Elektronische Gesundheitskarte und Telematikinfrastruktur

Spezifikation
TI-Messenger-Fachdienst

Version:	1.0.6
Revision:	457305
Stand:	04.05.2022
Status:	in Bearbeitung
Klassifizierung:	öffentlich_Entwurf
Referenzierung:	gemSpec_TI-Messenger-FD

Dokumentinformationen

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

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

Änderungen zur Vorversion

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

Dokumentenhistorie

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
1.0.0	01.10.2021		Erstversion des Dokumentes	gematik
1.0.5	14.04.2022		Arbeitsversion zur Information	gematik
1.0.6	04.05.2022		Arbeitsversion zur Information	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 zwischen verschiedenen Akteuren im deutschen Gesundheitswesen. Dieser 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 TI-Messenger-Anbieter bereitstellen MUSS. Bei den dezentralen Teilkomponenten handelt es sich um die Messenger-Services. Ein Messenger-Service besteht aus einem Matrix-Homeserver und den Teilkomponenten Messenger-Proxy und PASSporT-Service, welche dafür sorgen, dass eine Föderation der Matrix-Homeserver nur zwischen verifizierten Domains stattfindet. Messenger-Services werden für einzelne Organisationen (z. B. Leistungserbringerinstitutionen, Verbände) bereitgestellt und erlauben die Nutzung durch alle berechtigten Akteure 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 diese Leistungserbringer notwendiges Authentifizierungsverfahren an.

Die Kommunikation zwischen einem TI-Messenger-Client und einem TI-Messenger-Fachdienst erfolgt immer über den Messenger-Proxy der Messenger-Services. Am Messenger-Proxy eines Messenger-Service findet zunächst die TLS-Terminierung der Verbindungen von den TI-Messenger-Clients statt. Der Messenger-Proxy kontrolliert die Zugehörigkeit zur TI-Föderation durch den Abgleich mit einer durch seinen Registrierungs-Dienst bereitgestellten Föderationsliste. Hierbei prüft der Messenger-Proxy, ob die beteiligten Matrix-Homeserver registrierte Mitglieder der Föderation sind und ein Teilnehmer berechtigt ist, Requests auf dem Matrix-Homeserver auszulösen.

Neben den dezentralen Messenger-Services besteht ein TI-Messenger-Fachdienst aus den zentralen Teilkomponenten Registrierungs-Dienst und Push-Gateway. Über den Registrierungs-Dienst bekommt der TI-Messenger-Anbieter die Möglichkeit Messenger-Services automatisiert Organisationen zur Verfügung zu stellen und die Matrix-Domain der von ihm bereitgestellten Messenger-Services in deren Organisationsressource in das zentrale VZD-FHIR-Directory einzutragen. Der Registrierungs-Dienst eines TI-Messenger-Fachdienstes bietet als weitere Funktion die Bereitstellung einer Föderationsliste für die Messenger Proxys-seiner Messenger-Services. Das Push-Gateway dient zur Übertragung von Benachrichtigungen (Notifications) an die jeweiligen TI-Messenger-Clients um den Eingang einer neuen Nachricht zu signalisieren.

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

vereinfachter Form dargestellt. Der in der Abbildung blau dargestellte TI-Messenger-Fachdienst zeigt alle Komponenten die in dieser Spezifikation beschrieben werden.

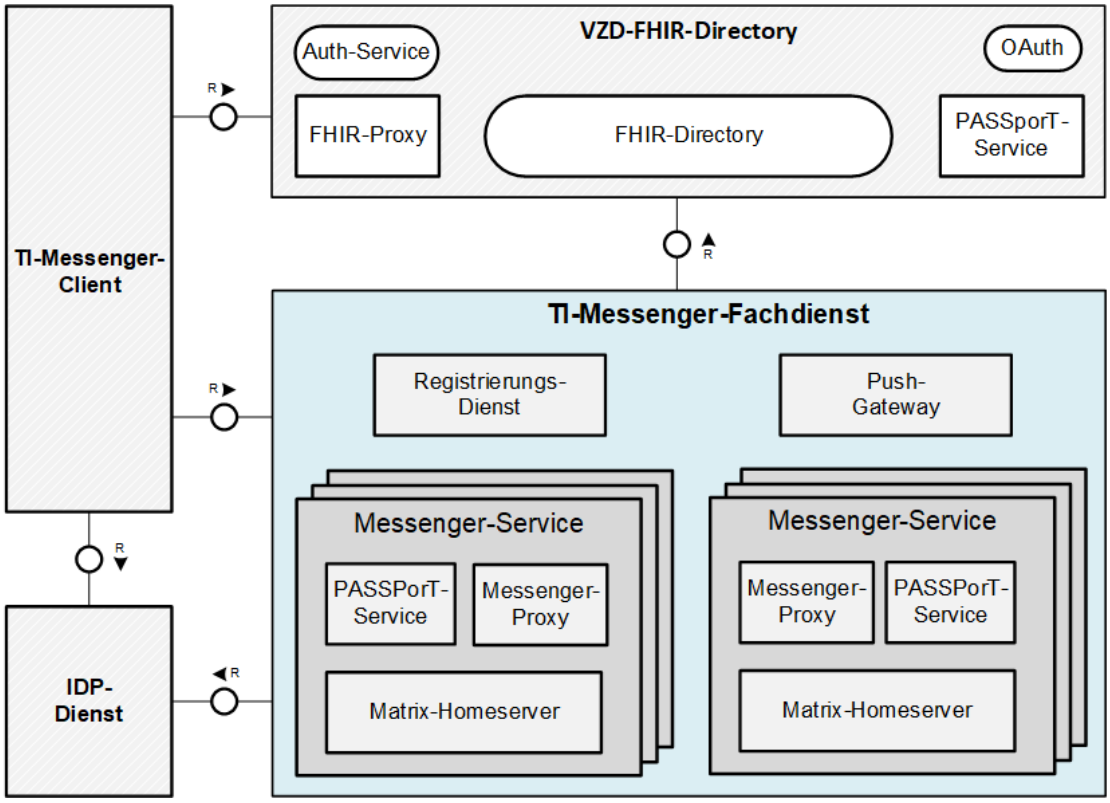


Abbildung 1: Systemüberblick (Vereinfachte Darstellung)

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 gehören zugelassene IDP-Dienste welche Authentisierungen und Autorisierungen auf Basis von SmartCard Identitäten durchführen, sowie das VZD-FHIR-Directory. Die in Kapitel 2 zu findende Abbildung *"Systemüberblick"* zeigt deren Beziehung zum TI-Messenger-Fachdienst.

Ein IDP-Dienst stellt allen berechtigten Akteuren ID_TOKEN, gemäß des durch die OpenID Foundation [OpenID] spezifizierten Protokolls, zur Verfügung. Dieses wird vom Auth-Service des VZD-FHIR-Directory verwendet, um ein `owner-accesstoken` oder ein `tim-search-accesstoken` für den Lese- bzw. Schreibzugriff auf das FHIR-Directory zu erhalten.

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 Registrierungs-Dienst des TI-Messenger-Fachdienst trägt bei erfolgreicher Verifizierung einer Organisation die Matrix-Domain des zugehörigen Messenger-Services der Organisation im VZD-FHIR-Directory (in die Organisationsressource des TI-Messenger-Anbieters) ein. Durch diesen Eintrag KANN der Messenger-Service an der Föderation des TI-Messenger-Dienstes teilnehmen. 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 der Messenger-Services erfolgt über den Registrierungs-Dienst eines TI-Messenger-Anbieters dezentral und kann *on-premise* innerhalb von Rechenzentren stattfinden. Jeder Messenger-Service MUSS einer Organisation zugeordnet sein. Die Messenger-Services unterscheiden sich lediglich durch die je Organisation verwendeten Authentifizierungsverfahren. Diese werden durch die jeweilige Organisation festgelegt und bereitgestellt, und ermöglichen damit die Nachnutzung bereits innerhalb der Organisation existierender Authentifizierungsverfahren. Die jeweilige Organisation MUSS die Kontrolle über die Benutzerverwaltung haben, um zu jedem Zeitpunkt Nutzer aus dem TI-Messenger ausschließen zu können. Dabei MÜSSEN Akteure 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 zum Beispiel bereits Systeme wie Active-Directory oder LDAP basierende Nutzerverzeichnisse innerhalb einer Organisation verfügbar, können diese entsprechend genutzt werden, indem der jeweilige 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.

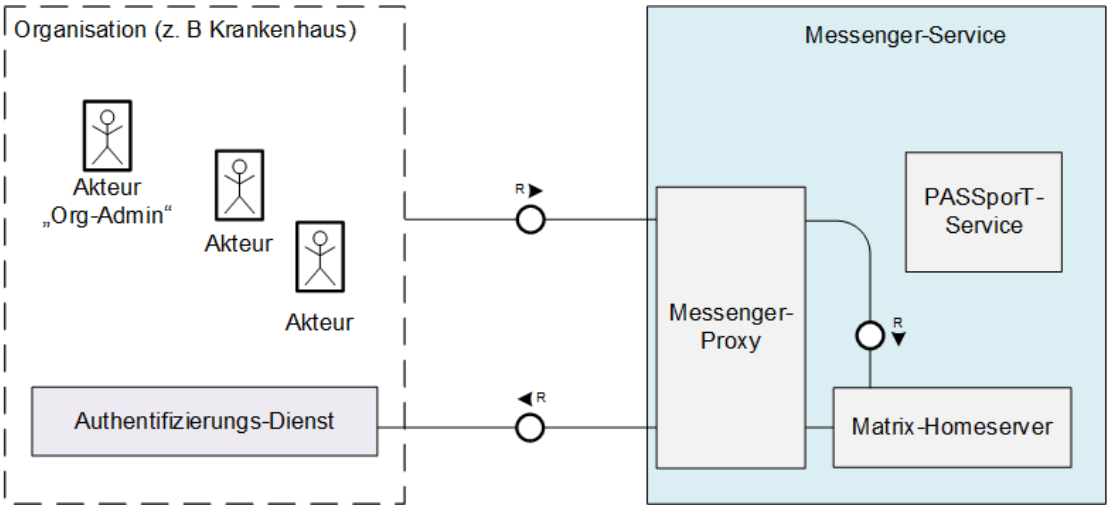


Abbildung 2: Beispiel - Authentifizierung von Nutzern einer Organisation

4 Übergreifende Festlegungen

4.1 Datenschutz und Sicherheit

A_22807 - 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.

[<=]

A_22808 - 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.

[<=]

A_22809 - 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 gemäß [gemSpec_Krypt].

[<=]

A_22810 - 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.

[<=]

A_22811 - Löschfristen für Homeserver

Betreiber MÜSSEN sicherstellen, dass ihre Homeserver eine Funktion anbieten, durch die Events, Gesprächsinhalten und mit einzelnen Gesprächen assoziierte Daten (z. B. versandte Dateien) nach einem Zeitraum von 6 Monaten seit letzter Aktivität in einem Raum gelöscht werden. Betreiber müssen sicherstellen, dass der Zeitraum durch den Kunden konfigurierbar ist. Diese Funktion DARF über Opt-Out durch den Kunden deaktivierbar sein.

[<=]

A_22812 - 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.
[<=]

A_22813 - 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.
[<=]

A_22814 - 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.
[<=]

A_22815 - Behandlung von kryptographischem Material für OAuth
Betreiber von TI-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.

Hinweis: Es ist lediglich ein HSM je Messenger-Anbieter notwendig. Die Verwendung von HSM-Modulen wird für die Lagerung von kryptographischem Material bei den Fachdiensten vorgeschrieben. Sofern eine Mandantentrennung gewährleistet werden kann, ist es nicht

erforderlich, mehrere getrennte HSM-Umgebungen zu betreiben.

A_22816 - 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.
[<=]

A_22817 - Explizites Verbot von Profiling für TI-Messenger-Fachdienste
~~Betreiber~~Hersteller 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 ~~Betreiber~~Hersteller 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.
[<=]

A_22818 - 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].
[<=]

A_22819 - 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-Client des Nutzers und den ggf. genutzten Backend-Diensten der zusätzlichen Funktionen inklusive ihrer Sicherheitsmaßnahmen und
- die Sicherheitsannahmen an den TI-Messenger-Client des Nutzers und die Ausführungsumgebung.

[<=]

A_22820 - 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 Organisations-Administratoren von Homeservern unter Kundenverwaltung informieren, dass im Room-State sichtbare Informationen gegenwärtig nicht verschlüsselt sind.

[<=]

4.2 Authentifizierung

Für die Teilnahme am TI-Messenger-Dienst MUSS sich eine Organisation am Registrierungs-Dienst registrieren. Ein Akteur in der Rolle "Org-Admin" MUSS sich hierfür über das vom TI-Fachdienst-Anbieter bereitgestellte Frontend seines Registrierungs-Dienstes mit der Identität (SMC-B) der Organisation gegenüber dem Registrierungs-Dienst authentifizieren.

Damit Akteure Ad-Hoc-Nachrichten austauschen können, MÜSSEN sich diese an ihrem Messenger-Service authentifizieren. Die Authentifizierung MUSS hierbei über OpenID-Connect oder über ein zwischen der Organisation und dem Fachdienst-Anbieter vereinbartes Authentifizierungsverfahren erfolgen. Haben sich Akteure erfolgreich an ihrem Messenger-Service authentifiziert, erhalten sie ein von ihrem Homeserver ausgestelltes Matrix-Access-Token, welches für die spätere Authentifizierung des TI-Messenger-Clients verwendet wird.

4.2.1 IDP-Dienst

Der zentrale IDP-Dienst der gematik wird benötigt um den Komponenten TI-Messenger-Client sowie den Registrierungs-Diensten Schreibzugriff auf das VZD-FHIR-Directory zu ermöglichen. Hierfür MUSS der TI-Messenger-Client sowie der jeweilige Registrierungs-Dienst am zugelassenen IDP-Dienst der gematik gemäß [gemSpec_IDP_FD] registriert sein. Diese Komponenten MÜSSEN den ausgestellten Security Tokens (ID_TOKEN) dieses IDP-Dienst vertrauen.

Im Rahmen der Registrierung des VZD-FHIR-Directory am IDP-Dienst werden notwendige Claims

für das ID_TOKEN (bestätigte Identifikationsmerkmale für den Akteur) festgelegt. Der Anbieter des TI-Messenger-Fachdienstes MUSS über einen organisatorischen Prozess beim zugelassenen IDP-Dienst folgende Claims im ID_TOKEN vereinbaren:

Tabelle 1: Inhalte der Claims für SMC-B/HBA

Leistungserbringerinstitutionen (SMC-B)	Leistungserbringer (HBA)
• ProfessionOID • idNummer • organizationName • acr • aud	• ProfessionOID • idNummer • given_name • family_name • acr • 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.

4.2.2 Verwaltung der Nutzersession

Die Verwaltung der Nutzersession MUSS wie 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 Hostnamen und einem optionalen Port besteht. Weitere Informationen finden sich in [Server-Server API#Server discovery].

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, der Testspezifikationen, der Testfälle und 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 zeitnaher IOP-Tests, die Synchronisierung von Meilensteinen und regelmäßigen 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 bereitge stellt 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 *2* : 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 Ende: Übermittlung Matrix-OpenID-Token

AF_10060	Messenger-Service bereitstellen	Registrierungs-Dienst, Messenger-Service	Start: AuthZ, Erstelle Messaging-Service Ende: Account Daten wurden übermittelt
AF_10061	TI-Messenger Remote Invite	Homeserver A, Messenger-Proxy A, Homeserver B, Messenger-Proxy B	Start Provider A: Eingang Request von Client A: Invite User B + PASSporT Ende: Ausgang Request an Provider B: Invite User B + PASSporT Start Provider B: Eingang Request von Provider A: Invite User B + PASSporT Ende: Versand Invite Request an Client B
AF_10062	Message senden (Remote)	Homeserver A, Messenger-Proxy A, Homeserver B, Messenger-Proxy B	Start Provider A: Eingang Request von Client A Ende: Ausgang Request an Provider B Start Provider B: Eingang Request von Provider A Ende: 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: Eingang Request am Homeserver vom Client. Ende: 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}/`	Start: Beginn des Nachrichtenabrufs durch

		`state/{eventType}/{stateKey}"`	Client Ende: (erfolgreiche) Übermittlung der Nachricht an Client
AF_10062	Fachdienst-Fachdienst-versendete PDUs	siehe Matrix Server-Server-API 4, vgl. synapse Metrik: `` `synapse_federation_client_sent_pdu_destinations:total` ``	Start: Request an Empfangsserver Ende: (erfolgreiche) Übermittlung der Nachricht an Empfangsserver
AF_10062	Fachdienst-Fachdienst-empfangene PDUs	siehe Matrix Server-Server-API 5.1, vgl. synapse Metrik: `` `synapse_federation_server_received_pdus` ``	Start: 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 und Außenschnittstellen als Whitebox dargestellt:

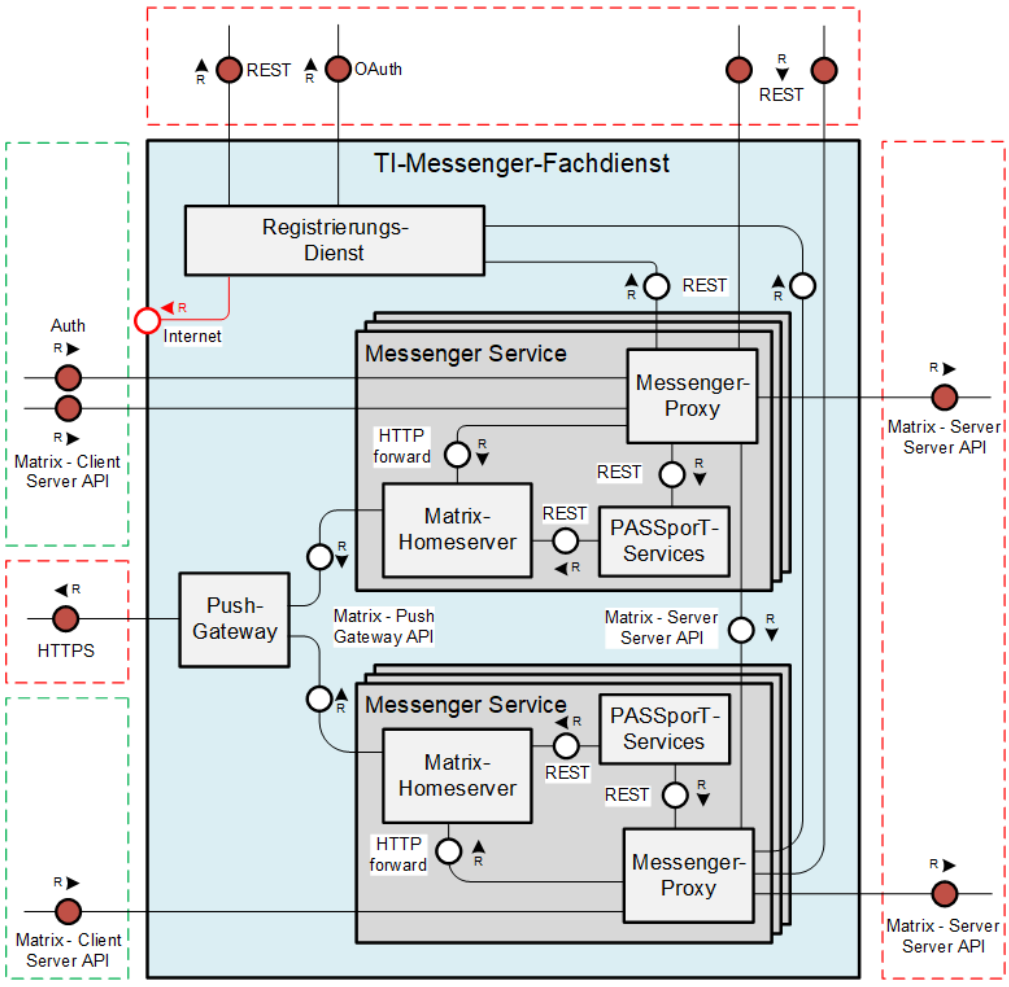


Abbildung 3: Funktionaler Aufbau des TI-Messenger-Fachdienstes

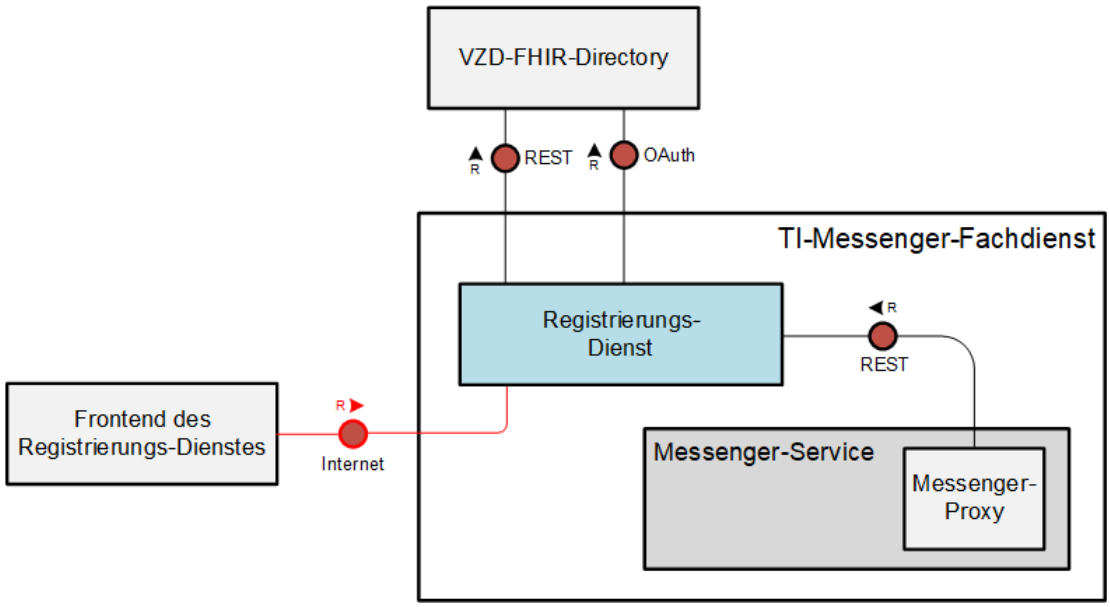
Die in der Abbildung grün dargestellten Boxen zeigen die Schnittstellen, die am TI-Messenger-Fachdienst aufgerufen werden. Rot dargestellte Boxen zeigen die Schnittstellen, über die der Fachdienst weitere Services anderer Komponenten nutzt. Eine Ausnahme bildet die Kommunikation zwischen den TI-Messenger-Fachdiensten. Hier wird die Kommunikation bilateral zwischen den zur TI-Föderation gehörenden Fachdiensten realisiert. Die in der Abbildung rot dargestellte Linie vom Registrierungs-Dienst zum Internet zeigt die vom Frontend des Registrierungs-Dienstes verwendete Schnittstelle. Diese wird nicht normativ von der gematik definiert. Die Ausgestaltung obliegt dem jeweiligen TI-Messenger-Anbieter.

5.1 Funktionen der Systemkomponenten

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

5.1.1 Registrierungs-Dienst

Der Registrierungs-Dienst bietet zwei Schnittstellen an, wobei die Schnittstelle für das Frontend des Registrierungs-Dienstes nicht durch die gematik normativ definiert wird. In der folgenden Abbildung sind die Schnittstellen des Registrierungs-Dienst dargestellt:



Administration

Der TI-Messenger-Fachdienst MUSS eine Schnittstelle für die Administration am Registrierungs-Dienstes bereitstellen. Dies ist notwendig, damit ein Onboarding-Prozess für die Registrierung von

Messenger-Services gewährleistet wird. Der Registrierungs-Dienst MUSS es ermöglichen einen neuen Messenger-Service über ein Frontend des Registrierungs-Dienstes zu erzeugen. Die Ausgestaltung des Frontends sowie der Schnittstelle am Registrierungs-Dienst ist dem jeweiligen TI-Messenger-Anbieter überlassen. Der Registrierungs-Dienst MUSS bei einer neuen Registrierungsanfrage automatisiert den durch den zuständigen IDP-Dienst ausgestellten ID_TOKEN (gemäß Kapitel "IDP-Dienst") validieren. Bei der Validierung MUSS der Registrierungs-Dienst die im ID_TOKEN enthaltene ProfessionOID gegen die in der Tabelle "" geli steten OIDs gemäß [gemSpec_OID] prüfen. Nach erfolgreicher Validierung MUSS der Registrierungs-Dienst einen dezentralen Messenger-Service automatisiert starten und die ihn der Registrierungsanfrage übergebene Matrix-Domain in eine Organisations-Ressource dieser Organisation (HealthcareService) im VZD-FHIR-Directory hinterlegen.

Nach erfolgreicher Authentifizierung einer Organisation MUSS ein Admin-Account für den "Org-Admin" der Organisation auf dem Registrierungs-Dienst angelegt werden. Für die Authentifizierung des Akteurs in der Rolle "Org-Admin" MUSS eine 2-Faktor-Authentifizierung verwendet werden.

Messenger-Service in die TI-Föderation aufnehmen

Für die Aufnahme eines Messenger-Services eines TI-Messenger-Fachdienstes in die Föderation des TI-Messenger-Dienstes, wird durch den Registrierungs-Dienst die vom Frontend des Registrierungs-Dienstes übergebene Matrix-Domain einer Organisation in den Endpoint der Organisations-Ressource (HealthcareService) im Attribut `address="Matrix-Domain"` eintrage n. Hierfür MUSS sich zuvor der Registrierungs-Dienst eines TI-Messenger-Fachdienstes gegenüber dem VZD-FHIR-Directory mittels OAuth2 Client Credentials Flow authentifizieren. Die dafür notwendigen Client-Credentials MUSS der TI-Messenger-Anbieter für seinen Registrierungs-Dienst beim VZD-FHIR-Directory-Anbieter beantragen. Die Beantragung erfolgt über einen Service-Request an betrieb@gematik.de und MUSS im Betreff "VZD-FHIR-Directory (De-)/Registrierung" enthalten.

Bereitstellung der Föderationsliste

Der Registrierungs-Dienst MUSS eine Liste aller verifizierten Domains des VZD-FHIR-Directory vorhalten und diese den dezentralen Messenger-Proxies über eine Schnittstelle bereitstellen. Daz u MUSS die am FHIR-Proxy des VZD-FHIR-Directory bereitgestellte Operation `GET/Federatio nList` aufgerufen werden. Um die Schnittstelle nutzen zu können MUSS sich der Registrierungs-Dienst des TI-Messenger-Anbieters, mit einem `admin-accesstoken` authentisieren, das vom OAuth-Server des VZD-Anbieters ausgestellt wird. Die Abfrage der Föderationsliste MUSS mindestens einmal am Tag erfolgen. Die Prüfung auf Aktualität dieser Föderationsliste beim FHIR-Proxy des 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. Inhalt der

Föderationsliste sind die hashes aller an der Föderation beteiligten Domainnamen. Der Registrierungs-Dienst MUSS für den Abruf der Föderationsliste durch die Messenger-Proxy eine REST-Schnittstelle bereitstellen. In der folgenden Tabelle ist die Ressourcen mit der jeweiligen HTTP-Methoden für die REST-Schnittstelle dargestellt. Die Operation ist eine Abstraktion auf einen Webservice Endpunkt.

Tabelle 3 Operation vom Registrierungs-Dienst

Operation	URI	Methode	Request	Response	Beschreibung
`getFederationList`	/FederationList/	GET	-	JSON	Liefert die Föderationsliste als JSON-Objekt

Es ist folgender Endpunkt zu verwenden:

```
servers:

- GET /_matrix/client/{version}/de.gematik.tim.passport/user/{mxid}
```

Der Registrierungs-Dienst MUSS die REST-Schnittstelle durch Verwendung von TLS mit serverseitiger Authentisierung sichern.

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 die eines Akteurs innerhalb der Föderation
503 Service Unavailable	der PASSporT-Service ist nicht erreichbar
500 Internal Server Error	interner Server Error

5.1.2 Messenger-Service

Ein Messenger-Service besteht aus den drei Teilkomponenten Matrix-Homeserver, Messenger-Proxy und einem PASSporT-Service und basiert auf dem offenen Kommunikationsprotokoll Matrix. Welche APIs der Matrix-Spezifikation im Messenger-Service nachgenutzt werden, ist in der folgende Abbildung dargestellt:

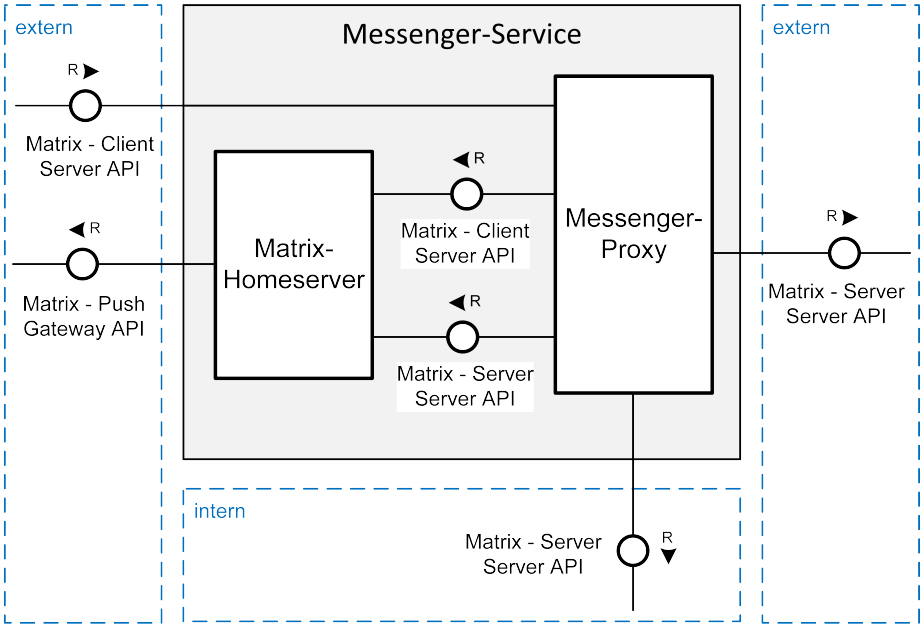


Abbildung 4: Matrix-API des Messenger-Service

Die Abbildung "*Matrix-API des Messenger Service*" zeigt die jeweils zu berücksichtigenden Schnittstellen der Matrix-API (Server-Server API , Client-Server API und Push Gateway API). Das jeweilige API MUSS vollständig und als RESTful API gemäß

- [Matrix Specification#Server-Server API],
- [Matrix Specification#Client-Server API],
- [Matrix Specification#Push Gateway API]

umgesetzt werden.

Die Webservices der Matrix-Homeserver werden nicht direkt von den TI-Messenger-Clients aufgerufen. Der Aufruf der Client-Server-API am Matrix-Homeserver erfolgt immer über den Messenger-Proxy. Dieser leitet alle durch ihn autorisierten 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 Matrix-Homeserver weitergeleitet. Zum Versenden von Push-Notifications nutzt der Matrix-Homeserver das 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 Matrix-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.

Messenger-Services KÖNNEN dezentral oder "*on-premise*" von einem TI-Fachdienst-Anbieter bereitgestellt werden. Werden durch einen TI-Messenger-Anbieter mehrere Matrix-Domains in einem gemeinsamen System betrieben so MUSS die logische Trennung der Matrix-Domains sichergestellt werden.

5.1.2.1 Matrix-Homeserver

Der Matrix-Homeserver MUSS alle Matrix-Spezifikationen vollständig umsetzen. Bereits existierende Produkte, die der Matrix Spezifikation folgen, können als Matrix-Homeserver verwendet werden.

Der Matrix-Homeserver eines Messenger-Services:

- MUSS Anfragen vom eigenen Messenger-Proxy akzeptieren und
- DARF Anfragen anderer Messenger-Proxies nicht akzeptieren.

Die vom Matrix-Homeserver verwendeten Authentifizierungsverfahren MÜSSEN konfigurierbar sein. Beim Anmeldeversuch eines neuen Akteurs an einem Matrix-Homeserver MUSS dieser alle, für seine Organisation unterstützten, Authentifizierungsverfahren zur Auswahl anbieten. Nach einer erfolgreichen Anmeldung eines Akteurs bei einem Matrix-Homeserver stellt dieser ein von ihm erstelltes Matrix-ACCESS_TOKEN sowie ein Matrix-OpenID-Token bereit (siehe gemSpec_TI-Messenger-Dienst#Verwendung der Token). Das Matrix-ACCESS_TOKEN wird zukünftig für jede weitere Autorisierung am Matrix-Homeserver verwendet. Das ausgestellte Matrix-OpenID-Token wird für eine spätere Authentisierung am Auth-Service des VZD-FHIR-Directory verwendet, um ein `tim-search-accesstoken` für den Lesezugriff im VZD-FHIR-Directory zu erhalten.

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. **[<=]**

5.1.2.2 Messenger-Proxy

Der Messenger-Proxy ist eine Kernkomponente der dezentralen Messenger-Services. Alle Anfragen der TI-Messenger-Clients und anderer Messenger-Services zum Matrix-Homeserver MÜSSEN über den Messenger-Proxy geleitet werden. Die TLS-Kommunikation zwischen den TI-Messenger-Clients und dem 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 Kommunikation 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 eines anderen Messenger-Service MUSS über den Messenger-Proxy geführt werden.

Für alle Server-to-Server Anfragen MUSS beim anfragenden Matrix-Homeserver im Messenger-Proxy geprüft werden, ob der Ziel-Matrix-Homeserver in der Anfrage Teil der Föderation ist. Hierfür MUSS 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 Ziel-Matrix-Homeserver gemäß [Server-Server API#Response Authentication] mittels TLS Zertifikat durchgeführt werden MUSS. Für eingehende Server-to-Server Anfragen MUSS der Messenger-Proxy eine Authentisierung gemäß [Server-Server API#Request Authentication] durchführen. Sobald der sendende Matrix-Homeserver damit authentisiert wurde, MUSS validiert werden, dass dieser Homeserver an der Föderation teilnimmt.

Die Prüfung, ob ein Matrix-Homeserver an der Föderation teilnimmt, basiert auf der Matrix-Domain. Eine Liste mit aktuell verifizierten und zugelassenen Matrix-Domains (Föderationsliste) kann vom VZD-FHIR-Directory über den Registrierungs-Dienst eines TI-Messenger-Fachdienstes durch aufrufen der Operation `getFederationList` angefragt werden. Der Messenger-Proxy MUSS die Operation `getFederationList` am Registrierungs-Dienst aufrufen, um eine aktuelle Föderationsliste für die Prüfung zu erhalten.

Prüfregeln

Der Messenger-Proxy MUSS Prüfregeln unterstützen. Hierbei MUSS Der Messenger-Proxy bei den RESTful-Endpunkten `Invite` und `Profiles` den Inhalt der Anfrage an den Matrix-Homeserver wie folgt prüfen.

- **Invite-Endpunkt**

Handelt es sich bei der Anfrage um ein `Invite-Event` gemäß [Server-Server API#Inviting to a

room] MUSS der Messenger-Proxy folgende Prüfregeln anwenden:

Der Messenger-Proxy MUSS prüfen, ob ein PASSporT im `Invite-Event` des TI-Messenger-Clients vorhanden und gültig ist und auch für den einladenden Nutzer ausgestellt wurde. Für die Prüfung der Signatur des PASSporT MUSS das öffentliche Zertifikat, auf welches im PASSporT referenziert wird, verwendet werden. Handelt es sich um ein `Invite-Event` innerhalb eines Messenger-Service MUSS diese Prüfung entfallen.

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**

Der Messenger-Proxy MUSS verhindern, dass Akteure den eigenen Displaynamen gemäß [Client-Server API#Profiles] ändern können. Der Displayname darf nur durch einen Akteur in der Rolle "Org-Admin" geändert werden.

5.1.2.3 PASSporT-Service

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

Der PASSporT-Service MUSS für die Erzeugung eines PASSporT eine REST-Schnittstelle bereitstellen. In der folgenden Tabelle ist die Ressource mit der HTTP-Methode für die REST-Schnittstelle dargestellt. Die Operation ist eine Abstraktion auf einen Webservice Endpunkt.

Tabelle 4: Schnittstelle - PASSporT-Service

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

Es MUSS der folgende Endpunkt verwendet werden:

```
servers:

- GET /_matrix/client/v1/de.gematik.tim.passport/user/{mxid}
```

Vor der Herausgabe des PASSporT durch den PASSporT-Service MÜSSEN die Berechtigungen der beabsichtigten Teilnehmer durch den PASSporT-Service geprüft werden. Dies betrifft zum einen die Berechtigung eines Akteurs die beabsichtigte Kommunikationsbeziehung aufzubauen und zum anderen, ob die übergebene MXID eines Akteurs einen in der Föderation enthaltenen Messenger-Service ausweist. Sollte es bei der Prüfung zu einem Fehler kommen, MÜSSEN die Fehlercodes gemäß der Tabelle "*Error-Code PASSporT-Service*" 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 die eines Akteurs 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 in das PASSporT MUSS wie folgt geschehen:

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

Das Erstellen des PASSporT MUSS durch den PASSporT-Service des einzuladenden 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-Event` auslösen wird. Diese MXID wird durch diesen Akteur 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-Event` auslöst. Die Zertifikate haben die `keyUsage = digitalSignature`. Das Zertifikat mit dem öffentlichen Schlüssel für die Prüfung der Signatur MUSS im PASSporT referenziert sein.

Zur besseren Veranschaulichung dient die folgende Darstellung:

Tabelle 6: Ablauf PASSporT-Erstellung

TI-Messenger-Client A	TI-Messenger-Client B
1. Client A übergibt seine MXID an den Client B	
	2. Client B ruft die Operation `getPassport` mit der MXID von Client A am PASSporT-Service seines Messenger-Services auf
	3. PASSporT-Service von B erzeugt PASSporT mit: „`dest`“: MXID von Akteur B „`Orig`“: MXID von Akteur A
	4. PASSporT wird von B an den Client A übergeben
5. Akteur A löst `Invite-Event` an Akteur B aus und übergibt den PASSporT	

5.1.3 Push-Gateway

Der TI-Messenger-Fachdienst MUSS ein Push-Gateway, gemäß [Matrix Specification#Push Gateway API], 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
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
[gemSpec_IDP_Dienst]	gematik: Spezifikation Identity Provider-Dienst

6.5.2 Weitere Dokumente

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[Matrix Specification]	Matrix Foundation: Matrix Specification https://spec.matrix.org/v1.2/
[OpenID]	OpenID Foundation https://openid.net/developers/specs/
[OWASP Proactive Control]	OWASP Proactive Controls https://owasp.org/www-project-proactive-controls/

[RFC 8225]	PASSporT: Personal Assertion Token https://datatracker.ietf.org/doc/html/rfc8225
[Client-Server API]	Matrix Foundation: Matrix Specification - Client-Server API https://spec.matrix.org/v1.2/client-server-api/
[Server-Server API]	Matrix Foundation: Matrix Specification - Server-Server API https://spec.matrix.org/v1.2/server-server-api/