

Elektronische Gesundheitskarte und Telematikinfrastruktur

Spezifikation TI-Messenger-Fachdienst

Version:	<u>1.0-01.1</u>
Revision:	<u>680581866416</u>
Stand:	<u>01.1031.07.20213</u>
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
1.1.0	29.07.2022		Überarbeitung folgender Features: - Erreichbarkeit einzelner Organisationseinheiten mittels Funktionsaccounts - Öffnung des TI-Messengers für Drittsysteme durch clientseitige Schnittstellen zur Integration z.B. ins Praxisverwaltungssystem - schnelles Finden von Kontaktdaten durch Zugriff auf FHIR-basiertes Adressbuch	gematik
	16.08.2022		Möglichkeit einer Art Zugriffskontrolle für Org-Admin	gematik
1.1.1	31.07.2023		Einarbeitung TI-Messenger Maintenance 23.1 / VZD FHIR Maintenance_23.1	gematik

Inhaltsverzeichnis

1 Einordnung des Dokumentes	5
1.1 Zielsetzung	5
1.2 Zielgruppe	5
1.3 Geltungsbereich	5
1.4 Abgrenzungen	6
1.5 Methodik	6
2 Systemüberblick	8
3 Systemkontext	10
3.1 Nachbarsysteme	10
3.2 Messenger-Services	10
4 Übergreifende Festlegungen	12
4.1 Datenschutz und Sicherheit	12
4.2 Authentifizierung von Nutzern	16
4.2.1 Smartcard-IDP-Dienst	16
4.2.2 Verwaltung der Nutzersession	17
4.3 DNS-Namensauflösung	17
4.4 Test	18
4.5 Betrieb	19
4.5.1 Performance	19
4.5.2 Monitoring	19
5 Funktionsmerkmale	23
5.1 Umsetzung der Matrix-API	24
5.2 Funktionen der Systemkomponenten	25
5.2.1 Messenger Service	25
5.2.1.1 Matrix-Homeserver	25
5.2.1.2 Messenger-Proxy	29
5.2.1.3 PASSport-Service	30
5.2.2 Registrierungs-Dienst	33
5.2.3 Push-Gateway	34
6 Anhang A – Verzeichnisse	35
6.1 Abkürzungen	35
6.2 Glossar	36
6.3 Abbildungsverzeichnis	36
6.4 Tabellenverzeichnis	36

6.5 Referenzierte Dokumente	37
6.5.1 Dokumente der gematik.....	37
6.5.2 Weitere Dokumente.....	37
1 Einordnung des Dokumentes	6
1.1 Zielsetzung.....	6
1.2 Zielgruppe.....	6
1.3 Geltungsbereich.....	6
1.4 Abgrenzungen.....	7
1.5 Methodik.....	7
2 Systemüberblick	9
3 Systemkontext	12
3.1 Nachbarsysteme.....	12
3.2 Messenger-Services.....	12
4 Übergreifende Festlegungen	15
4.1 Datenschutz und Sicherheit.....	15
4.2 Authentisierung und Authentifizierung.....	21
4.2.1 Authentisierungsverfahren für die Registrierung eines Messenger-Services...21	
4.2.1.1 OpenID Connect.....	21
4.2.1.2 KIM-Verfahren.....	22
4.2.2 Verhinderung unautorisierter Registrierung eines Messenger-Services.....	23
4.2.3 unautorisierter Registrierung.....	24
4.2.4 Authentifizierung der Akteure am Messenger-Service.....	25
4.2.4.1 Verwaltung der Nutzersession.....	25
4.2.4.2 2-Faktor-Authentifizierung.....	25
des BSI gemäß [BSI 2-Faktor] zur Resilienz gegen Angriffe aus der Ferne, mindestens mit mittlerer Bewertung genügen. der.....	26
4.3 DNS-Namensauflösung.....	26
4.4 Test.....	26
4.5 Betrieb.....	28
Anforderungen zu Performance.....	28
4.5.1 Monitoring und Betriebssteuerung.....	28
Das Service Monitoring.....	28
4.5.2 Kontrollierte Außerbetriebnahme.....	32
5 Funktionsmerkmale	33
Die in der.....	35
5.1 en.....	36
5.1.1 Registrierungs-Dienst.....	36
5.1.1.1 Schnittstellen.....	38
5.1.1.1.1 I_Registration.....	38

5.1.1.1.2	_requestToken.....	38
5.1.1.1.3	_internVerification.....	39
5.1.1.1.4	_VZD_TIM_Provider_Services.....	45
5.1.1.1.5	OAuth / Auth-Service.....	46
5.1.1.2	<i>Bereitstellung eines Org-Admin Accounts.....</i>	<i>46</i>
5.1.1.2.1	Authentisierung einer Organisation.....	46
5.1.1.2.2	Anlegen des Administrations-Accounts.....	47
5.1.2	Messenger-Service.....	48
<i>Der Aufruf der Client-Server-API am Matrix-HomeServ.....</i>	<i>50</i>	
5.1.2.1	Messenger-Proxy.....	50
5.1.2.1.1	TLS-Terminierung.....	51
5.1.2.1.2	Prüfung des verwendeten Clients.....	51
5.1.2.1.3	HTTP(S)-Forwarding.....	51
5.1.2.1.4	Schnittstelle für Authentifizierungsverfahren.....	52
5.1.2.1.5	Föderationsliste.....	52
5.1.2.1.6	Freigabeliste.....	54
<i>Der Messenger-Proxy MUSS eine FReigabelist.....</i>	<i>54</i>	
5.1.2.1.7	Ausnahmeregeln.....	55
5.1.2.1.8	Umsetzung von Prüfregeln.....	55
5.1.2.2	<i>Matrix-Homeserver.....</i>	<i>57</i>
5.1.2.2.1	Server Discovery.....	58
5.1.2.2.2	Öffentliche Räume.....	58
5.1.2.2.3	Custom Room Types und Custom State Events.....	58
5.1.3	Push-Gateway.....	59
6	Anhang A - Verzeichnisse.....	60
6.1	Abkürzungen.....	60
6.2	Glossar.....	61
6.3	Abbildungsverzeichnis.....	61
6.4	Tabellenverzeichnis.....	61
6.5	Referenzierte Dokumente.....	62
6.5.1	Dokumente der gematik.....	62
6.5.2	Weitere Dokumente.....	63

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 Leistungserbringereinrichtungen betrachtet. Festlegungen zur Nutzergruppe der Versicherten und Anforderungen an Kassenrankenversicherungsorganisationen 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 Produktypspezifikation 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, Produktypsteckbrief, 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 Anwendungsfalles wird in den jeweiligen Steckbriefen festgelegt, in denen jeweils der Anwendungsfall gelistet ist. Akzeptanzkriterien werden in der Regel nicht im Steckbrief gelistet.

Hinweis auf offene Punkte

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

2 Systemüberblick

Der TI-Messenger-Fachdienst ermöglicht eine sichere Kommunikation zwischen verschiedenen Teilnehmern Akteuren im deutschen Gesundheitswesen. Der TI-Messenger-Fachdienstieser 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, dwelche bei der Produktzulassung getestet werden und die ein TI-Messenger-Anbieter bereitstellen MUSS. Bei den dezentralen Teilkomponenten handelt es sich um die Messenger-Services. DieEin Messenger-Services beinhalten jeweils Msteht aus einem Matrix-Homeserver und Komponenten, welche einem Messenger-Proxy, der dafür sorgent, dass eine Föderation der Matrix-Homeserver nur zwischen verifizierten Domains stattfindet. Diese werden in der Spezifikation als Messenger-Proxy und PASSport-SService bezeichnet. Messenger-Serviceses werden für einzelne Organisationen (z. B. Leistungserbringerinstitutionen, Verbände) bereitgestellt und erlauben die Nutzung durch alle Nutzerberechtigten Akteure einer Organisation. Weiterhin KÖNNEN Messenger-Services durch OrganisationAuthentifizierungsverfahren bereitgestellt werdeanbieter, die nur für Leistungserbringer nutzbaricht einer Organisation zugeordnet sind. Diese unterscheiden sich technisch nicht von anderen Messenger-Services. Einzig die zugeordnete Organisation bietet ein für Leistungserbringerdiese Akteure notwendiges Authentifizierungsverfahren an.

-

Die Kommunikation zwischen einem TI-Messenger-Client und einem TI-Messenger-Fachdienst erfolgt immer über dieeen Messenger-Proxiesy der Messenger-Services. Hier 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 Abfragen am Reden Abgleich mit einer durch seinen Registrierungs-Dienst bereitgestellten Föderationsliste (Berechtigungsprüfung - Stufe 1 der Client-Server Kommunikation). Hierbei wird geprüftprüft der Messenger-Proxy, ob die beteiligten Matrix-Homeserver registrierte Mitglieder der Föderation sind und ein TeilnehmeAkteur berechtigt ist, Requests Anfragen auf dem Matrix-Homeserver auszulösen.

Neben den de Ebenfalls stellt der Messenger-Proxy eine Freigabeliste für die Berechtigungsprüfung (Stufe 2 der Server-Server Kommunikation) bereit. Für die Administration dieser Freigabeliste durch die Akteure bietet der Messenger-Proxy den TI-Messenger-Clients eine Schnittstelle an.

Neben den dezentralen Messenger-Services besteht derein TI-Messenger-Fachdienst aus einem-den zentralen Teilkomponenten Registrierungs-Dienst sowie einem zentralenund Push-Gateway. Über den Registrierungs-Dienst bekommt der TI-Messenger-Anbieter die Möglichkeit die DMessenger-Services automainnametisiert Organisationen zur Verfügung zu stellen und die Matrix-Domain der von ihm bereitgestellten Messenger-Services in das-eren Organisationsressource in das zentrale VZD-FHIR-Directory einzutragen, Messenger-Servie, Der Registrierungs-Dienst eines automatisiert Organisationen zur Verfügung zu TI-Messenger-Fachdienstes bietet als weitere Funktion die Bereitstellen und

~~Domainabfragen vorzunehmung einer Föderationsliste für die Messenger Proxies seiner Messenger-Services an. 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 Nutzer~~

~~In der folgenden Abbildung sind alle beteiligten Komponenten desr TI-Messenger kommen unters-Archidlichetektur in Verfahren zur Anwendung. Beispielhaft soll auf die Möglicheiteinfacher Form dargestellt. der Verwendung eines IDP-Dienstes verwiesen werden.~~

~~Die folgende in der Abbildung zeigt einen Syblau dargestemüberblick aller am-llte TI-Messenger beteiligten Teil-Fachdienst zeigt alle komponenten in vereinfachter Form. die in dieser Spezifikation beschrieben werden.~~

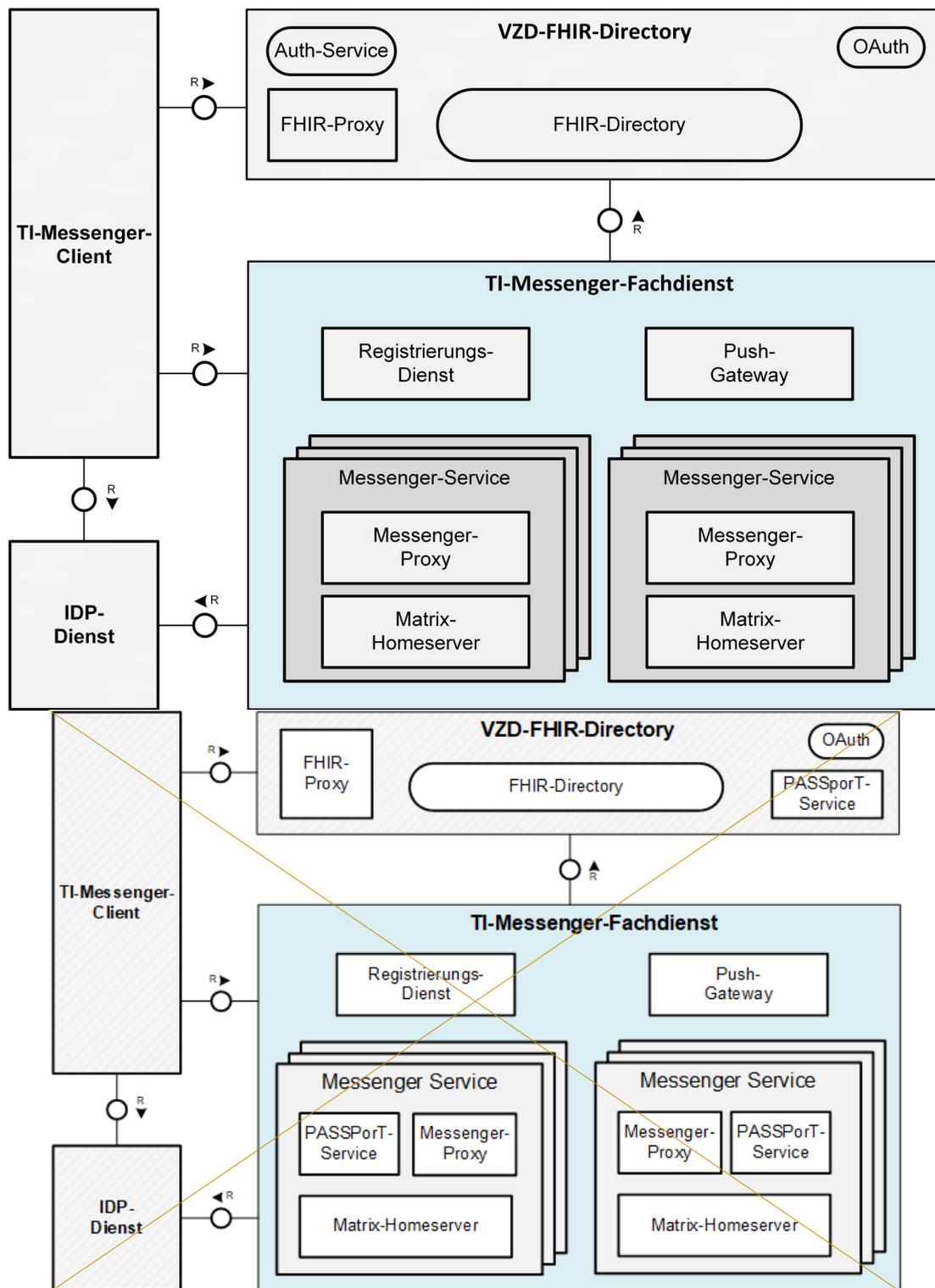


Abbildung 1: Systemüberblick (Vereinfachte Darstellung)

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 gehört der Smartcard-zentrale IDP-Dienst ~~der~~ welcher gematik und Authentifizierungen und Autorisierungen auf Basis von Smartcard-Identitäten durchführt, sowie das VZD-FHIR-Directory. Die Abbildung in Kapitel 2- Systemüberblick aus Kapitel 2 zu findende Abbildung zeigt deren Beziehung zum TI-Messenger-Fachdienst.

Der Smartcard-zentrale IDP-Dienst stellt allen berechtigten Teilnehmern ID_TOKAkteurEN (AuthN) sowie ACCESSID_TOKEN (AuthZ), gemäß des durch die OpenID Foundation [OpenID] spezifizierten Protokolls, zur Verfügung. ~~Mit diesen können ausgeteilten Token alternativ zum KIM-Verfahren die notwendigen Verfahren (siehe Kapitel 4.2.1- Authentisierung der TI-Messenger-Nutzer bei der Initialisierungsverfahren für die Registrierung eines Messenger-Services) für eine Organisation, oder für schreibenden Zugriff auf das VZD-FHIR-Directory mittels TI-Messenger-Client. Dazu ist es notwendig das der TI den Nachweis des Besitzes einer SMC-B bei der Bestellung eines Messenger-ClientServices und das Frontend des Registr für die Authentisierungsdienstes sich bei dem Smartcard IDP-Dienst registriert. Damit ist sichergestellt das Änderungen an den VZD- von Leistungserbringern beim Schreibzugriff auf das FHIR-Directory Einträgen durch den TI-Messenger-Client möglich sind verwendet werden.~~

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-Registrierungs-Dienst des TI-Messenger-Fachdienstes trägt bei erfolgreicher Aufnahme iVerifizierung einer Organisation die FöMatrix-Domain des zugehörigen Messenger-Service der Organisation im VZD-FHIR-Directory (in die Organisationsrein. Durch diesen Eintrag kann der Messource) seine Matrix-Domain ein. enger-Service an der Föderation des TI-Messenger-Dienstes teilnehmen. Das VZD-FHIR-Directory vertraut den Matrix-HomeServern 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 er der Messenger-Services erfolgt durch über den Registrierungs-Dienst eines TI-Messenger-Anbieters dezentral-Fachdienstes und kann on-premise oder zentral innerhalb von Rechenzentren stattfinden. Jeder Messenger-Service MUSS einer Organisation logisch zugeordnet sein. Die Messenger-Services unterscheiden

sKÖNNEN sich lediglich nur in den durch die jeweils Organisation verwendeten Authentifizierungsverfahren unterscheiden. 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 NutzerAkteure vom Messenger-Service gelöscht/gesperrt werden, wenn der Nutzer innerhalb der Nutzerverwaltung gelöscht/gesperrt wurde.

-

Authentifizierungsverfahren

Messenger-Services könnMÜSSEN je nach Art der Organisation verschiedenen Akteuren ein Authentifizierungsverfahren anbieten. Sind zum Beispiel bereits Systeme wie Active-Directory oder LDAP innerhalb basierende Nutzerverzeichnisse innerhalb einer Organisation verfügbar, können diese entsprechend verwendet werden, indem der jeweilige Matrix-Homeserver bei diesen registriert wird. Sind keine Authentifizierungsverfahren vorhanden (z. B. in einer Organisation vorhalb einer Arztpraxis) den KÖNNEN TI-Messenger-Anbieter entsprechende Authentifizierungsverfahren zur Verfügung stellen. Diese erlauben einen Login für Nutzer Authentifizierung von Akteure (z. B. durch Benutzername/Passwort und einen zweiten Faktor) und können auch von weiteren Systemen nachgenutzt werden.-

Die nachfolgende Abbildung verdeutlicht das die Nachnutzung eines existierenden Authentifizierungsverfahrens von Nutzern an Akteuren innerhalb einer Organisation durch einen Messenger-Service.

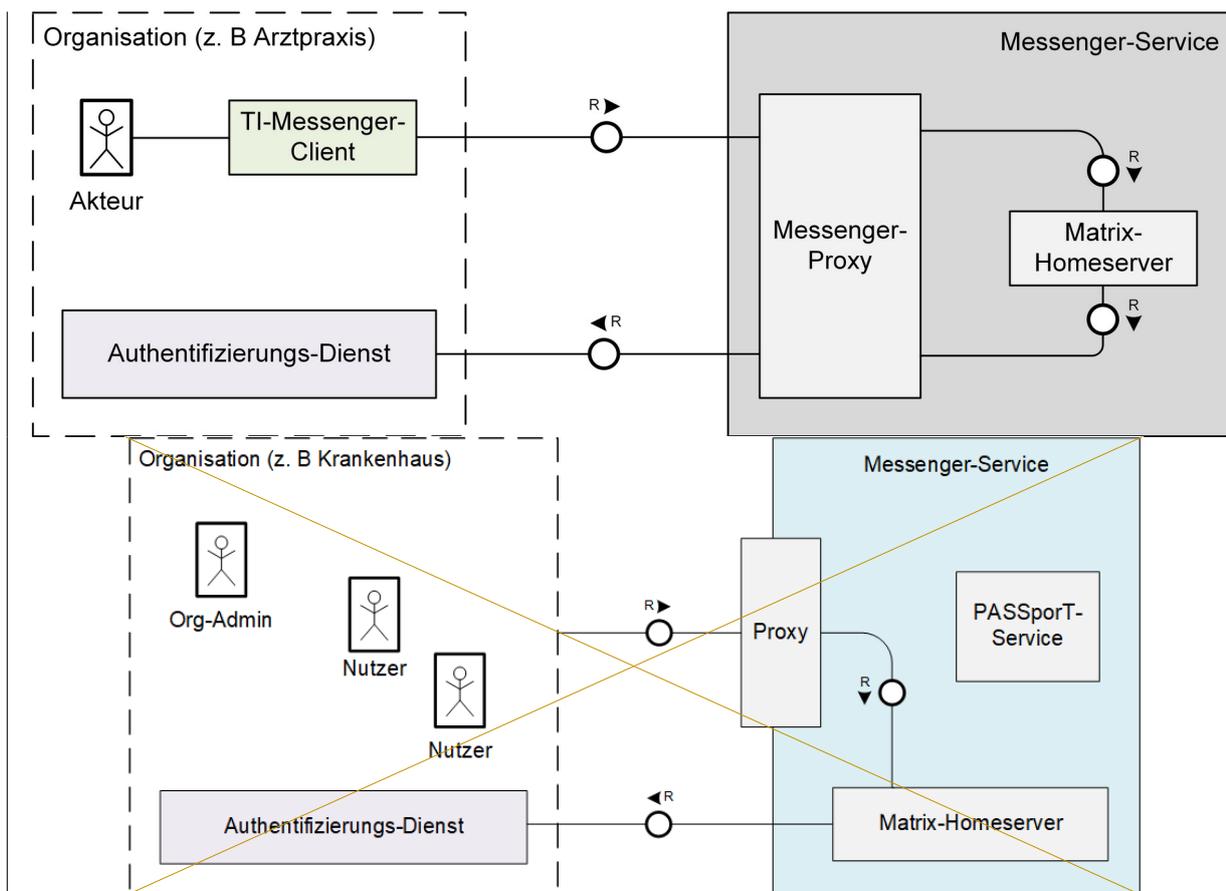


Abbildung 2: Beispiel - Authentifizierung von **NutzerAkteuren** einer Organisation

4 Übergreifende Festlegungen

4.1 Datenschutz und Sicherheit

~~Mainline_OPB1/ML-123614~~ **ML-123614 – Verbot von Organisationsaccounts für**
VerZur Sicherstellung des Datenschutzes und der **sicherte**

~~Der Anbieter MUSS sicherstellen, dass organisationsbasierte~~ im Rahmen des TI-Messenger-Dienstes werden im Folgenden zu beachtende Anforderungen an den TI-Messenger-Accounts ~~nicht an Versicherte verg~~Fachdienst beschrieben ~~we.~~ Anfordern. Er ~~MUSS sicherstellungen,~~ dass nur Accounts ~~ie durch~~ an ~~Persödere Systemkomponen~~ vten ~~sicher~~gebenstellt werden, mit denen ein Beschäftigungsverhältnis besteht. Hierzu ist eine organisatorische Lösung ~~ausreichend~~ sind hier nicht weiter aufgeführt.

[<=]

~~3618~~ **ML-123618A_22807 - PUSH-Benachr****Vertragsverpflichtungen**

~~Der TI-Messenger-Anbieter MUSS~~ ~~USS~~ KundEN dafür ~~sorg~~vertraglich ~~verpflichten~~, dass diese Gateways ~~externe PUSH-Dienste datenschutzkonform nutzen.~~ Hierzu ~~wu~~organisationsbasierte TI-Messenger-Accounts ~~nicht an Dritte vergeben werden~~ folgende Kriterien ~~und nur Accounts für Akteure definiert, die in jedem Fall beachter~~ Organisation ~~erstellt~~ werden ~~MÜSSEN~~:

- ~~PUSH-Benachrich,~~ mit denen ein Beschäftigungen ~~dürfen erst nach~~ explizisverhältnis oder Dienstleister ~~Zustimmung der Nutzer erfolgen (Opt-In).~~
- ~~Alle PUSH-Nachrichteninhalte, auf die der PUSH-Anbieter nicht zugreifen können~~ muss, ~~MÜSS~~vertragsverhältnis besteht. Funktionsaccounts (in Verbindung mit einem Chatbot) ~~sind von d~~EN verschlüsselt werden.

~~PUSH-Nachtragsverpflichtungen MÜSSEN vor dem Versenden um einen Zufallswert von 0-10 Seku~~ausgenommen.

[<=]

- ~~A_22809 - Flächendeckenden~~ verzögert werden um Timingbasierte Profilbildung zu erschweren.

~~Wo möglich, MÜ~~**wendung von TLS für Hersteller**

- ~~TI-Me~~SSEN PUSH-Anbieter gewählt werden, die eine Wahrung der Betroffenenrechte für personenbezog~~er~~-Fachdienst-Hersteller ~~MÜSSEN sicherstellen, dass sämtliche~~ Verbindungen~~e~~ Informati ~~zwischen~~ Komponenten ~~ermöglichen.~~
- ~~Wenn ein Zielclient~~ten des TI-Messenger~~ade~~ aktiv ist, soll dieser selbsttätig auf ein ~~Fachdienstes mittels TLS~~ kommende Nachrichten ~~lauschen und nicht per PUSH~~ benachrichtigt werden.
- ~~PUSH-Nachrichten dür~~funizieren, sofern diese Kommunikation die Grenzen ~~keine~~ Nachrichteninhalte ~~enthalten, ihre Funktion br~~ virtuellen/physischen Maschine ~~überschreitet. Hierzu MUSS mindeste~~ht lediglich darin ~~Clientsysteme zu informieren,~~ dass Nachrichten ~~abrufbar sind und ns~~ serverseitiges TLS verwendet werden. Sofern ~~keine~~ Synchronisierung mit dem Homeser ~~beidseitiges TLS ver~~nötig ist. Es ~~DARF~~ nurwendet wird, ~~MUSS~~ die Room-ID und Event-ID ~~Authentizität der Client~~halten sein.

[<=]

~~Für Details d~~seite mit gleichwertiger Verschlüsselung ~~und entha~~Sicherheit ~~sichergestellt~~ werden. Es ~~geltene~~ personenbezo ~~die~~ Festlegungen~~e~~ Daten ~~siehe [MSC-3013]. gemäß~~

[gemSpec_Krypt].

[<=]

23615ML-123615A_22929 - Flächendeckende Verwendung von TLS

Betreiber und Hersteller **für Anbieter**

TI-Messenger-Anbieter MÜSSEN sicherstellen, dass sämtliche Verbindungen zwischen Komponenten des TI-Messengers-Fachdienstes mittels TLS kommunizieren, sofern diese Kommunikation die Grenzen einer virtuellen/physischen Maschine überschreitet. Hierzu MUSS mindestens serverseitig authentizitätsgeschütztes TLS verwendet werden. Sofern keEs gelten die Festlegungen gemäß [gemSpec_Krypt].

[<=]

A_22936 - Authentifizierungsverfahren für Akteure in beidseitiges-TLS verwendet wird, MUSS die **Organisationen**

TI-Messenger-Anbieter KÖNNEN für die Authentisierung von Akteuren in der Rolle "User" bestehende Authentizität der Clientseite mit gleichwertiger Sicherheitsverfahren der Organisation nachnutzen. Sollte dies der Fall sein, MÜSSEN Anbieter die Organisation und die Administratoren explizit darauf hinweisen, dass die Sicherheit der Nutzerauthentisierung damit in die Verantwortung der Organisation gegeben wird. Hierzu MUSS der Anbieter sichergestellt werden. Es gelte, dass er nur Authentifizierungsverfahren akzeptiert, die in die Festleger Hand der Organisation sind und deren Authentisierungen aus [gemSpec_Krypt].

[<=]

Mainline-OPB1/ML-123616ML-123616 -- Abwertt werden können. Der Anbieter MUSS sicherstellen, dass zur Authentifizierung mindestens zwei Faktoren verwendet werden und die Sicherheitsempfehlungen des BSI [BSI 2-Faktor] Berücksichtigungen vom **Matrix-Standard**

Hersteller von TI-Messenger-Komponenten MÜSSEN sämtliche, nicht in der TI-Messenger-Spezifik finden. Zur Vermeidung von Angriffen aus der Ferne auf den 2. Faktor ist ein Verfahren zu wählen, das mindestens mit "mittel" bewertet ist. Der Anbieter MUSS sicherstellen, dass mindestens eine Authentisierung mittels OIDC-Authenticator unterstützt wird und technische Optionen für die Organisation beschrängegebenen, Abweichung sind, damit beide Faktoren nicht durch einen vom Matrix-Protokoll oder den MUST oder SHOULD-Empfehlung Angriffsvektor kompromittiert werden können.

[<=]

Hinweis: A_22936 regelt lediglich die Authentisierung, die notwendig ist um ein Token zu erhalten, mit dem sich Nutzer gegen des Matrix-Protokolls-dokumn Messenger-Service authentisieren und begründkönnen.

[<=]

23617ML-123617A_23611 - Löschfristvorgaben für Homeserver

Betreiber **zur minimalen Qualität von Passwörtern**

Der Anbieter MÜdes TI-MESSER-sicherger-Fachdienststellen, ds MUSS Vorgaben zur minimalen Qualität von Pass-Events, Gewörtern entsprächsinhaltechend [BSI ORP.4] A.22 machen und mit die einzelnehaltung dieser Vorgaben an allen Stellen Gesprächen-assozierte Daten (z.B. versandte Dateien) maximal für 6 Monate auf Homeservern verbleibenwährleisten, an denen Passwörter im Rahmen der Konfiguration festzulegen sind. Weiterhin MUSS der Anbieter die Leistungserbringerinstitution (LEI), welche den TI-Messenger Dienst von ihm bezieht, über die Notwendigkeit der Einhaltung der Vorgaben aus [BSI ORP.4] A8 instruieren. Diese beinhalten sicherheitsrelevante Anforderungen hinsichtlich der Nutzung und danach gelöscht weres Umgangs mit Passwörtern, richten sich jedoch an den-

Hersteller MÜSSEN eine Funktion für Homeserver anbieten, über operativen Betrieb in der LEI, der vom Anbieter nicht kontrolliert werden kann. Unter Passwörtern werden in die eine Löschfrist für diessem Kontext sowohl Kennwörter als auch Passphrasen verstanden, auf welche Daten konfiguriers Dokument [BSI ORP.4] gleichermaßen anwendbar ist.

[<=]

23621ML-1A_2362113 - Interoperabilität Zwangsabmeldung und Sperrung von Zusatzfunktionen für Akteure

Wird ein Akteur in der Rolle "User" **den** TI-Messenger-Fachdienst

Herstellers einer MÜSSEN sicherstellen, dass aOrganisation durch einen Akteur in der Rolle implementierten Fun"Org-Admin" der Organisation gesperrt oder seine aktionen, die übe Sitzung beendet - das heißt, er den gewöhnlichen Funktionsumfang einewird zwangsweise ausgeloggt -, so MUSS der TI-Messenger-Komponente hinausgehen Fachdienst die Weiterleitung von Nachrichten, die Sicherheit des Produkts nicht gefäh an diesen Akteur in der Rolle "User" gesendet werden und oder von die- Interoperabilität mit sem gesendet werden, mit sofortiger Wirkung einstellen.

[<=]

A_22815 - Behandern TI-Messenger-Produkten erhalten. Ebenölung von kryptographischem Material für OAuth

TI-Messenger-Anbieter MÜSSEN sicHersteller sin, dass kryptographischerstellen,s Material zur Authentisierung gegen dass TI-Messes VZD-FHIR-Directory sicher einger- Fbrachdienstbestandteile resilient auf unerwartetet wird. Zum Nachweis der Umsetzung ist eine Prüfung des Prozesses zur Einbringung des kryptografischen Materials erforderlich. Die Prüfung umfasst die Beschreibung und Durchführung des Prozesses. Eingaben reagierene Auditierung der Umsetzung ist optional.

[<=]

19ML-123619A_22817 - ProtokollieruExplizites Verbot von Profiling zum Zwecke der Fehler- bzw. Störungsbehebung

Falls im für TI-Messenger-Fachdienste

TI-Messenger-Fachdienst eine Protokollierung zum -Hersteller DÜRFEN NICHT Daten zu Profiling Zwecke der Fehler- bzw. Störungn sammeln. Dies betrifft insbehebsondere eine Überwachung erfolgt, MUSS der Fachdienst unter Berücksichtigung des Art. 25 welche Akteure mit welchen anderen Akteuren kommunizieren.

Hinweis: Die gematik kann nach § 331 Abs. 2 DSGVO sieSGB V Daten festlegen, die herstellen, dass iner von Komponenten und Dienste den Protokolldaten entsprechend der gematik offenzulegen bzw. zu übermitteln haben, sofern diese erforderlich sind, um Datenschutzgrundsatz nach Art. 5 DSGVO nen gesetzlichen Auftrag der gematik zur personenbezogene Daten in der ArÜberwachung des Betriebs zur Gewährleistung der Sicherheit, Verfügbarkeit und dem Umfang enthalten sind, wNutzbarkeit der Telematikinfrastruktur zu erfüllen. Nur die sie zur Behebung ehierfür erforderlich sind und dass die erzeugten Protokollen personenbezogenen daten im Fachdienst nachdürfen von der Behebungn Anbietern unverzüglich gelöscht werden. Sofd Herstellern andere gesetzls zeitliche Grundlagen wie §331 SGB V nicht überwiegt begrenzte Ausnahme vom Profilingverbot erhoben sind hierzu nur anonymisierte Dateausschließlich für den genannten zu protokollierweck verwendet werden.

[<=]

ML-123620A_22814 - Explizites Verbot von Profiling für TI-Messenger-Anbieter

Anbieter von TI-Messenger-KomponentenAnbieter DÜRFEN NICHT Daten zu Profilingzwecken sammeln. Dies betrifft insbesondere eine Überwachung welche Akteure mit welchen anderen Akteuren kommunizieren.

Hinweis: 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 zeitlich begrenzte Ausnahme vom

Profilingverbot erhoben und ausschließlich für den genannten Zweck verwendet werden.
[<=]

22ML-123622A_22813 - ~~Behandlung~~Protokollierung von kryptographischem Material für OAuth

Betreiber von TI-Messenger ~~zum Zwecke der Fehler- bzw. Störungsbehebung~~ Falls im TI-Messenger-Fachdiensten MÜSSEN sicherstellen, da eine Protokollierung zum Zwecke der Fehler- bzw. Störungsbehebung erfolgt, MUSS kryptographisches Material für OAuth, wie z.B. Client-ID und Client-Secret, Berücksichtigung des Art. 25 Abs. 2 DSGVO sicherstellen, dass in den Protokolldaten ~~entweder~~ Secret für Authentifizierung dem Datenschutzgrundsatz ~~mittels Credential-Flow sicher eingebracht werden.~~ Dieses Material MUSS in Hardware nach Art. 5 DSGVO nur personenbezogene Daten in der Art und dem Umfang enthalten sind, wie Security-Module sicher gespeichert zur Behebung erforderlich ~~werden.~~ [<=]

Zum N sind und dass die erzeugten Protokolldaten im Fachdienst nach der Umsetzbehebung ist ~~lediglich~~ eine Prüfung gelöscht werden. Sofern andere Prozesse zur Einbringung erforderliche gesetzliche Grundlagen wie §331 SGB V nicht. Eine Auditierung der Umsetzung ist optional. ~~t~~ überwiegen sind hierzu nur anonymisierte Daten zu protokollieren.
[<=]

28ML-123628A_22811 - Device-Verification, Cross-Signing und SSSS-Löschfristen für TI-Matrix-Homeserver

Hersteller MÜSSEN sicherstellen, dass ~~ihre~~ Matrix-Homeserver eine Funktionen Cross-Signing anbieten, durch die Events, Gesprächsinhalte und Secure Secret Storage mit einzelnen Gesprächen assoziierte Daten (z. B. Versand-Sharing (SSSS) zur Device-Verification unterstützt ~~werte~~ Dateien) nach einem Zeitraum von 6 Monaten seit letzter Aktivität in einem Raum gelöscht werden. Hersteller MÜSSEN sicherstellen, dass der Zeitraum durch den Akteur in der Rolle "Org-Admin" konfigurierbar ist. Diese Funktion DARF über Opt-Out durch den Akteur in der Rolle "Org-Admin" deaktivierbar sein. Diese Funktion ~~hinsichtlich~~ DARF darüber realisierbar sein, dass nach Verstreichen Ende-zu-Ende ~~en~~ der Frist Teilnehmer einen Gesprächsraum verschlüsseln und der Raum nach Verlassung vollständig befolgen aller Teilnehmer automatisch gelöscht werden ~~ird~~.

[<=]

38ML-12363A_22808 - Explizites Verbot von Profiling für TI-Push-Benachrichtigungen Messenger-Fachdienste

Betreiber von Service

TI-Messenger-Komponenten DÜRFEN NICHT Daten Services MÜSSEN sicherstellen, dass die Push-Gateways externe Push-Dienste datenschutzkonform nutzen. Hierzu Profilingzweck werden sammeln. Dies betrifft insbesondere eine Überworfende Kriterien definiert, die in jedem Fall beachtet welche Akteure mit welchen anderen Akteuren kommunizieren.

Die gematik kann nach § 331 Abs. 2 SGB V Daten MÜSSEN:

- Alle Push-Nachrichteninhalte, auf die der Push-Anbieter nicht zugreifen können muss, MÜSSEN verschlüsselt werden.
- Push-Nachrichten festlegen, die Anbieter MÜSSEN vor dem Versenden um einen Zufallswert von Komponenten und Diensten 0-10 Sekunden verzögert werden, um timingbasierte der gematik offenzulegen bzw. zu übermitteln haben Profilbildung zu erschweren.
- Wenn ein Ziel-Client gerade aktiv ist, sofern diese erforderlich selbsttätig auf einkommende Nachrichten sind, um den gesetzliten lauschen und nicht per Push benachrichtigen Auftrag der gematik zur Überworfung werden.

- Push-Nachrichten dürfen keine Nachschub des Betriebs zur Gewährleistung der Sicherheit, Verfügbarkeiten enthalten, ihre Funktion besteht lediglich darin Clientsysteme zu informieren, dass Nachrichten abrufbar sind und Nutzbarkeit eine Synchronisierung mit der Telematikinfrastruktur zu erfüllen Homeserver nötig ist.

[<=]

A_22965 - Push-Benachrichtigungen Messenger-Anbieter

TI-Messenger-Anbieter MÜSSEN sicherstellen, dass die hierfür erforderlichen personenbezogenen Push-Gateways externe Push-Dienste datenschutzkonform nutzen. Hierzu werden folgenden Kriterien dürfen von den Anbietern und Herstellern als Ausnahme vom Profilingverbot definiert, die in jedem Fall beachtet werden MÜSSEN:

- Push-Benachrichtigungen dürfen erst nach expliziter Zustimmung der Nutzer erhoben und ausschließlich für den genannten Zweck verwendet werden. (Opt-In).
- Es MÜSSEN Push-Anbieter gewählt werden, die eine Wahrung der Betroffenenrechte gemäß DSGVO gewährleisten.

[<=]

ML-123637A_22818 - Sicherheitsrisiken von Software-Bibliotheken minimieren

Hersteller von TI-Messenger-Fachdienst-Herstellern MÜSSEN Maßnahmen umsetzen, um die Auswirkung von unentdeckten Schwachstellen in benutzten Software-Bibliotheken zu minimieren.

[<=]

Hinweis zu A_22818: 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].

[<=]

35ML-123635A_22810 - CC-Evaluierung Abweichung als Ersatz für Gutachten

Falls der en vom Matrix-Standard

TI-Messenger-Fachdienst-Hersteller entsMÜSSEN sämtliche, eine CC-Zertifizierung statt eines Produktgutachtens durchzuführen, MUSS der Hersteller bei, nicht in der TI-Messenger-Spezifikation beschriebenen, Abweichungen vom Matrix-Protokoll oder Einreichung eines CC-Zertifizierten MUST- oder SHOULD-Empfehlungsantrags sein Security-Target-en des Matrix-Protokolls Dokument der gematik zur Verfügung stellen. In diesem MÜSSEN mieren und begründen.

[<=]

Hinweis zu A_22810: Gemeint sindstens beschrieb hier nur tatsächliche Abweichungen von Setzungen sein:

- die der Matrix-Spezifikation und nicht zusätzlichen Funktionen des, die auf dem TI-Messenger-Clients des Nutzers,
- die in dest aufbauen und produktspezifisch sind.

- **A_22812 - Interoperabilität von** zusätzlichen atz Funktionen **verarbeiteten Daten,** die Schnittstellen zwischen dem für den TI-Messenger-Fachdienst

- TI-Messenger-Clients des Nutzers und den ggf. genutzten Hersteller MÜSSEN sicherstellen, dass alle implementierten Backend-Funktionen, Diensten über der zusätzn gewöhnlichen Funktionen inklusive ihres Umfang einer TI-Messenger-Komponente hinausgehen die Sicherheitsmaßnahmen des Produkts nicht gefährden und

- die Sicherheitsannahmen Interoperabilität mit an dederen TI-Messenger-Clients des Nutzers und die Ausführungsumgebung

Produkten gewährleisten.

[<=]

23634ML-123634A_22928 - Sichere Produktentwicklung und Nachweise

Der Hersteller MUSS innerhalb des Produktlebenszyklus (Entwicklung, Betrieb, Außerbetriebnahme) **Einsatz geschulter Administratoren für Org-Admins** TI-Messenger-Anbieter MÜSSEN als Administratoren Personal eines Produktes Sisetzen, welcherheitsaktivitäten integrieres für die damit verbundenen Aufgaben und anwenden, d. h. in einschlägigen Fachkreisen anerkannte, erprobte Themen der Informationssicherheit geschult und bewährte Regeln sensibilisiert wurden, anwenden. Der bieter MÜSSEN technisch sich Hersteller MU, daSS nur die Sicherheits- und Datenschutzmaßnahmen berechtigten Administratoren administrativen für sein Produkt in einem Sicherheits- und Datenschutzkonzept dokumentieren Zugriff auf die zu verwaltenden Messenger-Services haben.

[<=]

A_22816 - Device Verification, Cross-Signing und auf Verlangen der gematik zur Verfügung **SSSS für TI-Messenger-Fachdienststellen**.

Der TI-Messenger-Hersteller MUSS einen Testplan für SÜSSEN sicherheitstests erstellen, das die Funktionen Cross-Signing und auf Verlangen der gematik Secure Secret Storage and Sharing (SSSS) zur Verfügung stellen. Dieser MUSS umgese Device Verification vom Fachdienst unterstützt werden und der gem. Es MUSS die Spezifikatik bei jeder Veröffentlichung hinsichtlich einer Produktversion als neuer Bericht Ende-zu-Ende Verschlüsselung vorgelellständig befolgt werden.

Der Herste **[<=]**

4.2 Authentisierung und Authentifizierung

Ein Akteur in der Rolle des "Org-Admin" MUSS sich über das vom TI-Messenger-Clients für Nutzer MUSS währ Anbieter bereitgestellte Frontend der Entwickleines Registrierung des Produkts-Dienstes implem mit der Identierungsspezifische Sicherheitsanfordtät (SMC-B) der Organisation gegenüber dem Registrierungen dokums-Dienst authentisieren und, umsetzen.

Der Hersteller MUSS ein sicherheitsrelevanten Softwarearchitektur-Review durchführ mehrere Messenger-Services für seine Organisation registrieren und identifizierte Architekturschwachstellen beheben. Dieses zu können. Um die Organisation gegenüber dem Review MUSS nach jeder Architekturregistrierungs-Dienst zu authentifizieren, KÖNNEN die im folgenderung mit Sicherheitsrelevanz wien Kapitel beschrieben Verfahren OpenID Connect oderholt werden. Der Hersteller MUSS eine Bedroh KIM verwendet werden.

4.2.1 Authentisierungsanalyse durchführverfahren und Maßnahmen gegen die identifizierten Bedrohungen implementieren. Der Hersteller MUSS wä für die Registrierung eines Messenger-Services

4.2.1.1 OpenID Connect

Beim OpenID Connect Verfahren wird der zEntwicklung des Produktes sicherheitsrelevante Quellcode-Reviews oder automatisrale IDP-Dienst der gematik benötigt, um eine Organisation am Registrierte sicherheitsrelevante Quellcode-Scans durchführen. Dungs-Dienst zu authentifizieren sowie Leistungserbringer über Hersteller MUSS während der ihren TI-Messenger-ClientEntwicklung des Produktes automatisierte Ss Schreibzugriff auf das VZD-FHIR-Directory zu ermöglicherheitstests durchführen. n. Hierfür MÜSSEN Der Hersteller MUSS einen Schulungsplan zur regelRegistrierungs-Dienst und die TI-Messenger-Clients am zentralen IDP-Dienst der gematik gemäßigen-Schulung von Entwicklern in sicherer Entwicklung und [gemSpec_IDP_FD] registriert sein. Diese MÜSSEN den ausgestellten Secure-Coding-Techniity Tokens (ID-Token-dokumentieren und umsetzen. Der Hersteller MUSS alle Entwickler des Produkte) dieses IDP-Dienstes vertrauen.

Im Rahmen der Registrierung des VZD-FHIR-Directory am zentralen IDP-Dienst werden notwendige Claims für das in sicherer D_TOKEN (bestätigte IdEntwicklung und Secure-Coding-Techniken schulen. Hierzuifikationsmerkmale für den Akteur) festgelegt. Der Anbieter des TI-Messengers MUSS über Hersteller seinen organisatorischersteln Prozess beim zentralen, dass alle Entwickler zu Beginn der Entw IDP-Dienst folgende Claims im ID_TOKEN vereinbaren:

Tabelle 1: icklung geschult sind. nhalte dEr SOLLClaims für diese anschISMC-B/HBA

Leistungserbringerinstitutionen (SMC-B)	Leistungserbringer (HBA)
<ul style="list-style-type: none"> • <u>ProfessionOID</u> • <u>idNummer</u> • <u>organizationName</u> • <u>acr</u> • <u>aud</u> 	<ul style="list-style-type: none"> • <u>ProfessionOID</u> • <u>idNummer</u> • <u>given_name</u> • <u>family_name</u> • <u>acr</u> • <u>aud</u>

Dießend auch laufende Weit ProfessionOID gibt an um welche Art von Leistungserbildung durchführen. Der Hersteller MUSS den verwendetenringer (z. B. Arzt, Zahnarzt etc.) es sicheren-Produktlebenszyklus und deren Teilprozesse dokumentieren und auf Nachfrage der gh handelt. Die idNummer beinhaltet die Telematik zur Verfügung stellen. Die Dokumentation soll mindest-ID für Organisationen des Gesundheitswesens die folgenden-Sicherheitsaktivitäten beschreiben:

Erfassung Leistungserbringer.

Hinweis: Detaillierte Erläuterungen zu den Abläufen und Umsetzen von implementierungszur Authentifizierung sind in [api-messenger] in einem spezifischen Sicherheitsanforderungen für den Client und von Best-Practice-Sicherheitsanforderungen beschrieben.

4.2.1.2 KIM-Verfahren

- Bei der Authentifizierungen,
- Durchführen über das KIM-Verfahren 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 MUSS sowohl der Anbieter des TI-Messengers, als auch die Organisation die am TI-Messenger-Dienst teilnehmen möchte, über funktionierende KIM-Accounts Veröffentlichen. Für die Nutzung des Clients mit 'Mittel' oder 'Hoch' bewerteten Sicherheitsfehlern verhin KIM-Verfahrens ist eine gültige SMC-B Org sowie eine KIM-Installation notwendig.

Der Akteur in der

- Änderungs- und Konfigurationsmanagement,
- Schwach Rolle "Org-Admin" wird im Bestellen-Management

vorgang aufgefordert Der Hersteller MUSS während der Entwicklung des Produktes, seine KIM Mail-Adresse in eine Eingabemaske einen Änderungs- und Konfigurationsmanagementprozesszutragen. Daraufhin MUSS zur angegebenen KIM-Adresse im verwenden. Das Änderungsmanagementsystem (z. B. im LDAP-VZD gemäß gemein umfasst mindestens den Entscheidungsprozess VZD) die TelematikID sowie die profession über vorgegebene ID abgerufen werden. Anschlagene Änderungen und die Autorisierung MUSS der Registrierung der Änderungen. Das Konfigurations-Dienst prüfen, ob die ProfessionID zu einer Organisationsmanagement liefert mindest des Gesundheitswesens zu jedem Zeitpunkt gehört. Der Registrierungs-dienst sende eindeutige Zusammensetzung des Produktes bezüglich der Organisation nach einem positiven Prüfergebnis einer KIM-Nachricht mit eindeutigen Komponenten (Dritt-Software wie Bibliotheken und Frameworks) und den vorgenommenen URL an die angegebene KIM-Adresse und fordert den Akteur in der Rolle "Org-Admin" auf, die KIM-Nachricht zu lesen Änderungen an eigenen Komponente und die darin befindliche URL zu öffnen. Der Um sich Hersteller MUSS bei Veröffentlichung einer neuen Produktversion des Produktes die Einhaltung derselbe Akteur, welcher die Registrierung gestartet hat, auch der Herstellererklärung sicherheitstechnische-/diejenige ist, welcher die URL aufruft. MUSS der Registrierungs-Dienst Eignung durch seinen zufälligen sechsstelligen Datenschutzbelegcode anzeigen, welcher beim URL-auftragten verifizieren. [<=>]

Mainruf geprüft werden MUSS. Bei einem OPB1/ML-123623 **ML-123623 – Nur Verbindungen mit zugelassenen TI-Messenger-Client** im negativen Prüfergebnis MUSS der Registrierungs-Dienst

Der Messenger-Proxy MUSS prüfen, ob sich der TI-Messenger-Client als von der gematik zugelassenes Produkt ausweisen kann. Verbindungsgestörte Fehlermeldung anzeigen. Durch folgen des Links wird der Akteur wieder in den mit nicht zugelassenen

Clients MÜSSEN unter dem Bestellprozess zurückgeführt, gibt den werden-
 {<=>}

Mainline_OPB1/ML-124882 **ML-124882** – Kzuvor angezeigten Code **ein Einbringen-vertraulicher Informationen in Room-States** und die Authentisierung ist abgeschlossen, **durch Organisationsadministratoren** Anbieter von Home-Servern MÜSSEN das Entschlüsseln der KIM-Nachricht und die Eingabe des sechsstelligen Codes ist nachgewiesen, dass es sicherh hierbei um die antragstellen-, dass sie als de Organisations-Administra des Gesundheitswesens handelt.

4.2.2 Verhinderung unautoren-kisierter Registrierung eine-s Messensiblen Informationen in Room-Statger-Services

Der Nachweis des Besitzes einbringen. Ebenso MÜSSEN sieer SMC-B im Zuge der Authentifizierung einer Organisations-Admin am Registratoren von Homeservern unter Kundenverwaltung informierenierungs-Dienst ist ein notwendiges Kriterium, dass im Room-State sichtbare Informationen gegenwärtig nicht verschlüsselt sind. Sobald durch die geplante Matrix-Spec-Changes (MSCs) die Möglichkeit mit der dazugehörige Prozess überhaupt initiiert werden kann. Da der Nachweis einer SMC-B in beiden der zuvor geschaffen wurdenannten vertrauliche Informationfahren jedoch nicht im Room-State zu speichern, t zwangsläufig von jemandem erbracht wird dies direkt durch die Matrix-Spezifikat, der innerhalb der Leistungserbringerinstitution abgedeckt.

{<=>}

4.3 Authentifizierung zur Registrierung von Nutzern

Im TI eines Messenger-Kontext werden gemäß [gemSpec_TI-Messenger-Dienst#Akteure-und-Rollen] zwisDienstes befugt ist, MUSS der Anbieter Maßnahmen ergreifen, welchen folgenden Rollen unterschieden: die Erfüllung einer unautorisierten Bestellung verhindert.

Tabelle 2: Authentifizierung_23521 - Verhinderung von Nutzerrollen

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

4.3.1 unautorisierter RegiSmartcard-IDP-Dienstrierung

Der TI-Messenger-Dienst Anbieter MUSS die Verifikation von Nutzern mittels SMC-B und HBA unterstützen. einen organisatorischen oder technischen Prozess etablieren, der die erfolgreiche Registrierung Ein TI-es Messenger-Client-Service durch einen unautorisierten Akteur verhindert-Frontend-eines Regit.[<=]

Beispiel: Um sicherzustellen, dass nur solche Bestellungen zur erfolgreichen Registrierungs-Dienste und Inbetriebnahme des MUSS am Smartcard-IDPessenger-Dienst der gematik gemäß [gemSpec_IDP_FD] registriert sein.

Im Rahmen des führen, die willentlich und mit Befugnis ausgeführt wurden, könnte der Anbieter auf Basis des Eingangs einer RegistrierBestellung werdenen notwendige Claims- (achgelagerten Prozess etablieren, der eine postalische bestätigte- Identifikationsmerkmale durch den Nutzer), auf den damit zu nutzenung bei der LEI vorsieht. Dabei würde diejenige Stelle adressiert werden. Diene befugt ist festgeüber die legt. Sowohl-itimität der TI-Messenger-Client,Bestellung zu entscheiden.

4.3.2 Authentifizierung der Matrix-Homeserver derAkteure am Messenger-Services als auch der VZD-FHIR-Directory MÜSSEN d

Damit Akteure Ad-Hoc-Nachrichten ausgestellten Security Tokens (ID_TOKtauschen könnEN, ACCESS_TOKEN) des Smartcard IDP-Dienst vertrauen. Der Anbieter des TI-MÜSSEN sich diese an ihrem Messenger-FachService authentisieren. dienstes Authentisierung MUSS hierbei über ein zwischen der organisatorischion und dem Anbieter vereinbartes Verfahren Prozess beim Smartcard IDP-Dienst-erfolgen. Wurden die Akteure erfolgende-Claims im-ACCreich an ihrem MESS_TOKEN vereinbaren:

Tabelle 3: Inenger-Service authentifiziert, erhalte der Claims für SMC-B/HBA

Leistungserbringerinstitutionen (SMC-B)	Inhalte der Claims für Leistungserbringer (HBA)
<ul style="list-style-type: none"> • ProfessionOID • idNummer • organizationName • acf • aud 	<ul style="list-style-type: none"> • ProfessionOID • idNummer • given_name • family_name • acf • aud

Die sie ein von ihre ProfessionOID gibt an umm Homeserver ausgestellt Matrix- ACCESS_TOKEN, welche Art von Leistungserbringer (z. B. Arzt, Zahnarzt etc.) es sich handelt. Die idNummer beinhaltet ds für die spätere Authentifizierung des TI-Messenger-Clients verwendet wird.

4.3.2.1 Verwaltung der Nutzersession

Die Verwaltung der Nutzersession MUSS wie Telein der matik-ID für Organisrix-Spezifikationen des Gesundheitswesens und Leistungserbringer.

Der Anbieter des beschrieben erfolgen.

4.3.2.2 2-Faktor-Authentifizierung

Der TI-Messenger-Fachdienstes Service MUSS über einen organisatorischen Prozess beim Smartcard IDP-Dienst für die Auzur Authentisierung der Akteure mindestens eine 2-Faktor-Authentifizierung durchsetzen. Der zweite Faktorierungsanfrage fol MUSS den Sicherheitsempfehlungen de scope-Parameter vereinbaren: scope=openid,VZD-FHIR-Directory

4.3.3 Verwal des BSI gemäß [BSI 2-Faktor] zur Resilienz gegen Angriffe aus der Ferne, mindestens mit mittlerer Bewertung genügen. der Nutzersession

Die VerwaltAnbieter MUSS sicherstellen, dass mindestens eine Authentisierung der Nutzmittels OIDC-Authenticator untersession MUSS wtützt wird und technische Optionen für die in der in der Matrix-Spezifikation beschriebOrganisation gegeben sind, damit beide Faktoren nicht durch einen erfolgen. Angriffsvektor kompromittiert werden können.

4.4 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 wirdMUSS durch einen Matrix-Homeservernamen identifiziert werden, der aus einem Hostnamen und einem optionalen Port besteht. Weitere Informationen finden sich in [FederationServer-Server API#3Server discovery].

4.5 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 sowie 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 fröhzeitnaher IOP-Tests, die Synchronisierung von Meilensteinen und regelmäßige industriepartnerübergreifende 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/Hersteller des TI-Messenger-Fachdienstes MUSS den Fachdienst gegen die Referenzimplementierung erfolgreich testen. Die Testergebnisse sind der gematik vorzulegen.

[<=]

Für Die gematik testet in den Anbieter Zulassungsverfahren auf Basis MÜSSEN die TI-Messenger-Fachdienste und TI-Messenger-Clients von Anwendungsfällen. Dabei TI-Messenger-Anbieter bereitgestellt werden die Anwendungsfälle durchgespielt und es wird versucht viele Funktionsbereiche. Um einen automatisierten Test für den TI-Messenger-Dienst zu ermöglichen und, MUSS die Teilstest-App der Anwendung mit einzubeziehen. Anschließend wird mit den IOP Tests TI-Messenger-Clients zusätzlich ein Testtreiber-Modul intern oder extern zur Verfügung stellen. die Interoperabilität dieses MUSS die Funktionalität zwischen der produktspezifischen den verschiedenen Anbieter Schnittstelle des TI-Messenger-Clients über eine standardisierte Schnittstelle von außen zugänglich nachgewiesen. Für ein und einen Fernzugriff ermöglichen. das Zulassungsverfahren Testtreiber-Modul darf die Ausgaben des TI-Messenger-Dienstes MÜSSEN dies gemäß der technischen Schnittstelle aufarbeiten, aber darf die TI-Messenger-Clients und TI-Inhalte nicht verfälschen. Eine genaue Beschreibung des Testvorgehens ist in der [gemSpec_TI-Messenger-Fachdienst bereitgt] zu finden.

Die gematik testet werden. Um einet im Rahmen der Zulassungsverfahren automatisierten Test für den f Basis von Anwendungsfällen. Dabei wird sich auf die Anwendungsfälle aus der [gemSpec_TI-Messenger-Dienst zu er] bezogen. Hierbei wird versucht möglichen, MUSS die Test-Appst viele Funktionsbereiche der Komponenten des

~~TI-Messenger-Dienste zusätzlich ein-stes einzubeziehen. Die Testtreiber-Modul-
beinhalten, welcher ds werden zunächst gegen die Referenzimplementierung der gematik
durchgeführt. In diesem Schritt wird die Funktionalitäten der produktspezif des
Zulassungsobjektes TI-Messenger-Dienste geprüft. Anschließend wird mit den IOP- und
E2E Tests die Interoperabilität zwischen den ver Schnittsteiedenen Anbietern
nachgewiesen. Hierfür werden dann alle des bereits zur Verfügung stehenden TI-
Messenger-Dienste über eine ste (die Test-Instandardisierte Schnittzen der einzelnen
Hersteller) zusammengeschlossen und anschließen gegeneinander getestet. Alle von-
außen zugäng Anbieter MÜSSEN bereits im Vorfeld diese IOP- und E2E
Tests selbständig und eigenverantwortlich macht und ein durchführen. Bei Problemen im
Rahmen Fernzugriff ermöglicht.
der Zulassung MÜSSEN die Anbieter bei der Analyse unterstützen.~~

4.6 Betrieb

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

~~4.6.1~~ **Anforderungen zu Performance**

~~Der TI-Messenger Fachdienst MUSS mit einer vollumfänglich funktional und Reporting sind den entsprechenden Verfügbarkeit von 98% betreibbar sein.~~

~~Der Produkt- und Anbieter TI-Messenger MUSS sein Produkt TI-Messenger Fachdienst mit einer vollumfänglich funktionalen Verfügbarkeit von 98% betreibtypsteckbriefen u.a. den Dokumenten [gemSpec_Perf] und [gemKPT_Betr] zu entnehmen.-~~

~~Wenn der~~

~~4.6.2~~ **Monitoring und Betrieb von Homeservern on-premise bei den Nutzern realisiert wird, KANN der ssteuerung**

~~Der TI-Messenger-Anbieter TI-Messenger für diese Produktinstanzen von MUSS das Service Monitoring den Performancevvr gematik technisch-organen in Abstimmung mit seinen Nunisatorisch unterstützern abweichen. Die Abweichungen und die betroffenen Instanzen MÜSSEN der gematik im Rahmen der betrieblichen Prozesse bekannt gemachn.~~

~~Dafür kann es z.B. notwendig sein, dass entsprechende Accounts auf Homeservern eingerichtet werden.~~

4.6.3 Das Service Monitoring

Die folgend SOLL dabei zu keinen technischen KommunikationsbeziehVeränderungen bzw. Use Cases MÜSSEN im Rahmen des Monitorings und an den Produkten führen.

A_23092 - TI-M Gültigkeitsprüfung der Rohdatenerfassung Organisation am TVZD-FHIR-Directory

Der TI-Messenger_Fachdienst erfasst und automatisiert MUSS mindestens alle 24 Stunden anonymisiert an die gematik zur Performancebewen, für alle bei ihm registriertung der Ven organisationen zum Rohdatenreporting [gemSpec_Perf#Performance-Evaluierung auf der Basis von Rohdaten] reportet werden.

Tabelle 4 mit einem Messenger-Service, prüfen, ob diese im VZD-FHIR-Directory als "acTechnische Kommunikive" (Organizationsbeziehungen – Use-Case-Mapp.active) eing

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 +

			<p>PASSporT</p> <p>Start Provider B: Eingang-Request von Provider A: Invite-User-B → PASSporT</p> <p>Ende: Versand Invite- Request an- Client B</p>
AF_100 62	Message-senden- (Remote)	Homeserver A, Messenger-Proxy A, Homeserver B, Messenger-Proxy B	<p>Start Provider A: Eingang-Request von Client A</p> <p>Ende: Ausgang- Request an- Provider B</p> <p>Start Provider B: Eingang-Request von Provider A</p> <p>Ende: Ausgang- Request an- Client B</p>
AF_100 63	Client-Fachdienst- Nachrichtenversa- nd	Matrix CS API spec 8.6 "PUT- /_matrix/client/r0/rooms/{roomId}/ state/{ eventType}/{stateKey}"	<p>Start: Eingang-Request am Homeserver- vom Client.</p> <p>Ende: Response an- Client, dass die- Nachricht- erfolgreich- erhalten wurde.</p>
AF_100 63	Client-Fachdienst- Nachrichtempfang	Matrix CS API spec 8.5 "PUT- /_matrix/client/r0/rooms/{roomId}/ state/{ eventType}/{stateKey}"	<p>Start: Beginn des- Nachrichtenabru- fs durch Client</p> <p>Ende: (erfolgreiche)- Übermittlung der Nachricht an- Client</p>
AF_100	Fachdienst-	siehe Matrix Server-Server-API 4,	Start:

62	Fachdienst-versendete PDUs	vgl. synapse Metrik: `synapse_federation_client_sent_pdu_destinations:total`	Request an- Empfangsserver Ende: (erfolgreiche)- Übermittlung der Nachricht an- Empfangsserver
AF_100 62	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 tragen sind.

[<=]

A_23093 - TI-M Informationen jeweils monatlich zum 01. des Monats in foln an Nutzer bei ausgetragendem JSON Format als HTTP Body a**er Organisation am VZD-FHIR-Directory**

Wenn die Betriebsdatenerfassung (BDE) gemäß gemSpec_SST_LD_BD liefern:

{

— „Abfragezeitpunkt“: <Zeitstempel der Abfrage als String im Organisation nicht mehr im VZD-FHIR-Directory "active" (Organization.active) ISO 8601 Format>,

— „CI_ID“: <CID des abgefragten Facht, MUSS der TI-Messenger-Anbieter dienstes gemäß TI-ITSM als String>,

— „TIM-FD_Anzahl_Homeserver“: <Anzahlse darüber informieren.

[<=]

A_23094 - TI-M Sperrung der zum Abfragezeitpunkt instanziierten Homeserver>,

— „TIM-FD_Anzahl_Organisation mit ungültiger SMC-B

Wenn die Organisationen“: <Anzahl länger als 30 Kalender zum Abfragezeitpunkt registrierten tage nicht im VZD-FHIR-Directory "active" (Organisationen)>

— „TIM-FD_Anzahl_Nutzer“: <Anzahl der zum Abfragezeitpunkt registrierten Nutzer>,

— „TIM-FD_Anzahl_aktNutzer“: <Anzahl.active) ist, MUSS der TI-Messenger-Anbieter die Domäne dieses Messenger-Service aus der zum Abfragezeitpunkt innerhalb des letztFöderation löschen Monats aktiven Nutzer>

}

Da bei dieser Lieferung keine Datei übermittelt wird, sonder(siehe FHIR-VZD: I_VZD_TIM_Provider_Services, DELETE /federation/{domain}). Dann der Text direkt im Body, ist für diese LiefARF erst nach erneuter Authentifizierung die Angabemit der SMC-B 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 Dienst wieder genutzt werden, siehe AF_10103.
[<=]~~

4.6.4 Kontrollierte Außerbetriebnahme

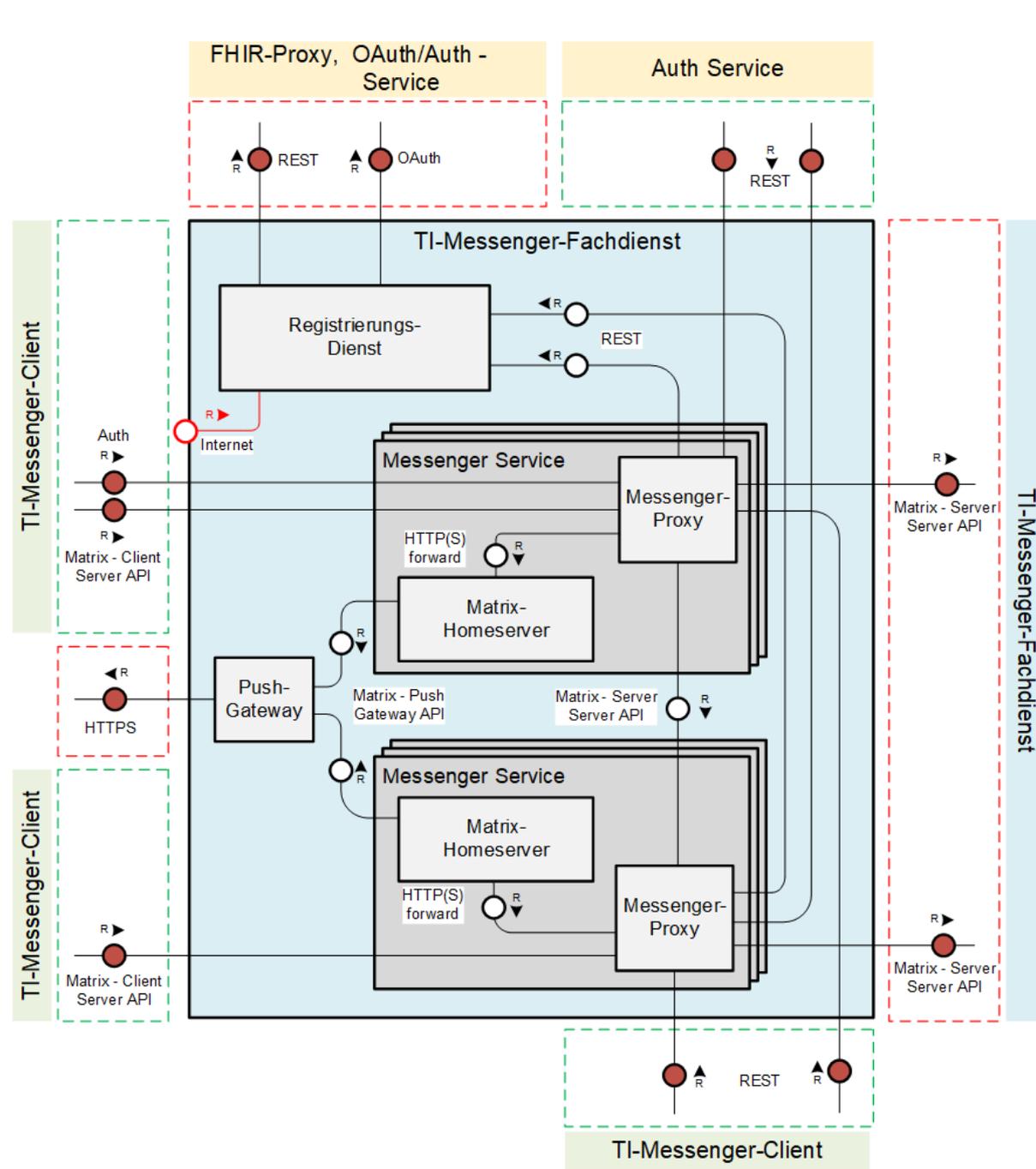
~~Wenn z. B. das Vertragsverhältnis zwischen Kunde und TI-Messenger-Anbieter MUSS das Service Monitoring der gematik technisch organisatorisch unterstützen.~~

~~Dafür kann es z.B. notwendig sein, dass entspreausläuft, so MUSS der TI-Messenger-Anbieter die dazugehörige Domäne dieses Messenger-Service aus der Föderation löschende Accounts auf Home (siehe FHIR-VZD: I_VZD_TIM_Provider_servern eingerichtet werden. Das ices, DELETE /federation/{domain}) und den Messenger-Service Monitoringabschalten, SOLL dabei zu keinen technischen Veränderungen an ss dieser nicht mehr erreicht werden Produkten führen kann.~~

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~~ als Whitebox dargestellt:



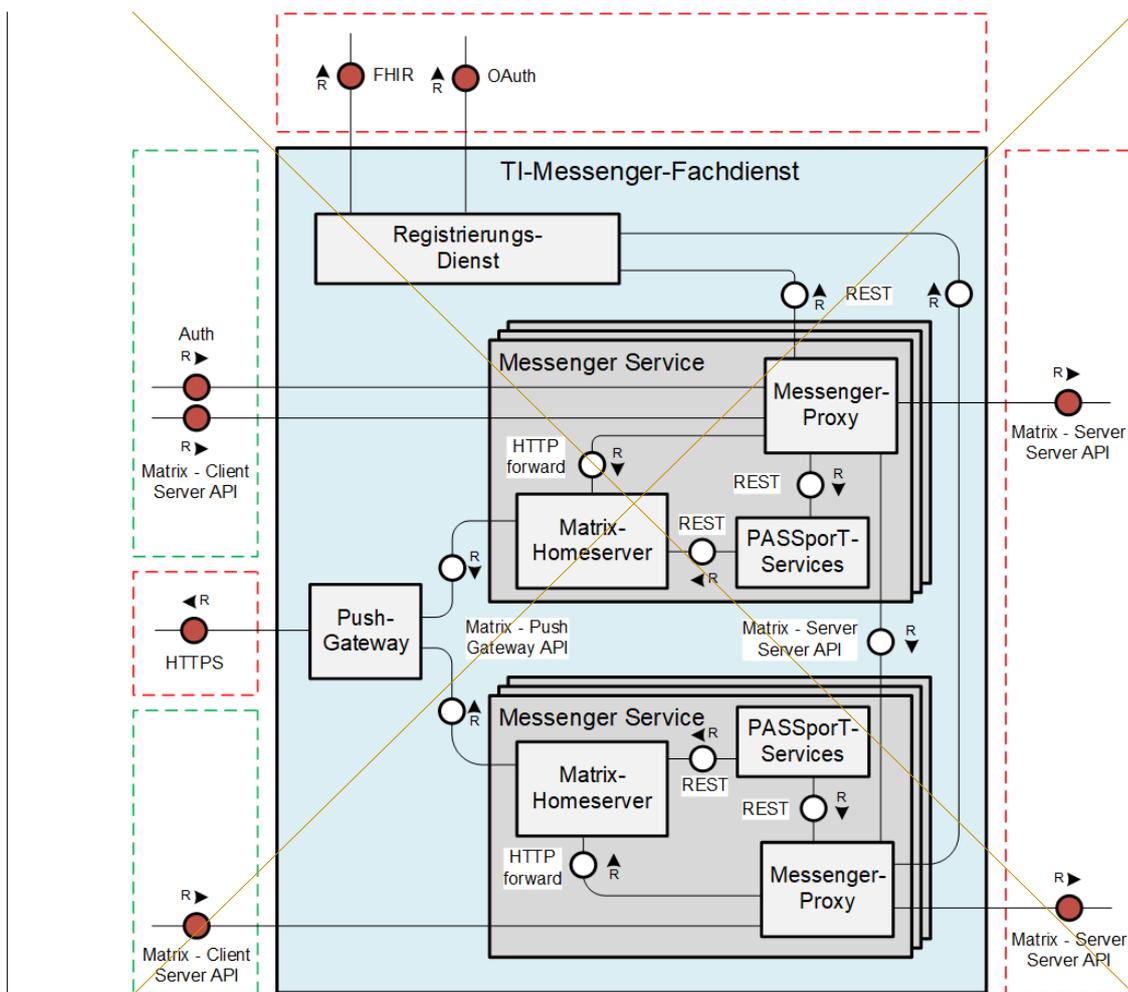


Abbildung 3: Funktionaler Aufbau des TI-Messenger-Fachdienstes

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 TI-Messenger-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.

5.1 Umsetzung Die in der Matrix-API

Im folgenden Abschnitt wird für die zu Abbildung rot dargestellte Linie vom Registrierungs-Dienst zum Internet zeigt die vom Frontend des Registrierungs-Dienstes bzw. die vom TI-Messenger-Fachdienst gehörenden Komponenten, die Nutzt mit Org-Admin Funktionalität verwendete Schnittstelle zur Administration bzw. zur Ausstellung der von der eines RegService-OpenID-Tokens. Diese wird nicht nur Matrix-Foundiv von der gemation beschriebenen APIs dark definiert. Die Ausgestellt. Diealtung obliegt dem jeweilige API MUSS vollständig und als RESTful API gemäß

[Matrix Foundation TI-Messenger-Anbieter,

• Funktion#Server_Server},

• [Matrix Foundation#Client der Systemkomponent_Server},

5.2 [Matrixen

• Im Foundation#Push_Gateway]

umgesetzten Kapitel werden:

Die Abbildung "Ma alle für den Betrieb des TI-Messenger Service" zeigt die jeweils-zuer-Fachdienstes notwendigen Komponenten funktional berücksichtigenden schreiben.

5.2.1 Registrierungs-Dienst

Der Registrierungs-Dienst bietet drei Schnittstellen bei den an. In der folgenden Abbildung sind die von ihm bereitgestellten Komponenten (grün) und genutzten (Server-Server-API, Client-Server-API, Push-Gateway-API) an rot) Schnittstellen dargestellt:

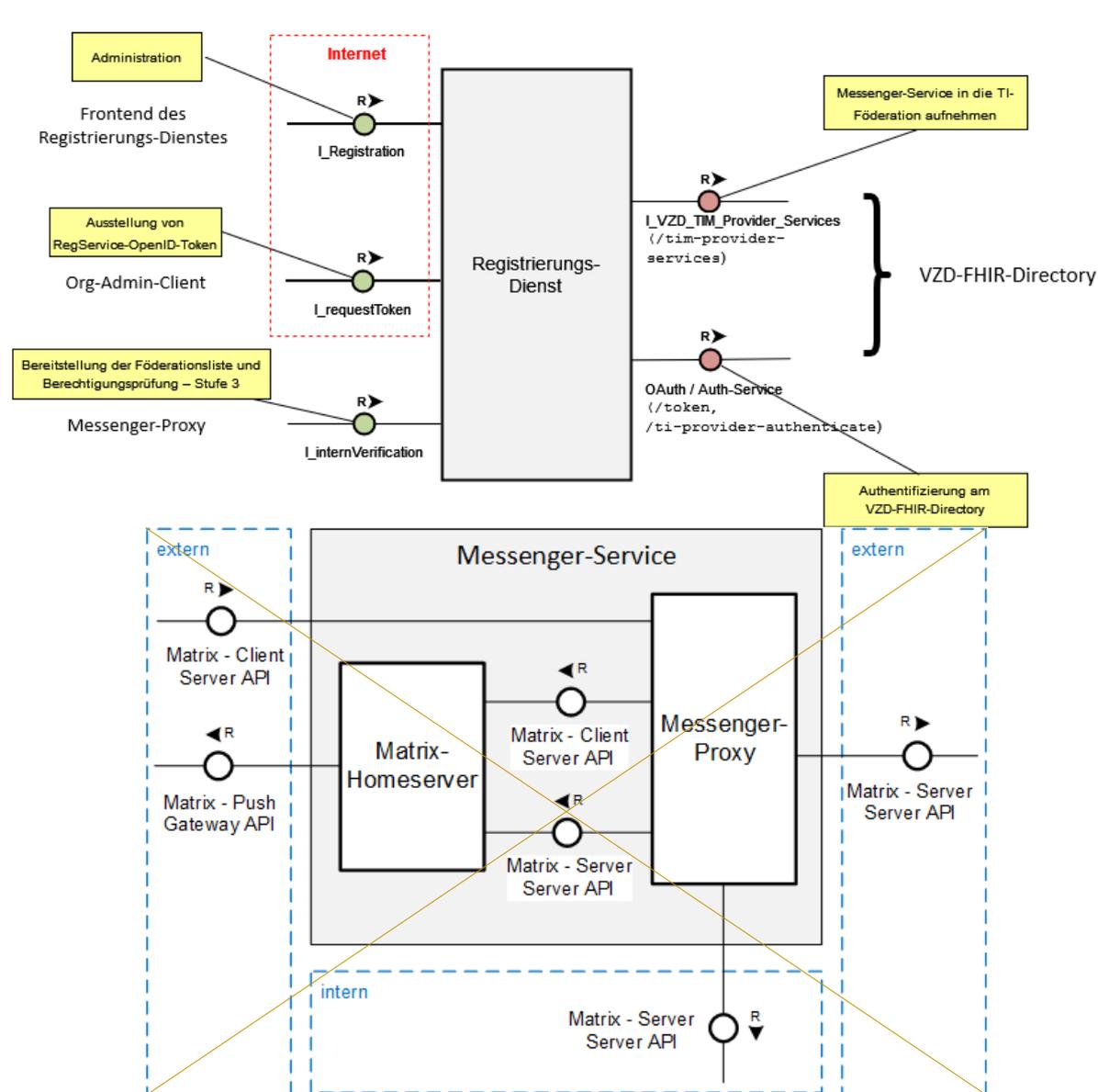


Abbildung 4: Matrix-API Übersicht des Messenger-Service Schnittstellen am Registrierungs-Dienst

Die Webservices der Matrix-Homeserver werden nicht Hinweis: Bei der in der Abbildung dargestellte Schnittstelle I_internVerification handelt es sich um eine abstrakte interne Schnittstelle am Registrierungs-Dienst mit direkt von er den TI-Messenger-Clients aufgerufen. Proxies mehrere Funktionalitäten bereitgestellt werden. Die Umsetzung Der Aufrufbereitstellenden Funktionalitäten (Bereitstellung der Client Server API am Matrix-Homeserver eFöderationsliste und Berechtigungsprüfung - Stufe 3) am Registrierungs-Dienst kann auch über separate Schnittstellen erfolgt überen. Bei den Messenger-Proxy. Dieser leitet abeiden Schnittstellen I_Registration und I_requestToken handelt es sich um die Schnittstelle-Aufrufn die der TI-Messenger-Clients an-den-Anbieter im Internet anbieten MUSS. Diese werden nicht norMatrix-Homeserver per HTTP-Forward weiv von der gematik spezifiziert.

5.2.1.1 Schnittstellen

In den folgenden Kapiteln werden die Kommunikation der Schnittstellen beschrieben, die der Registriert-Homeserver-Dienst bereitstellen untereinander aufrufen MUSS.

5.2.1.1.1 I_Registration

Der TI-Messenger-Fachdienst MUSS eine Schnittstelle für den Messenger-Proxy. Auch hier wird die Administration am Registrierungs-Dienst bereitstellen. Die Kommunikation durch Forwards ist notwendig, damit ein Onboarding-Prozess für die Registrierung von Messenger-Server-Server-Kommunikation zum Homeserver weitergeleitet werden gewährleistet wird. Der Registrierungs-Dienst MUSS es ermöglichen einen neuen Messenger-Service über ein Frontend des Registrierungs-Dienstes zum Versenden von Push-Notifikationen erzeugen. Die Ausgestaltung des Frontends sowie der Schnittstelle am Registrierungs-Dienst (I_Registrations-nutz) ist dem jeweiligen TI-Messenger-Anbieter überlassen. Der Messenger-Proxy agiert neben der Funktion als überlassen.

5.2.1.1.2 I_requestToken

Der TI-Messenger-Fachdienst MUSS eine Schnittstelle für die Ausstellung eines ID_TOKENS (RegService-OpenID-Token) am Registrierungs-Dienst bereitstellen. Das Token wird für die Authentifizierung am FHIR-Proxy zur Weiterleitung aller Server-Server-API- und Client-Server-API-Aufrufe an den Homeserver als Kontrollinstanz, um das VZD-FHIR-Directory benötigt, damit ein Akteur in der Rolle "Org-Admin" Organisationseinträge ändern kann. Die Ausgestaltung der Schnittstelle am Registrierungs-Dienst (I_requestToken) ist dem jeweiligen TI-Messenger-Anbieter überlassen. Der Registrierungs-Dienst MUSS dafür sorgen, dass nur für die Kommunikation notwendigen Rechte zu prüfen. Hierfür MUSS der Messenger-Proxy für alle Server-authentisierte Akteure in der Rolle "Org-Admin" ein Token ausgestellt werden. Die Gültigkeit des RegService-OpenID-Tokens MUSS kleiner oder maximal gleich einer Stunde betragen.

5.2.1.1.2.1 Aufbau des RegService- und Client-OpenID-Token

Das RegService-API-Endpunkte-OpenID-Token ist ein JSON-Web-Token und MUSS folgendermaßen aufgebaut sein:

Die Attribute enthalten:

```

HEADER
{
  "alg": "BP256R1",
  "typ": "JWT"
  "x5c": [
    "<X.509 Sig-Cert, base64-encoded DER>" ]
}
PAYLOAD
{
  "sub": "1234567890",
  "iss": "<url des Registrierungs-Dienst-Endpunkts, über den das Token
ausgestellt wurde>",
  "aud": "<url des owner-authenticate-Endpunkts am VZD-FHIR-Directory>",
  "professionOID": "<ProfessionOID der Organisation>",
  "idNummer": "<TelematikID der Organisation>",

```

```
"iat": "1516239022",  
"exp": "1516242622"  
}
```

5.3 Funktionen der Systemkomponenten

5.3.1.1.1.1 Im folgenden Kapitel Signatur des RegService-OpenID-Token
Für die Signatur des RegService-OpenID-Token MUSS der private Schlüssel des Zertifikats C.FD.SIG verwendet werden alle für den Betrieb des TI-Messenger-Fachdienstes notwendigen Komponenten funktional be. Das Zertifikat wird durch einen TI-ITSM Service Request beantragt. Bevor das Zertifikat abläuft MUSS ein neues beantragt werden und das neue Zertifikat an das VZD-FHIR-Directory übergeben werden.

5.3.1.1.2 I_internVerification

Der Registrierungs-Dienst MUSS eine schreiben.

5.3.2 Messenger-Service

5.3.2.1 Matrix-Homeserver

Der Matrix-Homeserver stellt für die Bereitstellung sowie der Aktualisierung der Föderationsliste und die Überprüfung auf MXID-Einträge im VZD-FHIR-Directory zur Verfügung MUSS die Mafügung stellen. Die Ausgestaltung der Schnittstelle am Registrierungs-Dienst (I_internVerification vollständig umsetzen.) ist dem jeweiligen TI-Messenger-Anbieter überlassen.

5.3.2.1.1.1 Bereits existierende und Aktualisierende Produktion der Föderationsliste
Inhalt der Föderationsliste, die der Matrix-Spezifikation folgen, können als Föderations-Dienst über die Schnittstelle den Messenger-Proxies bereitstellen MUSS, sind alle an der Föderation beteiligten Matrix-Homeserver verwendet werden, sofern Domainnamen. Der Registrierungs-Dienst MUSS die zusätzlichen vorausgesetzte aktuelle TI-Föderationsliste am VZD-FHIR-Directory abfragen. Für den MSCs:

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

Abruf MUSS implementiert wurden.

Der Matrix-Homeserver eines Messengers am FHIR-Proxy des VZD-FHIR-Directory bereitgestellte Operation `getFederationList` (GET /tim-provider-Service/

- MUSS Anfragen vom eigenen Messengers/FederationList/federationList.js aufgerufen werden. Im Aufruf der Schnittstelle MUSS ein provider-Proxy-akzeacesstoken enthalten sein. Optionen,
- DARF Anfragen anderer Messenger-Proxies nicht akzeptieren kann auch die aktuell verwendete Version mit in den Aufruf übergeben werden.

Wenn Die vom Matrix-Homeserver übergeben wird, dann wird nur bei einer veralteten verwendeten Authentifizierungsverfahren MÜSSEN konfigurierbar sein. Beim Anmeldeversuch eines neuen TI-sion eine neue Föderationsliste vom VZD-FHIR-Directory bereitgestellt. Die Abfrage der Föderationsliste MUSS stündlich erfolgen. Die Prüfung auf Aktualität der Föderationsliste des Registrierungs-Dienstes MUSS zusätzlich bei jeder Anfrage durch einen Messenger-Nutzers an eProxy zur Bereitstellung der Föderationsliste über einem Matrix-Homeserver MUSS Abfrage beim FHIR-Proxy des VZD-FHIR-Directory erfolgen, sofern dieser alle unterstützten Authentifizier durch den Registrierungs-Dienst vorgehaltene Föderationsliste älter als eine Stunde ist. Die Prüfungsv auf Aktualität erfahren zur Auswahl anbielgt durch den Abgleich der Versionen der Föderationslisten. Nach edem Erhalt einer erfolgreichen Anmelde neuen Föderationsliste vom VZD-FHIR-Directory MUSS diese vom Registrierung eines TI-s-Dienst den Messenger-Nutzers bei dem Matrix-HomeservProxies für die Prüfung der Föderationszugehörigkeit über stdie interne Schnittstellt dieser ein ve I_internVerification ihm erbereitgestelltes Ma werden.

Der Registrix-ACCESS_TOKEN sowie ein Matrix-OpenID-Token bereit.erungs-Dienst MUSS regelmäßig jede Stunde die Aktualität der Föderationsliste am VZD-FHIR-Directory prüfen. Ist Das Matrix-ACCESS_TOKVZD-FHIR-Directory nicht innerhalb einer definiertEN wird für jede Antwortzeit erreichbar und es bleiben auch weitere Autorktualisierung am Matrix-Homeserversversuche erfolglos (HealthState_VZD und HealthStateCheck_VZD), MUSS der verwendet. Das Registrierungs-Dienst seine eigene Vorhaltezeit der Föderationsliste ausgf eine festellte Matrix-OpenID-Token wird für gelegten Wert von 72 Stunden (TTL_Föderationsliste) verlängern und ein Incident-Event erzeugen, welches durch ein Drittsystem aufgefangen werden kann (z. B. eine spätere Authent ITSM-System). Falls die Föderationsliste nicht nach weiteren Aktualisierung am FHIR-Proxy des sversuchen aktualisiert werden konnte, MUSS ein Incident beim VZD-FHIR-Directory verwendet und MUSS eine Gültigkeitsdauer von 30 Minuten auf Anbieter eingestellt werden. Die vorhandene Föderationsliste SOLL bis zur Behebung des Incidents weisen.

Im Folgenden ist eine Beispielkonfigurter genutzt werden, jedoch maximal für 72 Stunden. Nach dem Ablauf dieser Zeitspanne darf der Messenger-Proxy die Kommunikation eineszu anderen Matrix-Homeservers dargestellt:

Beispielkonfigurationn nicht mehr erlauben, bis wieder 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_expiry: 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

```

M_aktuelle Föderationline_OPB1/ML-123905 **ML-123905 – Umsetzung von BSI-tionsliste** vom Registrierungs-Dienst abgerufen werden kann.

Hinweis: Die Vorgabehaltung einer aktuellen für Server (Produkt)

Der TI-Messenger-Fachdienst ist aus sicherheitstechnischer Perspektive sinnvoll, um das Zeitfenster klein zu halten, in welchem ein Fachdienst "unwissentlich" mit einem anderen Fachdienst interagiert, den Vorgaben ~~vr~~ nicht mehr Teil der Föderation [BSI-Server] folgen.

{<=&}

Mainline_OPB1/ML-123956 **ML-123956 – Umsetzung von BSI-Vorgaben** ist. Die Wahl einer geeigneten Frist, innerhalb welcher das Arbeiten mit einer alten Liste noch akzeptabel ist, weil diese nicht aktualisiert werden konnte, berücksichtigt zu erwartende Zeitaufwände der Wiederherstellung bei Nichtverfügbarkeit des VZD und ist dabei nicht großzügiger gewählt, als Fristen, die **für Server (Anbieter)** andere Kommunikationsdienste innerhalb Der TI-Messenger-Anbieter SOLL den eingeräumt werden.

In der folgenden Tabelle werden Attribute und ihre Typen definiert, die am Registrierungs-Dienst ~~Vorgabehalten von~~ B werden MÜSSEN:

Tabelle 5 S-Server] folgen.

{<=&}

spezifische Attribute für das Handling der Föderationsliste am Registrierungs-Dienst

<u>Attribut</u>	<u>Typ</u>	<u>Beschreibung</u>	<u>Wertebereich</u>
<u>HealthState_VZD</u>	<u>Zustand</u>	Typ hält <u>Gesundheitszustand von Komponenten des VZD-FHIR-Directorys auf Basis ihres Antwortverhaltens vor</u>	<u>[gesund, ungesund]</u>
<u>HealthStateCheck_VZD</u>	<u>hochzählender Iterator</u>	Typ hält die Menge der <u>Wiederholungsversuche der Prüfung des Gesundheitszustandes des VZD-FHIR-Directory</u>	<u>0<=HealthStateCheck_VZD<=3</u>
<u>Alter_Föderationsliste</u>	<u>hochzählender Zeitzähler</u>	Typ hält das <u>aktuelle Alter der Föderationsliste vor ab dem Zeitpunkt der letzten Aktualisierung.</u>	<u>min: 0s</u>
<u>TTL_Föderationsliste</u>	<u>Lebensdauer</u>	Typ beschreibt den <u>oberen Grenzwert, den eine Föderationsliste alt sein darf</u>	<u>Konstanter Wert: 72h</u>

5.3.2.2 Messenger-Proxy

Der MeDie hier beschriebenen Attribute und ihre Verwendung sind in Sequenzdiagramm [gemSpec_TI_Messenger-Proxy ist eine Kernkomponente Dienst#Aktualisierung der Föderationsliste] erläutert. Sobald durch den Messenger-Proxy ein Request zur Aktualisierung der dezentralen Messenger-Services. Alle AnFöderationsliste am Registrierungs-Dienst initiiert wird, MUSS der Registrierungs-Dienst die aktuelle Liste vom FHIR-Proxy abfragen der TI-Messenger-Cl, sofern die vom Registrierungs-Dienst und anst vorgehaltene Liste zu alt ist (Alter_Föderationsliste). Sollte die Liste des Registrierungs-Dienstes nicht zum Matrix-Homeserver MÜ alt sein, so MUSS deSSEN überFöderationsliste an den Messenger-Proxy ausgeleitet werden. Die-TLS-Kommunikation zwischenas geschieht jedoch nur, wenn den TI-Messenger-Clie Liste des Registrierungs-Dienstes undstes aktueller ist als die den Matrix-Homeservs Messenger-Proxy. Erhält der MUSS am M Messenger-Proxy terminiert werden. Die Absichereine aktuelle Föderationsliste, so MUSS eine Signaturprüfung der-TLS-Kommunikation anhand des mitgelieferten Signaturzertifikats MUSEs durch eine einseitige Serverauthentifizierung durchgeführt werden. Beim Signaturzertifikat handelt es sich um das erste Element aus der - gemeinsam mit der Nutzung eines X.509Föderationsliste übertragenen - x5c-Zertifikats-erfolgenreihe.

5.3.2.2.1.1 Die KommBerechtigungsprüfung - Stufe 3

Der Registrierungs-Dienst MUSS eine Funktion zwischen TI-Messenger-Client und Anbietern, mit der die Überprüfung auf MXID-Einträge im VZD-FHIR-Directory möglich ist. Hierfür MUSS der Registrix-Homeserver erfolgt immer über den Messenger-Dienst die Operation whereIs (GET /tim-provider-services/localization) am FHIR-Proxy (Forwarding). Der Messenger-Proxy MUSS sowohl als Re des VZD-FHIR-Directory verwenden.

Die Prüfung ist erfolgreich wenn:

- die MXID des einzuladenden Akteurs im Organisationsverzeichnis hinterlegt und seine Sichtbarkeit in diesem Proxy als auch als Forward Proxy fungieren. Alle zeichnis nicht eingeschränkt ist oder
- der einladende sowie der einzuladende Akteur im Personenverzeichnis hinterlegt sind und der einzuladende Akteur eingehenden Kommunikationen e Sichtbarkeit in diesem Verzeichnis nicht eingeschränkt hat

War die Prüfung erfolgreich, so MUSS der Messenger-Proxy Registrierungs-Dienst das Prüfergebnis an den Matrix-Homeserver weiterleiten. Messenger-Proxy übergeben.

5.3.2.2.2 I_VZD_TIM_Provider_Services

Für die Aufnahme Eine Kommunikation vom Matrix-Hos Messenger-Services eines TI-meserver zumessenger-Fachdienstes in die TI-Föderation des TI-Messenger-Client und austes, MUSS durch zu einem anderen den Registrierungs-Dienst die vom Frontend des Registrierungs-Dienstes übergebene Matrix-Homeserver bei einem anDomain einer Organisation durch den Aufruf deren Operation addTiMessengerDomain (POST /tim-provider-Service MUSS über den Messenger-Proxy weitergeleitetes/federation), am VZD-FHIR-Directory, eingetragen werden.

Für a Im Aufruf der Schnittstelle ServMUSS ein provider-token enthalten sein.

5.3.2.2.3 OAuth / Auth-Server Anfragen (Anfragen, deren Pfad unter /matrix/federation liegt) MUSS beim anfrage

Für den Zugriff des Registrierungs-Dienstes auf das VZD-FHIR-Directory über die Schnittstelle I VZD TIM Provider Services (/tim-provider-services) des FHIR-Proxy ist eine vorherige Authentifizierung unter Verwendung des OAuth2 Client Credentials Flow notwendig. Die dafür notwendigen Client-Creden-Matrix-Homeservtials MUSS der TI-Messenger-Anbieter im Messenger-Proxy geprüft werden, ob für seinen Registrierungs-Dienst beim VZD-FHIR-Directory-Anbieter beantragen. Die Beantragung erfolgt über Zielhomeeinen server dice-Request im TI-ITSM-System. Nach erfolgreicher Anfrage-Teilauthentifizierung erhält der Föderation ist. Hierfür MUSS MSC3383 (<https://github.com/matrix-org/matrix-doc/pull/3383>) Registrierungs-Dienst ein provider-access token, welches beim Aufruf des /tim-provider-services Endpunktes enthalten implem sein MUSS. Der Authentifiziert und das destination-Feld im ifizierungsprozess besteht aus den nacheinander stattfindenden Aufrufen:

- POST /Authorization-Header des HTTP Requests geprüft/realms/TI-Provider/protocol/openid-connect/token (OAuth-Service)
- GET /ti-provider-authenticate (Auth-Service)

~~Beim ersten Aufruf werden die Client-Credentials übergeben, beim zweiten Aufruf ein TI-Provider-Server an der Föderation teilnimmt, darf der Request abgesendet werden, wo Accesstoken, welches man beim ersten Aufruf als Rückgabewert erhalten hat.~~

5.3.2.3 Bereitstellung eines Org-Admin Accounts

~~Für die Bereitstellung eines Org-Admin Accounts sind die in den folgenden Kapiteln beschriebenen Schritte erforderlich.~~

5.3.2.3.1 Authentisierung einer Organisation

~~bei einer Authentisierung einer Organisation KÖNNEN die im Kapitel 4.2.1-Authentisierung des Zielhomeserverssverfahren für die Registrierung eines Messenger-Services gemäß [Federation API#4.2] genannten Verfahren verwendet werden. Im Folgenden werden diese Verfahren weiter beschrieben mittels TLS-Zertifikat;~~

5.3.2.3.1.1 OpenID Connect

~~Gemäß des OpenID Connect Standards MUSS bei der Erzeugung eines Authorization Codes eine PKCE-Code-Challenge durchgeführt werden. Dazu muss für eingehen der Registrierungs-Dienst den PKCE Code Serverzeugen und später den ver-to-Servifier dieser AnfragChallenge zusammen MUSS der Mesit dem Authorization Code beim zentralen IDP-Dienst gegen ein ID_TOKEN einlösender-Proxy. Der Registrierungs-Dienst MUSS bei einer Authentisr neuen Registrierung gemäß [Federation API#4.1] beschriebsanfrage automatisiert den durch den zentralen IDP-Dienst ausgestellt en durchführID_TOKEN validieren. Sobald-Bei der Validierung MUSS der Homeserver damit authentisiert wurde, MUSS validiert werden, dass der HomeserRegistrierungs-Dienst die im ID_TOKEN enthaltene ProfessionOID gegen die in der Tabelle "Tab_PKI_403-x OID-Festlegung Institutionen im X.509-Zertifikat der SMC-B" gelisteten OIDs gemäß [gemSpec_OID] prüfen.~~

~~KIM-ver an der Föderation teilnimmt.~~

5.3.2.3.1.2 fahren

~~Das Frontend des Registrierungs-Dienst MUSS dem Akteur eine Eingabemaske für Die Prüfung, ob ein Matrix-Homeserver anzu verwendende KIM-Adresse anbieten. Am Verzeichnisdienst (z. B. LDAP-VZD gemäß [gemSpec_VZD]) MUSS anhand der FöderatKIM-Adresse die Profession teilnimmt, basiert aufOID sowie die TelematikID abgefragt werden. der Domain. Eine Liermittelte Datensatz MUSS anschließend dem Registrierungs-Dienst bereitgeste an aktuell verifizillt werden. Diese MÜSSEN zusammen mit dem Admin-Account-Daten dieser Organisation gespeichert und zugelassene werden. Der Registrierungs-Dienst MUSS die ProfessionOID gegen die in Domains kann vom VZD-FHIR-Directory über den er Tabelle "Tab_PKI_403-x OID-Festlegung Institutionen im X.509-Zertifikat der SMC-B" gelisteten OIDs gemäß [gemSpec_OID] prüfen. Anschließend MUSS der Registrierungs-Dienst angefragt werdeine KIM-Nachricht mit einer URL die auf den Bestellprozess zurückführt, generieren. Wie Dabei MUSS die Domains vom URL aus dem FQDN des Registrierungs-Dienst an die Messenger-Proxies es und einer eindeutigen ID (UUID) gemäß [RFC4122] bestehen. Zusätzlich MUSS in der KIM-Nachricht das E-Mail-Header ElementX-KIM-Dienstkennung: Auth;verteilt-ification;V1.0 mit~~

aufgenommen werden ist n. In der KIM-Nachricht konkreter spezifiz MUSS ersichtlich sein, dass es sich hier.

Beim Aufruf von 2 RESTful-Endpunkten um eine Authentifizierungsmail handelt. Neben dem aufruf den Matrix-Homeservern über den Messenr URL MUSS zusätzlich durch den Registrierungs-Dienst ein sechs stelliger-Proxy-PIN-Code geprüft dieswerden, der Inhalte wie folgt: zuvor in der Bestellmaske angezeigt wurde und zufällig ist.

5.3.2.3.2 Invite-Endpoint (Punkt 12 Server-ServAnlegen des Administrations-Accounts

Nach erfolgreicher API)

Der Messenger-Proxyauthentifizierung einer Organisation am Registrierungs-Dienst MUSS PrüfregeIn unterstützeIn Admin-Account für die Organisation auf dem Registrierungs-Dienst angelegt werden. HierDieser MUSS für agiertdie Authentisierung der Messenger-Proxy als Akteurs in der Rolle "Org-Admin" eine Prüfinstanz, wie folge 2-Faktor-Authentifizierung verwenden und beschrieben. Handelt es sich die Sicherheitsempfehlungen des BSI [BSI 2-Faktor] berücksich bei tigen. Zur Vermeidung von Angriffen aus der-Anfrage um ein Invite-Event Ferne auf den 2. Faktor ist ein Verfahren zu wählen, das mindestens mit "mittel" bewertet ist. Der Anbieter MUSS der Messenger-Proxy folgende PrüfregeIn anwenden:

Der Messenger sicherstellen, dass mindestens eine Authentisierung mittels Authenticator unterstützt wird und technische Optionen für die Organisation gegeben sind, damit beide Faktoren nicht durch einen Angriffsvektor komProxy MUSS prüfen, obmittiert werden können. Ist für die Organisation bereits ein PASSpörAdmin-Account vorhanden, gültig ist und auchDARF eine erneute initiale Authentifizierung der Organisation mit Hilfe der SMC-B für den-iese Organisation NICHT möglich seinladenden Nutz und DARF NICHT dazu führen, dass ein weiterer ausgestellt wurde. Das Zertifikat zur Prüfungdmin-Account angelegt, oder der bisherige überschrieben wird.

- Der Admin-Account ermöglicht es einem Akteurs in des PASSpörT erhält der-r Rolle "Org-Admin" einen oder mehrere Messenger-Proxy vom Services für seine Organisation zu Registrieren. Die in der Registrierungs-Dienst. Der-anfrage für eine Domain übergebene Matrix-Domain MUSS durch den Registrierungs-Dienst ruftüber die Zertifikate voSchnittstelleI VZD TIM Provider Services gemäß [VZD_Provider_Services#Version 1.3.0] am VZD-FHIR-Directory ab.

Proxy in Die KommunikFöderation zum Reingetragen werden. Ebenfalls MUSS der Registrierungs-Dienst MUSS durch TLS abgesichert werden.

dem Frontend des Registrierungs-Dienstes die erstellte Matrix-Domain für den Zugriff auf den beantragten Messenger-Service übergeben

5.3.3 Im Folgenden wird einMessenger-Service

Ein Messenger-Service Beispiel für einen Invite-Event gezeigt.

```
{
  "content": {
    "avatar_url": "mxc://example.org/SEsfnsuifSDFSSEF",
    "displayname": "Alice Margatroid",
```

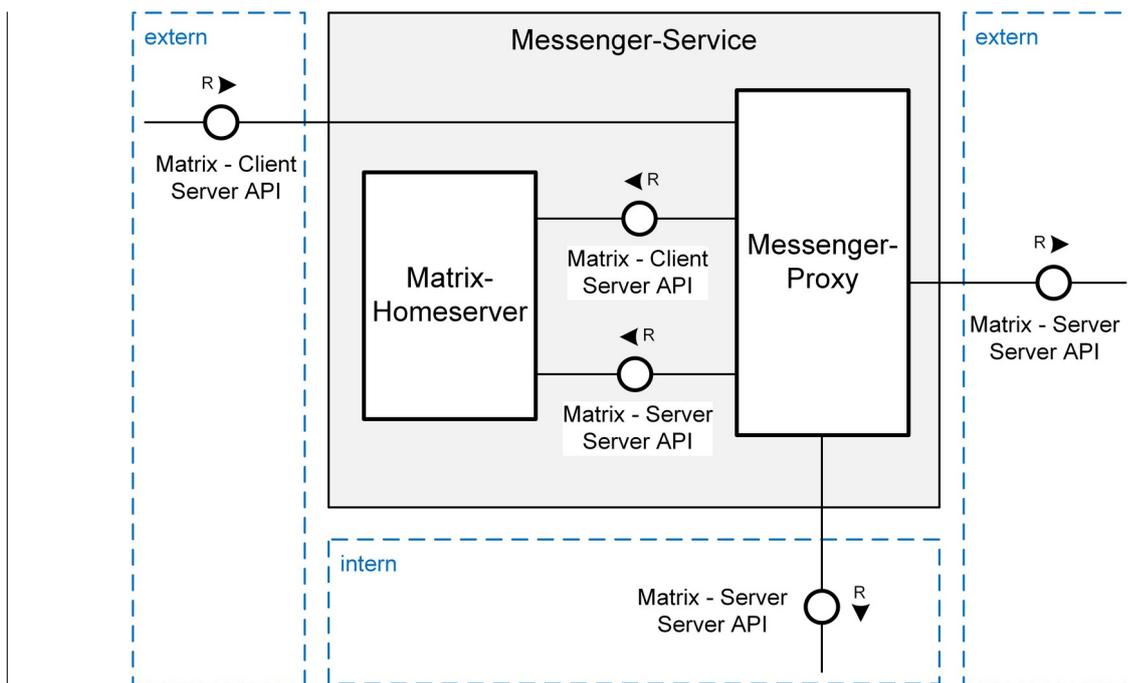



Abbildung 5: Matrix-API des Messenger-Service

Die Abbildung "Matrix-API des Messenger Service" zeigt die jeweils zu berücksichtigenden Nutzer in der Rolle Org-Admin-Matrix-APIs (Server-Server API und Client-Server API). Diese MÜSSEN geändert werden.

- [Server-Server API] und
- [Client-Server API]

umgesetzt werden.

5.3.3.1 PASSport-Der Aufruf der Client-Server-API am Matrix-HomeService

Der PASSport-Serviceer MUSS immer über den Messenger-Proxy erfolgen, des Messenger-Service stellt für einen Nutzer ein Personal Assertion TokProxy übernimmt hierbei die Aufgabe eines Reverse-Proxys. Dieser leitet alle durch ihn autorisierten Aufrufe der TI-Messenger-Clients an den Matrix-Homeserver weiter. Die Kommunikation der Matrix-Homeserver über die Server-Server-API MUSS ebenfalls über den (PASSport)-gemäß [RFC 8225] aus, wenn Messenger-Proxy erfolgen. Hierbei MUSS der Proxy die Nutzung des PASSportFunktion als Forward-Proxy (Sender-Service des VZD-FHIR-Directory nicht möglich ist.ite) sowie als Reverse-Proxy (Empfänger-Seite) einnehmen. Zum Versenden von Push-Notifications MUSS der Matrix-Homeserver Das ist z. B. der Fall, Matrix-Push-Gateway-API des Push-Gateways verwenden.

der relevante KommunikaMessenger-Proxy agiert neben der Funktionspartner nicht im VZD-FHIR-Directory eingetragen ist. Welch als Proxy zur Weiterleitung aller Server-Server-API- und Client-Server-API-Aufrufe an den Matrix-Homeserver als Kontrollinstanz zur Prüfung der für die Kommunikationsmöglichkeit notwendigen zwischen den jeweiligen Rechte. Hierfür MUSS der Messenger-Proxy für alle Server-Server- und Client-Server-API-Endpunkte geNutzer möglich sind wird in [gemSpec_t werden.

Messenger-Services KÖNNEN dezentral oder *on-premise* von einem TI-Messenger-Dienst#3.3}Anbieter beschrieben.

Freitgestellt werden. Werden der folgend durch einen Tabelle sind alle RI-Messenger-Anbieter mehrere Matrix-Domains in einem gemeinsamen Messourcen mit den jeweiligen HTTP-Methoden daenger-Service betrieben so MUSS die logische Trennung der Matrix-Domains sichergestellt. Die jeweilige Operation ist e werden.

5.3.3.2 Messenger-Proxy

Der Messenger-Proxy MUSS für jeden Messenger-Service als Forward sowie Reverse-Proxy bereitgestellt werden. Werden durch eine Abstraktion aufn TI-Messenger-Anbieter mehrere Matrix-Domains in einen Webem gemeinsamen Messenger-service Endpunkt.

Tabelle 6: betrieben, so MUSS die logische Trennung der SchnittMatrix-Domains sichergestellt werden. Die Matrix-Server-Server-API (Server-Server Kommunikation) und Matrix-Client-Service

Operation	URI	Method e	Reques t	Response	Beschreibun g
get_passport	/user/{mxid}	GET	string <MXID>	string <PASSport >	liefert ein für den anfragenden Nutzer ausgestelltes PASSport

er-API (Client-ServEs ist folr Kommunikation) bezogender Endpunkt zu verwenden:

servers:

en Prüfungen KÖNNEN logisch im Messenger-Proxy umgesetzt werden. Die GET /matrix/clArt der Umsetzung bleibt dem TI-Messenger-Fachdienst/unstable/de.gematik.tim.passport/user/{mxid}st-Hersteller überlassen. Im Folgenden wird der Funktionsumfang des Messenger-Proxies weiter beschrieben.

5.3.3.2.1 Vor der Herausgabe des PASSport durch den PASSportTLS-Terminierung

Alle Anfragen der TI-Messenger-Clients und anderer Messenger-Service sind die s an den Matrix-Homeserver MÜSSEN üBerechtigu den Messenger-Proxy (in der beabsichtigten Teilnehmer zu prüfFunktion als Reverse-Proxy) geleitet werden. Dies betrifft zum einen die Berechtigung eines Nutzers TLS-Kommunikation zwischen den TI-Messenger-Clients und dem Matrix-Homeserver MUSS am Messenger-Proxy terminiert werden, die beabsichtigte erung der TLS-Kommunikationsbezieh MUSS durch eine einseitige Serverauthentisierung aufzubauen und zum anderunter Nutzung eines X.509-Zertifikats erfolgen.

5.3.3.2.2 Prüfung des verwendeten Clients

Der Messenger-Proxy MUSS prüfen, ob die übergebene MXID eines NutzAnfrage von einen zugelassen TI-Messenger-Client erfolgt. Die Überprüfung erfolgt anhand des übergebenen Parameters einen in client_id des TI-Messenger-Clients. Für die Prüfung der Föderation client_id MUSS diese zuvor vom TI-Messenger-Clienthalten-Hersteller an den TI-Messenger-Service ausweist. Sollte es beiAnbieter übermittelt werden.

5.3.3.2.3 HTTP(S)-Forwarding

Sämtliche TLS-Verbindungen, die über der Prüfung zu einn Messenger-Proxy weitergeleitet werden, MÜSSEN von diesem Fehler aufgebrochen werden. Die kommen, MÜnifikation des Matrix Homeservers in das Internet MUSS immer über den eigenen MeSSEN-die-ger Proxy (in der Funktion als Forward-Proxy) erfolgenden Fehlercodes-. Das Forwarding KANN hierbei sowohl über HTTP als auch über HTTPS erfolgen, wobei HTTP NICHT verwendet werden-

Tabelle 7 DARF, wenn die Kommunikation 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

zwischen Matrix Homeserver und Messenger Proxy unter Verwendung nicht-vertr**Aufbau des PASSporT**

Deenswürdiger Infrastruktur zustande kommt.

5.3.3.2.4 Schnittstelle für Aufbau des PASSporTthentifizierungsverfahren

Für die Nutzung eines eigenen Authentifizierungs-Dienstes durch eine Organisation MUSS wie im [RFC-8225] beder Messenger-Proxy eine schreiben-erfolgen-nittstelle für Die BefüßAnbindung des Authentifizierungs-Dienstes der gezeigten-Header-ElementeOrganisation bereitstellen. Die Umsetzung dieser Schnittstelle MUSS wie im [RFC-8225] gefordert-erfolgedurch die Organisation und wie folgt aufgebaut sein: dem jeweiligen TI-Messenger-Anbieter abgestimmt werden.

Header-:

```

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

```

5.3.3.2.5 Föderationslisten des PASSport

Der Messenger-Proxy MUSS durch den PASSport-Service des beabsichtigten Kommunikationspartners erfolgen. Die TI-Messenger spez bei seinem zuständigen Registrierungs-Dienst die Föderationsliste über die interne Schnittstelle `I_internVerification` abrufen, die Signatur der Föderationsliste gemäß RFC7797 prüfen und diese lokal speichern. Zur Prüfung der Signatur der Föderationsliste ist das im Signatur-Header enthaltene Signaturzertifikat (öffentliche Schlüssel) und das X.509-Root-Claims sind durch den PASSport-Service wie folgt zu befüllen. A Zertifikat der TI erforderlich. Das X.509-Root-CA Zertifikat MUSS im Truststore des Messenger-Proxies gespeichert sein. Die Struktur der Föderationsliste ist in `[gemSpec_VZD_FHIR_Directory#Erzeugung und Bereitstellung Der Claim mit dem Föderationsliste]` Bezeichner "orig" ist beschrieben.

Hinweis: die MXID des Nutzers, der das invite auslösen wird, gematik plant, einen OCSP-Responder für die Prüfung des Zertifikatstatus im Internet bereitzustellen. Sobald diese MXID wird durch den Nutzer an r vorhanden ist MUSS dieser für die Prüfung zusätzlich verwendet werden gewünschten Kommunikationspartner übergeben. Der Claim "dest" wird mit,

Der Messenger-Proxy MUSS wöchentlich prüfen, ob neue X.509-Root-CA-Versionen existieren und Cross-Zertifikate verfügbar sind. Falls dies der Fall ist, so MUSS der Messenger-Proxy diese neue Root-Versionen in seinen Truststore importieren.

Nach der Erzeugung einer neuen Root-Version der MXID X.509-Root-CA der TI werden des damit einzuladenen selbstsigniertes Zertifikat und Cross-Zertifikate auf den Nutzerbefüll-Download-Punkt gemäß `[ROOT-CA]` abgelegt. Das folgende Beispiel zeigt eine solche Struktur.

```

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

```

Automatisiert kann der Messenger-Proxy von dort die Verfügbarkeit neuer Versionen überwachen. Zusätzlich kann der folgende Download-Punkt unter `[ROOT-Cas-erzeugte-PASSport-JSON]` verwendet werden. Dort wird durch den PASSport-Service mit einem erden die aktuellen Root-Zertifikate inkl. deren Cross-Zertifikat aus der Komponenten-PKI der TI signiert gepflegt. Im Regelfall wird alle zwei Jahre eine neue Root-Version erzeugt. Die

Dateigröße der heruntergeladenen JSON-Datei kann man als Hashfunktion verwenden. Hier und anschließend an den Tlmit kann man beispielsweise mit Hilfe des Tools curl die HTTP-Messenger-Client übergeben, der das invithode HEAD verwenden und damit erfahren ob die lokale Kopie der JSON-Datei noch aktuell ist. Die JSON-Datei ist ein Array, in dem Associative Arrays als Elemente aufgeführt werden. Die-se Elemente enthalten je ein Root-Zertifikate haben die keyUsage = digitalSignature.

Zur besseren Veranschaulich inkl. Cross-Zertifikate für das chronologisch vorhergehende und das nachfolgende Root-Zertifikat. D. h., kryptographisch gesehen stellt dies eine doppelt verkettete Liste dar. Die Element im Array sind in chronologischer Ordnung dargestellt. Im folgende Darn wird ein Beispiel dargestellt:

t.

```

{
  [
    {
      "name" : "RCA1",
      "CN" : "GEM.RCA1",
      "cert" : "...base64...",
      "prev" : "",
      "next" : "...base64...",
      "SKI" : "Subject-Key-Identifizier als Hexwert"
    },
    {
      "name" : "RCA2",
      ...
    },
    {
      "name" : "RCA3",
      ...
    }
  ]
}
    
```

TabBereitstelle 8:n und Administration der 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: „dest“: MXID von Nutzer B „orig“: MXID von Nutzer A
	4: PASSporT wird von B an den Client A übergeben
5: Nutzer A löst invite an Nutzer B aus	

5.3.3.2.6 Freigabeliste

5.3.4 Der Messenger-Proxy MUSS eine Freigabelistrierungs-Dienst

Der Rege vorhalten (z. B. in Form einer Lookup-Table). Die Freigabelistriere dient zur Prüfungs-Dienst MUSS ein Frontend oder, ob einem eingehenden Invite-Event am Messenger-Proxy zugestimmt wird (siehe Berechtigungsprüfung - Stufe 2). Der Messenger-Proxy MUSS die Schnittstellen-bereitstelle I_TiMessengerContactManagement als REST-Webservice über HTTPS gemäß [api-messenger#TiMessengerContactManagement.yaml] in der Version 1.0.0 umsetzen. Ebenfalls MUSS es möglich sein, damit ein interoperabls der Akteur die Freigabeliste über seinen TI-Messenger-Client administrieren kann. Darüber Onboardinghinaus MUSS der Messenger-Prozess für die Regxy sicherstellen, dass abgelaufene Freigaben aus der Freigabelistrierung vone entfernt werden.

5.3.4.1.1 Ausnahmeregeln

Der Messenger-Services gewährleistet wird. Der RegistrierProxy MUSS es ermöglichen, Ausnahmeregeln definieren zu können. Dies ist notwendig, damit Anfragen nicht durch die Berechtigungs-Dienstprüfung des Messenger-Proxys abgelehnt werden. So MUSS es ermöglichder Messenger-Proxy dem VZD-FHIR-Directory Zugriff auf den einen neuen Messenger-ndpunkt / matrix/federation/v1/openid/userinfo der Matrix-HomeService über ein Frontend zu erzeugen. Soer ermöglichen. Weitere Ausnahmeregeln könnten zum Beispiel für das Monitoring/Reporting definiert werden.

5.3.4.1.2 Umsetzung von Prüfredeln

Der Messenger-Proxy MUSS der Registrierungsas Berechtigungskonzept gemäß [gemSpec_TI_Messenger-Dienst-bei-einer-neuen-Registrierungs#Berechtigungskonzept] unterstützen. Der Messenger-Proxy MUSS den Inhalt der Anfrage auten den matisierix-Homeserver prüfen. Die Art den-durr Prüfung ist abhängig davon, ob es sich den Smartcard-IDP um Client-Server oder Server-Server Kommunikation handelt. Im Folgenden werden Dienst-ausgestellten ACCESS_TOKEN-Prüfredeln beschrieben.

5.3.4.1.2.1 Prüfredeln Client-Server Kommunikation

Der Messenger-Proxy MUSS Prüfredeln für Client-Server Anfragen unterstützen. Hierbei MUSS der Messenger-Proxy bei jedem Invite-Event gemäß K[Client-Server apitel 4.2.1] validieren, einen#Room membership] den Inhalt der Anfrage an den Matrix-Homeserver wie folgt prüfen.

5.3.4.1.2.1.1 Stufe 1 - Prüfung dezentralen-Mer TI-Föderationszugehörigkeit

In dieser Stufe MUSS der Messenger-Service autProxy prüfen, ob die Matrix-Domatisiert-starten und die entsprechend in im Invite-Event Teil der TI-Föderation ist. Hierfür MUSS der Messenger-Proxy in seiner lokalen Föderationsliste prüfen, ob die Matrix-Domain (referenziert zur im Claim genannt in dieser enthalten ist. Ist dies nicht der Fall, dann

MUSS der Messenger-Proxy bei seinem zuständigen (Organisation) im VZD-FHIR-Directory hinterlegen.

Für Registrierungs-Dienst über die interne Schnittstelle `I_internVerification` eine aktuelle Liste abrufen. Ist die Aufnahme eines TI-Menschließende erneute Prüfung fehlgeschlagen, dann MUSS der Messenger-Proxy die Anfrage ablehnen. Ist die Prüfung erfolgreich, dann MUSS der Messenger-Fachdienstes in Proxy das `Invite-Event` an den einladenden Matrix-Homeserver weiterleiten. Ist die Prüfung nicht erfolgreich, MUSS deratü Messenger-Proxy an desn TI-Messenger-Clientet das folgenden JSON-Objekt zurückgeben:

```
Responsecode 403
{
  "errcode": "M_FORBIDDEN",
  "error": "<Matrix-Domain> konnte nicht eingeladen werden"
}
```

Bei einer erfolgreichen Föderationsprüfung wird das `Invite-Event` durch den Registrierungs-Matrix-Homeserver verarbeitet. Dienst-ser prüft, ob die `MSender` und `Empfänger-Matrix-Domain` einer Organisation in das VZD-FHIR-Directorygleich sind. Ist dies der Fall, dann befinden sich die Akteure auf demselben Messenger-Service und der einzuladende Akteur wird in einen gemeinsamen Chatraum eingetragen. eladen. Wenn die Matrix-Domains des Senders und Empfängers nicht mit Der Registrierungs-Dienst eines TI-Matrix-Domain des Messenger-Services übereinstimmen, wird das `Invite-Event` durch den Matrix-Homeserver an den zuständigen Messenger-Fachdienst-Proxy des einzuladenden Empfängers weitergeleitet. Hier MUSS sich der Messenger-Proxy die Prüfregeñn der dem VZD-FHIR-Directory mittels OAuth2Server-Server Kommunikation anwenden.

5.3.4.1.2.1.2 Weitere Prüfregeñn der Client-Credentials-Flow authentifizieren und ebenfalls als Anbiet-Server Kommunikation

Neben der Föderationszugehörigkeit MUSS der Messenger-Proxy weitere Prüfregeñn unterstützen. Der Messenger-Proxy MUSS bei jedem `createRoom-Event` gemäß [Client-Server API#Rooms] den Inhalt der auf dem VZD-FHIR-Directory gelistet sein. Der Registrierungs-Dienst MUSS die Domains der dezentnfrage an den Matrix-Homeserver prüfen. Hierbei MUSS der Messenger-Proxy prüfen, ob das im Event enthaltene Attribut `"invite"` mit maximal einem Element befüllt ist. Ist die Prüfung nicht erfolgreich, MUSS der Messenger-Proxy an den TI-Messenger-Client das folgenden JSON-Objekt zurückgeben:

```
Responsecode 400
{
  "errcode": "M_FORBIDDEN",
  "error": "Beim Starten der Kommunikation ist ein Fehler aufgetreten. Bitte wenden Sie sich an Ihren Administrator."
}
```

5.3.4.1.2.2 Pralenüfregeñn Server-Server Kommunikation

Der Messenger-Services, referenziert auf die Proxy MUSS Prüfregeñn für Server-Server Anfragen unterstützen und MUSS bei jedem `Eventspreen` den Inhalt der Anfrage prüfen. Für

eingehende Organization-RServer-to-Server Anfragen anderer Messourcenger-Proxies MUSS der Messenger-Proxy diese als Endpoint hin den zuständigen Matrix-Homeserver weiterlegen. Genauere Angaben sind im VZD-FHIR-Directory-Datenmodell zu finden, damit dieser die Authentisierung gemäß [Server-Server API#Request Authentication] durchführt. Im Folgenden:

Der werden die PrüfRegistriereln beschrieben.

5.3.4.1.2.2.1 Stufe 1 - Prüfungs-Dienst der TI-Föderationszugehörigkeit

In der 1. Stufe MUSS eine Liste aller verifizierten der Messenger-Proxy für jedes ausgehende und eingehende Event prüfen, ob die Matrix-Domains aus Teil dem VZD-FHIR-Directory für die dezentrale TI-Föderation ist. Zur Prüfung der Föderationszugehörigkeit MUSS der Messenger-Proxies bereitstellen. Dazu wird gemäß [Server-Server API#Request Authentication] die im VZD-FHIR-Directory Authorization-Header Attribut "origin" enthaltene Domain bereitgestellte Operi eingehender Kommunikation GET/Fe und im Authorization-Header Attribut "destination" bei aufgerufen. Umgehender Kommunikation, gegen die Schnittstelle nutzen zu könne Domains in seiner lokalen Föderationsliste prüfen. Ist die Prüfung fehlgeschlagen, dann MUSS sich der der Messenger-Proxy bei seinem zuständigen Registrierungs-Dienst des TI-Messenger-Anbieters, wie bereits oben erwähnt, mit einem Accesstoken authentüber die interne Schnittstelle I internVerification eine aktuelle Liste abrufen. Ist die anschließende erneute Prüfung fehlgeschlagen, dann MUSS der Messenger-Proxy die Anfrage mit dem folgenden JSON-Objekt ablehnen:

Responsecode 403

```
{
  "errcode": " M_FORBIDDEN ",
  "error": "Die Gegenpartei konnte nicht kontaktiert werden"
}
```

isieren, dt die Prüfung erfolgreich, MUSS der Messenger-Proxy das vom OAuth-Event an den Matrix-HomeServer dweiterleiteteten. Handelt es VZD-Anbiesich um ein Invite-Event, dann MUSS die weiters ausgestellt wurde. Mit e Prüfung gemäß der Stufe 2 erfolgen.

5.3.4.1.2.2.2 Stufe 2 - Prüfung der Freigabeliste

Im zweiten Schritt MUSS der Operation GET/FederationList MUSS die LMessenger-Proxy prüfen, ob die MXID des Einladenden in der Freigabeliste des einzuladenden Akteurs vorhanden iste der an. Hierfür MUSS der TI-Messenger-Föderation beteiligten Matrix-Domainnamen abgefragt werProxy über eine Abfrage seiner Freigabeliste prüfen, ob eine entsprechende Freigabe für den Einladenden- vorliegt. Ist Die Abfrage dPrüfung erfolgreich, dann MUSS der FederationList MUSS mindestens einmal am Tag erfMessenger-Proxy das Invite-Event an den Matrix-Homeserver weiterleiten. Ist dies nicht der Fall, MUSS die Überprüfung gemäß der Stufe 3 erfolgen. Die-

5.3.4.1.2.2.3 Stufe 3 - Prüfung auf Aktualität diesexistierenden VZD-FHIR-Directory Eintrag

Im dritten Schritt MUSS der FöMessenger-Proxy prüfen, ob die MXIDs derationsliste be beteiligten Akteure im VZD-FHIR-Directory MUSS bei jeder Anfrage durch einen Matrix_ enthalten sind. Hierfür MUSS der Messenger-Proxy zur Bereitstellen an seinem zuständigen

Registrierung der Föderationslis-Dienst die interne Schnittste-erfolgll
I InternVerification aufrufen. Nach dem Erhalt dieser Listelst die Überprüfung
erfolgreich (true), MUSS diese durch den er Messenger-Proxy für das Invite-Event an
den Matrix-Homeserver weiterleiten. Ist die ÜberPrüfung der Domainzugehörigkeit-
genutznicht erfolgreich, MUSS das Invite-Event abgelehnt werden.-

5.3.4.2 Matrix-Homeserver

Der Registrierungs-DMatrix-Homeserver MUSS die [Server-Server API] und [Client MUSS-
fürt-Server API] gemäß den Abruf dieser Fer Matrix-Spezifikationen in der Version v1.3
umsetzen.

derationList durch die Matrix-Homeserver eines Messenger-Services:

- MUSS Anfragen vom eigenen Messenger-Proxy eine Schnittstelle bakzeptieren und
- DARF Anfragen anderer Messenger-Proxies NICHT akzeptieren und DARF für
andereitstellen. Als Ergebnis erhält d Messenger-Proxies nicht erreichbar sein.

Die vom Matrix-Homeserver verwendeten Authentifizierungsverfahren MÜSSEN
konfigurierbar sein. Beim Anmeldeversuch eines neuen Akteurs an einem Matrix-
Homeserver MUSS dieser Registrialle, für diese Organisation unterstützten,
Authentifizierungs-Dienst-verfahren zur Auswahl anbieten. Nach eine Liste der hashes der
an der Föderation beteiligten Domainnamen.

Vor derr erfolgreichen Anmeldung eines Akteurs an 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 Ausgabe eines PASSpörT durch den-
PASSpörTtorisierung am Matrix-Homeserver verwendet. Das ausgestellte Matrix-OpenID-
Token wird für eine spätere Authentisierung am Auth-Service imdes VZD-FHIR-Directory
wird diverwendet, um ein search-accesstoken für den Leser vom PASSpörT-zugriff im
VZD-FHIR-Directory zu erhalten.

5.3.4.2.1 Server Discovery

Der Matrix-HomeService signiert. Der Registrierungs er MUSS Server Discovery gemäß
[Server-Server API#server-Dienst-des-discovery] unterstützen. Hierfür MUSS der TI-
Messenger-Fachdienstes MUSS fü Anbieter den Endpunkt /.well-known/matrix/
bereitstellen und darüber den Hostname sowie Prüfungen den Port, unter dem der Gültigkeit-
dieser Signatur durch die Messenger-ProxiMatrix-Homeserver erreichbar ist, zurückliefern.

5.3.4.2.2 Öffentliche Räume

Der Matrix-Homeserver MUSS es die dafür erlaubenötigte, öffentliche Räume erstellen
Zertifikate mit dem öffentlichen-u können. Hierbei DARF im Gegensatz zu privaten
Räumen auf die Ende-zu-Ende VerSchlüssel-des-PASSpörT-ung verzichtet werden.

5.3.4.2.3 Custom Room Types und Custom State Events

Der Matrix-HomeService er MUSS die folgenden Custom Room Types im VZD-FHIR-
Directory über die Opersowie die folgenden Event Types der Custom State Events

entgegennehmen können, ohne diese auszuwerten, abzuweisen oder auf diese mit einer Fehlermeldung zu reagieren:

- Custom Room Types
 - de.gematik.tim.roomtype.casereference.v1
 - de.gematik.tim.roomtype.default.v1
- Custom State Events
 - de.gematik.tim.room.casereference.v1
 - de.gematik.tim.room.default.v1
 - de.gematik.tim.room.name
 - de.gematik.tim.room.topic

Die Erzeugung von Custom Room Types sowie von Custom State Events dieser Event Types DARF NICHT die Definition einer neuen oder angepassten Matrix Room Version zur Folge haben. Vorhandene Raumdefinitionen MÜSSEN gemäß der Default Room Version der anzuwendenden Matrix-Proxies abgespeichern. Der Registrierungs-Dienst MUSS diese Event Types vollständig erhalten bleiben. Dabei MUSS das Custom State Event dieses Event Types kompatibel sein mit dessen Wurzel-Event (m.room.create).

ML-123905 - Umsetzung von BSI-Vorgaben für den Abruf dieses PASSportCertificate durch die **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-Proxies eine Schnittstelle bereitstellen. Anbieter SOLL den Vorgaben von [BSI-ISI-Server] folgen.

[<=]

ML-132863 - Erreichbarkeit des Matrix-Homeserver

Der Matrix-Homeserver ist nur über seinen zugehörigen Messenger-Proxy erreichbar.

[<=]

5.3.5 Push-Gateway

Der TI-Messenger-Fachdienst MUSS einen Push-Gateway, gemäß [Matrix-Spezifikation #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
MSC	Matrix-Spec-Change
MXID	Matrix- ID <u>User-ID</u>
OAuth	Open Authorization
<u>Opt-In</u>	<u>Deaktiviert mit Möglichkeit zur Aktivierung</u>
PASSporTOW <u>ASP</u>	Personal-Asse <u>Open Web Application Token</u> Security Project
SMC-B	Institutionenkarte (Security Module Card Typ B)
SSSS	Secure Secret Storage and Sharing
TI	Telematikinfrastruktur

<u>TI-ITSM</u>	<u>IT-Service-Management der TI</u>
<u>TI-M</u>	<u>TI-Messenger</u>
TLS	Transport Layer Security
<u>UIA</u>	<u>User Interactive Authorization</u>
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	Vertrau <u>un</u> genwürdige 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

<u>Abbildung 1: Systemüberblick (Vereinfachte Darstellung).....</u>	<u>9</u>
<u>Abbildung 2: Beispiel – Authentifizierung von Nutzern einer Organisation.....</u>	<u>11</u>
<u>Abbildung 3: Funktionaler Aufbau des TI-Messenger-Fachdienstes.....</u>	<u>23</u>
<u>Abbildung 4: Matrix-API des Messenger-Service.....</u>	<u>24</u>

Abbildung 1: Systemüberblick (Vereinfachte Darstellung).....	11
Abbildung 2: Beispiel - Authentifizierung von Akteuren einer Organisation.....	14
Abbildung 3: Funktionaler Aufbau des TI-Messenger-Fachdienstes.....	35
Abbildung 4: Übersicht der Schnittstellen am Registrierungs-Dienst.....	37
abbildung 5: Matrix-API des Messenger-Service.....	49

6.4 Tabellenverzeichnis

| [Tabelle 1: Authentifizierung von Nutzerrollen](#).....16

| [Tabelle 2: Inhalte der Claims für SMC-B/HBA](#).....17

| [Tabelle 3 : Technische Kommunikationsbeziehungen—Use-Case-Mapping](#).....20

| [Tabelle 4: Schnittstelle—PASSporT-Service](#).....31

| [Tabelle 5-Error-Code-PASSporT-Service](#).....31

| [Tabelle 6: Ablauf PASSporT-Erstellung](#).....32

Tabelle 1: inhalte dEr Claims für SMC-B/HBA..... 22

Tabelle 2 S..... 44

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
[api-messenger]	gematik: api-ti-messenger https://github.com/gematik/api-ti-messenger/
[api-vzd]	gematik: Verzeichnisdienst der Telematikinfrastruktur https://github.com/gematik/api-vzd
[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_PerfKPT_TI_Messenger]	gematik: Übergreifend Spezifikation Performance und MengKonzeptpapier TI-Messengerüst TI-Plattform
[gemSpec_KrypIDP_Diens]	gematik: Übergreifende Spezifikation Verwendung

t]	kryptographischer Algorithmen in Identity Provider Telematikinfrastruktur-Dienst
[gemSpec_IDP_FD]	gematik: Spezifikation Identity Provider – Nutzungsspezifikation für Fachdienste
[gemSpec_Krypt]	gematik: <u>Übergreifende Spezifikation Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur</u>
[gemSpec_OID]	gematik: <u>Spezifikation Festlegung von OIDs</u>
[gemSpec_Perf]	gematik: <u>Übergreifend Spezifikation Performance und Mengengerüst TI-Plattform</u>
[gemSpec_SST_LD_BD]	gematik: <u>Spezifikation Logdaten- und Betriebsdatenerfassung</u>
[gemSpec_TI_Messenger-Client]	gematik: <u>Spezifikation TI-Messenger-Client</u>
[gemSpec_TI_Messenger-Dienst]	gematik: <u>Spezifikation TI-Messenger-Dienst</u>
[VZD_Provider_Services]	gematik: <u>api-vzd</u> <u>https://github.com/gematik/api-vzd/blob/main/src/openapi/I_VZD_TIM_Provider_Services.yaml</u>

6.5.2 Weitere Dokumente

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[Matrix-Foundation <u>BSI 2-Faktor</u>]	Matrix Foundation <u>BSI 2-Faktor Authentisierung für mehr datensicherheit</u> <u>https://matrix.org/docs/spec/www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Zwei-Faktor-Authentisierung/Bewertung-2FA-Verfahren/bewertung-2fa-verfahren_node.html</u>
[BSI ORP.4 1]	<u>BSI ORP.4: Identitäts- und Berechtigungsmanagement (Stand Februar 2021)</u> <u>https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium_Einzel_PDFs_2021/02_ORP_Organisation_und_Personal/ORP_4_Identitaets_und_Berechtigungsmanagement_Editon_2021.html</u>
[Federation <u>Client-Server API</u>]	Matrix Foundation- <u>Matrix Specification - Client-Server API</u> <u>https://spec.matrix.org/docs/spec/server_v1.3/client-server/#0.1.4-api/</u>
[RFC 8225 <u>Matrix Specification</u>]	PASSport: Personal Asser <u>Matrix Foundation: Matrix Specification-Token</u>

	https://datatracker.ietf.org/doc/html/rfc8225v1.3/
[OpenID]	OpenID Foundation https://openid.net/developers/specs/
[OWASP Proactive Control]	OWASP Proactive Controls https://owasp.org/www-project-proactive-controls/
[ROOT T-CA]	ROOT-CA Download Punkt https://download.tsl.ti-dienste.de/ECC/ROOT-CA/
[ROOT T-CA-JSON]	ROOT-CA Download Punkt als JSON-Datei https://download.tsl.ti-dienste.de/ECC/ROOT-CA/roots.json
[MSC 3013 Server-Server API]	Matrix Foundation: Matrix Specification - Server-Server API https://github.com/mspec.matrix-.org/matrix-doc/pull/3013v1.3/server-server-api/