MUSS die Authentizität der Clientseite mit gleichwertiger Sicherheit sichergestellt werden. Es gelten die Festlegungen aus [gemSpec_Krypt].
**[<=]**

**ML-123616 - Abweichungen vom Matrix-Standard**
Hersteller von TI-Messenger-Komponenten MÜSSEN sämtliche, nicht in der TI-Messenger-Spezifikation beschriebenen, Abweichungen vom Matrix-Protokoll oder den MUST- oder SHOULD-Empfehlungen des Matrix-Protokolls dokumentieren und

begründen.
**[<=]**

**ML-123617 - Löschfristen für Homeserver**
Betreiber MÜSSEN sicherstellen, dass Events, Gesprächsinhalten und mit einzelnen Gesprächen assoziierte Daten (z.B. versandte Dateien) maximal für 6 Monate auf Homeservern verbleiben und danach gelöscht werden.
Hersteller MÜSSEN eine Funktion für Homeserver anbieten, über die eine Löschfrist für diese Daten konfigurierbar ist.
**[<=]**

**ML-123621 - Interoperabilität von Zusatzfunktionen für den TI-Messenger-Fachdienst**
Hersteller MÜSSEN sicherstellen, dass alle implementierten Funktionen, die über den gewöhnlichen Funktionsumfang einer TI-Messenger-Komponente hinausgehen die Sicherheit des Produkts nicht gefährden und die Interoperabilität mit anderen TI-Messenger-Produkten erhalten. Ebenso MÜSSEN Hersteller sicherstellen, dass TI-Messenger-Fachdienstbestandteile resilient auf unerwartete Eingaben reagieren.
**[<=]**

**ML-123619 - Protokollierung zum Zwecke der Fehler- bzw. Störungsbehebung**
Falls im TI-Messenger-Fachdienst eine Protokollierung zum Zwecke der Fehler- bzw. Störungsbehebung erfolgt, MUSS der Fachdienst unter Berücksichtigung des Art. 25 Abs. 2 DSGVO sicherstellen, dass in den Protokolldaten entsprechend dem Datenschutzgrundsatz nach Art. 5 DSGVO nur personenbezogene Daten in der Art und dem Umfang enthalten sind, wie sie zur Behebung erforderlich sind und dass die erzeugten Protokolldaten im Fachdienst nach der Behebung unverzüglich gelöscht werden. Sofern andere gesetzliche Grundlagen wie §331 SGB V nicht überwiegen sind hierzu nur anonymisierte Daten zu protokollieren.
**[<=]**

**ML-123620 - Explizites Verbot von Profiling für TI-Messenger-Anbieter**
Anbieter von TI-Messenger-Komponenten DÜRFEN NICHT Daten zu Profilingzwecken sammeln. Dies betrifft insbesondere eine Überwachung welche Akteure mit welchen anderen Akteuren kommunizieren.

Die gematik kann nach § 331 Abs. 2 SGB V Daten festlegen, die Anbieter von Komponenten und Dienste der gematik offenzulegen bzw. zu übermitteln haben, sofern diese erforderlich sind, um den gesetzlichen Auftrag der gematik zur Überwachung des Betriebs zur Gewährleistung der Sicherheit, Verfügbarkeit und Nutzbarkeit der Telematikinfrastruktur zu erfüllen. Nur die hierfür erforderlichen personenbezogenen Daten dürfen von den Anbietern und Herstellern als Ausnahme vom Profilingverbot erhoben und ausschließlich für den genannten Zweck verwendet werden.
**[<=]**

**ML-123622 - Behandlung von kryptographischem Material für OAuth**
Betreiber von TI-Messenger-Messenger-Fachdiensten MÜSSEN sicherstellen, dass kryptographisches Material für OAuth, wie z.B. Client-ID und Client-Secret für Authentisierung mittels Credential-Flow sicher eingebracht werden. Dieses Material MUSS in Hardware Security Modules sicher gespeichert werden.**[<=]**

Zum Nachweis der Umsetzung ist lediglich eine Prüfung der Prozesse zur Einbringung erforderlich. Eine Auditierung der Umsetzung ist optional.

**ML-123628 - Device Verification, Cross-Signing und SSSS für TI-Messenger-Fachdienste**
Hersteller MÜSSEN sicherstellen, dass die Funktionen Cross-Signing und Secure Secret Storage and Sharing (SSSS) zur Device Verification unterstützt werden. Es MUSS die

Spezifikation hinsichtlich Ende-zu-Ende Verschlüsselung vollständig befolgt werden.
**[<=]**

**ML-123638 - Explizites Verbot von Profiling für TI-Messenger-Fachdienste**
Betreiber von TI-Messenger-Komponenten DÜRFEN NICHT Daten zu Profilingzwecken sammeln. Dies betrifft insbesondere eine Überwachung welche Akteure mit welchen anderen Akteuren kommunizieren.

Die gematik kann nach § 331 Abs. 2 SGB V Daten festlegen, die Anbieter von Komponenten und Dienste der gematik offenzulegen bzw. zu übermitteln haben, sofern diese erforderlich sind, um den gesetzlichen Auftrag der gematik zur Überwachung des Betriebs zur Gewährleistung der Sicherheit, Verfügbarkeit und Nutzbarkeit der Telematikinfrastruktur zu erfüllen. Nur die hierfür erforderlichen personenbezogenen Daten dürfen von den Anbietern und Herstellern als Ausnahme vom Profilingverbot erhoben und ausschließlich für den genannten Zweck verwendet werden.
**[<=]**

**ML-123637 - Sicherheitsrisiken von Software-Bibliotheken minimieren**
Hersteller von TI-Messenger-Fachdiensten MÜSSEN Maßnahmen umsetzen, um die Auswirkung von unentdeckten Schwachstellen in benutzten Software-Bibliotheken zu minimieren.
Hinweis: Beispielmaßnahmen sind in [OWASP Proactive Control#C2] zu finden. Das gewählte Verfahren MUSS die gleiche Wirksamkeit aufweisen, wie die Kapselung gemäß [OWASP Proactive Control#C2 Punkt 4].
**[<=]**

**ML-123635 - CC-Evaluierung als Ersatz für Gutachten**
Falls der Hersteller entscheidet, eine CC-Zertifizierung statt eines Produktgutachtens durchzuführen, MUSS der Hersteller bei der Einreichung eines CC-Zertifizierungsantrags sein Security-Target-Dokument der gematik zur Verfügung stellen. In diesem MÜSSEN mindestens beschrieben sein:

- die zusätzlichen Funktionen des TI-Messenger-Clients des Nutzers,
- die in den zusätzlichen Funktionen verarbeiteten Daten,
- die Schnittstellen zwischen dem TI-Messenger-Clients des Nutzers und den ggf. genutzten Backend-Diensten der zusätzlichen Funktionen inklusive ihrer Sicherheitsmaßnahmen und
- die Sicherheitsannahmen an den TI-Messenger-Clients des Nutzers und die Ausführungsumgebung

**[<=]**

**ML-123634 - Sichere Produktentwicklung und Nachweise**
Der Hersteller MUSS innerhalb des Produktlebenszyklus (Entwicklung, Betrieb, Außerbetriebnahme) seines Produktes Sicherheitsaktivitäten integrieren und anwenden, d. h. in einschlägigen Fachkreisen anerkannte, erprobte und bewährte Regeln anwenden.
Der Hersteller MUSS die Sicherheits- und Datenschutzmaßnahmen für sein Produkt in einem Sicherheits- und Datenschutzkonzept dokumentieren und auf Verlangen der gematik zur Verfügung stellen.
Der Hersteller MUSS einen Testplan für Sicherheitstests erstellen und auf Verlangen der gematik zur Verfügung stellen. Dieser MUSS umgesetzt werden und der gematik bei jeder Veröffentlichung einer Produktversion als neuer Bericht vorgelegt werden.

Der Hersteller des TI-Messenger-Clients für Nutzer MUSS während der Entwicklung des Produktes implementierungsspezifische Sicherheitsanforderungen dokumentieren und umsetzen.
Der Hersteller MUSS ein sicherheitsrelevanten Softwarearchitektur-Review durchführen und identifizierte Architekturschwachstellen beheben. Dieses Review MUSS nach jeder Architekturänderung mit Sicherheitsrelevanz wiederholt werden.
Der Hersteller MUSS eine Bedrohungsanalyse durchführen und Maßnahmen gegen die identifizierten Bedrohungen implementieren.
Der Hersteller MUSS während der Entwicklung des Produktes sicherheitsrelevante Quellcode-Reviews oder automatisierte sicherheitsrelevante Quellcode-Scans durchführen.
Der Hersteller MUSS während der Entwicklung des Produktes automatisierte Sicherheitstests durchführen.
Der Hersteller MUSS einen Schulungsplan zur regelmäßigen Schulung von Entwicklern in sicherer Entwicklung und Secure-Coding-Techniken dokumentieren und umsetzen.
Der Hersteller MUSS alle Entwickler des Produktes in sicherer Entwicklung und Secure-Coding-Techniken schulen. Hierzu MUSS der Hersteller sicherstellen, dass alle Entwickler zu Beginn der Entwicklung geschult sind. Er SOLL für diese anschließend auch laufende Weiterbildung durchführen.
Der Hersteller MUSS den verwendeten sicheren Produktlebenszyklus und deren Teilprozesse dokumentieren und auf Nachfrage der gematik zur Verfügung stellen. Die Dokumentation soll mindestens die folgenden Sicherheitsaktivitäten beschreiben:

- Erfassen und Umsetzen von implementierungsspezifischen Sicherheitsanforderungen für den Client und von Best-Practice-Sicherheitsanforderungen,
- Durchführen von sicherheitsrelevanten Architektur- und Design-Reviews,
- Durchführen von Bedrohungsanalysen,
- Durchführen von sicherheitsrelevanten Quellcode-Reviews,
- Durchführen von Sicherheitstests während der Qualitätssicherungsphase,
- Etablieren von Quality Gates, die eine Veröffentlichung des Clients mit 'Mittel' oder 'Hoch' bewerteten Sicherheitsfehlern verhindert
- Änderungs- und Konfigurationsmanagement,
- Schwachstellen-Management

Der Hersteller MUSS während der Entwicklung des Produktes einen Änderungs- und Konfigurationsmanagementprozess verwenden. Das Änderungsmanagement umfasst mindestens den Entscheidungsprozess über vorgeschlagene Änderungen und die Autorisierung der Änderungen. Das Konfigurationsmanagement liefert mindestens zu jedem Zeitpunkt die eindeutige Zusammensetzung des Produktes bezüglich seiner eindeutigen Komponenten (Dritt-Software wie Bibliotheken und Frameworks) und den vorgenommenen Änderungen an eigenen Komponenten.
Der Hersteller MUSS bei Veröffentlichung einer neuen Produktversion des Produktes die Einhaltung der Herstellererklärung sicherheitstechnische Eignung durch seinen Datenschutzbeauftragten verifizieren.
**[<=]**

**ML-123623 - Nur Verbindungen mit zugelassenen TI-Messenger-Clients**
Der Messenger-Proxy MUSS prüfen, ob sich der TI-Messenger-Client als von der gematik zugelassenes Produkt ausweisen kann. Verbindungen mit nicht zugelassenen Clients

MÜSSEN unterbunden werden.
**[<=]**

**ML-124882 - Kein Einbringen vertraulicher Informationen in Room-States durch Organisationsadministratoren**
Anbieter von Home-Servern MÜSSEN sicherstellen, dass sie als Organisations-Administratoren keine sensiblen Informationen in Room-States einbringen. Ebenso MÜSSEN sie Organisations-Administratoren von Homeservern unter Kundenverwaltung informieren, dass im Room-State sichtbare Informationen gegenwärtig nicht verschlüsselt sind. Sobald durch die geplante Matrix-Spec-Changes (MSCs) die Möglichkeit geschaffen wurde vertrauliche Informationen sicher im Room-State zu speichern, wird dies direkt durch die Matrix-Spezifikation abgedeckt.

**[<=]**

## 4.2 Authentifizierung von Nutzern

Im TI-Messenger-Kontext werden gemäß [gemSpec_TI_Messenger-Dienst#Akteure und Rollen] zwischen folgenden Rollen unterschieden:

**Tabelle 1: Authentifizierung von Nutzerrollen**

| Rolle | Matrix-Homeserver | VZD-FHIR-Directory |
|---|---|---|
| User-HBA | Authentifizieren mittels des vereinbarten Authentifizierungsverfahren | Schreibzugriff: HBA (C.HP.AUT)<br>Lesezugriff: Matrix-OpenID-Token |
| User | | Lesezugriff: Matrix-OpenID-Token |
| Org-Admin | | Schreibzugriff: SMC-B (C.HCI.AUT)<br>Lesezugriff: Matrix-OpenID-Token |

### 4.2.1 Smartcard-IDP-Dienst

Der TI-Messenger-Dienst MUSS die Verifikation von Nutzern mittels SMC-B und HBA unterstützen. Ein TI-Messenger-Client oder Frontend eines Registrieungs-Dienstes MUSS am Smartcard IDP-Dienst der gematik gemäß [gemSpec_IDP_FD] registriert sein.

Im Rahmen der Registrierung werden notwendige Claims (bestätigte Identifikationsmerkmale durch den Nutzer), auf den damit zu nutzenden Dienst festgelegt. Sowohl der TI-Messenger-Client, der Matrix-Homeserver der Messenger-Services als auch der VZD-FHIR-Directory MÜSSEN den ausgestellten Security Tokens (ID_TOKEN, ACCESS_TOKEN) des Smartcard IDP-Dienst vertrauen. Der Anbieter des TI-Messenger-Fachdienstes MUSS über einen organisatorischen Prozess beim Smartcard IDP-Dienst folgende Claims im ACCESS_TOKEN vereinbaren:

**Tabelle 2: Inhalte der Claims für SMC-B/HBA**

| Leistungserbringerinstitutionen (SMC-B) | Inhalte der Claims für Leistungserbringer (HBA) |
|---|---|
| • ProfessionOID<br>• idNummer<br>• organizationName<br>• acr<br>• aud | • ProfessionOID<br>• idNummer<br>• given_name<br>• family_name<br>• acr<br>• aud |

Die ProfessionOID gibt an um welche Art von Leistungserbringer (z. B. Arzt, Zahnarzt etc.) es sich handelt. Die idNummer beinhaltet die Telematik-ID für Organisationen des Gesundheitswesens und Leistungserbringer.

Der Anbieter des TI-Messenger-Fachdienstes MUSS über einen organisatorischen Prozess beim Smartcard IDP-Dienst für die Autorisierungsanfrage folgende `scope`-Parameter vereinbaren: `scope=openid,VZD-FHIR-Directory`

### 4.2.2 Verwaltung der Nutzersession

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

## 4.3 DNS-Namensauflösung

Für die Namensauflösung der vom TI-Messenger-Fachdienst angebotenen Außenschnittstellen, werden DNS-Server im Internet verwendet. Der vereinbarte Abfrage-Record MUSS durch den jeweiligen TI-Messenger-Anbieter bereitgestellt werden und MUSS in öffentlichen DNS-Servern eingetragen sein.

Wird bei der Nutzung eines Messenger-Service für eine Organisation eine auf die Domain der Organisation bezogene Benamung gewählt, erfolgt die Eintragung der notwendigen DNS-Records auf DNS-Server im Internet durch die Administration der Organisation.

#### Identifizierung von Messenger-Services

Jeder Messenger-Service wird durch einen Matrix-Homeservernamen identifiziert, der aus einem Hostname und einem optionalen Port besteht. Weitere Informationen finden sich in [Federation API#3].

## 4.4 Test

Produkttests zur Sicherstellung der Konformität mit der Spezifikation sind vollständig in der Verantwortung der Anbieter/Hersteller des TI-Messenger-Fachdienstes. Die gematik konzentriert sich bei der Zulassung auf das Zusammenspiel der Produkte durch E2E- und IOP-Tests.

Die eigenverantwortlichen Produkttests bei den Industriepartnern umfassen:

- Testumgebung entwickeln,
- Testfallkatalog erstellen (für eigene Produkttests) und
- Produkttest durchführen und dokumentieren

Die Hersteller der TI-Messenger-Fachdienste MÜSSEN zusichern, dass die gematik die Produkttests der Industriepartner in Form von Reviews der Testkonzepte, Testspezifikationen, Testfälle sowie mit dem Review der Testprotokolle (Log- und Trace-Daten) überprüfen kann.

Die gematik fördert eine enge Zusammenarbeit und unterstützt Industriepartner dabei, die Qualität der Produkte zu verbessern. Dies erfolgt durch die Organisation früher IOP-Tests, die Synchronisierung von Meilensteinen und regelmäßige industriepartnerübergreifenden Test-Sessions. Die Test-Sessions umfassen gegenseitige IOP- und E2E Tests.

Die gematik stellt eine TI-Messenger-Fachdienst Referenzimplementierung zur Verfügung. Zur Sicherstellung der Interoperabilität zwischen verschiedenen TI-Messenger-Fachdiensten innerhalb des TI-Messenger-Dienstes MUSS der TI-Messenger-Fachdienst eines TI-Messenger-Anbieters gegen die Referenzimplementierung (TI-Messenger-Client und TI-Messenger Fachdienst) getestet werden.

**ML-124200 - Test des TI-Messenger-Fachdienstes gegen die Referenzimplementierung**
Der Anbieter des TI-Messenger-Fachdienstes MUSS den Fachdienst gegen die Referenzimplementierung erfolgreich testen. Die Testergebnisse sind der gematik vorzulegen.
**[<=]**

Die gematik testet in den Zulassungsverfahren auf Basis von Anwendungsfällen. Dabei werden die Anwendungsfälle durchgespielt und es wird versucht viele Funktionsbereiche und Teile der Anwendung mit einzubeziehen. Anschließend wird mit den IOP Tests die Interoperabilität zwischen den verschiedenen Anbieter nachgewiesen. Für das Zulassungsverfahren des TI-Messenger-Dienstes MÜSSEN die TI-Messenger-Clients und TI-Messenger-Fachdienste bereitgestellt werden. Um einen automatisierten Test für den TI-Messenger-Dienst zu ermöglichen, MUSS die Test-App des TI-Messenger-Clients zusätzlich ein Testtreiber-Modul beinhalten, welcher die Funktionalitäten der produktspezifischen Schnittstelle des TI-Messenger-Clients über eine standardisierte Schnittstelle von außen zugänglich macht und einen Fernzugriff ermöglicht.

## 4.5 Betrieb

Der Betrieb des Fachdienstes wird durch den TI-Messenger-Anbieter verantwortet. Entsprechend dem Betriebskonzept [gemKPT_Betr#Anbieterkonstellationen], KANN der Betrieb jedoch aus- bzw. verlagert werden. Zum Beispiel für ein on-premise Hosting. Die Koordination der jeweiligen Komponenten sowie die Erfüllung der Anforderungen verbleiben jedoch am Anbieter. Dieser KANN in Abstimmung mit seinen Nutzern und Dienstleistern Verträge abschließen um den sicheren Betrieb aufrecht zu erhalten.

### 4.5.1 Performance

Der TI-Messenger Fachdienst MUSS mit einer vollumfänglich-funktionalen Verfügbarkeit von 98% betreibbar sein.

Der Anbieter TI-Messenger MUSS sein Produkt TI-Messenger-Fachdienst mit einer vollumfänglich-funktionalen Verfügbarkeit von 98% betreiben.

Wenn der Betrieb von Homeservern on-premise bei den Nutzern realisiert wird, KANN der Anbieter TI-Messenger für diese Produktinstanzen von den Performancevorgaben in Abstimmung mit seinen Nutzern abweichen. Die Abweichungen und die betroffenen Instanzen MÜSSEN der gematik im Rahmen der betrieblichen Prozesse bekannt gemacht werden.

### 4.5.2 Monitoring

Die folgenden technischen Kommunikationsbeziehungen bzw. Use Cases MÜSSEN im Rahmen des Monitorings und der Rohdatenerfassung am TI-Messenger-Fachdienst erfasst und automatisiert und anonymisiert an die gematik zur Performancebewertung der Vorgaben zum Rohdatenreporting [gemSpec_Perf#Performance-Evaluierung auf der Basis von Rohdaten] reportet werden.

**Tabelle 3 : Technische Kommunikationsbeziehungen – Use-Case-Mapping**

| Use-Case-Referenz | Use-Case-Titel | Matrix-Operation bzw. Use-Case-Mapping auf TI-Messenger Fachdienst-Komponente(n) | Start und Ende der Messung am TI-Messenger-Fachdienst |
|---|---|---|---|
| AF_10057 | Anmeldung eines Nutzers am Messenger-Service | Messenger-Service | Start: Messenger Service erhält Login Request durch Client<br><br>Ende: Übermittlung |

| | | | |
|---|---|---|---|
| | | | Matrix-OpenID-Token |
| AF_10060 | Messenger-Service bereitstellen | Registrierungs-Dienst, Messenger-Service | Start:<br>AuthZ, Erstelle Messaging-Service<br><br>Ende:<br>Account Daten wurden übermittelt |
| AF_10061 | TI-Messenger Remote Invite | Homeserver A, Messenger-Proxy A, Homeserver B, Messenger-Proxy B | Start Provider A:<br>Eingang Request von Client A: Invite User B + PASSporT<br><br>Ende:<br>Ausgang Request an Provider B: Invite User B + PASSporT<br><br>Start Provider B:<br>Eingang Request von Provider A: Invite User B + PASSporT<br><br>Ende:<br>Versand Invite Request an Client B |
| AF_10062 | Message senden (Remote) | Homeserver A, Messenger-Proxy A, Homeserver B, Messenger-Proxy B | Start Provider A:<br>Eingang Request von Client A<br><br>Ende:<br>Ausgang Request an Provider B<br><br>Start Provider |

| | | | |
|---|---|---|---|
| | | | B:<br>Eingang Request von Provider A<br><br>Ende:<br>Ausgang Request an Client B |
| AF_10063 | Client-Fachdienst-Nachrichtenversand | Matrix CS API spec 8.6 "`PUT /_matrix/client/r0/rooms/{roomId}/state/{eventType}/{stateKey}`" | Start:<br>Eingang Request am Homeserver vom Client.<br><br>Ende:<br>Response an Client, dass die Nachricht erfolgreich erhalten wurde. |
| AF_10063 | Client-Fachdienst-Nachrichtenempfang | Matrix CS API spec 8.5 "`PUT /_matrix/client/r0/rooms/{roomId}/state/{eventType}/{stateKey}`" | Start:<br>Beginn des Nachrichtenabrufs durch Client<br><br>Ende:<br>(erfolgreiche) Übermittlung der Nachricht an Client |
| AF_10062 | Fachdienst-Fachdienst-versendete PDUs | siehe Matrix Server-Server-API 4,<br>vgl. synapse Metrik:<br>`` `synapse_federation_client_sent_pdu_destinations:total` `` | Start:<br>Request an Empfangsserver<br><br>Ende:<br>(erfolgreiche) Übermittlung der Nachricht an Empfangsserver |
| AF_10062 | Fachdienst-Fachdienst-empfangene PDUs | siehe Matrix Server-Server-API 5.1,<br>vgl. synapse Metrik:<br>`` `synapse_federation_server_received_pdus` `` | Start:<br>Eingang des Requests am Empfangsserver |

| | | | |
|---|---|---|---|
| | | | Ende: (erfolgreiche) Übermittlung der Nachricht am Empfangsserver |

**Bestandsdaten**
Der TI-Messenger Fachdienst MUSS die nachfolgenden Informationen jeweils monatlich zum 01. des Monats in folgendem JSON Format als HTTP Body an die Betriebsdatenerfassung (BDE) gemäß gemSpec_SST_LD_BD liefern:
{
„Abfragezeitpunkt": <Zeitstempel der Abfrage als String im ISO 8601 Format>,
„CI_ID": <CI ID des abgefragten Fachdienstes gemäß TI-ITSM als String>,
„TIM-FD_Anzahl_Homeserver": <Anzahl der zum Abfragezeitpunkt instanziierten Homeserver>,
„TIM-FD_Anzahl_Organisationen": <Anzahl der zum Abfragezeitpunkt registrierten Organisationen>
„TIM-FD_Anzahl_Nutzer": <Anzahl der zum Abfragezeitpunkt registrierten Nutzer>,
„TIM-FD_Anzahl_aktNutzer": <Anzahl der zum Abfragezeitpunkt innerhalb des letzten Monats aktiven Nutzer>
}

Da bei dieser Lieferung keine Datei übermittelt wird, sondern der Text direkt im Body, ist für diese Lieferung die Angabe des filenames im HTTP Header gemäß [A_17112] (Tab_I_LogData_002 Operation I_LogData::fileUpload) in der gemSpec_SST_LD_BD NICHT notwendig.

**Service Monitoring**

Der TI-Messenger Anbieter MUSS das Service Monitoring der gematik technisch-organisatorisch unterstützen.

Dafür kann es z.B. notwendig sein, dass entsprechende Accounts auf Homeservern eingerichtet werden. Das Service Monitoring SOLL dabei zu keinen technischen Veränderungen an den Produkten führen.

# 5 Funktionsmerkmale

Im folgenden Kapitel wird der TI-Messenger-Fachdienst bezogen auf seine Teilkomponenten funktional beschrieben. Der TI-Messenger-Fachdienst ist die Kernkomponente des TI-Messenger-Dienstes. Dieser stellt alle Schnittstellen bereit, die für die Kommunikation innerhalb des TI-Messenger-Dienstes benötigt werden.

In der folgenden Abbildung ist der TI-Messenger-Fachdienst mit seinen Funktionsmerkmalen als Whitebox dargestellt:

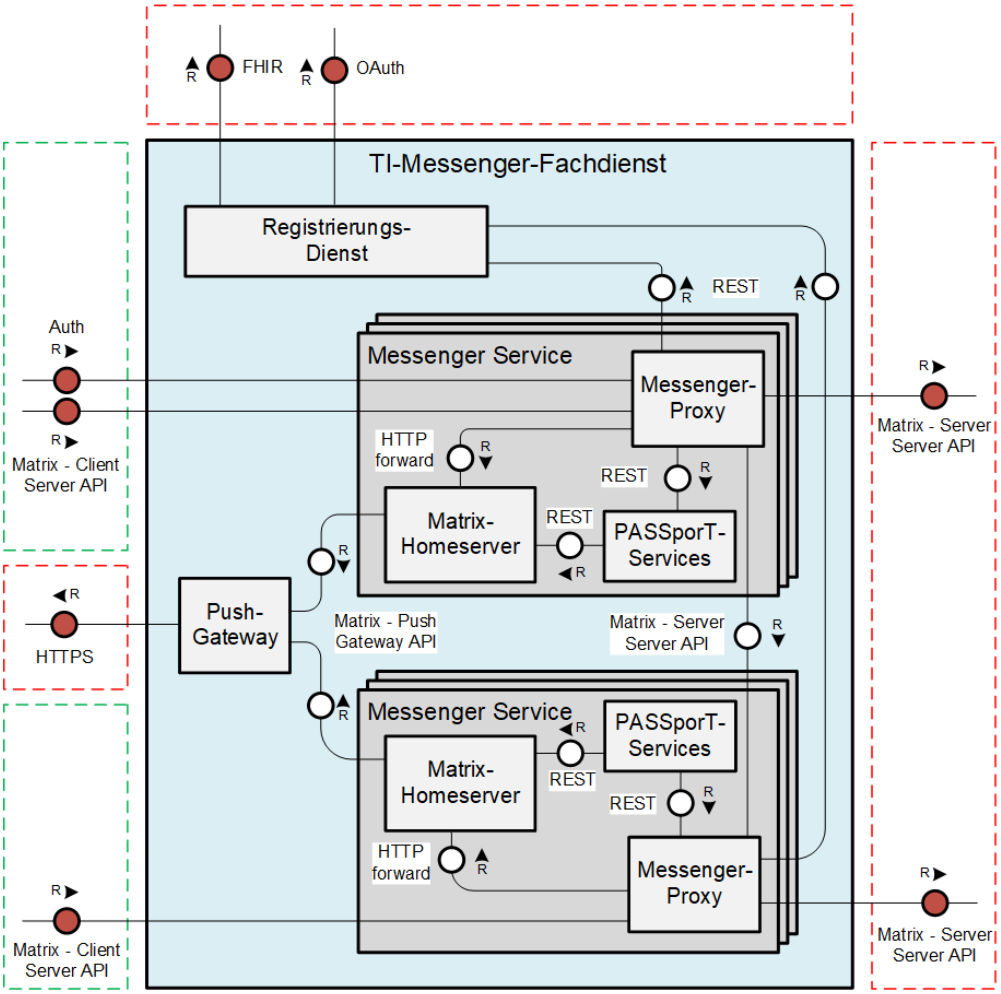


**Abbildung 3: Funktionaler Aufbau des TI-Messenger-Fachdienstes**

Die in der Abbildung grün dargestellten Boxen zeigen die Schnittstellen, die am TI-Messenger-Fachdienst aufgerufen werden. Rot dargestellte Boxen zeigen die Schnittstellen, über die der Fachdienst weitere Services anderer Komponenten nutzt. Eine Ausnahme bildet die Kommunikation zwischen den TI-Messenger-Fachdiensten. Hier wird die Kommunikation bilateral zwischen den zur Föderation gehörenden Fachdiensten realisiert.

## 5.1 Umsetzung der Matrix-API

Im folgenden Abschnitt wird für die zum TI-Messenger-Fachdienst gehörenden Komponenten, die Nutzung der von der Matrix-Foundation beschriebenen APIs dargestellt. Die jeweilige API MUSS vollständig und als RESTful API gemäß

- [Matrix Foundation#Server_Server],
- [Matrix Foundation#Client_Server],
- [Matrix Foundation#Push_Gateway]

umgesetzt werden.

Die Abbildung "*Matrix-API des Messenger Service*" zeigt die jeweils zu berücksichtigenden Schnittstellen bei den bereitzustellenden Komponenten (Server-Server API , Client-Server API, Push Gateway API) an.

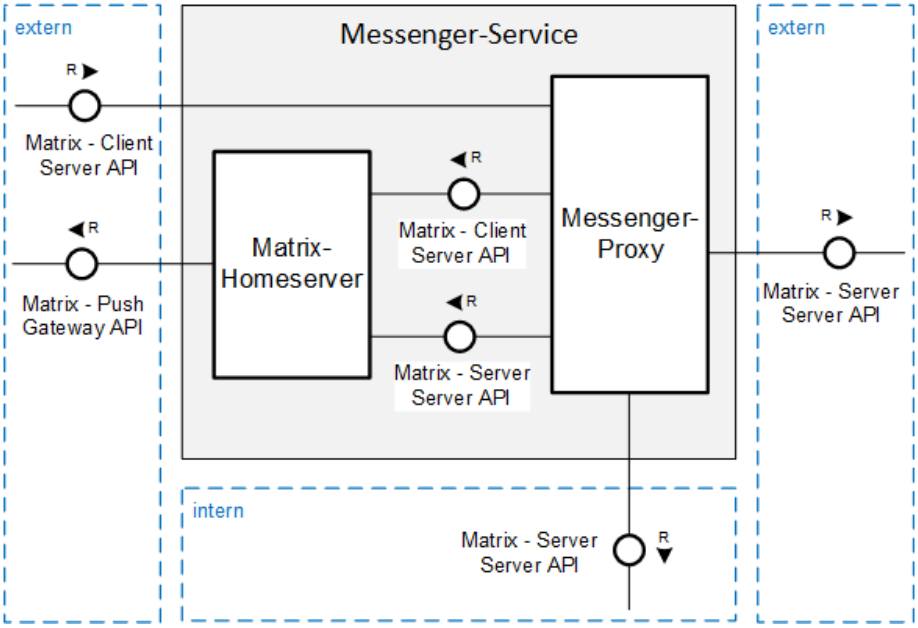


**Abbildung 4: Matrix-API des Messenger-Service**

Die Webservices der Matrix-Homeserver werden nicht direkt von den TI-Messenger-Clients aufgerufen. Der Aufruf der Client-Server-API am Matrix-Homeserver erfolgt über den Messenger-Proxy. Dieser leitet alle Aufrufe der TI-Messenger-Clients an den Matrix-Homeserver per HTTP-Forward weiter. Die Kommunikation der Matrix-Homeserver untereinander erfolgt ebenfalls über den Messenger-Proxy. Auch hier wird die Kommunikation durch Forwarding für die Matrix-Server-Server-Kommunikation zum Homeserver weitergeleitet. Zum Versenden von Push-Notifications nutzt der Matrix-Homeserver die Matrix-Push-Gateway-API des Push-Gateways.

Der Messenger-Proxy agiert neben der Funktion als Proxy zur Weiterleitung aller Server-Server-API- und Client-Server-API-Aufrufe an den Homeserver als Kontrollinstanz, um

für die Kommunikation notwendigen Rechte zu prüfen. Hierfür MUSS der Messenger-Proxy für alle Server-Server- und Client-Server-API-Endpunkte genutzt werden.

## 5.2 Funktionen der Systemkomponenten

Im folgenden Kapitel werden alle für den Betrieb des TI-Messenger-Fachdienstes notwendigen Komponenten funktional beschrieben.

### 5.2.1 Messenger-Service

#### 5.2.1.1 Matrix-Homeserver

Der Matrix-Homeserver MUSS die Matrix-Spezifikation vollständig umsetzen. Bereits existierende Produkte, die der Matrix Spezifikation folgen, können als Matrix-Homeserver verwendet werden, sofern die zusätzlichen vorausgesetzten MSCs:

- MSC3013: Encrypted Push
- MSC3359: Delayed Push
- Opportunistic Direct Push

implementiert wurden.

Der Matrix-Homeserver eines Messenger-Service:

- MUSS Anfragen vom eigenen Messenger-Proxy akzeptieren,
- DARF Anfragen anderere Messenger-Proxies nicht akzeptieren.

Die vom Matrix-Homeserver verwendeten Authentifizierungsverfahren MÜSSEN konfigurierbar sein. Beim Anmeldeversuch eines neuen TI-Messenger-Nutzers an einem Matrix-Homeserver MUSS dieser alle unterstützten Authentifizierungsverfahren zur Auswahl anbieten. Nach einer erfolgreichen Anmeldung eines TI-Messenger-Nutzers bei dem Matrix-Homeserver stellt dieser ein von ihm erstelltes Matrix-ACCESS_TOKEN sowie ein Matrix-OpenID-Token bereit. Das Matrix-ACCESS_TOKEN wird für jede weitere Autorisierung am Matrix-Homeserver verwendet. Das ausgestellte Matrix-OpenID-Token wird für eine spätere Authentisierung am FHIR-Proxy des VZD-FHIR-Directory verwendet und MUSS eine Gültigkeitsdauer von 30 Minuten aufweisen.

Im Folgenden ist eine Beispielkonfiguration eines Matrix-Homeservers dargestellt:

**Beispielkonfiguration eines Synapse Servers**

```
acme:
    bind_addresses:
    - '::'
    - 0.0.0.0
    enabled: false
    port: 80
    reprovision_threshold: 30
    url: https://acme-v02.api.letsencrypt.org/directory
alias_creation_rules:
```

```
-   action: allow
    alias: '*'
    user_id: '*'
allow_guest_access: false
app_service_config_files: []
autocreate_auto_join_rooms: true
bcrypt_rounds: 12
database:
    args:
        cp_max: 10
        cp_min: 5
        database: synapse
        host: /var/run/postgresql
        password: min_32_recommended
        user: synapse
    name: psycopg2
dynamic_thumbnails: false
enable_group_creation: true
enable_metrics: true
enable_registration: false
event_cache_size: 10K
expire_access_token: false
federation_rc_concurrent: 3
federation_rc_reject_limit: 50
federation_rc_sleep_delay: 500
federation_rc_sleep_limit: 10
federation_rc_window_size: 1000
form_secret: min_32_alphanumeric_recommended
key_refresh_interval: 1d
listeners:
-   bind_addresses:
    - '::'
    - 0.0.0.0
    port: 8008
    resources:
    -   compress: true
        names:
        - client
    -   compress: false
        names:
        - federation
    type: http
    x_forwarded: true
-   bind_addresses:
    - 0.0.0.0
    port: 9001
    type: metrics
log_config: /opt/synapse/log.config
macaroon_secret_key: min_32_alphanumeric_recommended
max_image_pixels: 32M
max_spider_size: 10M
max_upload_size: 23M
media_store_path: /opt/synapse/media_store
no_tls: true
old_signing_keys: {}
password_config:
    enabled: true
```

```
password_providers:
-   config:
        algorithm: HS512
        allow_registration: true
        require_expiracy: true
        secret: min_32_alphanumeric_recommended
    module: token_authenticator.TokenAuthenticator
perspectives:
    servers:
        matrix.org:
            verify_keys:
                ed25519:auto:
                    key: Noi6WqcDj0QmPxCNQqgezwTlBKrfqehY1u2FyWP9uYw
pid_file: /opt/synapse/synapse.pid
public_baseurl: https://matrix-client.meine-arztpraxis.hausaerzte-
berlin.de
push:
    include_content: false
rc_login:
    account:
        burst_count: 10
        per_second: 1
    address:
        burst_count: 100
        per_second: 10
rc_message_burst_count: 10.0
rc_messages_per_second: 0.2
# optional, for using synapse workers
redis:
    enabled: false
    host: redis_host
    password: min_128_alphanumeric_recommended
    port: 6379
registration_shared_secret: min_32_alphanumeric_recommended
report_stats: true
report_stats_endpoint: https://synapse-stats.gematik.de/push
room_prejoin_state:
    additional_event_types:
    - m.room.type
    - de.gematik.ti-messenger.passport
    disable_default_event_types: false
server_name: meine-arztpraxis.hausaerzte-berlin.de
signing_key_path: /opt/synapse/tls/meine-arztpraxis.hausaerzte-
berlin.de.signing.key
soft_file_limit: 0
thumbnail_sizes:
-   height: 32
    method: crop
    width: 32
-   height: 96
    method: crop
    width: 96
-   height: 240
    method: scale
    width: 320
-   height: 480
    method: scale
```

```
    width: 640
-   height: 600
    method: scale
    width: 800
tls_certificate_path: /opt/synapse/tls/meine-arztpraxis.hausaerzte-
berlin.de.crt
tls_fingerprints: []
tls_private_key_path: /opt/synapse/tls/meine-arztpraxis.hausaerzte-
berlin.de.key
track_appservice_user_ips: false
trusted_third_party_id_servers: []
turn_allow_guests: true
turn_shared_secret: min_64_recommended
turn_uris:
- turns:matrix-voip.tim-provider.de:3478?transport=udp
- turns:matrix-voip.tim-provider.de:3478?transport=tcp
turn_user_lifetime: 2h
uploads_path: /opt/synapse/uploads
url_preview_enabled: true
url_preview_ip_range_blacklist:
- 127.0.0.0/8
- 10.0.0.0/8
- 172.16.0.0/12
- 192.168.0.0/16
- 100.64.0.0/10
- 169.254.0.0/16
- ::1/128
- fe80::/64
- fc00::/7
url_preview_url_blacklist:
-   username: '*'
-   netloc: google.com
-   netloc: '*.google.com'
-   netloc: twitter.com
-   netloc: '*.twitter.com'
-   netloc: t.co
-   netloc: '*.t.co'
use_presence: true
```

**ML-123905 - Umsetzung von BSI-Vorgaben für Server (Produkt)**
Der TI-Messenger-Fachdienst SOLL den Vorgaben von [BSI-ISI-Server] folgen.
**[<=]**

**ML-123956 - Umsetzung von BSI-Vorgaben für Server (Anbieter)**
Der TI-Messenger-Anbieter SOLL den Vorgaben von [BSI-ISI-Server] folgen.
**[<=]**

### 5.2.1.2 Messenger-Proxy

Der Messenger-Proxy ist eine Kernkomponente der dezentralen Messenger-Services. Alle Anfragen der TI-Messenger-Clients und anderen Messenger-Services zum Matrix-

Homeserver MÜSSEN über den Messenger-Proxy geleitet werden. Die TLS-Kommunikation zwischen den TI-Messenger-Clients und den Matrix-Homeserver MUSS am Messenger-Proxy terminiert werden. Die Absicherung der TLS-Kommunikation MUSS durch eine einseitige Serverauthentisierung unter Nutzung eines X.509-Zertifikats erfolgen.

Die Kommunkation zwischen TI-Messenger-Client und Matrix-Homeserver erfolgt immer über den Messenger-Proxy (Forwarding). Der Messenger-Proxy MUSS sowohl als Reverse Proxy als auch als Forward Proxy fungieren. Alle eingehenden Kommunikationen MUSS der Messenger-Proxy an den Matrix-Homeserver weiterleiten. Eine Kommunikation vom Matrix-Homeserver zum TI-Messenger-Client und auch zu einem anderen Matrix-Homeserver bei einem anderen Messenger-Service MUSS über den Messenger-Proxy weitergeleitet werden.

Für alle Server-to-Server Anfragen (Anfragen, deren Pfad unter `/_matrix/federation` liegt) MUSS beim anfragenden Matrix-Homeserver im Messenger-Proxy geprüft werden, ob der Zielhomeserver der Anfrage Teil der Föderation ist. Hierfür MUSS MSC3383 ( https://github.com/matrix-org/matrix-doc/pull/3383) implementiert und das `destination`-Feld im `Authorization`-Header des HTTP Requests geprüft werden. Wenn der Server an der Föderation teilnimmt, darf der Request abgesendet werden, wobei eine Authentisierung des Zielhomeservers gemäß [Federation API#4.2] beschrieben mittels TLS Zertifikat durchgeführt werden muss. Für eingehende Server-to-Server Anfragen MUSS der Messenger-Proxy eine Authentisierung gemäß [Federation API#4.1] beschrieben durchführen. Sobald der Homeserver damit authentisiert wurde, MUSS validiert werden, dass der Homeserver an der Föderation teilnimmt.

Die Prüfung, ob ein Matrix-Homeserver an der Föderation teilnimmt, basiert auf der Domain. Eine Liste an aktuell verifizierten und zugelassenen Domains kann vom VZD-FHIR-Directory über den Registrierungs-Dienst angefragt werden. Wie die Domains vom Registrierungs-Dienst an die Messenger-Proxies verteilt werden ist nicht konkreter spezifiziert.

Beim Aufruf von 2 RESTful-Endpunkten auf den Matrix-Homeservern über den Messenger-Proxy prüft dieser Inhalte wie folgt:

### Invite-Endpunkt (Punkt 12 Server-Server API)

Der Messenger-Proxy MUSS Prüfregeln unterstützen. Hierfür agiert der Messenger-Proxy als eine Prüfinstanz, wie folgend beschrieben. Handelt es sich bei der Anfrage um ein `Invite-Event` MUSS der Messenger-Proxy folgende Prüfregeln anwenden:

- Der Messenger-Proxy MUSS prüfen, ob ein PASSporT vorhanden, gültig ist und auch für den einladenden Nutzer ausgestellt wurde. Das Zertifikat zur Prüfung des PASSporT erhält der Messenger-Proxy vom Registrierungs-Dienst. Der Registrierungs-Dienst ruft die Zertifikate vom VZD-FHIR-Directory ab.

Die Kommunikation zum Registrierungs-Dienst MUSS durch TLS abgesichert werden.

Im Folgenden wird ein Beispiel für einen `Invite-Event` gezeigt.

```
{
    "content": {
        "avatar_url": "mxc://example.org/SEsfnsuifSDFSSEF",
        "displayname": "Alice Margatroid",
        "membership": "invite"
    },
    "event_id": "$143273582443PhrSn:example.org",
    "origin_server_ts": 1432735824653,
    "room_id": "!jEsUZKDJdhlrceRyVU:example.org",
    "sender": "@orig:example.org",
    "state_key": "@dest:example.org",
    "type": "m.room.member",
    "unsigned": {
        "age": 1234,
        "invite_room_state": [
            {
                "content": {
                    "token": "<PASSporT>"
                },
                "sender": "@orig:example.org",
                "state_key": "@dest:example.org",
                "type": "de.gematik.ti-messenger.passport"
            },
            {
                "content": {
                    "join_rule": "invite"
                },
                "sender": "@orig:example.org",
                "state_key": "",
                "type": "m.room.join_rules"
            }
        ]
    }
}
```

**Profiles Endpunkt (Punkt 11.2 Client-Server API)**

Der Messenger-Proxy MUSS verhindern, dass Nutzer den eigenen Displaynamen ändern können. Der Displayname darf nur durch einen Nutzer in der Rolle *Org-Admin* geändert werden.

### 5.2.1.3 PASSporT-Service

Der PASSporT-Service des Messenger-Service stellt für einen Nutzer ein *Personal Assertion Token* (PASSporT) gemäß [RFC 8225] aus, wenn die Nutzung des PASSporT-Service des VZD-FHIR-Directory nicht möglich ist. Das ist z. B. der Fall, wenn der relevante Kommunikationspartner nicht im VZD-FHIR-Directory eingetragen ist. Welche Kommunikationsmöglichkeiten zwischen den jeweiligen Nutzer möglich sind wird in [gemSpec_TI-Messenger-Dienst#3.3] beschrieben.

In der folgenden Tabelle sind alle Ressourcen mit den jeweiligen HTTP-Methoden dargestellt. Die jeweilige Operation ist eine Abstraktion auf einen Webservice Endpunkt.

**Tabelle 4: Schnittstelle - PASSporT-Service**

| Operation | URI | Methode | Request | Response | Beschreibung |
|---|---|---|---|---|---|
| `get_passport` | /user/{mxid} | GET | string <MXID> | string <PASSporT> | liefert ein für den anfragenden Nutzer ausgestelltes PASSporT |

Es ist folgender Endpunkt zu verwenden:

```
 servers:
- GET /_matrix/client/unstable/de.gematik.tim.passport/user/{mxid}
```

Vor der Herausgabe des PASSporT durch den PASSporT-Service sind die Berechtigungen der beabsichtigten Teilnehmer zu prüfen. Dies betrifft zum einen die Berechtigung eines Nutzers die beabsichtigte Kommunikationsbeziehung aufzubauen und zum anderen, ob die übergebene MXID eines Nutzers einen in der Föderation enthaltenen Messenger-Service ausweist. Sollte es bei der Prüfung zu einem Fehler kommen, MÜSSEN die folgenden Fehlercodes verwendet werden.

**Tabelle 5 Error-Code PASSporT-Service**

| Error-Code | Beschreibung |
|---|---|
| 403 Forbidden | der Nutzer ist nicht berechtigt ein PASSporT für den `Invite` auszulösen |
| 404 Not Found | die übergebe MXID ist nicht von einem Nutzer innerhalb der Föderation |
| 503 Service Unavailable | der PASSporT-Service ist nicht erreichbar |
| 500 Internal Server Error | interner Server Error |

### Aufbau des PASSporT

Der Aufbau des PASSporT MUSS wie im [RFC 8225] beschrieben erfolgen. Die Befüllung der gezeigten Header Elemente MUSS wie im [RFC 8225] gefordert erfolgen und wie folgt aufgebaut sein:

```
Header:
   {
      "typ":"passport",
      "alg":"ES256",
      "x5u":"https://cert.example.org/passport.cer"
   }
```

Das Erstellen des PASSporT MUSS durch den PASSporT-Service des beabsichtigten Kommunikationspartners erfolgen. Die TI-Messenger-spezifischen PASSporT-Claims sind durch den PASSporT-Service wie folgt zu befüllen. Der Claim mit dem Bezeichner "orig" ist die MXID des Nutzers, der das`invite` auslösen wird. Diese MXID wird durch den Nutzer an den gewünschten Kommunikationspartner übergeben. Der Claim "dest" wird mit der MXID des damit einzuladenden Nutzers befüllt. Das folgende Beispiel zeigt eine solche Struktur.

```
Claims:
  {
      "orig": {
          "uri": "matrix:u/me:example.org"
      },
      "dest": {
          "uri": [
             "matrix:u/you:example.org"
          ]
      }
  }
```

Das erzeugte PASSporT wird durch den PASSporT-Service mit einem Zertifikat aus der Komponenten PKI der TI signiert und anschließend an den TI-Messenger Client übergeben, der das `invite` auslöst. Die Zertifikate haben die keyUsage = digitalSignature.

Zur besseren Veranschaulichung dient die folgende Darstellung:

**Tabelle 6: Ablauf PASSporT-Erstellung**

| Client A | Client B |
|---|---|
| 1: Client A übergibt seine MXID an den Client B | |
| | 2: Client B nimmt MXID von A und übergibt diese an den PASSporT-Service seines Messenger-Service `<get_passport>` |

| | |
|---|---|
| | 3: PASSporT-Service von B erzeugt PASSporT mit:<br>„dest“: MXID von Nutzer B<br>„Orig“: MXID von Nutzer A |
| | 4: PASSporT wird von B an den Client A übergeben |
| 5: Nutzer A löst invite an Nutzer B aus | |

### 5.2.2 Registrierungs-Dienst

Der Registrierungs-Dienst MUSS ein Frontend oder Schnittstellen bereitstellen, damit ein interoperabler Onboarding-Prozess für die Registrierung von Messenger-Services gewährleistet wird. Der Registrierungs-Dienst MUSS es ermöglichen einen neuen Messenger-Service über ein Frontend zu erzeugen. So MUSS der Registrierungs-Dienst bei einer neuen Registrierungsanfrage automatisiert den durch den Smartcard IDP-Dienst ausgestellten ACCESS_TOKEN (gemäß Kapitel 4.2.1) validieren, einen dezentralen Messenger-Service automatisiert starten und die entsprechende Matrix-Domain (referenziert zur im Claim genannten Organisation) im VZD-FHIR-Directory hinterlegen.

Für die Aufnahme eines TI-Messenger-Fachdienstes in die Föderation des TI-Messenger-Dienstes wird durch den Registrierungs-Dienst die Matrix Domain einer Organisation in das VZD-FHIR-Directory eingetragen. Der Registrierungs-Dienst eines TI-Messenger-Fachdienst MUSS sich gegenüber dem VZD-FHIR-Directory mittels OAuth2 Client Credentials Flow authentifizieren und ebenfalls als Anbieter auf dem VZD-FHIR-Directory gelistet sein. Der Registrierungs-Dienst MUSS die Domains der dezentralen Messenger-Services, referenziert auf die entsprechende Organization-Ressource als Endpoint hinterlegen. Genauere Angaben sind im VZD-FHIR-Directory Datenmodell zu finden.

Der Registrierungs-Dienst MUSS eine Liste aller verifizierten Domains aus dem VZD-FHIR-Directory für die dezentralen Messenger-Proxies bereitstellen. Dazu wird die im VZD-FHIR-Directory bereitgestellte Operation `GET/FederationList` aufgerufen. Um die Schnittstelle nutzen zu können MUSS sich der Registrierungs-Dienst des TI-Messenger-Anbieters, wie bereits oben erwähnt, mit einem Accesstoken authentisieren, das vom OAuth-Server des VZD-Anbieters ausgestellt wurde. Mit der Operation `GET/FederationList` MUSS die Liste der an der TI-Messenger-Föderation beteiligten Matrix-Domainnamen abgefragt werden. Die Abfrage der `FederationList` MUSS mindestens einmal am Tag erfolgen. Die Prüfung auf Aktualität dieser Föderationsliste beim VZD-FHIR-Directory MUSS bei jeder Anfrage durch einen Matrix-Proxy zur Bereitstellung der Föderationsliste erfolgen. Nach dem Erhalt dieser Liste MUSS diese durch den Messenger-Proxy für die Prüfung der Domainzugehörigkeit genutzt werden. Der Registrierungs-Dienst MUSS für den Abruf dieser `FederationList` durch die Messenger-Proxy eine Schnittstelle bereitstellen. Als Ergebnis erhält der Registrierungs-Dienst eine Liste der hashes der an der Föderation beteiligten Domainnamen.

Vor der Ausgabe eines PASSporT durch den PASSporT-Service im VZD-FHIR-Directory wird dieser vom PASSporT-Service signiert. Der Registrierungs-Dienst des TI-Messenger-Fachdienstes MUSS für die Prüfung der Gültigkeit dieser Signatur durch die Messenger-Proxies die dafür benötigten Zertifikate mit dem öffentlichen Schlüssel des PASSporT-Services im VZD-FHIR-Directory über die Operation `GET/PASSporTCertificate` vom VZD-FHIR-Directory abfragen und für die spätere Nutzung durch die Messenger–

Proxies abspeichern. Der Registrierungs-Dienst MUSS für den Abruf dieses `PASSporTCertificate` durch die Messenger–Proxies eine Schnittstelle bereitstellen.

### 5.2.3 Push-Gateway

Der TI-Messenger-Fachdienst MUSS einen Push-Gateway, gemäß Matrix-Spezifikation, für den TI-Messenger-Client bereitstellen. Es obliegt den TI-Messenger-Anbietern der einzelnen TI-Messenger-Clients, ob eine Push-Funktion unterstützt wird.

# 6 Anhang A – Verzeichnisse

## 6.1 Abkürzungen

| Kürzel | Erläuterung |
|---|---|
| API | Application Programming Interface |
| AuthN | Authentication |
| AuthZ | Authorization |
| CC | Common Criteria |
| DSGVO | Datenschutz-Grundverordnung |
| FHIR | Fast Healthcare Interoperable Resources |
| HBA | Heilberufsausweis |
| HTTP | Hyptertext Transfer Protocol |
| IDP | Identity Provider |
| JSON | JavaScript Object Notation |
| KVNR | Krankenversichertennummer |
| MSC | Matrix Spec Change |
| MXID | Matrix-ID |
| OAuth | Open Authorization |
| PASSporT | Personal Assertion Token |
| SMC-B | Institutionenkarte (Security Module Card Typ B) |
| SSSS | Secure Secret Storage and Sharing |
| TI | Telematikinfrastruktur |
| TLS | Transport Layer Security |
| UIA | User Interactive Authorization |

| | |
|---|---|
| VZD | Verzeichnisdienst |

## 6.2 Glossar

| Begriff | Erläuterung |
|---|---|
| MXID | Eindeutige Identifikation eines TI-Messenger-Nutzers (Matrix-User-ID) |
| on-premise | Das Produkt wird auf eigener oder gemieteter Hardware betrieben |
| Relying Party | Vertraurungswürdige Komponente, die Zugriff auf eine sichere Anwendung ermöglicht |
| X.509-Zertifikat | Ein Public-Key-Zertifikat nach dem X.509-Standard |

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

## 6.3 Abbildungsverzeichnis



## 6.4 Tabellenverzeichnis

## 6.5 Referenzierte Dokumente

### 6.5.1 Dokumente der gematik

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

| [Quelle] | Herausgeber: Titel |
|---|---|
| [gemGlossar] | gematik: Einführung der Gesundheitskarte – Glossar |
| [gemKPT_TI_Messenger] | gematik: Konzeptpapier TI-Messenger |
| [gemSpec_TI_Messenger-Dienst] | gematik: Spezifikation TI-Messenger-Dienst |
| [gemKPT_Betr] | gematik: Betriebskonzept Online-Produktivbetrieb |
| [gemSpec_Perf] | gematik: Übergreifend Spezifikation Performance und Mengengerüst TI-Plattform |
| [gemSpec_Krypt] | gematik: Übergreifende Spezifikation Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur |
| [gemSpec_IDP_FD] | gematik: Spezifikation Identity Provider – Nutzungsspezifikation für Fachdienste |

### 6.5.2 Weitere Dokumente

| [Quelle] | Herausgeber (Erscheinungsdatum): Titel |
|---|---|
| [Matrix Foundation] | Matrix Foundation<br>https://matrix.org/docs/spec/ |
| [Federation API] | Matrix Foundation<br>https://matrix.org/docs/spec/server_server/r0.1.4 |
| [RFC 8225] | PASSporT: Personal Assertion Token<br>https://datatracker.ietf.org/doc/html/rfc8225 |

| | |
|---|---|
| [OpenID] | OpenID Foundation<br>https://openid.net/developers/specs/ |
| [OWASP Proactive Control] | OWASP Proactive Controls<br>https://owasp.org/www-project-proactive-controls/ |
| [MSC 3013] | https://github.com/matrix-org/matrix-doc/pull/3013 |