

Elektronische Gesundheitskarte und Telematikinfrastruktur

Spezifikation TI-Messenger (Basis)

Version:	1.2.0 CC
Revision:	1394627
Stand:	14.10.2025
Status:	zur Abstimmung freigegeben
Klassifizierung:	öffentlich_Entwurf
Referenzierung:	gemSpec_TI-M_Basis

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	13.06.202 4		initiale Erstellung	gematik
1.1.0	13.11.202 4		Einarbeitung Matrix-Update V1.11	gematik
1.1.1	09.12.202 4		Update TI-Messenger_24_2-1 u. TI- Messenger_24_3-1	gematik
1.1.2	12.03.202 5		Einarbeitung Patch TI-Messenger_25_1- 1 und TI-Messenger_25_1-2	gematik
1.2.0 CC	14.10.202 5		Einarbeitung TI-Messenger_25_3 - zur Abstimmung freigegeben	gematik

Inhaltsverzeichnis

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.....	8
2.1 TI-Messenger Föderation.....	9
2.2 Matrix.....	10
2.3 Akteure und Rollen.....	10
2.3.1 Rolle: "User".....	11
2.3.2 Rolle: "Org-Admin".....	11
2.4 Berechtigungskonzept.....	11
2.5 Nachbarsysteme.....	12
2.5.1 Authentifizierungs-Dienst für Akteure.....	12
2.5.2 IDP-Dienst.....	12
2.5.3 VZD-FHIR-Directory.....	13
2.5.3.1 Auth-Service.....	13
2.5.3.2 OAuth.....	13
2.5.3.3 FHIR-Proxy.....	13
2.5.4 Externer Push-Dienst.....	14
2.6 Zugriffstoken.....	14
3 Zerlegung des Produkttyps (Systemkomponenten).....	17
3.1 TI-M Client.....	17
3.1.1 Ausprägungen nach Nutzergruppen.....	21
3.1.1.1 TI-M Client für Akteure in der Rolle "Org-Admin" (Org-Admin-Client).....	21
3.1.1.2 TI-M Client für Akteure in der Rolle "User".....	22
3.1.2 Ausprägungen nach Plattform.....	23
3.1.2.1 TI-M Client für mobile Szenarien.....	23
3.1.2.2 TI-M Client für stationäre Szenarien.....	24
3.1.3 Matrix Spezifikation.....	24
3.1.3.1 Umdefinition der Module.....	24
3.1.3.2 Raumerzeugung und Öffentlichkeit von Räumen.....	26
3.1.3.3 Instant Messaging.....	27
3.1.3.4 Weitere Ergänzungen/Einschränkungen zur Matrix-Spezifikation.....	27
3.1.4 Push-Notifications.....	30
3.1.5 Client Identifikation.....	30
3.1.6 Archivierung von Gesprächsinhalten.....	30
3.1.7 Tracking und Reporting.....	31
3.1.8 Schlüssel-Backup.....	32
3.1.9 VZD-FHIR-Directory.....	33
3.1.9.1 Lesezugriff.....	33

3.1.10 Registrierungs-Dienst.....	34
3.1.11 Testtreiber.....	34
3.2 TI-M FD.....	34
3.2.1 Registrierungs-Dienst.....	36
3.2.1.1 <i>I_Registration</i>	36
3.2.1.1.1 Authentisierung einer Organisation.....	36
3.2.1.1.2 Anlegen des Administrations-Accounts.....	38
3.2.1.2 <i>I_Admin</i>	39
3.2.1.3 <i>I_internVerification</i>	39
3.2.1.3.1 Bereitstellung und Aktualisierung der Föderationsliste.....	39
3.2.1.4 <i>OAuth / Auth-Service</i>	40
3.2.1.5 <i>I_VZD_TIM_Provider_Services</i>	40
3.2.2 Messenger-Service.....	40
3.2.2.1 Schnittstelle für Authentifizierungsverfahren.....	41
3.2.2.2 Messenger-Proxy.....	41
3.2.2.2.1 Ausnahmeregeln definieren.....	42
3.2.2.2.2 Föderationslistensignatur.....	42
3.2.2.3 <i>Matrix-Homeserver</i>	43
3.2.2.3.1 Matrix Spezifikation.....	43
3.2.2.3.2 Ergänzungen zur Matrix Spezifikation.....	44
4 Übergreifende Festlegungen.....	47
4.1 Datenschutz und Sicherheit.....	47
4.2 Test.....	49
4.3 Betrieb.....	50
4.3.1 TI-M Client.....	53
4.4 Sonstige.....	54
4.4.1 Rechte und Pflichten des Herstellers.....	54
5 Funktionsmerkmale.....	55
5.1 Anwendungsfälle.....	55
5.1.1 Authentisieren einer Organisation.....	55
5.1.2 Bereitstellung eines Messenger-Service für eine Organisation.....	59
5.1.3 Föderationszugehörigkeit prüfen.....	61
5.1.4 Austausch von Events zwischen Akteuren innerhalb einer Organisation.....	64
5.1.5 Einladung von Akteuren außerhalb einer Organisation.....	65
5.1.6 Austausch von Events zwischen Akteuren außerhalb einer Organisation.....	67
5.1.7 Aktualisierung der Föderationsliste.....	69
5.2 Berechtigungsmanagement.....	75
5.2.1 Prüfung der Föderationszugehörigkeit.....	75
5.2.1.1 <i>Client-Server Prüfungen</i>	75
5.2.1.2 <i>Server-Server Prüfungen</i>	76
5.2.2 Akteursspezifische Berechtigungskonfiguration.....	76
5.2.2.1 <i>Berechtigungen setzen</i>	76
5.2.3 Berechtigungsprüfung.....	78
5.3 Push-Benachrichtigungen.....	78
5.3.1 Push-Konfiguration.....	78
5.3.2 Push-Zustellung.....	79
5.3.3 TI-M Client App.....	80

5.3.4 Push-Gateway.....	81
5.3.5 TI-M FD.....	81
5.4 Raumversionen.....	81
5.5 TI-M spezifische Kommunikation.....	82
5.5.1 Basis-Anwendungsfall.....	82
5.5.1.1 TI-M Client.....	82
5.5.1.2 Matrix-Homeserver.....	83
5.5.2 Föderierte und intersektorale Kommunikation.....	83
5.5.2.1 TI-M Client.....	84
5.5.2.2 Matrix-Homeserver.....	84
5.6 Löschen von Inhalten.....	84
5.6.1 Serverseitiges Löschen.....	84
5.6.1.1 Matrix-Events.....	84
5.6.1.2 Medien.....	84
5.6.2 Clientseitiges Löschen.....	85
5.6.3 Redactions.....	86
6 Anhang A - Verzeichnisse.....	88
6.1 Abkürzungen.....	88
6.2 Glossar.....	88
6.3 Abbildungsverzeichnis.....	88
6.4 Tabellenverzeichnis.....	89
6.5 Referenzierte Dokumente.....	90
6.5.1 Dokumente der gematik.....	90
6.5.2 Weitere Dokumente.....	91

1 Einordnung des Dokumentes

1.1 Zielsetzung

Beim vorliegenden Dokument handelt es sich um die Festlegungen zum TI-Messenger. Mit dem TI-M soll die Ad-hoc-Kommunikation zwischen Akteuren des Gesundheitswesens gewährleistet werden. Teilnahmeberechtigte Akteure sind dabei grundsätzlich Angehörige solcher Organisationen, deren eigene Institutions-OID mit einer der in "Tab_PKI_403-x OID-Festlegung Institutionen im X.509-Zertifikat der SMC-B" der [gemSpec_OID] gelisteten ProfessionOIDs übereinstimmt.

Dieses Dokument beschreibt die Basisfunktionalitäten für die systemspezifische Lösung des TI-Messengers für das deutsche Gesundheitswesen. Dieses Dokument stellt somit nicht die Spezifikation für einen Produkttyp dar. Sie definiert die Basisfunktionalitäten, welche dann - noch um produktspezifische Anforderungen angereichert - in gesonderten Spezifikationsdokumenten für featurebasierte Produktausprägungen spezifiziert werden.

1.2 Zielgruppe

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

1.3 Geltungsbereich

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

Diese Basisspezifikation hegt nicht den Anspruch einen Produkttypen ableiten zu können, sondern stellt eine wiederverwertbare Definition von Grundfunktionalitäten dar. Die vollständige Anforderungslage für den Produkttyp ergibt sich aus weiteren Konzept- und Spezifikationsdokumenten. Diese sind in dem Produkttypsteckbrief des jeweiligen Produkttyps verzeichnet.

1.5 Methodik

Anwendungsfälle und Anforderungen als Ausdruck normativer Festlegungen werden durch eine eindeutige ID, Anforderungen zusätzlich durch die dem RFC 2119 [RFC2119] entsprechenden, in Großbuchstaben geschriebenen deutschen Schlüsselworte MUSS, DARF NICHT, SOLL, SOLL NICHT, KANN gekennzeichnet.

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 werden außerdem um Pronomen in Großbuchstaben ergänzt, wenn dies den Sprachfluss verbessert oder die Semantik verdeutlicht.

Anwendungsfälle und Anforderungen werden im Dokument wie folgt dargestellt:

<AF-ID> - <Titel des Anwendungsfalles>

Text / Beschreibung

[<=]

bzw.

<AFO-ID> - <Titel der Afo>

Text / Beschreibung

[<=]

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

2 Systemüberblick

Der sichere Nachrichtenaustausch zwischen beteiligten Akteuren des deutschen Gesundheitswesens erfolgt über die von TI-Messenger-Anbietern bereitgestellten TI-Messenger Fachdienste (TI-M FD) und TI-Messenger Clients (TI-M Client). Ein TI-M FD besteht aus einem oder mehreren Messenger-Services (basierend auf dem Matrix-Protokoll), die jeweils für eine Organisation (SM(C)-B-Inhaber) des Gesundheitswesens durch von der gematik zugelassene TI-Messenger-Anbieter bereitgestellt werden. Das vollständige Produkt, bestehend aus dem TI-M Client und dem TI-M FD, wird im folgenden als TI-Messenger Dienst (TI-M Dienst) bezeichnet.

Die Messenger-Services des TI-M Dienstes werden zu einer TI-Föderation zusammengefasst, um nicht zugehörige Messenger-Dienste auszuschließen. Um Teil der Föderation des TI-M Dienstes zu werden, muss die jeweilige Domain eines Messenger-Services vom TI-Messenger-Anbieter über den Registrierungs-Dienst des TI-M FD beim VZD-FHIR-Directory hinterlegt werden. Der TI-Messenger basiert auf dem offenen Kommunikationsprotokoll Matrix, das bereits von der Matrix Foundation gemäß [Matrix Specification] spezifiziert ist. In den von der Matrix Foundation erstellten Spezifikationen ist sowohl die Client-Server-, die Server-Server-Kommunikation als auch die API des Matrix-Push-Gateways beschrieben. Im Kontext des TI-Messengers kann die Kommunikation zwischen den TI-M Clients der beteiligten Messenger-Services Ende-zu-Ende-verschlüsselt stattfinden. Die Adressierung der Akteure innerhalb eines Messenger-Services erfolgt über die Matrix-User-ID und wird in Kurzform als MXID bezeichnet. Um die beteiligten Akteure über den Eingang neuer Nachrichten zu informieren, können über ein Push-Gateway die gängigen Push-Provider angebunden werden.

Hinweis: Im Sinne des Matrix-Protokolls sind sogenannte Enden Endgeräte (in der Matrix-Spezifikation als "devices" bezeichnet), welche die Fähigkeit haben, die an sie gesendeten Daten erstmalig nach der vollständigen Übertragung zu entschlüsseln. Dabei ist zu beachten, dass mit 'Endgeräten' dedizierte Client-Instanzen und nicht zwangsläufig physische Geräte gemeint sind, die eindeutig über ihre `device_ID` identifizierbar sind und von einem Client in dem Moment erzeugt werden, in dem dieser zur Anmeldung an einem Nutzerkonto verwendet wird. Damit sind ein oder mehrere Endgeräte einem Nutzerkonto, das selbst durch eine kryptographische Identität gekennzeichnet ist, untergeordnet und befähigen den Nutzer überhaupt erst zum Empfang und Versand Ende-zu-Ende-verschlüsselter Daten. Erst nach der Entschlüsselung der Daten können diese von einem Nutzer gelesen und von den von ihm eingesetzten Systemen wie beispielsweise einem Krankenhausinformationssystem dem Zweck entsprechend verarbeitet werden.

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

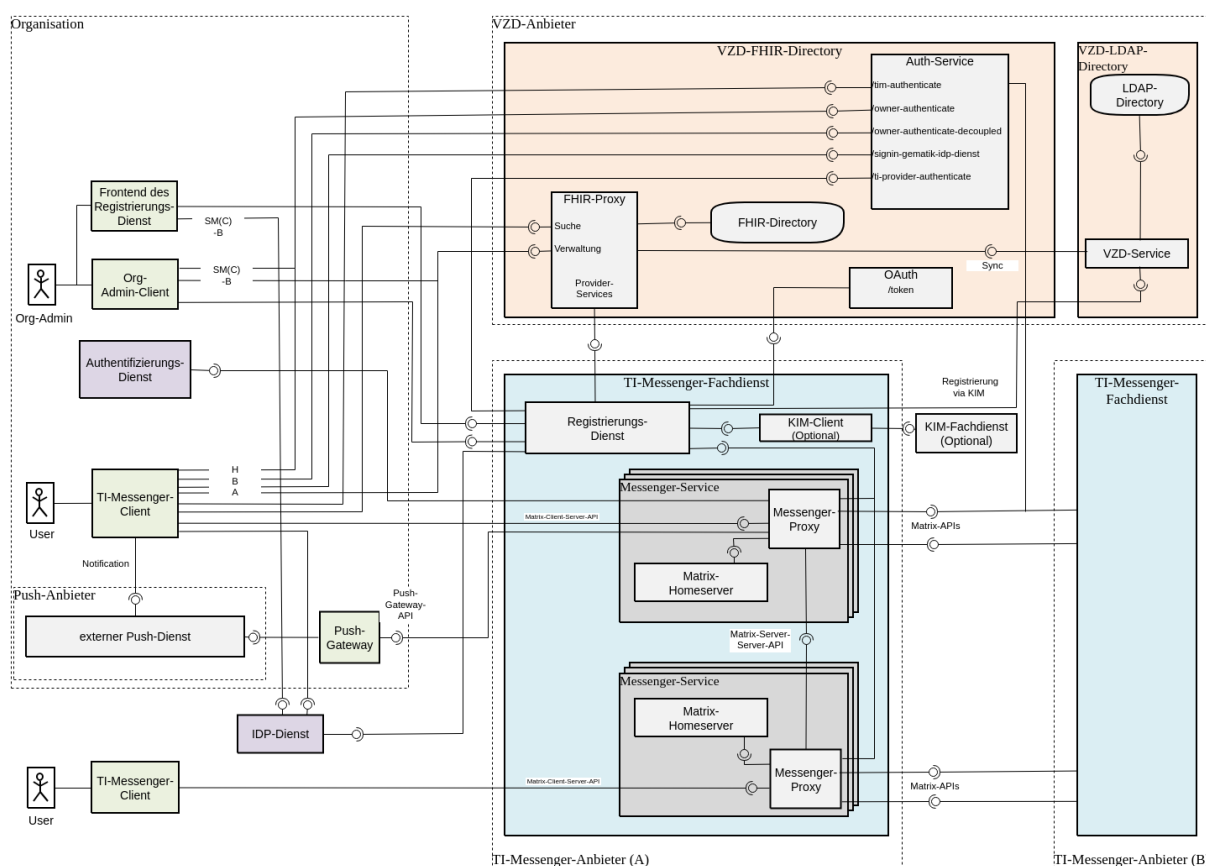


Abbildung 1: Komponenten der TI-Messenger-Architektur (vereinfachte Darstellung)

In den folgenden Kapiteln werden zuerst die nicht zum TI-Messenger gehörigen Systeme und Schnittstellen beschrieben. Kapitel 3- Zerlegung des Produkttyps (Systemkomponenten) befasst sich dann mit den Komponenten und Schnittstellen des TI-Messengers.

2.1 TI-Messenger Föderation

Da der TI-M Dienst auf dem offenen und dezentralen Kommunikationsprotokoll Matrix basiert, muss gewährleistet werden, dass nur berechtigte Matrix-Homeserver eines Messenger-Services teilnehmen.

Um allen berechtigten Akteuren des deutschen Gesundheitswesens den Zugang zum TI-M Dienst zu gewähren, muss ein Anbieter eines TI-Messengers für Organisationen des deutschen Gesundheitswesens eigene Messenger-Services bereitstellen. Um nicht zum TI-M Dienst gehörende Matrix-Homeserver ausschließen zu können, werden die Domainnamen (im Weiteren auch als Matrix-Domain bezeichnet) der Matrix-Homeserver der Messenger-Services in einer Föderationsliste zusammengefasst. Diese wird durch das [gemSpec_VZD_FHIR_Directory] bereitgestellt und kann nach einer erfolgreichen Zulassung durch den Registrierungs-Dienst bezogen werden.

A_25528 -Kein Bridging

Ein serverseitiges Bridging zu anderen Messaging-Protokollen DARF NICHT vom TI-M FD unterstützt werden.[<=]

2.2 Matrix

Für den TI-Messenger wird das offene Kommunikationsprotokoll der Matrix-Foundation verwendet. Im Rahmen der Spezifikation wird das Server-Server- (gemäß [Server-Server API]) und das Client-Server-Protokoll (gemäß [Client-Server API]) nachgenutzt. Für die Kommunikation der Matrix-Homeserver in der Föderation wird die API gemäß [Server-Server API] verwendet. Der TI-M Client setzt bei der Kommunikation mit den Matrix-Homeservern die API gemäß Matrix-Client-Server-Protokolls um. Für die Benachrichtigung der Akteure über eingehende Nachrichten wird ein Push-Gateway verwendet, welches gemäß [Push Gateway API] nachgenutzt wird. Bei der Kommunikation selbst werden REST-Webservices über HTTPS (JSON-Objekte) aufgerufen.

A_25641-01 -Matrix Spezifikationsversion

Als Basis MUSS die Matrix Spezifikation in der Version 1.11 verwendet werden. [≤=]

2.3 Akteure und Rollen

Im Kontext des TI-M Dienstes werden verschiedene Akteure und Rollen definiert. Ein Akteur ist eine natürliche Person oder ein automatisiertes System, für den ein Benutzeraccount auf dem Fachdienst angelegt wird und von diesem genutzt werden kann um mit einem TI-M FD zu interagieren.

Die folgende Tabelle gibt einen Überblick über die im Kontext des TI-M Dienstes definierten Rollen, abhängig vom verwendeten Authentifizierungsverfahren, die ein Akteur einnehmen kann. Die Tabelle stellt alle möglichen Nutzerszenarien nach erfolgreicher Authentifizierung einer Organisation am Registrierungs-Dienst dar.

Tabelle 1: Akteure und Rollen

Welcher Akteur bin ich	Wie authentisiere ich mich	Welcher Dienst authentifiziert mich	Welche Rolle nehme ich ein
Nutzer des TI-Messengers	Authentifizierungsverfahren der Organisation + 2. Faktor	Messenger-Service	User
	Admin-Account Credentials + 2. Faktor	Registrierungs-Dienst	Org-Admin
Beauftragter Administrator eines TI-Messenger-Anbieters	Admin-Account Credentials + 2. Faktor	Registrierungs-Dienst	Org-Admin

Hinweis: Bei den in der Tabelle genannten Nutzerszenarien mit der 2-Faktor-Authentifizierung sind die in 2.5.1- Authentifizierungs-Dienst für Akteure genannten Anforderungen zu berücksichtigen.

Abhängig von dem verwendeten Authentifizierungsverfahren am Messenger-Service eines TI-M FD ergeben sich unterschiedliche Rollen, die ein Akteur einnehmen kann. Im Folgenden werden diese Rollen ausführlicher beschrieben.

2.3.1 Rolle: "User"

Die Rolle "User" ist die Basisrolle im Kontext des TI-Messengers. Jeder Akteur, der an der Kommunikation in der Messenger-Föderation teilnimmt, besitzt diese Basisrolle. Die Authentifizierung des Akteurs erfolgt hierbei über ein vom Messenger-Service bereitgestelltes Authentifizierungsverfahren.

In dieser Rolle kann ein Akteur:

- sich gegenüber einem Messenger-Service authentisieren und
- sich an einem Messenger-Service anmelden.

2.3.2 Rolle: "Org-Admin"

Die Rolle "Org-Admin" stellt eine besondere Rolle im TI-Messenger Kontext dar. Mitarbeiter einer Organisation können diese Rolle einnehmen, nachdem sie ihre Organisation zuvor erfolgreich am Registrierungs-Dienst per SM(C)-B oder durch das KIM-Verfahren authentisiert haben (siehe Anwendungsfall [5.1.1- Authentisieren einer Organisation](#)). Nach der erfolgreichen Authentifizierung wird ein Admin-Account am Registrierungs-Dienst des TI-M FDs angelegt. Mit der Anmeldung am Registrierungs-Dienst über den Admin-Account nimmt ein Akteur die Rolle "Org-Admin" ein. Dieser kann Messenger-Services für seine Organisation registrieren. Für die Rolle "Org-Admin" besteht die Notwendigkeit, Administratoren einzusetzen, welche für Themen der Informationssicherheit geschult und sensibilisiert wurden. Dabei ist es auch möglich, dass die Organisation den TI-Messenger-Anbieter beauftragt, die Rolle "Org-Admin" zu übernehmen.

In dieser Rolle kann ein Akteur:

- Messenger-Services für seine Organisation registrieren
- Authentifizierungsmethoden für Akteure an Messenger-Services seiner Organisation festlegen
- die Accounts der Akteure dieser Messenger-Services verwalten
- die Matrix-Homeserver-Konfigurationen für seine Organisation vornehmen

2.4 Berechtigungskonzept

Das Berechtigungskonzept für den TI-Messenger ist in 2 Stufen unterteilt. Stufe 1 umfasst die Prüfung der Föderationszugehörigkeit bei ein- und ausgehender Kommunikation am TI-M Fachdienst. In Stufe 2 können Akteure selbst steuern wer sie kontaktieren darf. TI-M Clients hinterlegen dazu eine akteurspezifische Berechtigungskonfiguration zentralisiert in Account Data auf dem TI-M Fachdienst, der die Konfiguration anschließend durchsetzt.

Weitere Details zu Ablauf und Konfiguration von Berechtigungen sind im Kapitel [5.2- Berechtigungsmanagement](#) beschrieben.

2.5 Nachbarsysteme

Die folgenden Kapitel beschreiben Systeme, die für die Funktionalität des TI-Messengers von essentieller Bedeutung, jedoch nicht Teil der Produkte TI-M Client und TI-M FD sind.

2.5.1 Authentifizierungs-Dienst für Akteure

Der Authentifizierungs-Dienst verwaltet die Identitäten der Akteure und übernimmt die Authentifizierung. Sind z. B. bereits Systeme wie Active-Directory oder LDAP basierende Nutzerverzeichnisse innerhalb einer Organisation verfügbar, können diese verwendet werden, indem das jeweilige Backend bei diesen registriert wird. Sind keine Authentifizierungsverfahren in der Organisation vorhanden, können TI-Messenger-Anbieter entsprechende Authentifizierungsverfahren zur Verfügung stellen. Bei der Ausgestaltung sind die folgenden Anforderungen zu berücksichtigen.

A_25304 -Nachnutzung bestehender Authentifizierungsverfahren

Anbieter des TI-Messenger-Dienstes KÖNNEN für die Authentisierung von Akteuren in der Rolle "User" bestehende Authentifizierungsverfahren der Organisation nachnutzen. [≤]

A_25305 -Verantwortung der Organisation bei Nachnutzung bestehender Authentifizierungsverfahren

Werden bestehende Authentifizierungsverfahren der Organisation für die Authentisierung von Akteuren in der Rolle "User" nachgenutzt, MÜSSEN Anbieter die Organisation und die Administratoren explizit darauf hinweisen, dass die Sicherheit der Nutzerauthentisierung damit in die Verantwortung der Organisation gegeben wird. [≤]

A_25306 -Kontrolle über genutzte Authentifizierungsverfahren

Der Anbieter MUSS sicherstellen, dass Authentifizierungsverfahren, die von einer Organisation für die Authentisierung von Akteuren in der Rolle "User" verwendet werden, unter Kontrolle der Organisation sind und entsprechende Authentisierungsmittel von dieser verwaltet und gesperrt werden können. Selbiges gilt, wenn der Anbieter die Nachnutzung bestehender Authentifizierungsverfahren der Organisation ermöglicht. [≤]

A_25307 -Verwendung von 2FA

Der Anbieter MUSS sicherstellen, dass zur Authentisierung mindestens zwei Faktoren verwendet werden und die Sicherheitsempfehlungen des BSI [BSI 2-Faktor] Berücksichtigung finden. [≤]

A_25308 -Resilienz der 2FA

Als 2. Faktor MUSS ein Verfahren gewählt werden, dass vom BSI hinsichtlich seiner Resilienz gegenüber Angriffen aus der Ferne mindestens mit "mittel" bewertet wurde [BSI 2-Faktor]. [≤]

2.5.2 IDP-Dienst

Der zentrale IDP-Dienst der gematik ermöglicht die sichere Identifikation der Akteure anhand der ihnen bereitgestellten Identifikationsmittel (z. B. SM(C)-B / HBA). Die Identifikation des Akteurs wird anhand einer Smartcard und der Auswertung des vom Authenticator-Modul an den IDP-Dienst übergebenen Authentifizierungszertifikats (aus der Smartcard) sichergestellt. Im Kontext des TI-Messenger übernimmt der IDP-Dienst die Identifikation der Akteure für die Registrierung und den Zugriff auf das VZD-FHIR-Directory.

2.5.3 VZD-FHIR-Directory

Beim VZD-FHIR-Directory handelt es sich um einen zentralen Verzeichnisdienst der TI, der die deutschlandweite Suche von Organisationen und HBA-Inhabern des TI-M Dienstes ermöglicht. Er basiert auf dem FHIR-Standard zum Austausch von definierten Informationsobjekten (FHIR-Ressourcen).

Der Verzeichnisdienst bietet zwei Arten von Verzeichnistypen an, die durchsucht werden können. Für die Suche von Organisationseinträgen wird das Organisationsverzeichnis

(HealthcareService) und für die Suche von Akteuren das Personenverzeichnis (PractitionerRole) verwendet. Im Organisationsverzeichnis sind alle auf eine Organisation bezogenen Ressourcen hinterlegt. Für die Suchen nach FHIR-Einträgen werden durch die TI-M Clients FHIR-Schnittstellen am VZD-FHIR-Directory aufgerufen.

Zusätzlich zur Bereitstellung der Verzeichnisse verwaltet das VZD-FHIR-Directory die Föderationsliste. Für die Registrierung der Matrix-Domain wird durch den Registrierungs-Dienst eine REST-Schnittstelle am VZD-FHIR-Directory aufgerufen, die mittels OAuth2 Client Credentials Flow gesichert ist. Dies ermöglicht es TI-Messenger-Anbietern ihre betriebenen Messenger-Services in die TI-Messenger-Föderation aufzunehmen und zu verwalten.

Allgemein besteht das VZD-FHIR-Directory aus mehreren Teilkomponenten (Auth-Service, OAuth-Service und FHIR-Proxy) die benötigt werden, um alle Funktionsmerkmale abbilden zu können. Im Folgenden werden die Teilkomponenten ausführlicher beschrieben. Weiterführende Informationen zum VZD-FHIR-Directory sind in [api-vzd] zu finden.

2.5.3.1 Auth-Service

Die Teilkomponente Auth-Service stellt den TI-M Clients sowie dem Registrierungs-Dienst eines TI-M FD die für den Aufruf der FHIR-Schnittstellen am FHIR-Proxy benötigten access-token aus. Hierbei werden die folgenden REST-Schnittstellen verwendet:

- /tim-authenticate
- /ti-provider-authenticate

Die Schnittstelle /tim-authenticate erwartet ein Matrix-OpenID-Token. Die Schnittstelle /ti-provider-authenticate wiederum erwartet ein ti-provider-accesstoken, welches zuvor vom OAuth-Service des VZD-FHIR-Directorys ausgestellt wurde.

2.5.3.2 OAuth

Die Teilkomponente OAuth stellt dem Registrierungs-Dienst über den /token-Endpunkt ein für den OAuth2 Client Credentials Flow temporäres ti-provider-accesstoken aus. Bevor der Registrierungs-Dienst den /token-Endpunkt am OAuth-Service aufrufen kann, muss sich der TI-Messenger-Anbieter zuvor beim VZD-Anbieter Client-Credentials beantragen, die bei Aufruf des Endpunktes mit übergeben werden.

2.5.3.3 FHIR-Proxy

Der FHIR-Proxy ist eine Teilkomponente des VZD-FHIR-Directory. Alle Anfragen an das FHIR-Directory werden über den FHIR-Proxy verarbeitet. Der FHIR-Proxy stellt die folgenden zwei Schnittstellen zur Verfügung, die durch die TI-M Clients sowie durch den Registrierungs-Dienst aufgerufen werden:

- eine Suchschnittstelle für die Suche nach Organisationen und Praktizierenden
- eine Schnittstelle zur Pflege eigener TI-M Provider Einträge

Bei Aufruf der Schnittstellen ist ein access-token mit zu übergeben. Bei erfolgreicher Authentifizierung leitet der FHIR-Proxy die Anfragen an das FHIR-Directory weiter.

2.5.4 Externer Push-Dienst

Ein externer Push-Dienst ist ein vom Gerätehersteller verwalteter Dienst, der Benachrichtigungen direkt an den TI-M Client auf dem Endgerät des Akteurs senden kann.

2.6 Zugriffstoken

Für die Nutzung des TI-M Dienstes kommen unterschiedliche Arten von Token zur Authentisierung und Autorisierung an weiteren Diensten zum Einsatz, die in verschiedenen Anwendungsfällen verwendet werden. Aus diesem Grund werden in der folgenden Tabelle die unterschiedlichen Token näher beschrieben.

Tabelle 2: Arten von Token

Token	ausgestellt vom	Beschreibung
ID_TOKEN	zentralen IDP-Dienst	<p>Dieses Token wird auf Basis von SM-Identitäten vom zentralen IDP-Dienst ausgestellt und beinhaltet die zugehörigen Identitätsdaten (TelematikID, ProfessionOID etc.).</p> <p>Der Registrierungs-Dienst nutzt dieses Token, um die enthaltene ProfessionOID auf einen gültigen Institutionstypen für ein SM-B bzw. eine SMC-B zu prüfen und im Rahmen einer Messenger-Service Bestellung die enthaltene TelematikID in die Föderationsliste einzutragen.</p>
Matrix-ACCESS_TOKEN	Matrix-Homeserver	<p>Nach der erfolgreichen Anmeldung eines Akteurs am Matrix-Homeserver wird ein Access-Token vom Matrix-Homeserver ausgestellt. Im Kontext des TI-M Dienstes wird das vom Matrix-Homeserver ausgestellte Access-Token als Matrix-ACCESS_TOKEN bezeichnet.</p> <p>Dieses Token wird bei jeder weiteren Interaktion mit dem ausstellenden Matrix-Homeserver verwendet, um den TI-M Client zu berechtigen bestimmte Dienste des Servers zu nutzen.</p>
Matrix-REFRESH_TOKEN	Matrix-Homeserver	<p>Nach der erfolgreichen Anmeldung eines Akteurs am Matrix-Homeserver wird neben dem Matrix-ACCESS_TOKEN zudem ein Refresh-Token ausgestellt. Das Refresh-Token besitzt eine längere Gültigkeit als das Access-Token und kann genutzt werden, um sich nach Ablauf des Access-Token ein neue Access-Token vom Homeserver ausstellen zu lassen.</p>

Matrix-OpenID-Token	Matrix-Homeserver	<p>Bei dem Matrix-OpenID-Token handelt es sich um ein 3rd-Party-Token, welches von einem Matrix-Homeserver gemäß [Client-Server API/#OpenID] bei Bedarf für einen Akteur ausgestellt wird. Im Kontext des TI-M Dienstes wird das 3rd-Party-Token als Matrix-OpenID-Token bezeichnet.</p> <p>Das Matrix-OpenID-Token wird für die Verifizierung eines Messenger-Services sowie für das Suchen von FHIR-Ressourcen im VZD-FHIR-Directory benötigt. Hierfür wird das Matrix-OpenID-Token im Auth-Service des Verzeichnisdienstes gegen ein search-accesstoken ersetzt, welches am FHIR-Proxy für die weitere Verarbeitung benötigt wird. Das ursprünglich ausgestellte Matrix-OpenID-Token wird dann nicht mehr benötigt. Zur Überprüfung der Gültigkeit des Matrix-OpenID-Token ruft der Auth-Service den Userinfo-Endpoint am jeweiligen Matrix-Homeserver auf.</p>
ti-provider-accesstoken / provider-accesstoken	OAuth / Auth-Service des VZD-FHIR-Directory	<p>Das ti-provider-accesstoken wird dem Registrierungs-Dienst durch den OAuth-Service und das provider-accesstoken durch den Auth-Service des VZD-FHIR-Directory bereitgestellt.</p> <p>Ein provider-accesstoken wird z. B. benötigt, wenn der Registrierungs-Dienst eines TI-M FD, nach der Bereitstellung eines neuen Messenger-Service für eine Organisation, einen neuen Förderationslisteneintrag für diese Organisation anlegt oder der Registrierungs-Dienst eine Förderationsliste vom FHIR-Proxy abfragen möchte. Hierfür übergibt der Registrierungs-Dienst im ersten Schritt vereinbarte Client-Credentials an den OAuth-Service des VZD-FHIR-Directory und erhält nach der erfolgreichen Prüfung dieser Credentials das ti-provider-accesstoken. Das ti-provider-accesstoken wird anschließend an den Auth-Service des VZD-FHIR-Directory übergeben und bei erfolgreicher Prüfung durch das VZD-FHIR-Directory wird ein provider-accesstoken ausgestellt.</p>
search-accesstoken	Auth-Service des VZD-FHIR-Directory	<p>Das search-accesstoken wird einem berechtigten Akteur durch den Auth-Service des VZD-FHIR-Directory bereitgestellt.</p> <p>Dieses wird für die Suche im VZD-FHIR-Directory benötigt und stellt sicher, dass nur berechnigte Akteure im VZD-FHIR-Directory eine Suche auslösen können. Dazu wird das vom Matrix-Homeserver ausgestellte Matrix-OpenID-Token an den Auth-Service des VZD-FHIR-Directory übergeben. Dieses dient in diesem Fall als Nachweis, dass ein Akteur bei einem der TI-Föderation angehörenden Messenger-Service</p>

		registriert ist. Nur dann wird durch den Auth-Service des VZD-FHIR-Directory ein search-accesstoken bereitgestellt. Es muss bei der dann folgenden Suche im VZD-FHIR-Directory im Aufruf enthalten sein. Die Prüfung erfolgt durch den FHIR-Proxy.
Push-Anbieter App Token	Push-Anbieter	Das Push-Anbieter App Token ist ein Token über welches eine App eindeutig für die Zustellung von Push-Nachrichten identifiziert werden kann.

3 Zerlegung des Produkttyps (Systemkomponenten)

Die folgenden Kapitel beschreiben die Komponenten und die jeweils an Sie gerichteten Anforderungen der Produkttypen TI-M Client und TI-M FD.

3.1 TI-M Client

Der TI-M Client wird als eine Anwendung (oder eingebettet in bestehende Anwendungen) auf dem Endgerät eines Akteurs ausgeführt und ermöglicht eine sichere, nachrichtenbasierte Kommunikation mit anderen Akteuren des TI-M Dienstes. Der TI-M Client folgt den offenen Standards des Kommunikationsprotokolls Matrix und synchronisiert, durch die Matrix Foundation festgelegte JSON-Objekte mit Matrix-Homeservern, welche als Teil des Messenger-Services eines TI-M FD bereitgestellt werden.

Die Kommunikation zwischen den Akteuren des TI-M Dienstes erfolgt in Räumen. Bei Verwendung von Ende-zu-Ende-Verschlüsselung werden die Nachrichten auf dem jeweiligen TI-M Client erstellt und verschlüsselt versendet. Die gesendeten Nachrichten werden verschlüsselt auf dem jeweiligen Matrix-Homeserver gespeichert. Der für die Entschlüsselung benötigte Schlüssel wird nur mit verifizierten Endgeräten innerhalb des jeweiligen Raumes geteilt. Die beteiligten Matrix-Homeserver können die Nachrichten nicht entschlüsseln.

Die Kommunikation zwischen einem TI-M Client und einem TI-M FD erfolgt über die Messenger-Proxies. Auf den Messenger-Proxies findet die TLS-Terminierung der Verbindungen von den TI-M Clients statt. Die Messenger-Proxies erlauben nur mit zugelassenen TI-M Clients das Anmelden eines Akteurs. Zusätzlich wird während des Anmeldevorgangs durch den TI-M Client am Auth-Service des VZD-FHIR-Directory geprüft, ob es sich um einen zugelassenen Matrix-Homeserver handelt.

In der folgenden Abbildung sind alle beteiligten Komponenten der TI-Messenger-Architektur in vereinfachter Form dargestellt und die TI-M Komponenten die im folgenden Kapitel erläutert werden, blau eingefärbt.

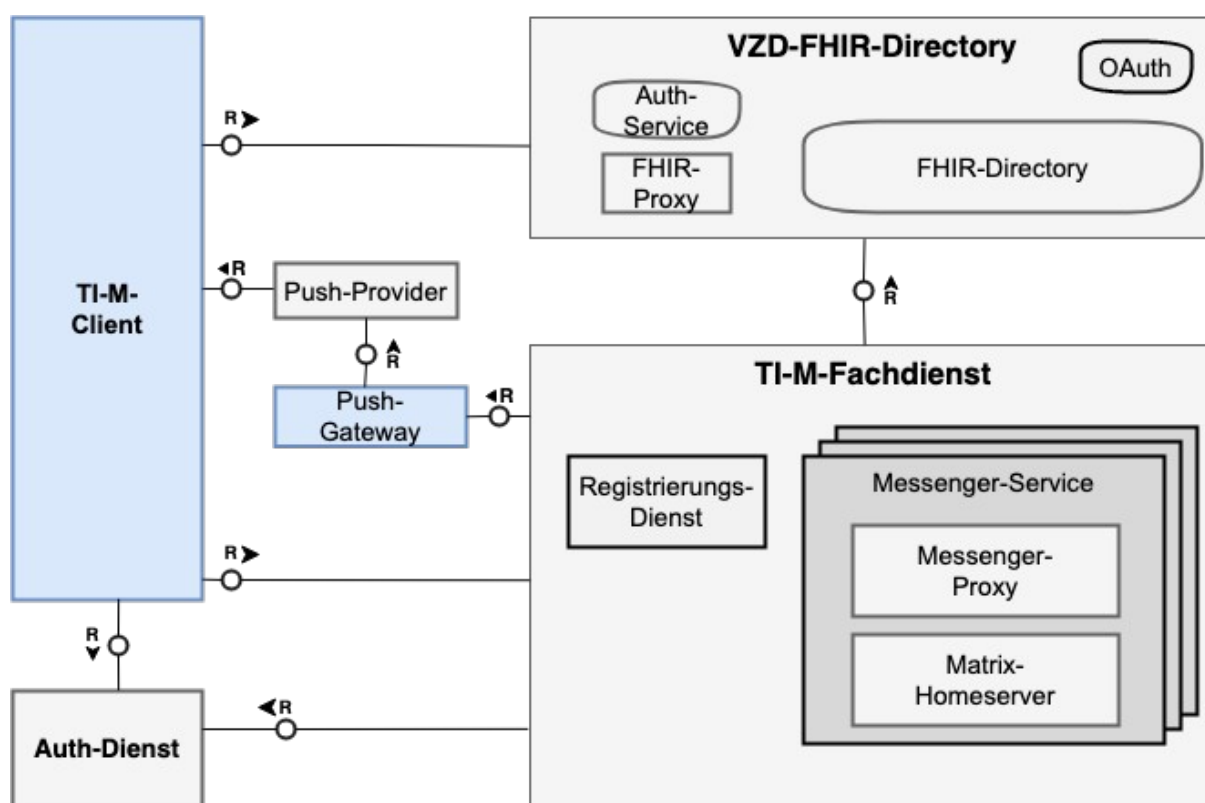


Abbildung 2: Systemüberblick TI-M Client

A_25491 -Bereitstellung von Datenschutzinformationen

Der TI-M Client MUSS für den Akteur klar erkennbar Datenschutzinformationen bereitstellen. [≤]

A_25495 -Anzeige von Fehlern beim Versand

Der TI-M Client MUSS den Nutzer über Fehler beim Versand informieren. [≤]

A_25512 -Trennung von Mandanten

TI-M Clients MÜSSEN verhindern, dass bei geteilten Endgeräten ein Akteur des TI-M Clients auf Daten oder Funktionen eines anderen Akteurs des TI-M Clients auf diesem Gerät zugreifen kann. [≤]

A_25513 -Mandantentrennung nicht durch Betriebssystem

Für den Schutz der Daten verschiedener Mandanten, DARF sich der TI-Messenger Client NICHT darauf verlassen, dass seitens des Betriebssystems eine Trennung von Nutzern vorgenommen wird, welche den Zugriff auf Daten anderer Akteure verhindert, da derartige Funktionalität nicht notwendigerweise genutzt wird. [≤]

Hinweis: Die Trennung von Mandanten erfordert nicht, dass mehrere Akteure gleichzeitig angemeldet sein können, deren Daten dann jeweils voreinander zu schützen sind. Stattdessen kann die Mandantentrennung auch so implementiert sein, dass zu jedem Zeitpunkt immer nur einer der möglichen Vielzahl von Akteuren angemeldet sein kann.

A_25519 -Schnittstelle für Virenschanner

TI-M Clients KÖNNEN über Schnittstellen und Funktionen verfügen, mit denen empfangene entschlüsselte Dateien zur Überprüfung auf Schadsoftware an Virenschanner übergeben werden, bevor diese verarbeitet werden. [≤]

A_25520 -Vorgehen bei Meldung von Schadsoftware

Nutzt ein TI-M Client die Möglichkeit zur Prüfung von Inhalten durch einen Virenschanner und meldet dieser Virenschanner das Vorhandensein von Schadsoftware im geprüften Inhalt, SOLL der TI-M Client diesen Inhalt verwerfen. [≤]

A_25521 -Information über Vorgehen bei Meldung von Schadsoftware

Verwirft der TI-M Client Inhalte, MUSS der Akteur darüber sowie über den Grund informiert werden. [≤]

A_25522 -Fehlschlag der Prüfung auf Schadsoftware

Nutzt ein TI-M Client die Möglichkeit zur Prüfung von Inhalten durch einen Virens Scanner und meldet dieser Virens Scanner ein Fehlschlagen der Prüfung, MUSS der TI-M Client den Akteur über den Prüfstatus und die mögliche Gefahr informieren. [≤]

A_25523 -Keine Ausführung aktiver Inhalte

Verfügt der TI-M Client über eine Funktion, Dokumente direkt über den TI-M Client ohne Nutzung von Third-Party Software anzuzeigen, MUSS er die Ausführung von aktiven Inhalten verhindern. [≤]

A_25524 -Anzeige von Metadaten

Verfügt der TI-M Client über eine Funktion, Dokumente direkt über den TI-M Client ohne Nutzung von Third-Party Software anzuzeigen, MUSS er es ebenfalls ermöglichen, zugehörige Metadaten auch ohne Öffnen oder Herunterladen der Datei selbst einzusehen. [≤]

A_25525 -Information über Gefahren von Schadsoftware

Der TI-M Client MUSS den Akteur darüber informieren, dass Dokumente Schadsoftware enthalten können und welche Maßnahmen der Akteur zum Selbstschutz vornehmen kann. [≤]

A_25569 -Einbringung von Schlüsseln und Token

TI-M Client-Hersteller MÜSSEN sicherstellen, dass Schlüssel und Token sicher in den TI-M Client eingebracht werden, das heißt unter Nutzung der von der Spezifikation und dem Matrix-Protokoll vorgesehenen Abläufe und Verfahren.

In diesem Sinne werden die verschiedenen Token (siehe Tabelle 2) mittels TLS-gesicherter Verbindung zum jeweiligen Fachdienst eingebracht, der diese nach erfolgreichem Handshake ausstellt. Die Einbringung von Schlüsseln folgt den Vorgaben und Funktionen des Matrix-Protokolls (SSSS, Key Sharing, Wiederherstellung aus verschlüsseltem Offline-Backup, Key Agreement, Schlüsselfortschreibung). [≤]

A_25570 -Speicherung von Schlüsseln und Token

TI-M Client-Hersteller MÜSSEN technisch sicherstellen, dass Schlüssel und Token nicht in andere Speicher ausgelagert werden können, als die dafür vorgesehenen Speicher der TI-M Clients oder dem [SSSS] des beteiligten Matrix-Homeservers. [≤]

A_26435 -Ver- und Entschlüsselung

Die Ver- und Entschlüsselung MUSS lokal auf dem TI-M Client erfolgen. [≤]

A_25573 -Verwendung von TLS zur Kommunikation mit dem Fachdienst und VZD-FHIR-Directory

TI-M Clients MÜSSEN mit anderen Komponenten des TI-M Dienstes sowie dem VZD-FHIR-Directory über TLS kommunizieren und die dafür erforderlichen Verfahren unterstützen. Hierzu gelten die Festlegungen der [gemSpec_Krypt]. [≤]

A_25580 -Sicherheitsrisiken von Software Bibliotheken minimieren

Der TI-M Client MUSS Maßnahmen umsetzen, um die Auswirkung von unentdeckten Schwachstellen in benutzten Software-Bibliotheken zu minimieren. [≤]

Hinweis: Beispielmaßnahmen sind in [OWASP Proactive Control#C2] zu finden. Das gewählte Verfahren muss die gleiche Wirksamkeit aufweisen, wie die Kapselung gemäß [OWASP Proactive Control#C2 Punkt 4].

A_25584 -Selbst-Update des TI-M Clients aus vertrauenswürdigen Quellen

Lädt und appliziert ein TI-M Client Selbstaktualisierungen, so MUSS er sicherstellen, dass Updates nur von bekannten und vertrauenswürdigen Quellen bezogen werden, nachdem die Authentizität der Quelle technisch erfolgreich verifiziert wurde. [≤]

A_25598 -Einsatz auditiertter Verschlüsselung

TI-M Clients MÜSSEN für die Verschlüsselung von Nachrichten eine auditierte und für ausreichend sicher befundene Implementierung von Olm/Megolm verwenden. [\leq]

Hinweis: Die gematik hat in Kooperation mit der Matrix-Foundation ein Audit für die Rust-Implementierung von Olm/Megolm - Vodozamac - durchführen lassen, das im Jahr 2022 abgeschlossen wurde. Weiterhin hat die gematik ein erneutes Audit der C/C++-Implementierung von Olm/Megolm - libolm - durchführen lassen, das im Jahr 2024 abgeschlossen wurde. Auf Basis dieser Audits werden Vodozamac und libolm als die von der gematik vorgesehenen Implementierungen benannt.

A_25599 -Verwendung anderer Implementierungen von Olm/Megolm

Sollte für die Umsetzung von Olm/Megolm eine andere Implementierung als eine der von der gematik vorgesehenen genutzt werden, MUSS der Hersteller einen Sicherheitsnachweis erbringen, welcher nach Art, Umfang und Ergebnis den Audits von Vodozamac und libolm entspricht und von nachweislich geeigneten und vom Hersteller unabhängigen Personen erbracht wurde. [\leq]

A_25501-01 -Sperrung des TI-Messenger Clients

Es MUSS sichergestellt sein, dass der Zugriff auf den TI-M Client, der kein Web-Client ist, erst nach Authentisierung gegenüber dem TI-M Client möglich ist. Mit Authentisierung ist die Überwindung einer App-Sperre gemeint. [\leq]

Hinweis: Geeignete Faktoren zur Implementierung der App-Sperre sind solche, die auch im Rahmen der Authentifizierungsverfahren des sektoralen IDP [gemSpec_IDP_Sek#Authentifizierungsverfahren] zulässig sind.

A_26023-01 -Mehr-Faktor-Authentisierung für den TI-M Client zzgl. Ersatzverfahren

Der TI-M Client MUSS, da er medizinische Daten lokal zwischenspeichern kann, dem Akteur mindestens eine Authentisierungsart mit mehreren Faktoren für die Überwindung der App-Sperre (des TI-M Clients) anbieten. [\leq]

A_25502-01 -Entsperrung per Biometrie

Wird für die Überwindung der App-Sperre zum Zugriff auf den TI-M Client das Mittel Biometrie als möglicher Faktor für die Authentisierung angeboten, MUSS es den Vorgaben aus [gemSpec_IDP_Sek], Kapitel 4.3.2.2 ("Nutzung von Biometrie") genügen. [\leq]

A_26024 -Hinweise zu Authentisierungsarten

Der TI-M Client SOLL dem Akteur die verfügbaren Authentisierungsarten in verständlicher Form darstellen und erklärende Hinweise zur Verfügung stellen. [\leq]

A_25503-02 -Notwendigkeit der Entsperrung

Die Überwindung der Sperre zum Zugriff auf den TI-M Client MUSS unter folgenden Bedingungen gefordert werden:

- nach jedem Start der Anwendung,
- nach jedem Benutzerwechsel am Betriebssystem,
- bei aktivierter App-Sperre

[\leq]

A_26512-01 -Inaktivitätsintervall für die Notwendigkeit der Entsperrung

Der TI-M Client MUSS den Zugriffsschutz der App nach spätestens 20 Minuten Inaktivität (Zeitspanne nach der letzten Nutzer-Aktivität) aktivieren.

[\leq]

A_27054 -Konfigurierbares Inaktivitätsintervall

Der TI-M Client KANN das Inaktivitätsintervall, nach dem erneut eine Entsperrung des TI-M Clients notwendig ist, dem Nutzer als konfigurierbar anbieten. [\leq]

A_26446 -Wechsel auf stärkeres Authentisierungsverfahren

Hat der Akteur ein niederschwelliges Verfahren zur Überwindung der App-Sperre gewählt, MUSS der TI-M Client dem Akteur jederzeit die Möglichkeit bieten, wieder auf ein stärkeres Verfahren zu wechseln.【<=】

Hinweis: Niederschwellige Verfahren sind Authentifizierungsverfahren mit einem geringeren Niveau als 'gematik-ehealth-loa-high', wie sie in der Spezifikation des sektoralen IDP, [gemSpec_IDP_Sek] Kapitel 4.3, beschrieben sind.

A_26227-01 -Längenbegrenzung von Annotationen in Reactions

Der TI-M Client MUSS sicherstellen, dass der Wert des Attributes key im Event-Content in Events des Typs m.reaction beim Erzeugen die Länge eines einzelnen Unicode-Characters bzw. dessen Code Point Repräsentation nicht überschreitet.【<=】

3.1.1 Ausprägungen nach Nutzergruppen

Gemäß der Architektur des TI-M Dienstes wird zwischen zwei Arten von TI-M Clients unterschieden. Die Unterscheidung ergibt sich ausschließlich aus der Sicht der Akteure.

Im Folgenden werden die beiden Ausprägungen beschrieben.

3.1.1.1 TI-M Client für Akteure in der Rolle "Org-Admin" (Org-Admin-Client)

Der TI-M Client mit Administrationsfunktionen ist ein Client für Akteure einer Organisation in der Rolle "Org-Admin". Dieser wird im Kontext des TI-M Dienstes auch als Org-Admin-Client bezeichnet. Der Org-Admin-Client dient der komfortablen Verwaltung der Messenger-Services bei einem TI-M FD. Die Bereitstellung des Org-Admin-Clients kann als eigenständiger Client erfolgen oder als eine Integration in einen TI-M Client für Akteure. Sofern reguläre Nutzerfunktionen und Administrationsfunktionen in demselben Client angeboten werden, muss auf eine klar erkennbare Unterscheidung zwischen Nutzer- und Administrationsfunktionen geachtet werden. Im Folgenden werden die durch den Org-Admin-Client bereitzustellenden Administrationsfunktionen genauer beschrieben.

Zusammenfassung

- Benutzerverwaltung (Liste aller Akteure, Anlegen, Bearbeiten, Löschen)
- Geräteverwaltung (Anzeigen, Abmelden, Löschen aller Geräte eines Messenger-Services seiner Organisation)
- Systemmeldungen an Akteure eines Messenger-Services senden (z. B. Wartungsfenster bekannt machen)

A_25472-01 -Nutzer Sessions Anzeige

Der Org-Admin-Client MUSS mindestens device_id, display_name, last_seen_ip, last_seen_ts zu aktiven Sessions von Devices anzeigen. Der Inhalt von last_seen_ts MUSS in ein gültiges Datumsformat bestehend aus dem Datum und Uhrzeit umgewandelt werden.【<=】

A_25473 -Akteur abmelden

Der Org-Admin-Client MUSS dem Org-Admin die Möglichkeit bieten die Access-Token & Refresh-Token der einzelnen Devices oder aller Devices zu invalidieren, um den Akteur abzumelden.【<=】

A_25474 -Infomeldungen

Der Org-Admin-Client MUSS das Senden von Informationen/Systemmeldungen an die an einem Messenger-Service angemeldeten TI-M Clients ermöglichen.【<=】

A_26394-01 -Administration von Benutzeraccounts

Der Org-Admin-Client MUSS folgende Verwaltungsaktionen, bezogen auf die Nutzer von Messenger-Services, die durch die eigene Organisation verwaltet werden, unterstützen:

- Auflisten der Gesamtmenge dieser Nutzer
- Löschen oder dauerhaftes Deaktivieren eines Nutzers

[<=]

A_26395 -Administration von Geräten

Der Org-Admin-Client MUSS folgende Verwaltungsaktionen, bezogen auf die Nutzer von Messenger-Services und deren Geräte, die durch die eigene Organisation verwaltet werden, unterstützen:

- Anzeigen aller Geräte bzw. Gerätebindungen eines Nutzers
- Löschen von Geräten und deren Nutzerzuordnung

[<=]

A_26396 -Org-Admin Authentisierung und Rollenwechsel

Der TI-M Client MUSS zur Erlangung der Rolle "Org-Admin" eine Authentisierung des Akteurs für diese Rolle erzwingen. Dieses gilt auch für einen Wechsel in diese Rolle aus einer bestehenden anderen Rolle.[<=]

3.1.1.2 TI-M Client für Akteure in der Rolle "User"

Der TI-M Client für Akteure in der Rolle "User" unterstützt die meisten aller, durch die Matrix-Spezifikation festgelegten Funktionalitäten eines Matrix-Messengers. Akteure können mit Hilfe dieses Clients Chatnachrichten senden und empfangen. Innerhalb der Chaträume erfolgt der Zugriff auf Chatverläufe oder das Austauschen von Medien. Ebenfalls besteht für Akteure die Möglichkeit eigene Geräte und Geräte von Gesprächspartnern zu verifizieren und das VZD-FHIR-Directory zu durchsuchen, um z. B. eine neue Chatkonversation mit einer Organisation zu starten. Es ist den Herstellern freigestellt wie die Oberfläche gestaltet wird. So besteht beispielsweise die Möglichkeit Chaträume nach unterschiedlichen Verwendungszwecken zu organisieren.

Hinweis: Der TI-M Client für Akteure in der Rolle "User" und der Org-Admin-Client können auch in einem TI-M Client integriert sein. Die Art der Umsetzung obliegt dem jeweiligen TI-M Client-Hersteller.

A_25601 -Separate Benutzeroberflächen für Administration und Kommunikation

TI-M Clients, die sowohl als Client für die Kommunikation, als auch als Org-Admin-Client genutzt werden, MÜSSEN zur Bereitstellung der Funktionalitäten für die jeweilige Rolle separate User-Interfaces verwenden, welche die für den jeweiligen Zweck relevanten Informationen anzeigen und Funktionen bereitstellen. [<=]

3.1.2 Ausprägungen nach Plattform

TI-M Clients haben je nach Plattform (Mobil/Stationär) unterschiedliche Anforderungen an Sicherheit, Datenschutz und Funktionalität. Im Folgenden werden die zu unterstützenden Plattformen näher beschrieben.

3.1.2.1 TI-M Client für mobile Szenarien

Es handelt sich hierbei um eine TI-M Client Anwendung, die speziell für die Nutzung auf mobilen Geräten entwickelt wurde (z. B. Android/iOS). Die Bereitstellung kann als native mobile Anwendung erfolgen oder als eine Integration in bereits bestehende Anwendungen.

A_25398-01 -QR-Code erstellen

Der TI-M Client für mobile Szenarien MUSS eine Funktion bereitstellen, 2D-Barcodes zu erstellen und diese auf dem Display des Endgerätes anzuzeigen. Hierbei MUSS der 2D-Code in eine QR-Code-Darstellung gemäß ISO/IEC 18004:2006 kodiert werden. Als Inhalt für die Generierung des 2D-Codes MÜSSEN mindestens die Felder des folgenden vCard-Objektes verwendet werden:

```
BEGIN:VCARD
VERSION:4.0
FN:<displayname aus dem Matrix User Profil>
IMPP:<Matrix-URI>
END:VCARD
```

Der Aufbau der Matrix-URI MUSS gemäß [Matrix Appendices/#uris] gebildet werden. [≤]

A_25422-01 -QR-Code verarbeiten

Der TI-M Client für mobile Szenarien MUSS eine Funktion bereitstellen, die es dem Akteur erlaubt, über die Kamera des Endgerätes einen 2D-Barcode (in einer QR-Code-Darstellung) einzuscannen. Der TI-Messenger MUSS den eingescannten 2D-Code gemäß ISO/IEC 18004:2006 decodieren und mindestens den Inhalt aus den Parametern FN und IMPP dem Akteur anzeigen, damit dieser die Daten in seine Kontaktliste übernehmen kann. [≤]

A_25496 -Keine dauerhafte Standortdatenerhebung

Der TI-M Client DARF Standortdaten NICHT dauerhaft erheben. [≤]

A_25500 -Auslösung der Standorterhebung

Bei der Erhebung von Standortdaten MUSS sichergestellt sein, dass diese Erhebung ausschließlich durch einen menschlichen Benutzer ausgelöst wird und nach Beendigung des Anwendungsfalls, der die Standortdaten erhebt, diese wieder aus dem TI-M Client-Kontext gelöscht werden. [≤]

A_25527 -Prüfung der Geräteintegrität

TI-M Clients für mobile Plattformen MÜSSEN prüfen, ob ein Rooting des Gerätes vorliegt. Ist dies der Fall, MUSS dem Nutzer eine Warnung angezeigt werden und der Versand von Anhängen verhindert werden. [≤]

A_25535 -Abschottung von Inhalten auf mobilen Plattformen

TI-M Clients für mobile Plattformen MÜSSEN sicherstellen, dass Daten, die lokal durch den TI-M Client selbst gespeichert und nicht explizit durch den Nutzer für die Verwendung in anderen Kontexten exportiert wurden, in einem geschützten Speicherbereich auf dem Endgerät abgelegt werden. Hierzu genügen die von mobilen Betriebssystemen üblicherweise zur Verfügung gestellten Mechanismen wie die Verschlüsselung des Dateisystems und die Kapselung von Anwendungen untereinander. [≤]

A_25579 -Schutz gegen OWASP Mobile Top 10 Risiken

Hersteller von TI-M Clients für mobile Szenarien MÜSSEN für die von ihnen angebotenen mobilen TI-M Clients gewährleisten, dass der Client resistent bezüglich der im aktuellen und den beiden vorherigen OWASP Mobile Top 10 Report(s) ausgewiesenen Risiken ist. [≤]

3.1.2.2 TI-M Client für stationäre Szenarien

Es handelt sich hierbei um eine TI-M Client Anwendung, die speziell für die Nutzung auf stationären Endgeräten entwickelt wurde (z. B. Windows/macOS). Die Bereitstellung kann sowohl als eigenständige Lösung erfolgen oder als eine Integration in bereits bestehende Lösungen.

A_25497 -Schutz gespeicherter Daten in Desktop-Clients

Handelt es sich bei dem TI-M Client um eine Desktop-Applikation, MUSS dieser für empfangene und gesendete Daten, die nicht explizit durch den Nutzer für die Verwendung in anderen Kontexten exportiert wurden, gewährleisten, dass diese im Falle der Speicherung auch nur durch den TI-M Client und nach Authentifizierung des jeweiligen Nutzers gelesen werden können.【<=】

3.1.3 Matrix Spezifikation

Die Kernbestandteile des TI-M Clients basieren auf der Matrix Client-Server API. Diese umfasst neben dem eigentlichen Funktionsumfang für einen Ad-hoc-Nachrichtendienst auch die Verwaltung der Sessions, Benachrichtigungen etc., worauf in dieser Spezifikation nicht weiter eingegangen wird. Die folgenden Kapitel beschreiben Anforderungen zur Verwendung der geforderten Matrix Version und definieren Anforderungen, die über diese Version der Matrix Spezifikation hinausgehen.

A_25396 -Client-Server API

TI-M Clients MÜSSEN die clientspezifischen Anteile der Matrix Client-Server API gemäß [Client-Server API] umsetzen.【<=】

A_25345 -Appendices TI-M Clients

TI-M Clients MÜSSEN die [Matrix Appendices] gemäß der Matrix-Spezifikationen umsetzen.【<=】

3.1.3.1 Umdefinition der Module

Die Matrix Spezifikation unterteilt die einzelnen Funktionen der Client-Server API in Module, die für unterschiedliche Clients verbindlich (Required) oder optional (Optional) definiert werden. Die folgende Anforderung definiert für die aufgeführten Module die in der Matrix Spezifikation [Client-Server API/#modules] festgelegten Vorgaben neu.

A_25395-03 -Matrix Module

Die folgende Tabelle listet die Module aus der Matrix Spezifikation und die Neudefinition der Vorgaben.

Tabelle 3: Matrix Module

Modul	Web-Anwendung	mobile Szenarien	stationäre Szenarien
Content Repository	MUSS	MUSS	MUSS
Direct Messaging	MUSS	MUSS	MUSS
Ignoring Users	KANN	KANN	KANN
Instant Messaging	MUSS	MUSS	MUSS
Presence	MUSS	MUSS	MUSS
Push Notifications	KANN	MUSS	KANN
Receipts	MUSS	MUSS	MUSS
Room History Visibility	MUSS	MUSS	MUSS

Room Upgrades	MUSS	MUSS	MUSS
Third-party Invites	DARF NICHT	DARF NICHT	DARF NICHT
Typing Notifications	MUSS	MUSS	MUSS
User and Room Mentions	MUSS	MUSS	MUSS
Voice over IP	KANN	KANN	KANN
Client Config	MUSS	MUSS	MUSS
Device Management	MUSS	MUSS	MUSS
End-to-End Encryption	MUSS	MUSS	MUSS
Event Annotations and Reactions	MUSS ³ / KANN ⁴	MUSS ³ / KANN ⁴	MUSS ³ / KANN ⁴
Event Context	KANN	KANN	KANN
Event Replacements	MUSS	MUSS	MUSS
Fully Read Markers	MUSS	MUSS	MUSS
Guest Access	DARF NICHT	DARF NICHT	DARF NICHT
Moderation Policy Lists	DARF NICHT	DARF NICHT	DARF NICHT
OpenID	MUSS	MUSS	MUSS
Reference Relations	KANN	KANN	KANN
Reporting Content	KANN	KANN	KANN
Rich replies	KANN	KANN	KANN
Room Previews	KANN	KANN	KANN
Room Tagging	KANN	KANN	KANN
SSO Client Login/Authentication	MUSS	MUSS	MUSS
Secrets	MUSS	MUSS	MUSS
Send-to-Device Messaging	MUSS	MUSS	MUSS

Server Access Control Lists (ACLs)	KANN	KANN	KANN
Server Administration	MUSS ¹ / KANN ²	MUSS ¹ / KANN ²	MUSS ¹ / KANN ²
Server Notices	MUSS	MUSS	MUSS
Server Side Search	KANN	KANN	KANN
Spaces	KANN	KANN	KANN
Sticker Messages	KANN	KANN	KANN
Third Party Networks	DARF NICHT	DARF NICHT	DARF NICHT
Threading	DARF NICHT	DARF NICHT	DARF NICHT

¹ für Akteure in der Rolle "Org-Admin" (Org-Admin-Client)

² für Akteure in der Rolle "User"

³ Fähigkeit zur Verarbeitung und Anzeige

⁴ Fähigkeit zur Erzeugung

[<=]

3.1.3.2 Raumerzeugung und Öffentlichkeit von Räumen

Räume können in Matrix durch die API/createRoom erzeugt werden. Hierbei ist zu beachten, dass Matrix kein ganzheitliches Konzept für die Öffentlichkeit von Räumen hat. Stattdessen werden Zugriffsbeschränkungen in verschiedenen Dimensionen erlaubt:

- Join Rules legen fest wie ein Raum betreten werden darf.
- Die History Visibility bestimmt wer historische Events in einem Raum einsehen darf.
- Die Room Directory Visibility definiert welche Räume unter /publicRooms lokal und föderiert abrufbar sind.
- Die Verschlüsselung definiert ob und wie Events durch die Teilnehmer eines Raumes verschlüsselt werden.

Diese Einstellungen sind prinzipiell unabhängig voneinander wobei aber nicht alle möglichen Kombinationen sinnvoll sind. Im Folgenden wird beschrieben wie die Einstellungen beim Anlegen von Räumen zu behandeln sind.

Die Join Rules, History Visibility und Verschlüsselung eines Raumes werden durch die State Events `m.room.join_rules`, `m.room.history_visibility` und `m.room.encryption` festgelegt. Diese State Events können beim Aufruf von /createRoom im Parameter `initial_state` gesetzt werden. Für die Room Directory Visibility kann der `visibility` Parameter von /createRoom verwendet werden.

A_25323-01 -Standardeinstellungen beim Anlegen von Räumen

Der TI-M Client MUSS beim Anlegen eines Raumes als Default folgende Einstellungen anbieten:

- Join Rule: invite
- History Visibility: invited
- Room Directory Visibility: private

- Verschlüsselung: aktiv

[<=]

Hinweis: Diese Einstellungen dürfen im UI des Clients auch kombiniert sein und müssen nicht einzeln angeboten werden.

3.1.3.3 Instant Messaging

A_28145 -Versenden von msgtypes

TI-M Clients MÜSSEN ihren Akteuren ermöglichen Nachrichten mit den msgtypes `m.text` und `m.file` zu versenden.[<=]

Hinweis: Es gibt keine Festlegungen zu den bei `m.file` zu unterstützenden MIME-Types.

A_28146 -Empfang und Darstellung von msgtypes

TI-M Clients MÜSSEN alle unter [Client-Server API/#mroommessage-msgtypes] aufgeführten msgtypes empfangen und so darstellen können, dass die Inhalte dem Akteur zugänglich sind.[<=]

Hinweis: Die Darstellung muss nicht zwingend vollintegriert erfolgen. So könnte z. B. eine Nachricht vom Typ `m.image` wahlweise über einen in den Client integrierten Image-Viewer oder als generische Datei mit der Option zum Download dargestellt werden. Beide Optionen können auch kombiniert werden, indem die Download-Variante z. B. nur für Bilder mit nicht unterstützten MIME-Types verwendet wird.

A_26514 -Mathematical Messages

TI-M Clients DÜRFEN LaTeX-basierte mathematische Ausdrücke¹ NICHT unterstützen.

¹ [Client-Server API/#mathematical-messages][<=]

3.1.3.4 Weitere Ergänzungen/Einschränkungen zur Matrix-Spezifikation

Die folgenden Anforderungen beschreiben Einschränkungen zu einzelnen Endpunkten der Matrix API, die nicht über die Definitionen im vorherigen Kapitel festgelegt werden konnten.

A_25559 -Unterstützung von Olm und Megolm

TI-M Clients MÜSSEN eine Ende-zu-Ende-Verschlüsselung auf Basis von Olm und Megolm unterstützen und dafür der Matrix-Spezifikation gemäß [Client-Server API/#end-to-end-encryption] folgen.[<=]

A_25517 -Größe versendeter Inhalte

TI-M Clients MÜSSEN in der Lage sein, Dateien mit einer Größe von mindestens 100 MB zu versenden.[<=]

A_25518 -Beschränkung der Größe versendeter Inhalte

TI-M Clients MÜSSEN die `inm.upload.size` definierte Größenbeschränkung zu versendender Inhalte berücksichtigen.[<=]

A_25557 -Device Verification, Cross-Signing und SSSS für TI-Messenger Clients

TI-M Clients MÜSSEN die Funktionen Cross-Signing und Secure Secret Storage and Sharing ([SSSS]) zur Device Verification unterstützen und dafür der Matrix-Spezifikation gemäß [Client-Server API/#sharing-keys-between-devices] folgen.[<=]

A_26196 -Unterstützung von hkdf-hmac-sha256

TI-M Clients MÜSSEN für die Device Verification das MAC-Verfahren `hkdf-hmac-sha256` unterstützen und beim Start der Verification zusätzlich zu `hkdf-hmac-sha256.v2` anbieten¹.

¹ [Client-Server API/#mac-calculation][<=]

A_25394 -Anforderung von refresh token durch den TI-M Client

Der TI-M Client MUSS bei Aufruf der [Client-Server API] Endpoints /register und /login den Parameter refresh_token mit dem Wert true benutzen.[<=]

A_25458 -Verwendung von refresh token

Der TI-M Client MUSS einen nicht mehr gültigen access_token durch Verwendung des refresh_token erneuern.[<=]

A_25399 -Displaynamen anpassen

Das Editieren des Displayname eines Akteurs in der Rolle "User" DARF NICHT durch den Akteur selbst möglich sein.[<=]

A_25431 -Eingabebenachrichtigungen

Eingabebenachrichtigungen MÜSSEN an- und abschaltbar sein und MÜSSEN gemäß Privacy-by-default (Art. 25 Abs. 2 DSGVO) standardmäßig deaktiviert sein.[<=]

A_25436 -Präsenzanzeige

Die Präsenzanzeige MUSS an- und abschaltbar sein und MUSS gemäß Privacy-by-default (Art. 25 Abs. 2 DSGVO) standardmäßig deaktiviert sein.[<=]

A_25433-01 -Konfiguration von Public Read Receipts

TI-M Clients MÜSSEN dem Nutzer erlauben, das Senden öffentlicher Lesebestätigungen (m.read) an- und abzuschalten.[<=]

A_26220 -Defaulteinstellung für Public Read Receipts

TI-M Clients MÜSSEN das Senden öffentlicher Lesebestätigungen standardmäßig deaktivieren ("Privacy by Default" gemäß Art. 25 Abs. 2 DSGVO).[<=]

A_26221 -Private Read Receipts

TI-M Clients MÜSSEN private Lesebestätigungen (m.read.private) versenden, sofern das Senden öffentlicher Lesebestätigungen deaktiviert ist.[<=]

A_25437 -Erwähnungen

TI-M Clients MÜSSEN es ermöglichen, dass über das Eingabefeld andere Raumteilnehmer gemäß [Client-Server API/#user-and-room-mentions] im jeweiligen Chatraum erwähnt werden können. Dazu MUSS der TI-M Client eine entsprechende Nutzerliste anzeigen, sobald der Nutzer ein neues Wort mit "@" startet.[<=]

A_26249 -Historie von Event Replacements

TI-M Clients MÜSSEN eine leicht erreichbare Funktion zur Anzeige der Änderungshistorie von Nachrichten, die durch m.replace-Relationen ersetzt wurden, anbieten.[<=]

A_26261 -Eindeutige Darstellung von Event Replacements

TI-M Clients MÜSSEN Nachrichten, die durch m.replace-Relationen ersetzt wurden, optisch eindeutig kennzeichnen, damit dem Nutzer die Ersetzung offensichtlich wird.[<=]

A_25423 -Retry and Order

Das unter [Client-Server API/#recommendations-when-sending-messages] beschriebene Verhalten für das Retry und die Order auf Clientseite ist mit MUSS und nicht mit SHOULD zu implementieren.[<=]

A_25514 -Key-Sharing zwischen Geräten eines Akteurs

TI-M Clients MÜSSEN sicherstellen, dass das Key-Sharing zwischen Geräten desselben Akteurs nur verifizierte Geräte umfasst. Geräte, die im Namen eines bestimmten Akteurs angemeldet, aber nicht verifiziert sind, sind vom Key-Sharing ausgeschlossen.[<=]

A_25430 -Barrierefreiheit

Hersteller eines TI-M Clients SOLLEN die in [ISO 9241] aufgeführten Qualitätsrichtlinien zur Sicherstellung der Ergonomie interaktiver Systeme und Anforderungen aus der Verordnung zur Schaffung barrierefreier Informationstechnik nach dem Behindertengleichstellungsgesetz (Barrierefreie-Informationstechnik-Verordnung - [BITV 2.0]) beachten.[<=]

A_26193 -Verbot der Push Rule Actions dont_notify und coalesce

Beim Anlegen oder Editieren von Push Rules DÜRFEN TI-M Clients die Actions dont_notify und coalesce NICHT verwenden. [≤]

A_26262 -Authenticated Media am Client

TI-M Clients MÜSSEN anstelle der Endpunkte

- GET /_matrix/media/v3/config
- GET /_matrix/media/v3/download/{serverName}/{mediaId}
- GET /_matrix/media/v3/download/{serverName}/{mediaId}/{fileName}
- GET /_matrix/media/v3/thumbnail/{serverName}/{mediaId}

die äquivalenten authentifizierten Endpunkte

- GET /_matrix/client/v1/media/config
- GET /_matrix/client/v1/media/download/{serverName}/{mediaId}
- GET /_matrix/client/v1/media/download/{serverName}/{mediaId}/{fileName}
- GET /_matrix/client/v1/media/thumbnail/{serverName}/{mediaId}

verwenden, sofern der Homeserver des angemeldeten Nutzers sie unterstützt. [≤]

Hinweis: Die Endpunkte mit /_matrix/media/v3/-Präfix wurden in Version 1.11 der [Matrix Specification] als deprecated markiert.

A_26268 -Verwendung des Request Headers für Matrix-ACCESS-TOKEN

TI-M Clients MÜSSEN ihr access_token (Token-Art: Matrix-ACCESS-TOKEN) ausschließlich im Authorization Request Header senden. [≤]

Hinweis: Das Senden von Tokens dieser Art im Request als Query Parameter wurde in Version 1.11 der [Matrix Specification] als deprecated markiert.

A_26574 -Entschlüsseln von Nachrichten nach Wiederanmeldung

TI-M Clients und Fachdienste MÜSSEN es Akteuren ermöglichen Nachrichten, die gesendet wurden nachdem der Akteur vollständig abgemeldet wurde, nach erneuter Anmeldung zu entschlüsseln. [≤]

A_26575 -Ablage von Schlüsseln zum Entschlüsseln von Nachrichten nach Wiederanmeldung

TI-M Clients MÜSSEN Schlüsselmateriale, das zum Entschlüsseln von Nachrichten nach Wiederanmeldung benötigt wird, wie in [SSSS] beschrieben speichern. [≤]

Hinweis: Ein mögliches Schema zur Erfüllung der Anforderungen A_26574 und A_26575 ist [MSC3814] (Dehydrated devices with SSSS).

3.1.4 Push-Notifications

Push-Notifications sind elementarer Bestandteil von Messenger-Anwendungen. Um TI-M Clients mit Benachrichtigungen über externe Push-Anbieter, wie z. B.

- Apple Push Notification service (APNs) für iOS oder
- Firebase Cloud Messaging (FCM) für Android,

zu versorgen, wird das Konzept aus der Matrix Spezifikation aufgegriffen, welches auf der einen Seite eine enge Kopplung zwischen einem Client und dem zugehörigen Push-Gateway vorsieht und auf der anderen Seite über den Homeserver den Clients die Flexibilität bietet, selbst das zu verwendende Push-Gateway zu definieren. Die dafür notwendigen Komponenten und Schnittstellen werden im Kapitel 5.3- Push-Benachrichtigungen ausführlich behandelt.

3.1.5 Client Identifikation

Zur Sicherstellung der Identifikation von zugelassenen TI-M Clients im Rahmen der Betriebsdatenerfassung ist eine User-Agent-Kennung bei jedem Verbindungsaufbau zu verwenden.

A_25483 -TI-M Client User-Agent

Der TI-M Client für Akteure und der Org-Admin-Client MÜSSEN folgende User-Agent-Kennung bei jedem Verbindungsaufbau zum TI-M FD übermitteln:

X-TIM-User-Agent: \$ua-client_id, \$ua-OSv[<=]

Hinweis:

- 1) Zur Beschreibung der Datenfelder, siehe [gemSpec_Perf].
- 2) Im TI-M Client als Web-Anwendung muss der Header nicht explizit gesetzt werden, solange die geforderten Informationen auch anderweitig am TI-M FD korrekt erfasst werden können.

3.1.6 Archivierung von Gesprächsinhalten

Um den Dokumentationspflichten von Akteuren unterschiedlicher Rollen nachzukommen, ist es notwendig, dass Chatverläufe mit Fallbezug auch über Löschung der Gesprächsdaten hinaus aufbewahrt werden können. TI-M Clients führen dabei selbst keine Archivierung durch und speichern selbst auch keine Archivdaten.

A_25424 -Archivierung in Archivsysteme

Der TI-M Client MUSS sicherstellen, dass Chatverläufe aus dem TI-M Client extrahiert werden können, damit diese beispielsweise in Archivsysteme überführt werden können. Die gematik macht keine Vorgaben, wie die Archivierung zu gestalten ist, da sowohl die Art der Archivierung als auch die anzubindenden Systeme stark variieren.[<=]

Hinweis: Mit der Ausleitung in ein Archivsystem verlassen potenziell schützenswerte Daten den Wirkungsbereich des TI-Messengers. Die Eignung des Archivierungssystems hinsichtlich Datenschutz und Informationssicherheit muss durch die für das Archivierungssystem Verantwortlichen gewährleistet werden.

3.1.7 Tracking und Reporting

Unter bestimmten Einschränkung kann ein Tracking und Reporting der Nutzung des TI-M Client erfolgen.

A_25585 -Verbot von Werbe-Tracking

Der TI-M Client DARF NICHT Werbe-Tracking verwenden.[<=]

A_25587 -Keine Auswertung durch Dritte

Der datenschutzrechtlich Verantwortliche für die TI-M Clients MUSS die Verarbeitung und Auswertung etwaiger gesammelter Tracking- und/oder Reporting-Daten der TI-M Clients selbst durchführen und DARF die Verarbeitung und Auswertung NICHT von einem Drittanbieter durchführen lassen.[<=]

A_25589 -Einschränkung der Art übermittelter Informationen

Der TI-M Client MUSS, falls er Tracking- und/oder Reporting-Funktionen ohne Einwilligung des Akteurs nutzt, sicherstellen, dass die übermittelten Informationen

- sich nur auf Clientnutzung (von der ersten Interaktion des Nutzers mit dem Client bis zum Schließen des Clients bzw. bis zum Inaktivitätstimeout) beziehen und nicht mit anderen Clientnutzungen des Akteurs verknüpft werden,

- über die unweigerlich anfallenden Verbindungsdaten hinaus weder personenbezogene noch pseudonymisierte personenbezogene Daten enthalten,
- keine nutzerbezogenen IDs oder gerätespezifischen IDs der Nutzergeräte enthalten,
- keinen Rückschluss auf Versicherte, deren Vertreter, Leistungserbringer oder Kostenträger ermöglichen, insbesondere Rückschlüsse anhand des Nutzerverhaltens über die Zeit oder über Clientnutzungen hinweg,
- nicht durch die Verknüpfung mit personenbezogenen Daten aus anderen Quellen de-anonymisiert werden können

[<=]

A_25590 -Information über Tracking und Reporting

Der TI-M Client MUSS, falls er Tracking- und/oder Reporting-Funktionen ohne Einwilligung des Akteurs nutzt, den Akteur über das Tracking und/oder Reporting im TI-M Client in verständlicher und leicht zugänglicher Form sowie in einer klaren und einfachen Sprache informieren, bevor die Informationen erhoben werden.[<=]

A_25591 -Zufällige Nutzungs-Identifizier

Der TI-M Client MUSS, falls er Tracking- und/oder Reporting-Funktionen ohne Einwilligung des Akteurs nutzt, für jede Clientnutzung neue Nutzungs-Identifizier zufällig generieren.

[<=]

A_25592 -Neugenerierung zufälliger Nutzungs-Identifizier

Der Akteur MUSS jederzeit in der Lage sein, die Neugenerierung von Nutzungs-Identifizieren, die vom TI-M Client im Rahmen von Tracking- und/oder Reporting-Funktionen genutzt werden, zu erzwingen.[<=]

A_25593 -Opt-In für Verknüpfung von Informationen

Der TI-M Client MUSS, falls er Tracking- und/oder Reporting-Funktionen mit Verknüpfung der Informationen mehrerer Clientnutzungen implementiert, technisch sicherstellen, dass diese Tracking- und/oder Reporting-Funktionen bei der Installation des TI-M Clients standardmäßig deaktiviert sind und nur nach expliziter Einwilligung durch den Akteur aktiviert werden (Opt-in). Die Ablehnung der Nutzung solcher Funktionen darf die Standardfunktionen des TI-M Clients nicht einschränken. Eine Umgehung des Opt-In unter Verweis auf AGBs oder Nutzungsbedingungen ist nicht zulässig.[<=]

A_25594 -Zweck von Tracking und Reporting

Falls der TI-M Client Tracking- und/oder Reporting-Funktionen implementiert, die erst nach expliziter Einwilligung aktiviert werden (Opt-In), MUSS der TI-M Client dem Akteur vor der Einwilligung in die Aktivierung dieser Funktionen in verständlicher und leicht zugänglicher Form sowie in einer klaren und einfachen Sprache folgende Einwilligungsinformationen anzeigen:

- welche Daten durch die Tracking-Funktionen erhoben werden,
- zu welchen Zwecken die Daten erhoben werden,
- welche Informationen durch die Auswertung der erhobenen Daten gewonnen werden und ob Rückschlüsse auf den Gesundheitszustand des Akteurs möglich wären,
- wer die Empfänger der Daten sind,
- wie lange die Daten gespeichert werden.

Unter verständlicher und leicht zugänglicher Form wird explizit eine kurze Erklärung in einfacher und nicht juristischer Sprache verstanden, die direkt im TI-M Client angezeigt wird.

[<=]

A_25595-01 -Deaktivierbarkeit zuvor aktivierten Trackings und Reportings

Falls der TI-M Client Tracking- und/oder Reporting-Funktionen implementiert, MÜSSEN diese jederzeit durch den Akteur deaktivierbar sein.

Dies betrifft nur die Tracking- und/oder Reporting-Funktionen, die nach expliziter Einwilligung erteilt wurden und nicht die Tracking- und/oder Reporting-Funktionen, die ohne Einwilligung des Akteurs genutzt werden.

[<=]

A_26001 -Information über die Deaktivierbarkeit des Trackings

Der TI-M Client MUSS den Akteur in klarer und einfacher Sprache über die Möglichkeit der Deaktivierung von Tracking und Reporting informieren.[<=]

A_25596 -Kein wiederholtes Erfragen der Einwilligung

Der TI-M Client DARF NICHT wiederholt beim Akteur anfragen um diesen durch Belästigung zu einer Einwilligung in die Nutzung von Tracking- und/oder Reporting-Funktionen zu nötigen. Nach einmaliger Ablehnung erfolgt die erneute Anzeige des zugehörigen Dialogs nur auf Veranlassung durch den Akteur.[<=]

3.1.8 Schlüssel-Backup

A_26077 -Server-seitiges Schlüssel-Backup

Der TI-M Client MUSS die für die Nutzung des serverseitigen Schlüssel-Backups [Client-Server API/#server-side-key-backups] benötigte Funktionalität implementieren und dem Akteur zur Verwendung anbieten.[<=]

A_25613 -Hinweis bei passwort-basiertem Schlüssel-Backup

Bietet der TI-M Client für den Schutz von kryptographischem Material (im Rahmen des Schlüssel-Backups) die Verwendung von Passwörtern an, um den Schlüssel für das Schlüssel-Backup zu verschlüsseln, so MUSS er den Nutzer zum Zeitpunkt der Passwortvergabe explizit darauf hinweisen, dass sich das zu vergebene Passwort zwingend von dem Passwort für das Nutzerkonto am Matrix-Homeserver unterscheiden muss, weil sonst die Ende-zu-Ende-Verschlüsselung wenigstens gegenüber dem Homeserver und jenen Akteuren, die diesen kontrollieren, nicht mehr wirksam ist.[<=]

A_25614-01 -Vorschlag von Passwörtern für das Schlüssel-Backup

Der TI-M Client MUSS dem Nutzer im Rahmen der Passwortvergabe ein Passwort vorschlagen, dessen Entropie mindestens gleichwertig ist zu einer zufälligen Kombination von 14 Zeichen, die sich aus Zahlen, Sonderzeichen, sowie Groß- und Kleinbuchstaben zusammensetzt.[<=]

A_25615 -Quelle des Zufalls für Vorschläge

Die Quelle für Zufall, die der TI-M Client zum Vorschlagen von Passwörtern verwendet, MUSS wenigstens die Güte haben, wie jene Quellen, die er im Rahmen der Aushandlung von Schlüsselmaterial für die Kommunikation benutzt.[<=]

A_25616 -Parameter für die passwort-basierte Schlüsselableitung

Bei der passwort-basierten Schlüsselableitung (PBKDF2) im Rahmen des Schlüssel-Backups MUSS der TI-M Client gemäß [OWASP PBKDF2] ≥ 210.000 Iterationen wählen; die Hash-Funktion ist mit SHA-512 durch die Matrix-Spezifikation vorgegeben.[<=]

A_25618 -Nutzung von Passphrasen

Schlägt der TI-M Client nicht Passwörter, sondern Passphrasen vor, so MUSS die Länge der Phrasen so weit erhöht werden, dass eine vergleichbare Entropie wie bei der Verwendung von Passwörtern nach A_25614 erreicht wird.[<=]

Hinweis: Sofern technisch möglich, kann der TI-M Client dem Nutzer Funktionen zur Verfügung stellen, die eine sichere Verwahrung von Passwörtern und Schlüsseln erleichtern, beispielsweise indem ein Export in einen installierten Passwort-Manager angeboten wird.

3.1.9 VZD-FHIR-Directory

Ein TI-M Client nutzt die FHIR-Schnittstellen der Teilkomponente FHIR-Proxy des VZD-FHIR-Directorys gemäß dem FHIR-Standard [FHIR] mit einer RESTful API.

Für den Zugriff auf das VZD-FHIR-Directory ist ein durch den Auth-Service ausgestelltes access-token notwendig. Hierfür sind die am Auth-Service bereitgestellten REST-Schnittstellen durch den TI-M Client zu nutzen.

TI-M Clients MÜSSEN sich gegenüber dem Auth-Service des VZD-FHIR-Directory mit Hilfe eines ID_TOKENS oder des Matrix-OpenID-Token authentifizieren.

Dem Matrix-OpenID-Token des Matrix-Homeservers wird vertraut, wenn der ausstellende Matrix-Homeserver als Matrix-Domain (einer verifizierten Organisation) in der Föderationsliste eingetragen wurde. Der Auth-Service des VZD-FHIR-Directory stellt nach erfolgreicher Prüfung des jeweiligen Matrix-OpenID-Token ein search-accesstoken aus.

3.1.9.1 Lesezugriff

Für den Lesezugriff auf das VZD-FHIR-Directory ist ein gültiges search-accesstoken notwendig. Durch den Aufruf einer Schnittstelle am FHIR-Proxy des VZD-FHIR-Directory kann ein TI-M Client unter Vorlage des search-accesstoken Suchanfragen an das FHIR-Directory stellen. Die Suchergebnisse sind abhängig von den eingetragenen FHIR-Ressourcen und deren Sichtbarkeit.

Liegt kein gültiges search-accesstoken vor, kann der TI-M Client dies beim Auth-Service des VZD-FHIR-Directory durch den Aufruf von GET /tim-authenticate unter Vorlage eines Matrix-OpenID-Token anfragen.

A_25479 -Search Token

Der TI-M Client MUSS dem Akteur einen search-accesstoken für die Suche im VZD-FHIR-Directory bereitstellen. [≤]

A_25428 -VZD-FHIR-Directory Inhalte

Der TI-M Client MUSS eine Funktion bereitstellen, damit Akteure das VZD-FHIR-Directory nach Ressourcen durchsuchen und die Ergebnisse inklusive Detailinformationen anzeigen können. [≤]

3.1.10 Registrierungs-Dienst

Der Registrierung-Dienst stellt dem Org-Admin-Client Schnittstellen zur Verfügung damit dieser neue Messenger-Services anlegen und diese Verwalten kann.

3.1.11 Testtreiber

Die gematik konzentriert sich bei der Zulassung auf das Zusammenspiel der Produkte durch E2E- und IOP Tests und testet übergreifend, die in dieser Spezifikation definierten Anwendungsfälle. Um einen automatisierten Test für den TI-Messenger zu ermöglichen, muss die Test-App des TI-M Clients zusätzlich ein Testtreiber-Modul bereitstellen, welches über eine definierte API die Remotesteuerung des Clients erlaubt. Details zum Testkonzept können unter [gematik Testkonzept] nachgelesen werden.

A_25363 -Testtreiber-Modul

Für jeden TI-M Client MUSS für die Zulassung ein Testtreiber Modul bereitgestellt werden, welches die von der gematik vorgegebene Schnittstelle [api-Testtreiber] anbietet. [≤]

A_25360 -kein Testtreiber in der produktiven Anwendung

Der Einsatz des Testtreiber-Moduls ist auf das Zulassungsverfahren in Test-Apps beschränkt und DARF NICHT in produktiven Werkbetriebs-Apps genutzt werden. [≤]

A_25361-01 -Keine Modifikation der Inhalte

Das Testtreiber-Modul DARF die ausgegebenen Inhalte des TI-M Clients NICHT verfälschen und keine Fachlogik des Clients umsetzen.【<=】

Hinweis: Das Testtreiber-Modul kann die Ausgaben des TI-M Clients gemäß der technischen Schnittstelle aufarbeiten.

3.2 TI-M FD

Der TI-M FD besteht aus Teilkomponenten, welche bei der Produktzulassung getestet werden und die ein TI-Messenger-Anbieter bereitstellt. Als zentrale Verwaltungskomponente existiert der Registrierungs-Dienst, über den die Bestellung und Verwaltung von Messenger-Services realisiert wird. Ein Messenger-Service besteht aus einem Matrix-Homeserver und einem Messenger-Proxy, der dafür sorgt, dass eine Föderation der Matrix-Homeserver nur zwischen verifizierten Domains stattfindet. Messenger-Services werden für einzelne Organisationen (z. B. Leistungserbringerinstitutionen, Verbände, Kostenträger, etc.) bereitgestellt und erlauben die Nutzung durch alle berechtigten Akteure einer Organisation. Die Kommunikation zwischen einem TI-Messenger Client und einem TI-M FD erfolgt immer über den Messenger-Proxy der Messenger-Services. Am Messenger-Proxy eines Messenger-Service findet zunächst die TLS-Terminierung der Verbindungen von den TI-M Clients statt. Der Messenger-Proxy kontrolliert die Zugehörigkeit zur TI-Föderation durch den Abgleich mit einer durch seinen Registrierungs-Dienst bereitgestellten Föderationsliste. Der Messenger-Service benachrichtigt das vom TI-M Client festgelegte Push-Gateway bei Events, die zu einer Notification auf Clientseite führen. In der folgenden Abbildung sind alle beteiligten Komponenten der TI-Messenger-Architektur in vereinfachter Form dargestellt und die TI-M Komponenten die im folgenden Kapitel erläutert werden, blau eingefärbt.

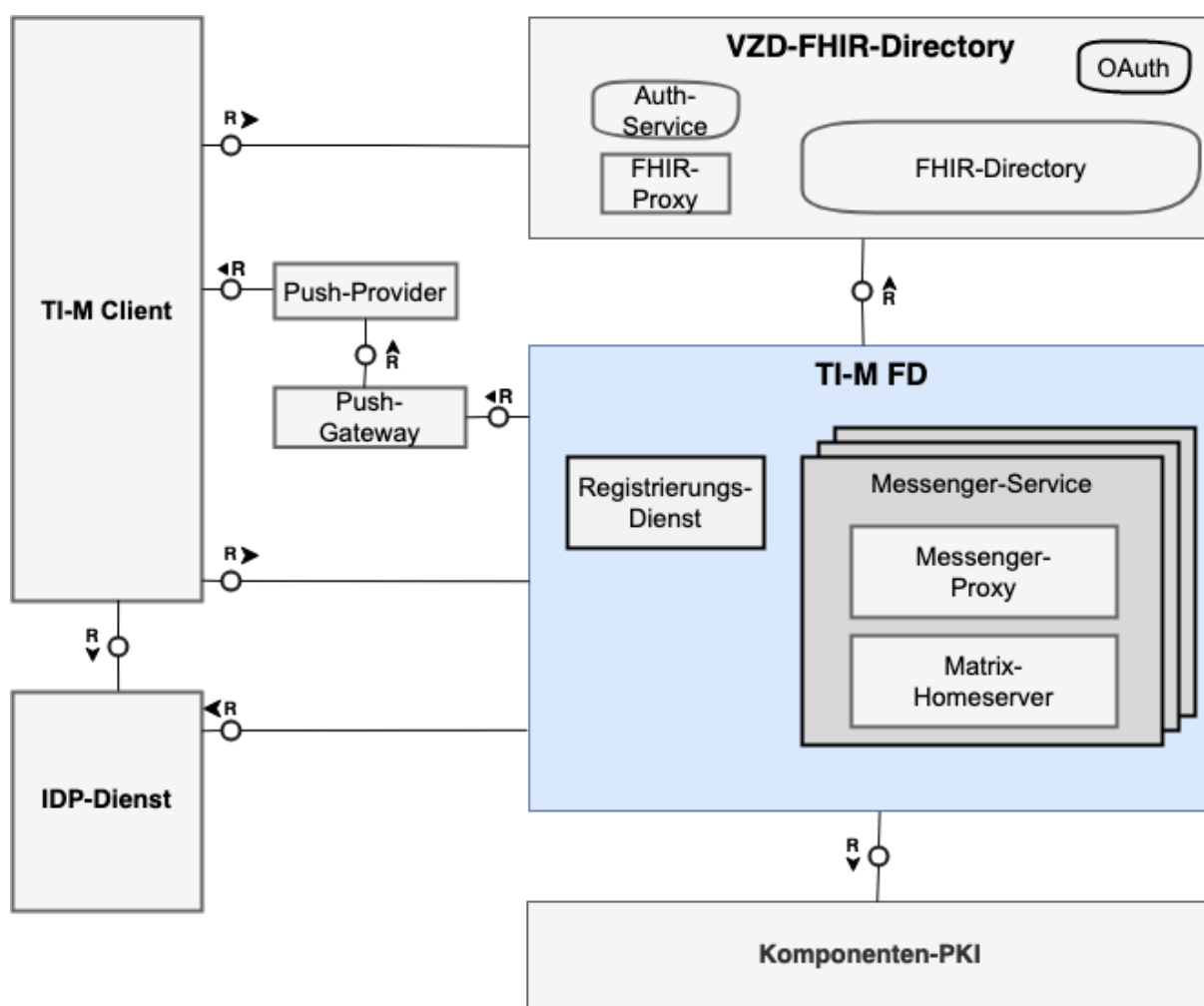


Abbildung 3: Systemüberblick TI-M FD

Hinweis: Der Messenger-Proxy muss nicht zwingend als physische Komponente umgesetzt werden, sondern kann z.B. auch als logische Komponente innerhalb des Matrix-Homeservers implementiert werden.

A_26228-01 -Längenbegrenzung von Annotationen in Reactions

Der TI-M FD MUSS sicherstellen, dass der Wert des Attributes key im Event-Content in Events des Typs m.reaction nur ein Emoji darstellt, sonst MUSS der Request mit dem Response Code 400 und dem Error Code M_BAD_JSON abgewiesen werden.[<=]

3.2.1 Registrierungs-Dienst

Der Registrierungs-Dienst bietet drei Schnittstellen an. In der folgenden Abbildung sind die von ihm bereitgestellten (grün) und genutzten (rot) Schnittstellen dargestellt:

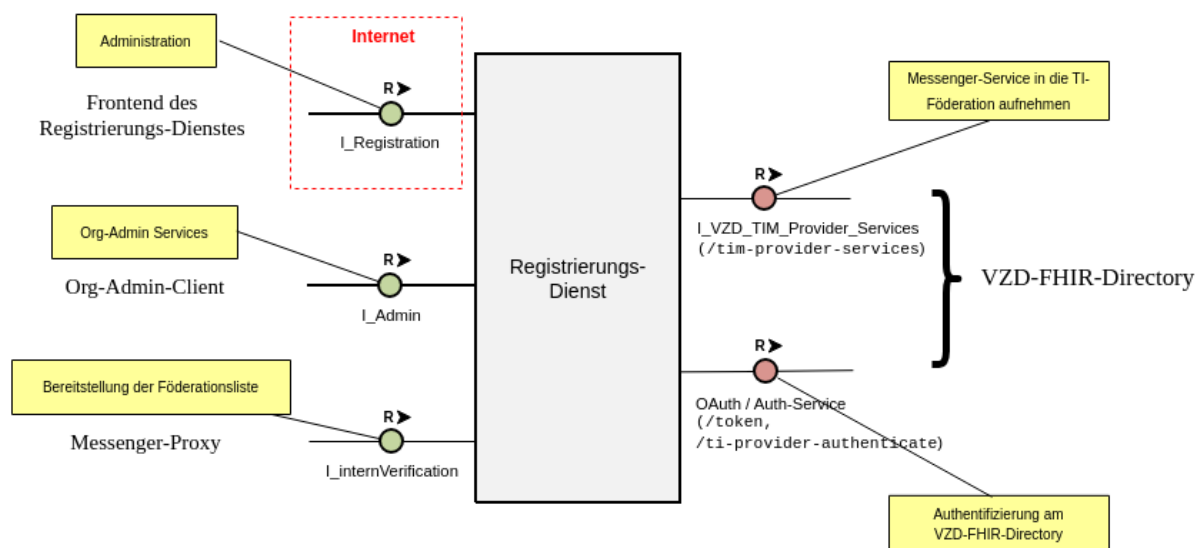


Abbildung 4: Übersicht der Schnittstellen am Registrierungs-Dienst

Hinweis: Bei der in der Abbildung dargestellte Schnittstelle `I_internVerification` handelt es sich um eine abstrakte interne Schnittstelle am Registrierungs-Dienst, mit der den Messenger-Proxies mehrere Funktionalitäten bereitgestellt werden. Die Umsetzung der bereitzustellenden Funktionalitäten (Bereitstellung der Föderationsliste und Berechtigungsprüfung - Stufe 3) am Registrierungs-Dienst kann auch über separate Schnittstellen erfolgen. Bei den beiden Schnittstellen `I_Registration` und `I_Admin` handelt es sich um die Schnittstellen, deren Ausgestaltung nicht normativ von der gematik spezifiziert wird.

Die einzelnen Schnittstellen werden in den folgenden Kapiteln detailliert beschrieben.

3.2.1.1 `I_Registration`

Über die Schnittstelle `I_Registration` werden 2 Funktionen bereitgestellt. Zum einen kann die eigene Organisation (z. B. per SM(C)-B) registriert werden, um einen Admin-Account zu erhalten. Zum anderen können anschließend über die Schnittstelle neue Messenger-Services bereitgestellt werden. Die Ausgestaltung des Frontends sowie der Schnittstelle am Registrierungs-Dienst (`I_Registration`) ist dem jeweiligen TI-Messenger-Anbieter überlassen.

3.2.1.1.1 Authentisierung einer Organisation

Bei der Authentisierung einer Organisation können die in den folgenden Unterkapiteln beschriebenen Verfahren verwendet werden.

A_26436 -Bereitstellung im Internet

Die Schnittstelle `I_Registration` bzw. das auf der Schnittstelle aufbauende Frontend SOLL für Organisationen, die einen TI-Messenger erwerben wollen, im Internet angeboten werden. [≤]

A_25354 -Registrierung einer Organisation

Für die initiale Registrierung einer Organisation, MUSS der TI-Messenger-Anbieter die Identität der Organisation mittels SM(C)-B feststellen. [≤]

A_25357 -Verfahren zum Nachweis der Identität einer Organisation

TI-Messenger-Anbieter MÜSSEN für die Feststellung der Identität einer Organisation im Rahmen deren Registrierung wenigstens eines der beiden folgenden Verfahren unterstützen:

- OpenID Connect-Verfahren mit SM(C)-B
- KIM-Verfahren

[<=]

3.2.1.1.1.1 OpenID Connect-Verfahren

Die Authentisierung kann z. B. unter Verwendung des gematik Authenticators [gematik Authenticator] mittels SMC-B durchgeführt werden. Dazu ist der eigene Fachdienst beim IDP-Dienst der gematik zu registrieren, um im Anschluss über einen Authorization Code Flow einen vom IDP-Dienst ausgestellten ID_TOKEN zu erhalten. Details zum Flow können der Spezifikation zum IDP-Dienst [gemSpec_IDP_Dienst] entnommen werden.

A_25359 -Authorization Code Flow mit PKCE

Der TI-Messenger-Anbieter MUSS sicherstellen, dass bei Verwendung des OpenID Connect-Verfahrens der Authorization Code Flow mit PKCE zum Einsatz kommt.[<=]

A_25362 -Durchführung der PKCE-Challenge

Bei Verwendung des OpenID Connect-Verfahrens, MUSS der Registrierungs-Dienst den PKCE-Code erzeugen und später den Verifier dieser Challenge zusammen mit dem Authorization Code beim zentralen IDP-Dienst gegen ein ID_TOKEN einlösen.[<=]

A_25364 -Validierung von ID_TOKEN

Der Registrierungs-Dienst MUSS das durch den zentralen IDP-Dienst ausgestellte ID_TOKEN validieren und die darin enthaltene Profession0ID 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.[<=]

A_25365 -Registrierung am IDP

Registrierungs-Dienste MÜSSEN am zentralen IDP-Dienst gemäß [gemSpec_IDP_FD] registriert sein und den von diesem IDP-Dienst ausgestellten ID_TOKEN vertrauen.[<=]

A_25366 -Claims in ID_TOKEN für Organisationen

Der Anbieter des TI-Messengers MUSS über einen organisatorischen Prozess beim zentralen IDP-Dienst folgende Claims für ID_TOKEN, die auf Basis der Authentisierung mittels SM(C)-B ausgestellt werden, vereinbaren:

- Profession0ID
- idNummer
- organizationName
- acr
- aud

Die Profession0ID gibt an, um welche Art von Institution es sich handelt. Die idNummer beinhaltet die Telematik-ID für Institutionen des Gesundheitswesens.[<=]

3.2.1.1.1.2 KIM-Verfahren

Alternativ zum im vorherigen Kapitel beschriebenen Verfahren kann die KIM-Mailadresse zur Authentisierung genutzt werden. Bei Verwendung des KIM-Verfahrens soll das Frontend des Registrierungs-Dienst dem Akteur eine Eingabemaske für die zu verwendende KIM-Adresse anbieten. Nach Eingabe der KIM-Adresse sind die folgenden Anforderungen zur Weiterführung des Registrierungsprozesses zu berücksichtigen:

A_25369 -Prüfung der KIM-Adresse

Bietet der TI-Messenger-Anbieter das KIM-Verfahren an und entscheidet sich die Organisation, deren Identität festgestellt werden soll, dieses Verfahren zu nutzen, MUSS der TI-Messenger-Anbieter die Profession0ID sowie die TelematikID für die von der Organisation mitgeteilte KIM-Adresse durch Abfrage am LDAP-VZD ermitteln und die Profession0ID 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.[<=]

A_25373 -Versand der KIM-Nachricht nach erfolgreicher Prüfung

War die Prüfung der KIM-Adresse hinsichtlich zugehöriger ProfessionOID und TelematikID, welche im Rahmen des KIM-Verfahrens durchgeführt wird, erfolgreich, MUSS der TI-Messenger-Anbieter eine KIM-Nachricht an die angegebene KIM-Adresse senden, welche eine URL enthält, die zurück in den Registrierungsprozess leitet.【<=】

A_25374 -Information zum Zweck der KIM-Nachricht

Versendet der TI-Messenger-Anbieter im Rahmen des KIM-Verfahrens eine KIM-Nachricht zur Fortführung des Registrierungsprozesses, MUSS er den Registrierenden über den Versand der KIM-Nachricht informieren und ihn dazu auffordern den Anweisungen innerhalb der KIM-Nachricht zu folgen.【<=】

A_25377 -Verifikation des Registrierenden

Um sicherzustellen, dass derjenige, der die KIM-Nachricht empfängt und die enthaltene URL aufruft auch der Registrierende ist, MUSS der Registrierungs-Dienst in dem Prozessschritt, der zum Versand der KIM-Nachricht führt, einen zufälligen sechsstelligen Code anzeigen, welcher innerhalb einer Eingabemaske nach Aufruf der URL vom Registrierenden einzugeben ist.【<=】

A_25375 -Form der KIM-Nachricht

Die vom TI-Messenger-Anbieter versendete KIM-Nachricht zur Fortführung des Registrierungsprozesses MUSS kenntlich machen, dass es sich hierbei um eine Authentifizierungsmail handelt und das E-Mail-Header ElementX-KIM-Dienstkennung: Auth;Verification;V1.0 enthalten.【<=】

A_25376 -Form der URL innerhalb der KIM-Nachricht

Um das Erraten der URL zu verhindern, MUSS der TI-Messenger-Anbieter sicherstellen, dass die URL innerhalb der KIM-Nachricht, die den Registrierenden zurück in den Registrierungsprozess führt, aus dem FQDN des Registrierungs-Dienstes und einer eindeutigen ID (UUID) gemäß [RFC4122] besteht.【<=】

3.2.1.1.2 Anlegen des Administrations-Accounts

Nach erfolgreicher Authentifizierung einer Organisation am Registrierungs-Dienst wird ein Admin-Account für die Organisation auf dem Registrierungs-Dienst angelegt. Für die Anmeldung des Org-Admin gelten die in 2.5.1- Authentifizierungs-Dienst für Akteure definierten Anforderungen.

Der Admin-Account ermöglicht es einem Akteur in der Rolle "Org-Admin" einen oder mehrere Messenger-Services für seine Organisation bereitzustellen. Details und Akzeptanzkriterien sind im Anwendungsfall 5.1.2- Bereitstellung eines Messenger-Service für eine Organisation beschrieben.

A_25309 -Authentisierung mittels SM(C)-B

Für Akteure in der Rolle "Org-Admin" MUSS der Registrierungs-Dienst sicherstellen, dass mindestens eine Authentisierung mittels SM(C)-B unterstützt wird.【<=】

A_25370 -Anlegen eines Org-Admin-Kontos

Könnte die Identität einer sich registrierenden Organisation bestätigt werden, MUSS der Registrierungs-Dienst des TI-Messenger-Anbieters ein Org-Admin-Konto für diese Organisation anlegen und in diesem Konto die ProfessionOID sowie die TelematikID der Organisation für den Org-Admin unveränderlich speichern.【<=】

A_25356 -Registrierung von TI-M Diensten

Der TI-Messenger-Anbieter MUSS sicherstellen, dass Registrierungen von TI-M Diensten nur durch einen authentifizierten Org-Admin durchgeführt werden können und auch nur für die jeweilige Organisation, der er - der Org-Admin - gemäß initialer Registrierung der Organisation angehört.【<=】

A_25628-01 -Bereitstellung von Messenger-Services

Der Org-Admin SOLL über das Frontend des Registrierungs-Dienstes neue Messenger-Services anlegen und diesen Domains zuweisen können.【<=】

3.2.1.2 I_Admin

Über die Schnittstelle I_Admin stellt der Registrierungs-Dienst dem Akteur in der Rolle "Org-Admin" Funktionen zur Verwaltung der eigenen Messenger-Services zur Verfügung.

A_25708 -I_Admin Zugriff

Der Registrierung-Dienst MUSS sicherstellen, dass ein Akteur in der Rolle "Org-Admin" über die Schnittstelle I_Admin nur Zugriff auf die Messenger-Services erhält, die er sich über den Anwendungsfall [ML-161405 - Bereitstellung eines Messenger-Service für eine Organisation](#).【<=】

3.2.1.3 I_internVerification

Über die Schnittstelle I_internVerification stellt der Registrierungs-Dienst den angeschlossenen Messenger-Proxies Funktionen bereit um Verwaltungsaufgaben an der Schnittstelle I_VZD_TIM_Provider_Services des VZD-FHIR-Directory durchzuführen. Die Ausgestaltung der Schnittstelle am Registrierungs-Dienst (I_internVerification) ist dem jeweiligen TI-Messenger-Anbieter überlassen.

3.2.1.3.1 Bereitstellung und Aktualisierung der Föderationsliste

Inhalt der Föderationsliste sind alle an der Föderation beteiligten Matrix-Domainnamen. Die Funktionsmerkmale zur Bereitstellung und Aktualisierung der Föderationsliste sind im Anwendungsfall 5.1.7- [Aktualisierung der Föderationsliste](#) vollständig erläutert. Erhält der Messenger-Proxy vom Registrierungs-Dienst eine aktuelle Föderationsliste, so muss eine Signaturprüfung lokal anhand des mitgelieferten Signaturzertifikates durchgeführt werden. Beim Signaturzertifikat handelt es sich um das erste Element aus der - gemeinsam mit der Föderationsliste übertragenen - x5c-Zertifikatsliste. Die x5c-Zertifikatsliste kann selbst auch nur einelementig sein und somit nur das Signaturzertifikat enthalten, ohne darauffolgende weitere Zertifikate der Zertifikatskette. Der in Kapitel 5.1.7- [Aktualisierung der Föderationsliste](#) beschriebene Ablauf bleibt davon unbetroffen. Zertifikate der Zertifikatskette, die nicht über die x5c-Zertifikatsliste bereitgestellt werden, werden anhand der Trust-Service Status List (TSL) bzw. ihrer Download-URLs zugänglich gemacht.

A_25607 -I_internVerification

Der Registrierungs-Dienst MUSS den Messenger-Proxies eine Schnittstelle für die Bereitstellung der Föderationsliste zur Verfügung stellen.【<=】

3.2.1.4 OAuth / Auth-Service

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-Credentials kann der TI-Messenger-Anbieter für seinen Registrierungs-Dienst beim VZD-FHIR-Directory-Anbieter beantragen. Die Beantragung erfolgt über einen Service-Request im TI-ITSM-System. Nach erfolgreicher Authentifizierung erhält der Registrierungs-Dienst ein provider-accesstoken, welches beim Aufruf des /tim-provider-services Endpunkts enthalten sein muss. Der Authentifizierungsprozess besteht aus den aufeinanderfolgenden Aufrufen:

- POST /auth/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-Access-Token, welches der erste Aufruf als Rückgabewert geliefert hat.

A_25625 -Registrierungs-Dienst VZD Provider Login

Der Registrierungs-Dienst MUSS die 2-stufige Anmeldung am VZD-FHIR-Directory für die `tim-provider-services` Schnittstelle unterstützen. [≤]

3.2.1.5 I_VZD_TIM_Provider_Services

Nach erfolgreicher Authentifizierung (3.2.1.4- OAuth / Auth-Service) mit vereinbarten Client-Credentials wird dem Registrierungs-Dienst ein `provider-access-token` ausgestellt, damit dieser stellvertretend die Schnittstelle `I_VZD_TIM_Provider_Services` am VZD-FHIR-Directory aufrufen und die Funktionalität über die Schnittstelle 3.2.1.3- `I_internVerification` den Messenger-Proxies zur Verfügung stellen kann.

A_25626 -TI-M Provider Services

Der Registrierungs-Dienst MUSS die an der Schnittstelle `I_VZD_TIM_Provider_Services` angebotenen Funktionen, den Messenger-Proxies und dem Frontend des Registrierungs-Dienstes zur Verfügung stellen. [≤]

3.2.2 Messenger-Service

Der Messenger-Service ist eine Teilkomponente des TI-M FD und wird für Organisationen des Gesundheitswesens (z. B. Arztpraxis, Krankenhaus, Krankenkasse Apotheke, Verband, etc.) bereitgestellt. Der Messenger-Service besteht aus einem Matrix-Homeserver (basierend auf dem Matrix-Protokoll) und einem Messenger-Proxy. Dieser stellt sicher, dass eine Kommunikation mit anderen Messenger-Services, als Teil des TI-M Dienstes, nur innerhalb der gemeinsamen TI-Föderation erfolgt. Die Teilkomponente Matrix-Homeserver basiert auf dem offenen Kommunikationsprotokoll Matrix. Welche APIs der Matrix-Spezifikation im Messenger-Service nachgenutzt werden, ist in der folgenden Abbildung dargestellt:

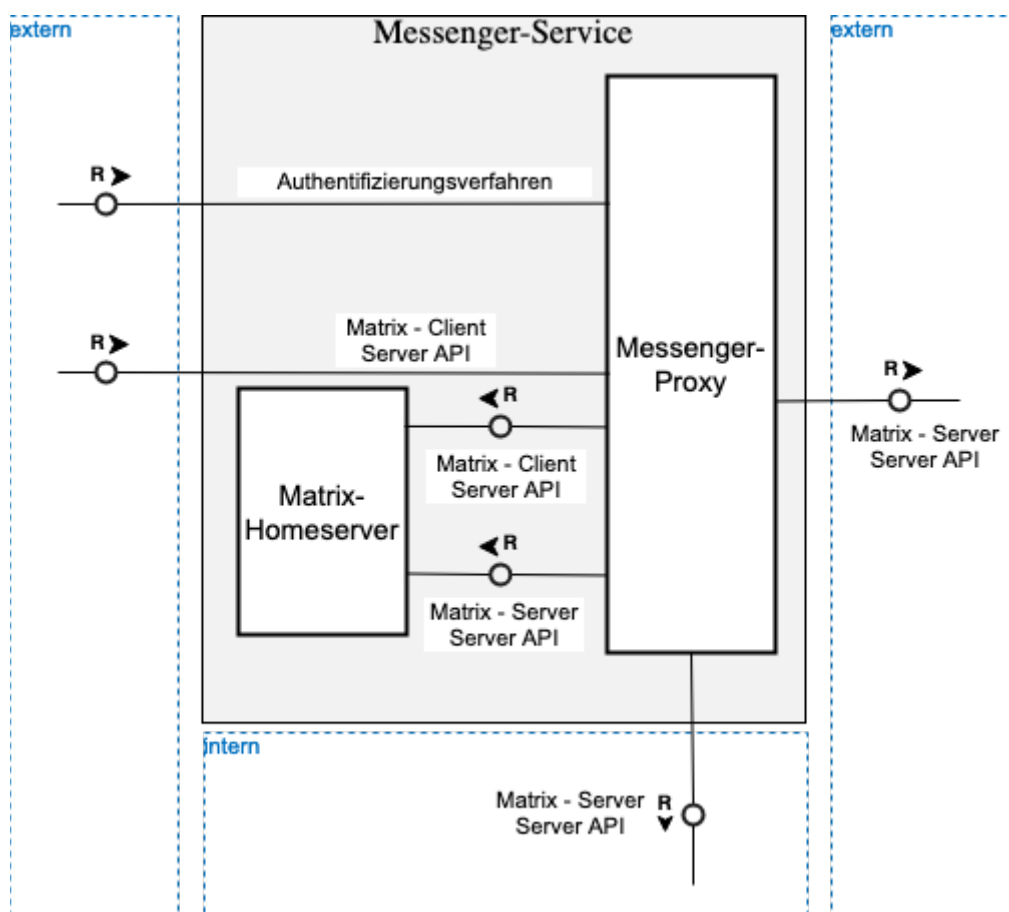


Abbildung 5: Matrix-API des Messenger-Service

Die obige Abbildung zeigt die jeweils zu berücksichtigenden Matrix-APIs (Server-Server API und Client-Server API). Diese sind gemäß [Server-Server API] und [Client-Server API] umzusetzen.

3.2.2.1 Schnittstelle für Authentifizierungsverfahren

Messenger-Services können den Akteuren unterschiedliche Authentifizierungsverfahren anbieten. Dabei können diverse Authentifizierungsmechanismen durch eine Organisation für Ihre Akteure bereitgestellt werden. Die Organisation und der von ihr gewählte TI-Messenger-Anbieter vereinbaren das zur Anwendung kommende Authentifizierungsverfahren bilateral und stimmen sich über die technische Realisierung der dafür notwendigen Anbindung ab. Möglich ist beispielsweise die Nachnutzung eines in der Organisation betriebenen Active Directory (AD/LDAP) oder eines geeigneten Single-Sign-On-Verfahrens (SSO).

3.2.2.2 Messenger-Proxy

Der Messenger-Proxy kann im Fachdienst wahlweise als physische oder logische Komponente umgesetzt werden und dient als Kontrollinstanz zur Prüfung der für die Kommunikation notwendigen Rechte. Hierfür muss sämtliche ein- und ausgehende Kommunikation am Homeserver über den Proxy geleitet werden.

Die konkreten vom Proxy durchzuführenden Prüfungen sind in Kapitel 5.2.1- Prüfung der Föderationszugehörigkeit beschrieben.

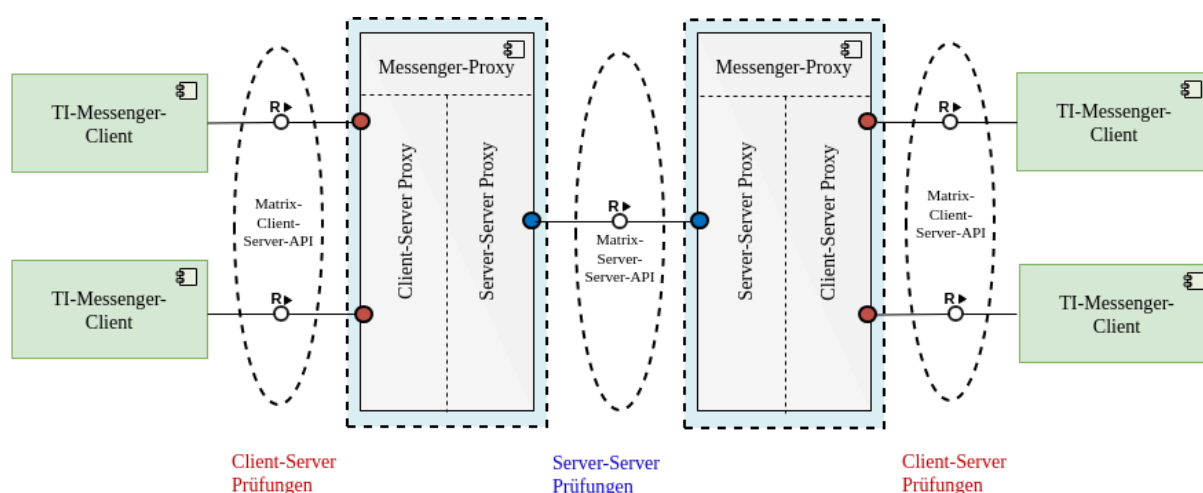


Abbildung 6: Prüfungen Messenger-Proxy

A_25378-01 -Forward- und Reverse-Proxy

Alle ein- und ausgehende Kommunikation des Matrix Homeservers MUSS über den eigenen Messenger-Proxy erfolgen. [=<=]

3.2.2.2.1 Ausnahmeregeln definieren

Der Messenger-Proxy muss zulassen, dass neben den Endpunkten der Client-Server-API zusätzliche Endpunkte für externe Anfragen bereitgestellt werden können. Für die Nutzerauthentifizierung an der Suchschnittstelle benötigt z. B. das VZD-FHIR-Directory Zugriff auf den userinfo Endpunkt des Matrix Homeservers.

A_25539 -Userinfo für VZD-FHIR-Directory

Der Messenger-Proxy MUSS dem VZD-FHIR-Directory Zugriff auf den Endpunkt `/_matrix/federation/v1/openid/userinfo` der Matrix-Homeserver ermöglichen. [=<=]

3.2.2.2.2 Föderationslistensignatur

Nach dem Abruf beim zuständigen Registrierungs-Dienst muss der Messenger-Proxy die Signatur der Föderationsliste gemäß RFC7797 prüfen und diese lokal speichern. Die Struktur der Föderationsliste ist in [gemSpec_VZD_FHIR_Directory#Erzeugung und Bereitstellung der Föderationsliste] beschrieben.

Die Prüfung erfolgt unter Verwendung eines OCSP-Responder und dem X.509-Root Zertifikat der TI. Nach der Erzeugung einer neuen Root-Version der X.509-Root-CA der TI, werden dessen selbstsigniertes Zertifikat und Cross-Zertifikate auf den Download-Punkt gemäß [ROOT-CA] abgelegt. Automatisiert kann der Messenger-Proxy von dort die Verfügbarkeit neuer Versionen überwachen. Zusätzlich kann der folgende Download-Punkt unter [ROOT-CA-JSON] verwendet werden. Dort werden die aktuellen Root-Zertifikate inkl. deren Cross-Zertifikate gepflegt. Im Regelfall wird alle zwei Jahre eine neue Root-Version erzeugt. Die Dateigröße der heruntergeladenen JSON-Datei kann man als Hashfunktion verwenden. Hiermit kann man beispielsweise mit Hilfe des Tools `curl` die HTTP-Methode 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. Diese Elemente enthalten je ein Root-Zertifikat inkl. Cross-Zertifikate für das chronologisch vorhergehende und das nachfolgende Root-Zertifikat. D. h., kryptographisch gesehen stellt dies eine doppelt verkettete Liste dar. Die Elemente im Array sind in chronologischer Ordnung sortiert. Im Folgenden wird ein Beispiel dargestellt.

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

A_25632 -Signatur der Föderationsliste

Der Messenger-Proxy MUSS zur Prüfung der Signatur der Föderationsliste das im Signatur-Header enthaltene Signaturzertifikat (öffentliche Schlüssel) und das X.509-Root-CA Zertifikat der TI verwenden.【<=】

A_25635 -OCSP-Responder

Die Gültigkeit des Signaturzertifikates MUSS mit Hilfe des [OCSP-Responder] validiert werden.【<=】

A_25634 -Zertifikatsaktualisierung

Der Messenger-Proxy MUSS wöchentlich prüfen, ob neue X.509-Root-CA-Versionen existieren und Cross-Zertifikate verfügbar sind. Ist dies der Fall, MUSS der Messenger-Proxy diese neuen Root-Versionen in seinen Truststore importieren.【<=】

3.2.2.3 Matrix-Homeserver

Der Matrix-Homeserver ist die zentrale Komponente für die Kommunikation zwischen den Akteuren und stellt den TI-M Clients die in der Matrix Spezifikation definierten Endpunkte zur Verfügung. Der Matrix-Homeserver verwaltet die Akteure selbst oder bietet eine Schnittstelle für einen externen Identity Provider an, um das Authentifizierungsverfahren der Organisation nachnutzen zu können.

3.2.2.3.1 Matrix Spezifikation

Die folgenden Anforderungen legen die grundlegende Funktionsweise des Matrix-Homeservers fest.

A_25530 -Client-Server API

TI-M FD MÜSSEN sicherstellen, dass die Matrix-Homeserver die [Client-Server API] umsetzen.【<=】

A_25344 -Server-Server API

TI-M FD MÜSSEN sicherstellen, dass die Matrix-Homeserver die [Server-Server API] umsetzen.【<=】

A_25531 -Appendices TI-M FD

TI-M FD MÜSSEN sicherstellen, dass die Matrix-Homeserver [Matrix Appendices] umsetzen.【<=】

3.2.2.3.2 Ergänzungen zur Matrix Spezifikation

A_26191 -Verbot des Ausstellens von Login-Tokens

Der TI-M Fachdienst MUSS jedes Request zum Endpunkt /login/get_token¹ mit einer HTTP 400/404 Response beantworten, ohne ein Token auszustellen.

¹ [Client-Server API/#post_matrixclientv1loginget_token][<=]

A_26243 -Verbot von Guest Accounts

Der TI-M Fachdienst MUSS das Registrieren von Gastzugängen unterbinden, indem er Requests zum Endpunkt /register¹ mit dem Queryparameter kind=guest mit einer HTTP 403 Response beantwortet ohne ein Access Token auszustellen.

¹ [Client-Server API/#post_matrixclientv3register][<=]

A_25393 -Ausgabe von access token durch den TI-M FD

Der TI-M FD MUSS die Komponente Matrix-Homeserver so implementieren, dass bei erfolgreichem Aufruf der [Client-Server API] Endpoints /login und /register neue access token und refresh token ausgegeben werden.[<=]

Hinweis: Durch diese Anforderung soll verhindert werden, dass gestohlene access token missbräuchlich genutzt werden können.

Nach Ablauf der Gültigkeit des access token, kann mit dem refresh token ein neues access token und refresh token

angefordert werden. Das bisherige refresh token wird dadurch ungültig.

A_25352 -Gültigkeitsdauer von access token des TI-M FD

Der TI-M FD MUSS die Komponente Matrix-Homeserver so implementieren, dass vom Matrix-Homeserver ausgestellte access token eine Gültigkeitsdauer von max. 24 Stunden haben.[<=]

A_25353 -Gültigkeitsdauer von refresh token des TI-M FD

Der TI-M FD MUSS die Komponente Matrix-Homeserver so implementieren, dass vom Matrix-Homeserver ausgestellte refresh token eine Gültigkeitsdauer von max. 6 Monaten haben.[<=]

A_26210 -Verpflichtende Unterstützung von Modulen durch TI-M FD

Der TI-M Fachdienst MUSS Client-Module aus 3.1.3.1- Umdefinition der Module, die den Anforderungs-Level MUSS, SOLL oder KANN tragen, verpflichtend unterstützen.[<=]

A_26224 -Abruf einzelner öffentlicher Schlüssel durch andere Fachdienste

Der TI-M Fachdienst MUSS die folgenden Endpunkte zum Abruf öffentlicher Schlüssel durch andere Fachdienste anbieten:

- GET /_matrix/key/v2/server/{keyId}
- GET /_matrix/key/v2/query/{serverName}/{keyId}

Das Response-Schema dieser Endpunkte MUSS identisch zu den gleichnamigen Endpunkten ohne {keyId} Pfadkomponente sein.[<=]

Hinweis: Der TI-M Fachdienst kann Requests zu den Endpunkten

/_matrix/key/v2/server/{keyId} und

/_matrix/key/v2/query/{serverName}/{keyId} auch mit allen Schlüsseln, d.h.

genauso wie die gleichnamigen Endpunkte ohne {keyId} Pfadkomponente, beantworten.

Dieses Verhalten wird aktuell u.a. vom Homeserver [Synapse] implementiert (Stand: v1.109.0 vom Juni 2024).

A_26226 -Verbot des Abrufes einzelner öffentlicher Schlüssel

Der TI-M Fachdienst DARF die Endpunkte/_matrix/key/v2/server/{keyId} und /_matrix/key/v2/query/{serverName}/{keyId} NICHT aufrufen.[<=]

Hinweis: Die Endpunkte mit {keyId} Pfadkomponente wurden mit Version 1.6 aus der Matrix-Spezifikation entfernt, werden von bestehenden Implementierungen u. U. aber noch verwendet. Entgegen der Matrix-Spezifikation unterstützt z. B. der [Synapse]

Homeserver diese Endpunkte daher weiterhin (Stand: v1.109.0 vom Juni 2024, siehe auch [Synapse/issues/17323]).

A_26263 -Unauthenticated Media

Der TI-M Fachdienst DARF den Download von Medien über die nicht authentifizierten Endpunkte

- GET /_matrix/media/v3/download/{serverName}/{mediaId}
- GET /_matrix/media/v3/download/{serverName}/{mediaId}/{fileName}
- GET /_matrix/media/v3/thumbnail/{serverName}/{mediaId}

NICHT durch einen Freeze¹ einschränken.

¹ [Client-Server API/#content-repo-client-behaviour][<=]

A_26344 -Verbot von URL-Previews

Der TI-M Fachdienst MUSS Requests zu folgenden Endpunkten mit einer HTTP 404 Response ablehnen ohne die übergebene URL aufzurufen:

- GET /_matrix/media/v3/preview_url
- GET /_matrix/client/v1/media/preview_url

[<=]

A_26265 -TI-M FD Org-Admin Support

Der TI-M Fachdienst MUSS den Endpunkt /.well-known/matrix/support bereitstellen um dort Kontaktmöglichkeiten zum Org-Admin hinterlegen zu können.[<=]

A_26266-01 -TI-M Anbieter Org-Admin Support

Der TI-M Anbieter MUSS am Endpunkt /.well-known/matrix/support Kontaktinformationen zum Org-Admin hinterlegen.[<=]

Hinweis: Die als Kontaktinformation hinterlegte Kontaktmöglichkeit soll keine persönliche Adresse sein, sondern eher eine Art Support-Adresse unter der die für die TI-Messenger Instanz verantwortliche Person erreicht werden kann.

A_26289 -Authentisierung von Profilabfragen

Der TI-M Fachdienst MUSS nicht authentifizierte Requests zu den folgenden Endpunkten mit einer HTTP 401 Response ablehnen:

- GET /_matrix/client/v3/profile/{userId}
- GET /_matrix/client/v3/profile/{userId}/avatar_url
- GET /_matrix/client/v3/profile/{userId}/displayname

[<=]

A_26374 -Profilabfragen bei gemeinsamen Räumen

Der TI-M Fachdienst MUSS Profilabfragen über die folgenden Endpunkte erlauben, sofern der anfragende und der angefragte Nutzer gemeinsame Räume haben:

- GET /_matrix/client/v3/profile/{userId}
- GET /_matrix/client/v3/profile/{userId}/avatar_url
- GET /_matrix/client/v3/profile/{userId}/displayname

[<=]

A_26330 -Authentisierung von Versionsabfragen

Der Matrix Homeserver MUSS ausgehende Requests zum Endpunkt /_matrix/federation/v1/version¹ gemäß [Server-Server API/#request-authentication] authentisieren.[<=]

Hinweis: Matrix erlaubt über den Endpunkt `/_matrix/federation/v1/version`¹ die Abfrage von Versionsinformationen zu einem Homeserver. Dieser Endpunkt unterliegt laut Matrix nicht der normalen Authentisierung von Server-Server Requests. Um den Zugriff auf diese Metadaten auf Homeserver aus der TI-Föderation zu beschränken wird die Authentisierung dieses Endpunktes daher für TI-M Fachdienste verpflichtend gemacht.

A_26331 -Ablehnung nicht authentisierter Versionsabfragen

Der TI-M Fachdienst MUSS nicht authentifizierte Requests zum Endpunkt `/_matrix/federation/v1/version`¹ mit einer HTTP 401 Response ablehnen.

¹ `[Server-Server API/#get_matrixfederationv1version][<=]`

4 Übergreifende Festlegungen

4.1 Datenschutz und Sicherheit

Zur Sicherstellung des Datenschutzes und der Sicherheit im Rahmen des TI-M Dienstes werden im Folgenden zu erfüllende Anforderungen an den TI-M FD und den TI-M Client, beziehungsweise deren Hersteller und Anbieter beschrieben. Anforderungen, die durch andere Systemkomponenten zu erfüllen sind, werden hier nicht aufgeführt.

Hinweis: Clients und Server im Sinne der folgenden Anforderung sind alle Komponenten des TI-M Dienstes, die miteinander kommunizieren, wobei der Client der Initiator einer Verbindung zu einem Server ist, der eine Ressource zur Verfügung stellt. Wenn TI-M-Clients und TI-M FD gemeint sind, werden diese auch explizit als TI-M-Clients und TI-M FD bezeichnet.

A_25299 -Flächendeckende Verwendung von TLS

Sämtliche Kommunikation zwischen Komponenten des TI-M Dienstes MUSS TLS-verschlüsselt erfolgen, sofern die Kommunikation die Grenzen einer virtuellen/physischen Maschine überschreitet.

[<=]

A_25303 -Mindestens serverseitiges TLS

Im Rahmen der Kommunikation per TLS MUSS mindestens serverseitiges TLS verwendet werden.

[<=]

A_25301 -Authentifizierung von Clients

Server MÜSSEN Clients authentifizieren, bevor Ihnen - den Clients - Zugriff auf Ressourcen gewährt wird, die nicht frei zur Verfügung stehen.

[<=]

A_25302 -Art der Client-Authentifizierung

Clients SOLLEN sich gegenüber Servern per TLS-Client-Zertifikat oder einem Verfahren mit vergleichbarem Sicherheitsniveau authentisieren.[<=]

A_25311 -Minimale Qualität von Passwörtern

Der Anbieter des TI-M FD MUSS Vorgaben zur minimalen Qualität von Passwörtern entsprechend [BSI ORP.4] A.22 machen und die Einhaltung dieser Vorgaben an allen Stellen gewährleisten, an denen Passwörter im Rahmen der Konfiguration festzulegen sind.[<=]

A_25312 -Instruktion über Einhaltung von Vorgaben zu Passwörtern

Der Anbieter MUSS die Organisation, 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 des Umgangs mit Passwörtern, richten sich jedoch an den operativen Betrieb durch die Leistungserbringerinstitution bzw. den Kostenträger, der vom Anbieter nicht kontrolliert werden kann.[<=]

Hinweis: Unter Passwörtern werden in diesem Kontext sowohl Kennwörter als auch Passphrasen verstanden, auf welche das Dokument [BSI ORP.4] gleichermaßen anwendbar ist.

A_25313 -Zwangsabmeldung und Sperrung von Akteuren

Wird ein Akteur in der Rolle "User" des TI-M Dienstes einer Organisation durch einen Akteur in der Rolle "Org-Admin" der Organisation gesperrt oder seine aktive Sitzung beendet - das heißt, er wird zwangsweise ausgeloggt -, so MUSS der TI-M FD die Weiterleitung von Nachrichten, die an diesen Akteur in der Rolle "User" gesendet werden oder von diesem gesendet werden, mit sofortiger Wirkung einstellen. [≤]

A_25314 -Einbringung kryptographischen Materials zur Authentisierung gegen das VZD-FHIR-Directory

TI-Messenger-Anbieter MÜSSEN sicherstellen, dass kryptographisches Material zur Authentisierung gegen das VZD-FHIR-Directory sicher eingebracht 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. Eine Auditierung der Umsetzung ist optional. [≤]

A_25315 -Explizites Verbot von Profiling für TI-Messenger-Hersteller

TI-Messenger-Hersteller 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 Hersteller von Komponenten und Diensten 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.

A_25316 -Explizites Verbot von Profiling für TI-Messenger-Anbieter

TI-Messenger-Anbieter 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 Diensten 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.

A_25317 -Protokollierung zum Zwecke der Fehler- bzw. Störungsbehebung

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

A_25327 -Sicherheitsrisiken von Software-Bibliotheken minimieren

TI-M FD-Hersteller MÜSSEN Maßnahmen umsetzen, um die Auswirkung von unentdeckten Schwachstellen in benutzten Software-Bibliotheken zu minimieren. [≤]

Hinweis: Beispielmaßnahmen sind in [OWASP Proactive Control#C2] zu finden.

A_25328 -Wirksamkeit von Maßnahmen zur Minimierung von Sicherheitsrisiken

Die zur Minimierung der Auswirkungen von unentdeckten Schwachstellen in benutzten Software-Bibliotheken umgesetzten Maßnahmen MÜSSEN wenigstens die gleiche Wirksamkeit aufweisen, wie die Kapselung gemäß [OWASP Proactive Control#C2 Punkt 4]. [≤]

A_25333 -Abweichungen vom Matrix-Standard

TI-M FD-Hersteller MÜSSEN sämtliche nicht in der TI-Messenger-Spezifikation beschriebenen Abweichungen vom Matrix-Protokoll oder den MUST- oder SHOULD-Empfehlungen des Matrix-Protokolls dokumentieren und begründen. [≤]

Hinweis: Gemeint sind hier nur tatsächliche Abweichungen von Festlegungen der Matrix-Spezifikation und nicht zusätzliche Funktionen, die auf dem TI-M Dienst aufbauen und produktspezifisch sind.

A_25334 -Interoperabilität von Zusatzfunktionen für den TI-M FD

TI-M FD-Hersteller MÜSSEN sicherstellen, dass alle implementierten Funktionen, die über den gewöhnlichen Funktionsumfang einer TI-Messenger-Komponente hinausgehen, die Sicherheit des Produkts nicht gefährden und die Interoperabilität mit anderen TI-Messenger-Produkten gewährleisten. [≤]

A_25342 -Einsatz geschulter Administratoren

TI-Messenger-Anbieter MÜSSEN als Administratoren Personal einsetzen, welches für die damit verbundenen Aufgaben und Themen der Informationssicherheit geschult und sensibilisiert wurden. [≤]

A_25343 -Berechtigung von Administratoren

TI-Messenger-Anbieter MÜSSEN technisch sicherstellen, dass nur die berechtigten Administratoren administrativen Zugriff auf die zu verwaltenden Messenger-Services haben. [≤]

4.2 Test

Für die Erlangung einer Produkt-/Anbieterzulassung müssen folgende Teststufen durchlaufen werden:

- Vorbereitung der Zulassung
 - allg. Festlegungen siehe [gemKPT_Test] (Testdokumentation, Eigenverantwortliche Tests usw.)
 - Tests der Hersteller gegen die Referenzimplementierung
- Zulassung der gematik
 - automatisierte Tests gegen die Referenzimplementierung
 - manuelle Tests
 - Look and Feel Workshop für jeden Client
 - automatisierte Tests mit anderen Herstellern zur Prüfung der Interoperabilität

Für die Tests der Hersteller und die automatisierten Tests der gematik gegen die Referenzimplementierung wird eine Testsuite [gematik Testsuite] bereitgestellt. Mit dieser Testsuite und der dazugehörigen Testtreiberschnittstelle [api-testtreiber] werden dann auch die Zulassungstests durchgeführt. Die Zulassungstests werden auf der Testinstanz der Hersteller durchgeführt.

A_25556 -Test des TI-M Clients gegen die Referenzimplementierung

Der TI-M Client MUSS gegen die Referenzimplementierung erfolgreich getestet werden. Die Testergebnisse sind der gematik vorzulegen. [≤]

A_25623 -Test des TI-M FD gegen die Referenzimplementierung

Der Hersteller des TI-M FD MUSS den Fachdienst gegen die Referenzimplementierung erfolgreich testen. Die Testergebnisse sind der gematik vorzulegen. [≤]

A_25619 -TI-Messenger Instanzen

Der TI-Messenger-Anbieter MUSS eine Referenzinstanz und mindestens eine Testinstanz des TI-M FD und TI-M Clients bereitstellen und betreiben.【<=】

Die Referenzinstanz hat die gleiche Version wie die Produktionsumgebung. Weiterhin wird die Referenzinstanz für die Reproduktion aktueller Fehler/Probleme aus der Produktionsumgebung genutzt. Der Zugriff auf die Referenzinstanz muss für die gematik zur Fehleranalyse und für weiterführende IOP Tests gewährleistet sein. Die Test-Instanz dient den Herstellern bei der Entwicklung neuer TI-M Clients und TI-Messenger Fachdienste Versionen, den IOP-Tests zwischen den verschiedenen TI-Messenger-Anbietern und wird auch von der gematik für die Zulassung genutzt.

A_25620 -Nutzung der Referenz- und Testinstanzen

Der TI-Messenger-Anbieter MUSS die verschiedenen Benutzer der Referenzinstanz und der Testinstanz koordinieren (z. B. Verwaltung eines Test-/Nutzungsplans).【<=】

A_25621 -Weitere Testinstanzen

Bei Bedarf (Entwicklung verschiedener Versionen, hoher Auslastung durch andere Hersteller oder durch die gematik) MUSS der TI-Messenger-Anbieter auch mehrere Testinstanzen mit der gleichen oder mit verschiedene Versionen bereitstellen und betreiben.【<=】

Eine detaillierte Beschreibung des Testvorgehens, der Testumgebung und der Testtreiberschnittstelle [api-testtreiber] befindet sich im Testkonzept [gematik Testkonzept].

A_25622 -Umsetzung des Testkonzepts

Die TI-Messenger Hersteller MÜSSEN sicherstellen, dass das Testkonzept [gematik Testkonzept] vollständig umgesetzt wird.【<=】

4.3 Betrieb

Ein Anbieter des TI-Messengers verantwortet im Betrieb mindestens folgende Produkttypen:

- TI-Messenger Fachdienst

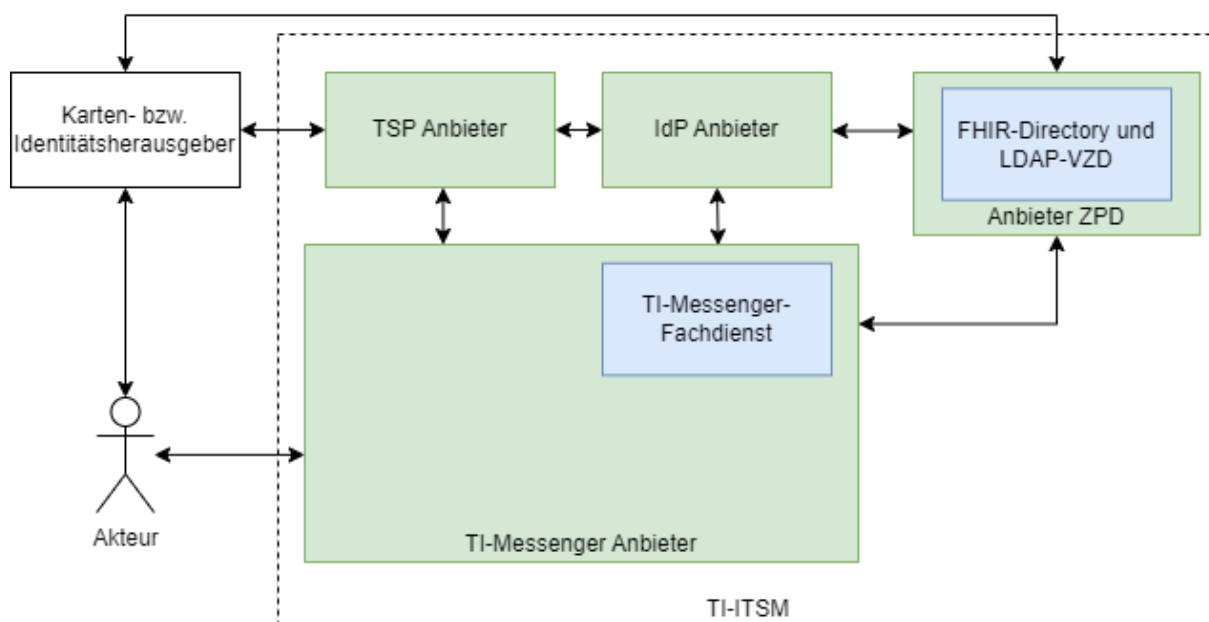


Abbildung 7: Betriebsmodell TI-M Basis

Hinweis: Die Abbildung bildet die organisatorischen Kommunikationsbeziehungen aus Sicht des TI-ITSM-Systems zwischen den jeweiligen Entitäten/Anbieterrollen ab. Die Produkte beim TI-Messenger Anbieter können einzeln zur Zulassung eingereicht werden.

A_25250 -TI-Messenger Anbieter - Produktverantwortung (Basis)

Der TI-Messenger Anbieter MUSS mindestens einen:

- TI-Messenger Fachdienst

anbieten.【<=】

Der Betrieb des Fachdienstes wird durch den TI-Messenger-Anbieter verantwortet. Entsprechend dem Betriebskonzept [gemKPT_Betr#Anbieterkonstellationen] kann der Betrieb auch an Unterauftragnehmer aus- bzw. verlagert werden oder *on-premise* gehostet werden. Die Koordination der jeweiligen Komponenten sowie die Erfüllung der Anforderungen verbleiben jedoch beim Anbieter. Dieser kann in Abstimmung mit seinen Nutzern und Dienstleistern Verträge abschließen, um den sicheren Betrieb aufrecht zu erhalten.

Anforderungen zu Performance und Reporting sind den entsprechenden Produkt- und Anbietertypsteckbriefen u.a. den Dokumenten [gemSpec_Perf] und [gemKPT_Betr] zu entnehmen.

Hinweis: Die Bereitstellung der Messenger-Services erfolgt über den Registrierungs-Dienst eines TI-M FD und kann on-premise oder zentral innerhalb von Rechenzentren stattfinden.

A_26219 -TI-M Anbieter Monitoring

Der TI-Messenger-Anbieter MUSS das Service Monitoring der gematik technisch-organisatorisch unterstützen.【<=】

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

A_25379 -TI-M Gültigkeitsprüfung der Organisation am VZD-FHIR-Directory

Der TI-M FD MUSS mindestens alle 24 Stunden, für alle bei ihm registrierten Organisationen mit einem Messenger-Service, prüfen, ob diese im VZD-FHIR-Directory als "active" (Organization.active) eingetragen sind.【<=】

A_25380 -TI-M Information bei ausgetragener Organisation am VZD-FHIR-Directory

Wenn die Organisation nicht mehr im VZD-FHIR-Directory "active" (Organization.active) ist, MUSS der TI-Messenger-Anbieter diese darüber informieren.【<=】

A_25381 -TI-M Sperrung der Organisation mit ungültigem SM-B bzw. ungültiger SMC-B

Wenn die Organisation länger als 30 Kalendertage nicht im VZD-FHIR-Directory "active" (Organization.active) ist, MUSS der TI-Messenger-Anbieter die Domäne dieses Messenger-Service aus der Föderation löschen (siehe FHIR-VZD: I_VZD_TIM_Provider_Services, DELETE /federation/{domain}). Dann DARF erst nach erneuter Authentifizierung per SM(C)-B der Dienst wieder genutzt werden, siehe AF_10103.【<=】

A_26095 -logische Trennung Messenger-Services

Werden durch einen TI-Messenger-Anbieter mehrere Domains in einem gemeinsamen Messenger-Service betrieben, so MUSS die logische Trennung der Matrix-Domains sichergestellt werden.

Hinweis: Die Anforderungen A_25381 & A_25382 erfordern die Zuordnung einer Organisation zu einer Domain, um einer Organisation die Teilnahme an der Föderation zu entziehen.

【<=】

A_25382 -TI-M kontrollierte Außerbetriebnahme

Wenn z. B. das Vertragsverhältnis zwischen Kunde und TI-Messenger-Anbieter ausläuft, so MUSS der TI-Messenger-Anbieter die dazugehörige Domäne dieses Messenger-Service aus der Föderation löschen (siehe FHIR-VZD: I_VZD_TIM_Provider_Services, DELETE /federation/{domain}) und den Messenger-Service abschalten, so dass dieser nicht mehr erreicht werden kann. [≤]

A_23658-01 -Produktnachweise im Rahmen der kontrollierten Inbetriebnahme

Das Produkt MUSS die Vorgaben zur Funktionalität, Sicherheit und Interoperabilität entsprechend des jeweiligen Produkttypsteckbriefs in der Produktivumgebung erfüllen. Die Nachweise dafür MÜSSEN entsprechend und im Rahmen des Konzepts zur kontrollierten Inbetriebnahme erbracht werden. [≤]

Hinweis: Die Anforderung A_23658-01 ist eine Ergänzung für die Produktivumgebung und ersetzt nicht die vorgelagerten Prüfverfahren der Produkte in der Referenzumgebung.

Der TI-Messenger-Anbieter kann auch mehrere TI-M Clients und mehrere TI-M FD anbieten. Der tatsächliche Betrieb kann gemäß [gemKPT_Betr#Anbieterkonstellationen] ausgelagert werden.

Der TI-Messenger-Anbieter muss seinen Nutzern und Organisationen einen Helpdesk entsprechend [gemKPT_Betr] anbieten, welcher auch Störungen zu allen verantworteten TI-M Clients und TI-M FD entgegennimmt.

Der TI-Messenger-Anbieter ist gemäß Betriebskonzept [gemKPT_Betr] ein Teilnehmer im TI-ITSM (IT-Service-Management der TI) mit allen damit verbundenen Rechten und Pflichten.

A_26247 -SRV Records

Verwendet ein TI-M Fachdienst Anbieter für die Auffindbarkeit seines Homeservers DNS-SRV-Einträge, so MUSS er neben einem Eintrag zum Servicenamen _matrix-fed auch einen Eintrag zum Servicenamen _matrix einpflegen. [≤]

4.3.1 TI-M Client

Die Betriebsbereitschaft des Clients bzw. der Clients des TI-Messenger-Anbieters bezieht sich in diesem Kapitel auf serverseitige Systeme, welche notwendig sind, damit der Client vom Nutzer sicher-funktional betrieben werden kann. Der sichere Betrieb im Sinne der Nutzung auf ihren Endgeräten des TI-M Clients liegt letztendlich in der Verantwortung der Nutzer bzw. Akteure des TI-Messengers.

A_25383 -TI-M Client Anbietersupport

Der TI-Messenger-Anbieter MUSS seine Nutzer bzw. die Akteure dabei unterstützen, einen sicheren und funktionalen Betrieb der TI-M Clients zu ermöglichen. [≤]

A_25548 -Information über Updates für den Client

Hersteller des TI-M Client MÜSSEN sicherstellen, dass Akteure über die Veröffentlichung von Updates für ihre TI-M Clients informiert werden, bspw. durch Mitteilung innerhalb und mittels des TI-M Clients. [≤]

A_25549 -Information über Notwendigkeit von Sicherheitsupdates

Hersteller des TI-M Clients MÜSSEN sicherstellen, dass Akteure geeignet über die Notwendigkeit der Installation sicherheitskritischer Updates informiert werden, um den TI-M Client weiterhin nutzen zu können. [≤]

A_25550 -Sperrung von Clients ohne Sicherheitsupdates

TI-M Client-Hersteller MÜSSEN sicherstellen, dass nach einer geeigneten Frist eine weitere Nutzung des TI-M Clients ohne vorheriges Sicherheitsupdate nicht möglich ist. Hierzu genügt eine client-seitige Sperre anstatt eines Nachweises gegenüber dem Matrix-Homeserver. [≤]

A_25551 -Fähigkeit zum Update im gesperrten Zustand

Ist ein TI-M Client wegen ausgebliebener Installation von Sicherheitsupdates nicht mehr für die Kommunikation nutzbar, MUSS die Möglichkeit der Installation von Updates weiterhin gegeben sein. [≤]

A_25552 -Information und Nachweis der Eignung

Der Hersteller des TI-M Clients MUSS die gematik bei Veröffentlichung einer neuen Produktversion informieren und eine Erklärung zur sicherheitstechnischen Eignung liefern. [≤]

A_25565 -Explizites Verbot von Profiling für TI-M Clients

TI-M Client-Hersteller und -Anbieter DÜRFEN NICHT Daten zu Profiling-Zwecken 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 Hersteller und Anbieter von Komponenten und Diensten der gematik offenzulegen bzw. zu übermitteln haben, sofern diese erforderlich sind, um dem gesetzlichen Auftrag der gematik zur Überwachung des Betriebs zur Gewährleistung der Sicherheit, Verfügbarkeit und Nutzbarkeit der Telematikinfrastruktur zu erfüllen. Nur die hierfür erforderlichen personenbezogenen Daten dürfen von den Anbietern und Herstellern als Ausnahme vom Profiling-Verbot erhoben und ausschließlich für den genannten Zweck verwendet werden.

4.4 Sonstige

4.4.1 Rechte und Pflichten des Herstellers

A_25582 -Vertrauenswürdige Bezugsquellen für den TI-M Client

Der Hersteller eines TI-M Clients MUSS Akteure über die vertrauenswürdigen Quellen informieren, von denen Akteure den TI-M Client beziehen können und wie sie die Vertrauenswürdigkeit der Quelle erkennen können. [≤]

A_25583 -Möglichkeit der Authentizitätsprüfung

Der Hersteller MUSS sicherstellen, dass der Akteur bei Erstbezug eines TI-M Clients die Authentizität der vertrauenswürdigen Bezugsquelle verifizieren kann. [≤]

5 Funktionsmerkmale

5.1 Anwendungsfälle

Die nachfolgend beschriebenen Anwendungsfälle sind spezifisch für den TI-Messenger und weichen daher teilweise von der Matrix-Client-Server-API ab. Das gleiche gilt für die auf dem Matrix-Server-Server-Protokoll ([Server-Server API]) basierenden Anwendungsfälle.

Im Kontext des TI-M Dienstes nehmen Akteure unterschiedliche Rollen ein (siehe Kapitel 2.3- Akteure und Rollen). Entsprechend der eingenommen Rolle eines Akteurs werden unterschiedliche Anwendungsfälle ausgelöst. Für die Rollen "Org-Admin" und "User" wird dies in den folgenden Abbildungen dargestellt.

Rolle: Org-Admin

Ein Akteur in der Rolle "Org-Admin" kann ein Leistungserbringer / beauftragter Mitarbeiter in einer Organisation oder ein beauftragter Administrator des TI-Messenger-Anbieters sein. Im Rahmen seiner administrativen Tätigkeiten löst dieser Akteur im Kontext des TI-Messengers die folgenden Anwendungsfälle aus:

- 5.1.1- Authentisieren einer Organisation
- 5.1.2- Bereitstellung eines Messenger-Service für eine Organisation

Werden durch eine Organisation mehrere Messenger-Services benötigt kann der letztgenannte Anwendungsfall mehrfach ausgeführt werden.

Rolle: User

Ein Akteur in der Rolle "User" kann die folgenden Anwendungsfälle auslösen:

- 5.1.4- Austausch von Events zwischen Akteuren innerhalb einer Organisation
- 5.1.5- Einladung von Akteuren außerhalb einer Organisation
- 5.1.6- Austausch von Events zwischen Akteuren außerhalb einer Organisation

Hinweis: Für eine bessere Lesbarkeit können die in den jeweiligen Anwendungsfällen dargestellten Laufzeitsichten als PlantUML-Quelle in [api-messenger] unter/src/images/TI-M_Basis und in Diagrammform unter/images/generated/TI-M_Basis abgerufen werden.

5.1.1 Authentisieren einer Organisation

AF_10103-02 -Authentisieren einer Organisation am TI-M Dienst

Mit diesem Anwendungsfall authentisiert ein Akteur, in der Rolle "Org-Admin", seine Organisation bei einem TI-Messenger-Anbieter. Für die Authentisierung einer Organisation stellt der TI-M FD eine Schnittstelle an seinem Registrierungs-Dienst bereit. Diese wird über das Frontend des Registrierungs-Dienstes für die Authentisierung verwendet. Die Authentisierung der Organisation erfolgt individuell und nutzungsabhängig durch einen Akteur in der Rolle "Org-Admin". Im Rahmen der Authentifizierung MUSS der Besitz einer gültigen SM(C)-B nachgewiesen werden, da nur Organisationen des Gesundheitswesens berechtigt sind einen Messenger-Service zu erhalten. Als Nachweis ist eines der folgenden Verfahren zu verwenden:

- Verfahren 1: bei der Authentisierung am zentralen IDP-Dienst eine freigeschaltete SM(C)-B verwendet werden oder
- Verfahren 2: eine KIM-Nachricht an die Adresse der Organisation mit der freigeschalteten SM(C)-B gesendet werden.

Als Nachweis zur Prüfung auf eine gültige Organisation ist vom Registrierungs-Dienst in beiden Verfahren zu prüfen, ob die ProfessionOID zu einer Organisation des Gesundheitswesens gehört. Bei erfolgreicher Verifizierung der Organisation wird ein Administrator-Account für die Organisation am Registrierungs-Dienst angelegt. Dies ermöglicht es einem Administrator Messenger-Services zu registrieren und seiner Organisation am TI-M Dienst teilzunehmen.

Tabelle 4: Tabelle : AF - Authentisieren einer Organisation am TI-M Dienst

AF_10103	Authentisieren einer Organisation am TI-M Dienst
Akteur	Beauftragter Mitarbeiter einer Organisation in der Rolle "Org-Admin"
Auslöser	Eine Organisation des deutschen Gesundheitswesens möchte am TI-M Dienst teilnehmen und benötigt die Berechtigung einen Messenger-Service zu registrieren.
Komponenten	<ul style="list-style-type: none"> • Frontend des Registrierungs-Dienstes, • Authenticator (Optional bei Verfahren 2), • Konnektor oder Basis-Consumer, • eHealth Kartenterminal mit gesteckter SMC-B oder HSM-B (SM-B im HSM), • Registrierungs-Dienst, • zentraler IDP-Dienst (Optional bei Verfahren 2) • KIM-Clientmodul und Mailclient (Optional bei Verfahren 1)
Vorbedingung	<ol style="list-style-type: none"> 1. Der Akteur kann über ein Frontend auf den Registrierungs-Dienst zugreifen. 2. Verifizierung der Organisation: <ul style="list-style-type: none"> • Verfahren 1: <ol style="list-style-type: none"> i. Der Registrierungs-Dienst ist beim zentralen IDP-Dienst registriert. ii. Auf dem Endgerät des Benutzers ist eine Authenticator Anwendung installiert, über die eine Challenge vom IDP-Dienst mit Hilfe einer SM(C)-B signiert wird. • Verfahren 2: <ol style="list-style-type: none"> iii. Der Anbieter des TI-Messenger verfügt über eine SMC-B Org und eine KIM-Adresse sowie ein eHealth Kartenterminal und einen Konnektor mit TI-Zugang. iv. Der Akteur verfügt über eine SM(C)-B und eine KIM-Adresse sowie ein eHealth Kartenterminal und einen Konnektor mit TI-Zugang oder alternativ über einen

	Basis-Consumer. 3. Die verwendete SM(C)-B ist freigeschaltet.
Eingangsdaten	Identität der Organisation, SM(C)-B, Alternativ KIM-Adresse
Ergebnis	Die Organisation wurde am Registrierungs-Dienst des TI-M FD verifiziert und ein Administrator Account für die Organisation wurde erfolgreich am Registrierungs-Dienst angelegt.
Ausgangsdaten	Admin-Account, Status

In der Laufzeitsicht sind die Interaktionen zwischen den Komponenten, die durch den Anwendungsfall genutzt werden, dargestellt. Für die Authentisierung einer Organisation wird in der Laufzeitsicht der zentrale IDP-Dienst der TI verwendet.

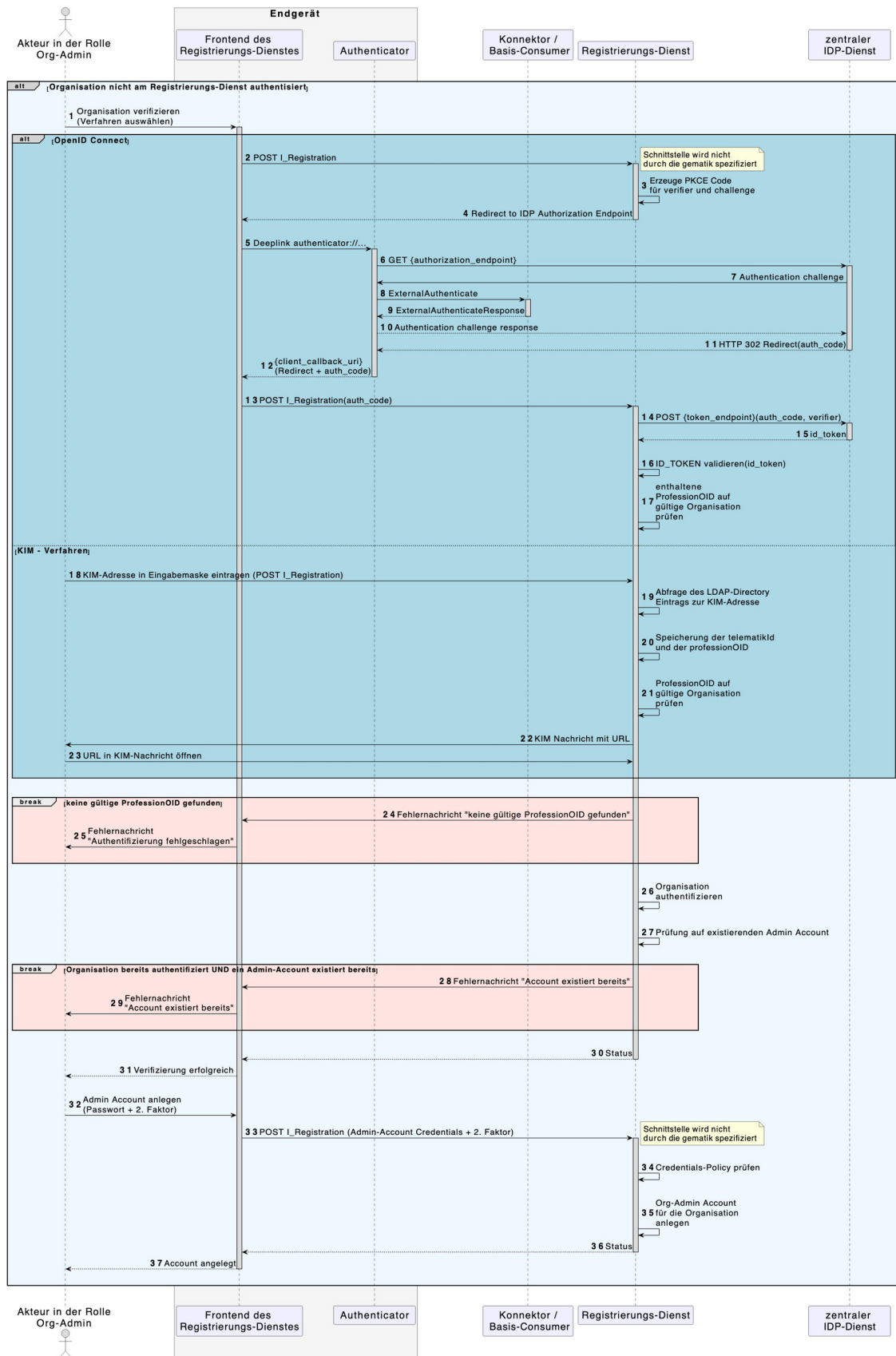


Abbildung 8: Laufzeitsicht - Authentisieren einer Organisation am TI-M Dienst

[<=]

A_25805 -AF_10103 - Organisation wurde erfolgreich verifiziert

Die im ID_TOKEN enthaltene ProfessionOID MUSS in der in [gemSpec_OID] in der Tabelle "Tab_PKI_403-x OID-Festlegung Institutionen im X.509-Zertifikat der SMC-B" gelisteten OIDs vorhanden sein.[<=]

A_25806 -AF_10103 - ID-Token wurde geprüft

Die Signatur des vom IDP-Dienst ausgestellten ID_TOKEN MUSS geprüft werden.[<=]

5.1.2 Bereitstellung eines Messenger-Service für eine Organisation

AF_10060-03 -Bereitstellung eines Messenger-Service für eine Organisation

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

Tabelle 5: AF - Bereitstellung eines Messenger-Service für eine Organisation

AF_10060	Bereitstellung eines Messenger-Service für eine Organisation
Akteur	Beauftragter Mitarbeiter einer Organisation in der Rolle "Org-Admin"
Auslöser	Eine Organisation des deutschen Gesundheitswesens möchte am TI-M Dienst teilnehmen und benötigt die Bereitstellung eines oder mehrerer Messenger-Services.
Komponenten	<ul style="list-style-type: none"> • Frontend des Registrierungs-Dienstes • Registrierungs-Dienst • VZD-FHIR-Directory • Messenger-Service
Vorbedingung	<ol style="list-style-type: none"> 1. Es besteht ein Vertragsverhältnis mit einem TI-Messenger-Anbieter. 2. Der Akteur verfügt über ein Frontend des Registrierungs-Dienstes für die Kommunikation mit dem Registrierungs-Dienst. 3. Das verwendete Frontend des Registrierungs-Dienstes ist beim zentralen IDP-Dienst registriert. 4. Die Organisation ist erfolgreich beim Registrierungs-Dienst authentifiziert und ein Admin-Account ist

	<p>vorhanden.</p> <p>5. Der Registrierungs-Dienst kann sich beim VZD-FHIR-Directory Server für Schreibzugriffe mit OAuth2 authentisieren.</p>
Eingangsdaten	Admin-Account
Ergebnis	<p>1. Der Messenger-Service für die Organisation wurde für die übergebene Domain erstellt.</p> <p>2. Die Domain des neuen Messenger-Services wurde in die Föderationsliste im VZD-FHIR-Directory eingetragen.</p>
Ausgangsdaten	Neuer Messenger-Service für die Organisation, Status

In der Laufzeitsicht sind die Interaktionen zwischen den Komponenten, die durch den Anwendungsfall genutzt werden, dargestellt. Für den Anwendungsfall wird die erfolgreiche Authentifizierung der Organisation mit Hilfe des Anwendungsfalles 5.1.1-1-Authentisieren einer Organisation am TI-M Dienst vorausgesetzt. Die Komponente Messenger-Service für die Organisation wird im Verlauf des Anwendungsfalles erstellt.

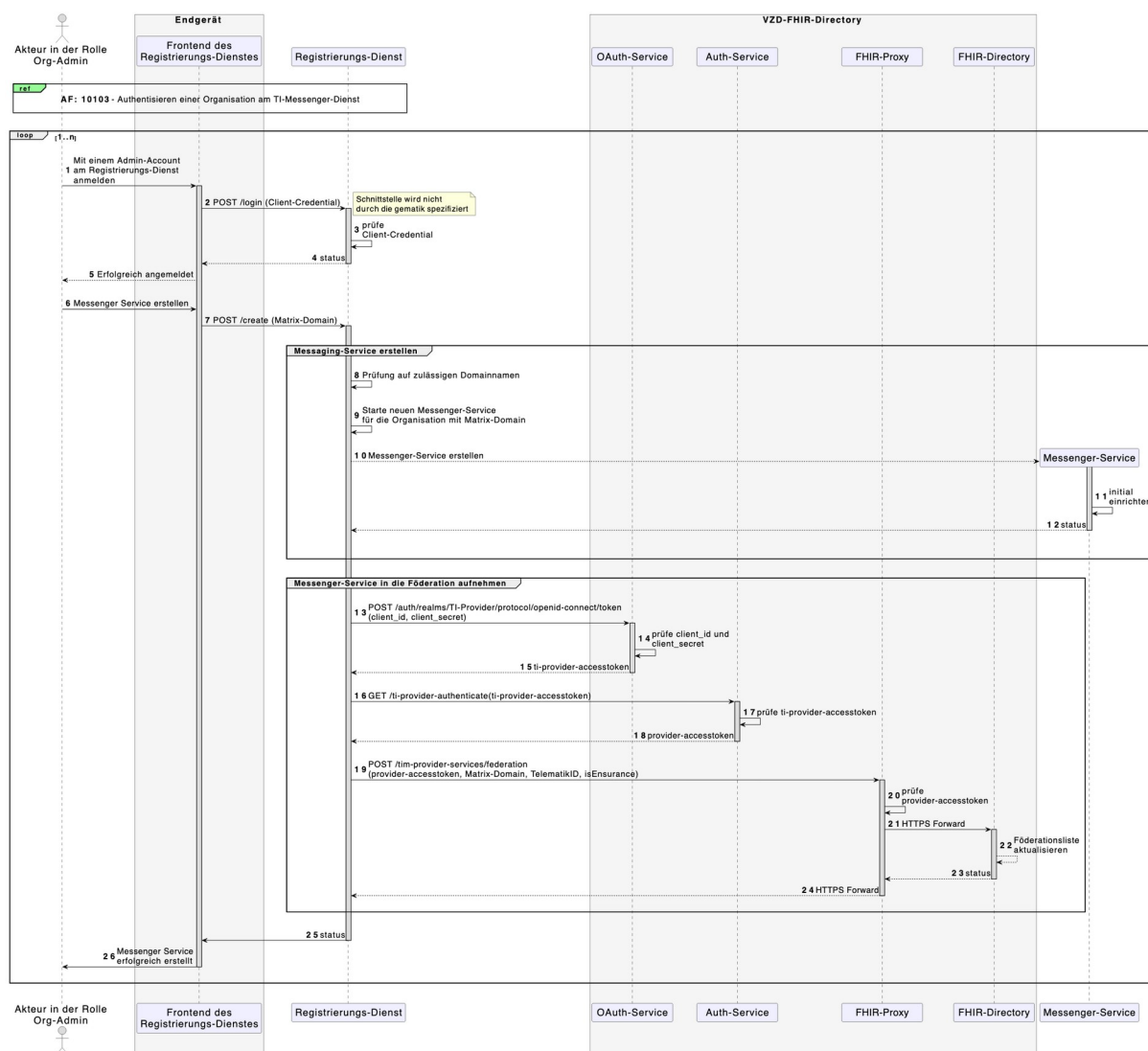


Abbildung 9: Laufzeitsicht - Bereitstellung eines Messenger-Service für eine Organisation

[<=]

5.1.3 Föderationszugehörigkeit prüfen

AF_10064-02 -Föderationszugehörigkeit eines Messenger-Service prüfen

Dieser Anwendungsfall prüft, ob ein Messenger-Service zugehörig zur TI-Messenger-Föderation ist, und gilt für alle Anwendungsfälle, welche die Matrix-Domain eines Messenger-Services überprüfen müssen. Für die Prüfung der Zugehörigkeit der Matrix-Domain zur TI-Messenger-Föderation verwendet der Messenger-Proxy eine Föderationsliste, die vom Registrierungs-Dienst seines TI-M FD bereitgestellt wird. Die Speicherdauer der Föderationsliste des Messenger-Proxies ist limitiert. Die Aktualisierung der Föderationsliste erfolgt wie in 5.1.7- Aktualisierung der Föderationsliste beschrieben.

Tabelle 6: Föderationszugehörigkeit eines Messenger-Service prüfen

AF_10064	Föderationszugehörigkeit eines Messenger-Service prüfen
Akteur	-
Auslöser	Der Messenger-Proxy empfängt oder sendet ein Matrix-Event und MUSS die im Request enthaltenen MXIDs auf Domain-Zugehörigkeit zur TI-Messenger-Föderation prüfen.
Komponenten	<ul style="list-style-type: none"> • Messenger-Proxy • Matrix-Homeserver
Vorbedingungen	keine
Eingangsdaten	Matrix-Event
Ergebnis	Der Messenger-Proxy leitet das Matrix-Event an den Homeserver weiter oder sendet ein HTTP 403 an den Sender. (siehe <input type="checkbox"/> ML-153098 – Missing cross-reference)
Ausgangsdaten	Status

In der Laufzeitsicht sind die Interaktionen zwischen den Komponenten, die durch den Anwendungsfall genutzt werden, dargestellt. Das auslösende Matrix-Event am Messenger-Proxy wird in der folgenden Abbildung nicht gezeigt.

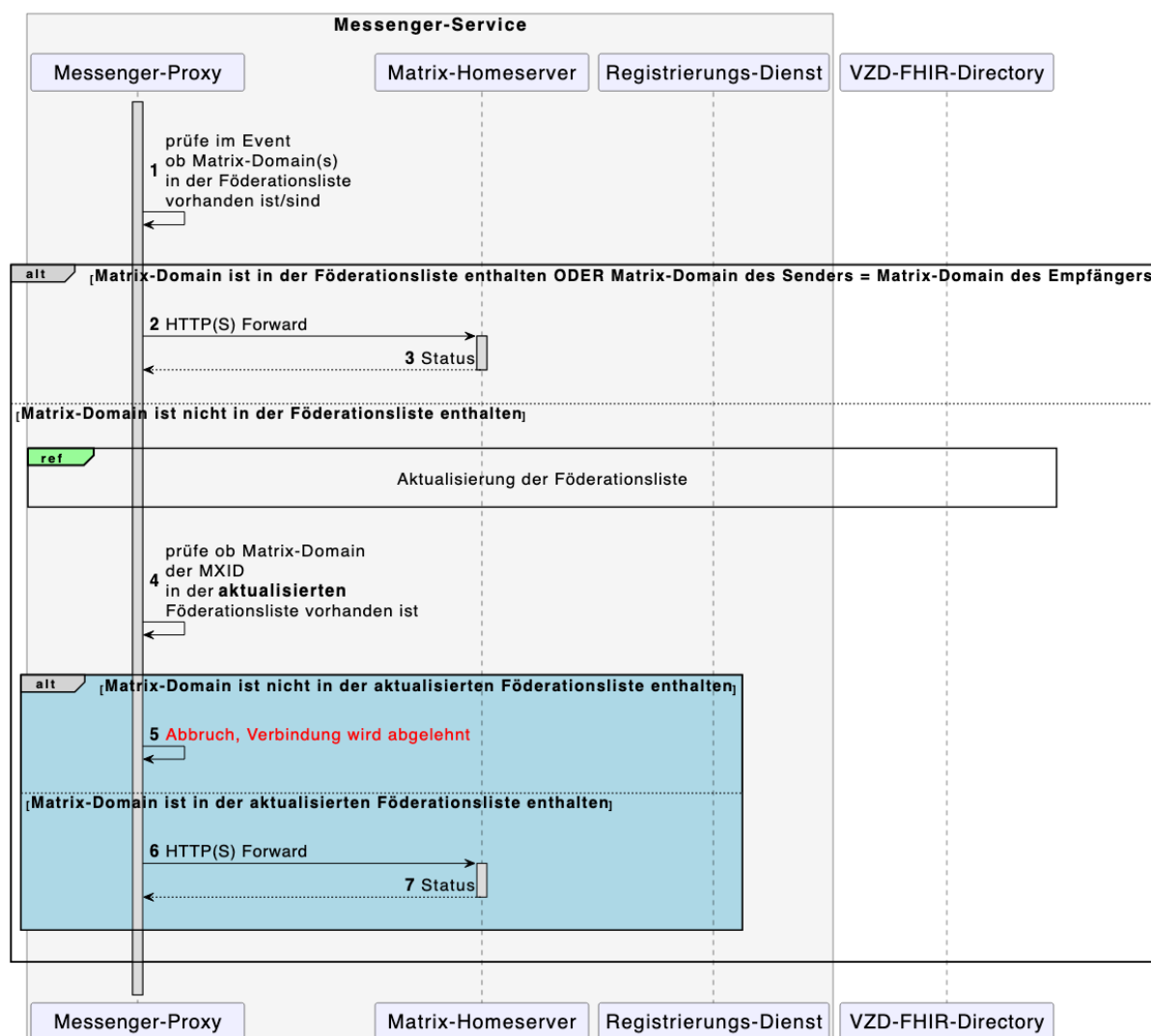


Abbildung 10: Laufzeitsicht - Föderationszugehörigkeit eines Messenger-Service prüfen

[<=]

A_26017 -AF_10064 - Matrix-Domain Teil der Föderationsliste & Aktualitätscheck

Es MUSS sichergestellt werden, dass der Registrierungs-Dienst die Föderationsliste auf Aktualität überprüft, bevor eine aktualisierte Liste durch den Messenger-Proxy abgerufen werden kann. Ebenfalls MUSS sichergestellt werden, dass der Messenger-Proxy tatsächlich überprüft, ob die Matrix-Domain des anderen Messenger-Service Teil der Föderationsliste ist.

[<=]

A_26018 -AF_10064 - Aktualität - Föderationsliste Messenger-Proxy

Es MUSS sichergestellt werden, dass die Föderationsliste vom Messenger-Proxy aktuell ist. Dafür MUSS der Messenger-Proxy in einem festen Intervall von einmal pro Stunde eine aktuelle Liste beim Registrierungs-Dienst anfordern.

[<=]

5.1.4 Austausch von Events zwischen Akteuren innerhalb einer Organisation

AF_10063-01 -Austausch von Events zwischen Akteuren innerhalb einer Organisation

Dieser Anwendungsfall ermöglicht es Akteuren, welche sich in einem gemeinsamen Raum innerhalb eines Messenger-Service befinden, Nachrichten auszutauschen und weitere durch die Matrix-Spezifikation festgelegte Aktionen (Events) auszuführen.

Tabelle 7: Austausch von Events zwischen Akteuren innerhalb einer Organisation

AF_10063	Austausch von Events zwischen Akteuren innerhalb einer Organisation
Akteur	Akteure in der Rolle "User"
Auslöser	Alle Matrix-Events die innerhalb eines Messenger-Service einer Organisation ausgeführt werden
Komponenten	<ul style="list-style-type: none"> • TI-Messenger Client A + B • Messenger-Proxy • Matrix-Homeserver • Push-Gateway
Vorbedingungen	<ol style="list-style-type: none"> 1. Die Akteure sind am selben Messenger-Service angemeldet. 2. Jeder Akteur hat einen zugelassenen TI-M Client. 3. Die Teilnehmer sind einem gemeinsamen Raum beigetreten.
Eingangsdaten	Matrix-Event
Ergebnis	<p>Das Matrix-Event wurde am TI-Messenger Client B erfolgreich verarbeitet.</p> <p>Optional erfolgt eine Benachrichtigung an Akteur B über das Event in dem Chatraum. (Sofern Akteur B Benachrichtigungen für diesen Event-Typ aktiviert hat.)</p>
Ausgangsdaten	Abhängig vom Matrix-Event

In der Laufzeitsicht sind die Interaktionen zwischen den Komponenten, die durch den Anwendungsfall genutzt werden, dargestellt. Hierbei handelt es sich um eine **vereinfachte Laufzeitansicht**, in der zum Beispiel die TLS-Terminierung am Messenger-Proxy auf Grund der Übersichtlichkeit nicht berücksichtigt wurde. Die in der Abbildung rot dargestellten Linien symbolisieren den Kommunikationsverlauf des auslösenden Matrix-Request. Für die vereinfachte Darstellung wird vorausgesetzt, dass

die TI-M Clients der beteiligten Akteure online sind.

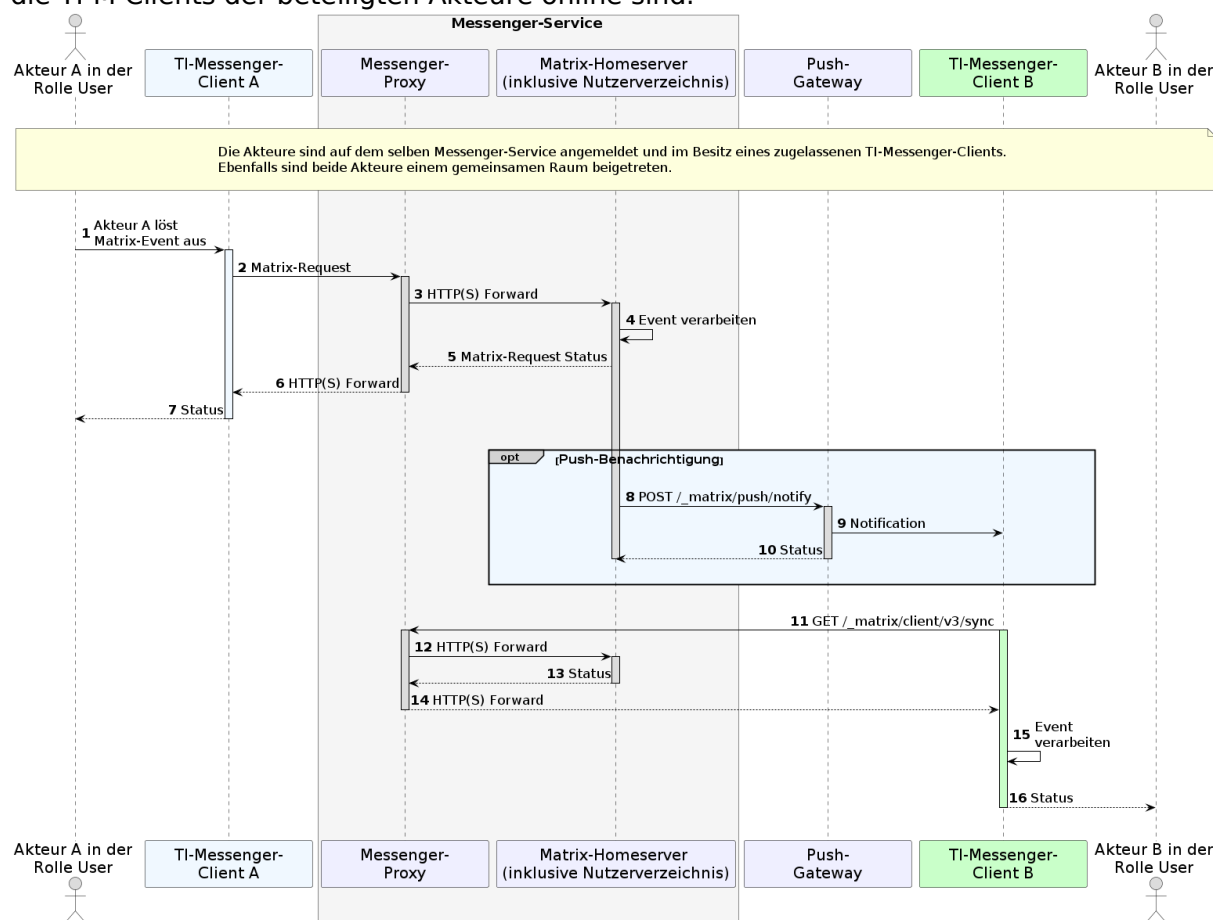


Abbildung 11: Laufzeitsicht - Austausch von Events zwischen Akteuren innerhalb einer Organisation

[<=]

5.1.5 Einladung von Akteuren außerhalb einer Organisation

AF_10061-04 -Einladung von Akteuren außerhalb einer Organisation

In diesem Anwendungsfall wird ein Akteur außerhalb einer Organisation eingeladen. Für die Suche nach Akteuren außerhalb der Organisation kann das VZD-FHIR-Directory verwendet werden. Ist die MXID des gesuchten Akteurs dort nicht vorhanden, muss es die Möglichkeit geben, die Kontaktaufnahme auch auf anderen Wegen zu ermöglichen, mindestens mittels manueller Eingabe der MXID. Weitere Optionen wie z. B. QR-Code-Scans sind zulässig.

Tabelle 8: AF - Einladung von Akteuren außerhalb einer Organisation

AF_10061	Einladung von Akteuren außerhalb einer Organisation
Akteur	Akteur in der Rolle "User"
Auslöser	Akteur A möchte mit Akteur B außerhalb einer Organisation einen gemeinsamen Chatraum einrichten.
Komponenten	<ul style="list-style-type: none"> • TI-Messenger Client A + B • Messenger-Proxy A + B • Matrix-Homeserver A + B • VZD-FHIR-Directory • Push-Gateway B
Vorbedingungen	<ol style="list-style-type: none"> 1. Die Akteure sind an ihren Messenger-Services angemeldet. 2. Die verwendeten Messenger-Services sind Bestandteile der TI-Messenger-Föderation. 3. Einladender ist Mitglied des Chatraums, in den eingeladen wird. 4. Einladender verfügt in diesem Chatraum über einen hinreichenden Powerlevel, um einen Teilnehmer einzuladen zu können.
Eingangsdaten	Invite-Event
Ergebnis	<p>Akteur A und Akteur B sind beide im Chatraum zu dem die Einladung ausgesprochen wurde.</p> <p>Optional erfolgt eine Benachrichtigung an Akteur B über die Einladung in den Chatraum. (Hat Akteur B den Akteur A auf seine BlockedUser-Liste gesetzt, dann erfolgt keine Benachrichtigung.)</p>
Ausgangsdaten	Status

In der Laufzeitsicht sind die Interaktionen zwischen den Komponenten, die durch den Anwendungsfall genutzt werden, dargestellt. Hierbei handelt es um eine **vereinfachte Laufzeitsicht**, in der z. B. die TLS-Terminierung am Messenger-Proxy auf Grund der Übersichtlichkeit nicht berücksichtigt wurde. Details zur optionalen Suche im VZD-FHIR-Directory sind im Anwendungsfall AF_10036 in [gemSpec_VZD_FHIR_Directory] beschrieben. Ebenfalls wurde für eine vereinfachte Darstellung darauf verzichtet, die Berechtigungsprüfung nach 5.2- Berechtigungsmanagement aufzuschlüsseln. In dieser Laufzeitansicht lädt der Akteur A den Akteur B unmittelbar in einen gemeinsamen Chatraum ein.

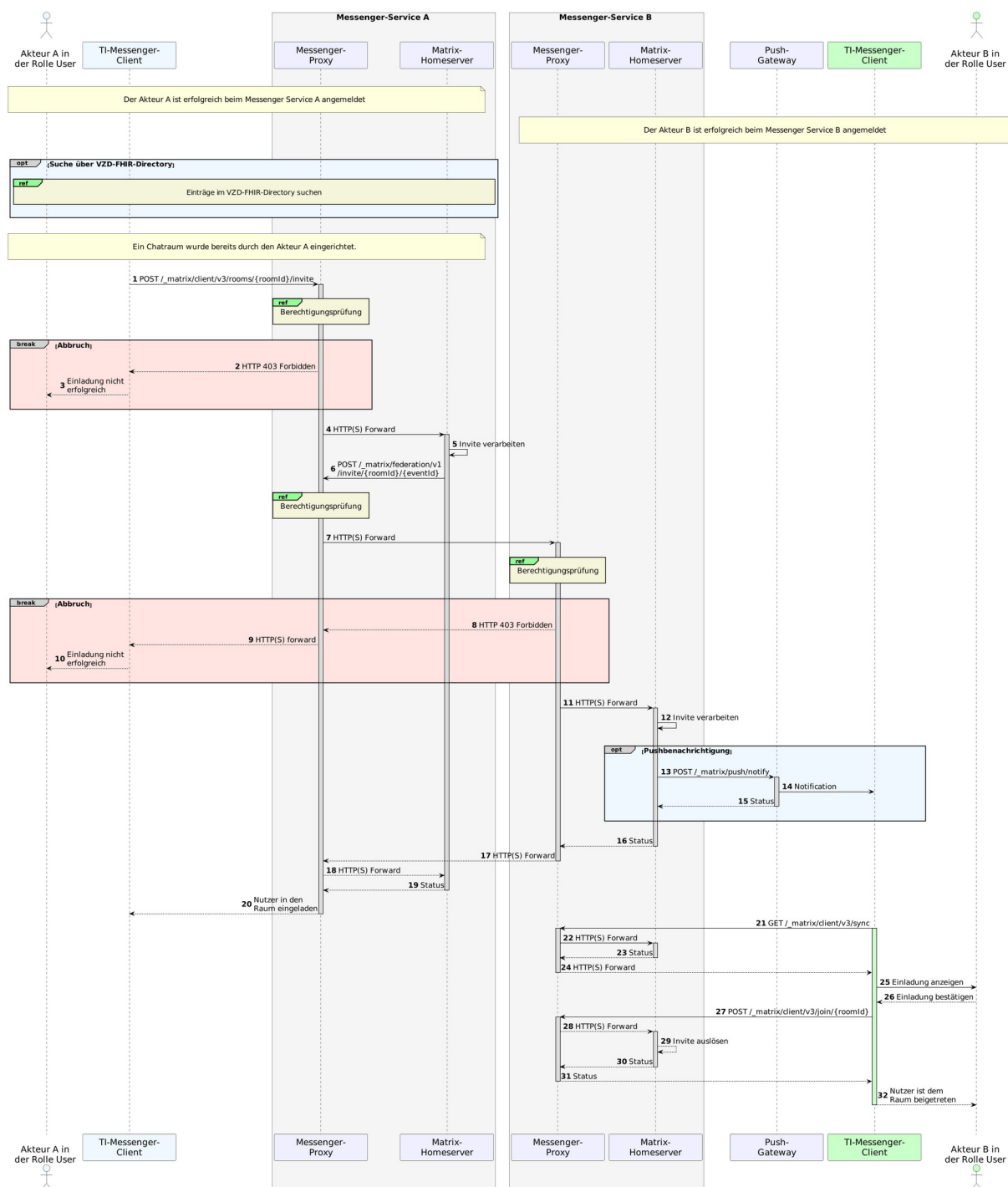


Abbildung 12: Laufzeitsicht - Einladung von Akteuren außerhalb einer Organisation

[<=]

5.1.6 Austausch von Events zwischen Akteuren außerhalb einer Organisation

AF_10062-03 -Austausch von Events zwischen Akteuren außerhalb einer Organisation

In diesem Anwendungsfall können Akteure, welche sich in einem gemeinsamen Raum befinden, Nachrichten austauschen und weitere in der Matrix-Spezifikation festgelegte Aktionen ausführen. Dieser Anwendungsfall setzt die erfolgreiche Annahme eines Invite-Events durch einen oder mehrere beteiligte Akteure voraus. Die Prüfung auf Domainzugehörigkeit findet bei jedem Event der Server-Server Kommunikation statt. In diesem Anwendungsfall sind die beteiligten Akteure in einem gemeinsamen Chatraum und auf unterschiedlichen Messenger-Services verteilt.

Tabelle 9: AF - Austausch von Events zwischen Akteuren außerhalb einer Organisation

AF_10062	Austausch von Events zwischen Akteuren außerhalb einer Organisation
Akteur	Akteur in der Rolle "User"
Auslöser	Alle Matrix-Events die zwischen Messenger-Services unterschiedlicher Organisationen ausgeführt werden.
Komponenten	<ul style="list-style-type: none"> • TI-M Client A + B • Messenger-Proxy A + B • Matrix-Homeserver A + B • Push-Gateway B
Vorbedingungen	<ol style="list-style-type: none"> 1. Die Akteure sind an ihren Messenger-Services angemeldet. 2. Beide Akteure sind Teilnehmer eines gemeinsamen Raumes. 3. Die Messenger-Proxies verfügen über eine aktuelle Föderationsliste.
Eingangsdaten	Matrix-Event
Ergebnis	<p>Das Matrix-Event wurde am TI-Messenger Client B erfolgreich verarbeitet.</p> <p>Optional erfolgt eine Benachrichtigung an Akteur B über das Event in dem Chatraum. (Sofern Akteur B Benachrichtigungen für diesen Event-Typ aktiviert hat.)</p>
Ausgangsdaten	Abhängig vom Matrix-Event, Status

In der Laufzeitsicht sind die Interaktionen zwischen den Komponenten, die durch den Anwendungsfall genutzt werden, dargestellt. Hierbei handelt es um eine **vereinfachte Laufzeitansicht**, in der z. B. die TLS-Terminierung am Messenger-Proxy auf Grund der Übersichtlichkeit nicht berücksichtigt wurde. Es wird in dem Anwendungsfall von lediglich zwei beteiligten Akteuren ausgegangen. Auf die bei der Berechtigungsprüfung nach 5.2. Berechtigungsmanagement durch den Messenger-Proxy notwendigen Interaktionen wird in der Laufzeitsicht verzichtet. Die in der Abbildung rot dargestellten Linien symbolisieren den Kommunikationsverlauf des auslösenden Matrix-Request.

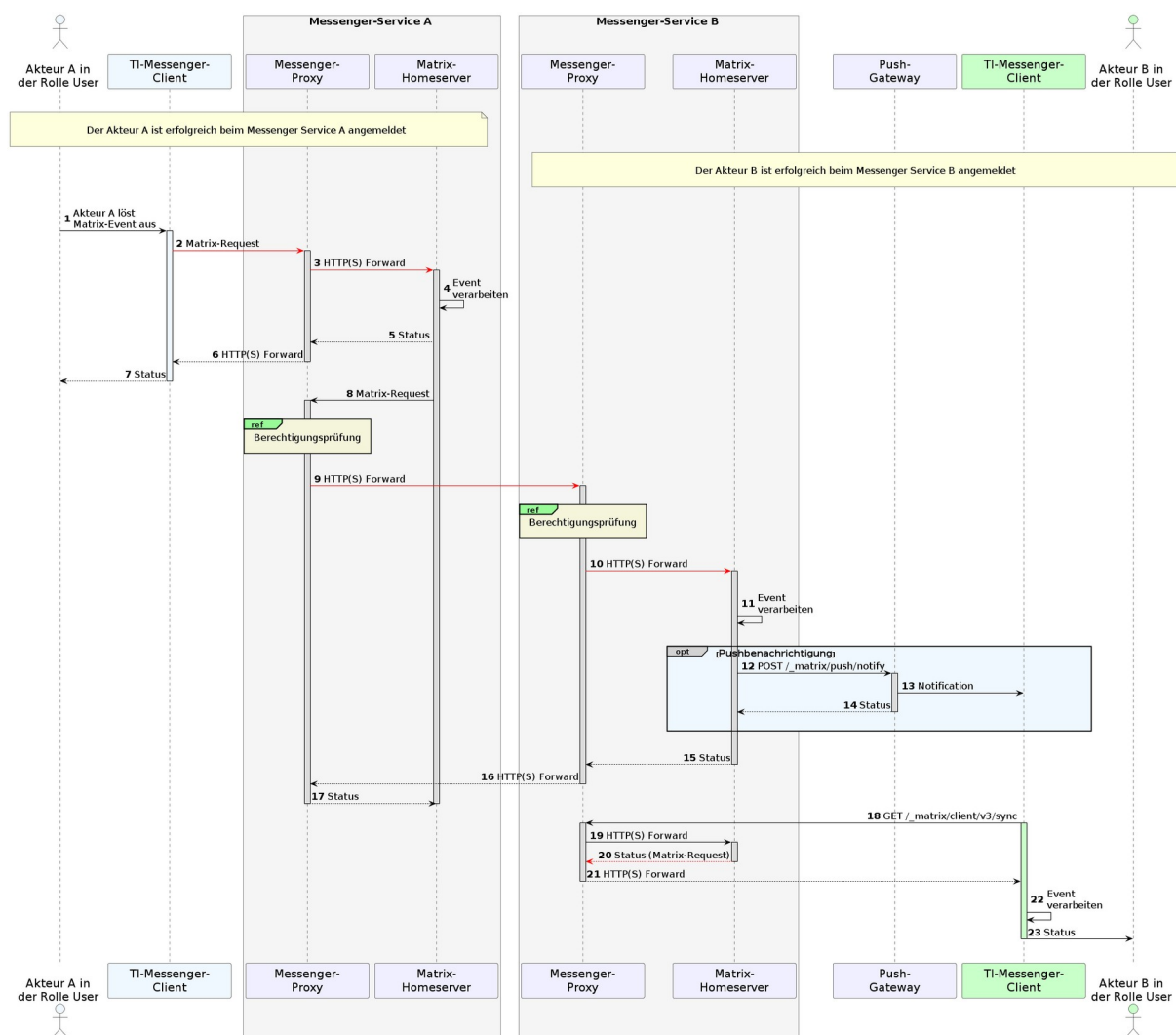


Abbildung 13: Laufzeitsicht - Austausch von Events zwischen Akteuren außerhalb einer Organisation

[<=]

5.1.7 Aktualisierung der Föderationsliste

AF_10378 -Aktualisierung der Föderationsliste

Der Anwendungsfall beschreibt, wie ein TI-M FD ressourcenschonend die Föderationsliste vom VZD-FHIR-Directory aktualisiert und eine aktuelle Kopie der Liste am Registrierungs-Dienst und Messenger-Proxy vorhält.

Tabelle 10: AF - Aktualisierung der Föderationsliste

Attribute	Bemerkung
Akteur	System
Auslöser	<ul style="list-style-type: none"> Scheduler Schnittstelleaufruf

Komponenten	<ul style="list-style-type: none"> • Messenger-Proxy • Registrierungs-Dienst • FHIR-Proxy • Auth-Service
Vorbedingungen	keine
Eingangsdaten	optional: aktuell verwendete Versionsnummer der Föderationsliste (FLVersion_MP) (Wenn die Version übergeben wird, dann wird nur bei einer veralteten Version eine neue Föderationsliste vom VZD-FHIR-Directory bereitgestellt.)
Ergebnis	Der Messenger-Proxy erhält die Information, eine aktuelle Liste zu besitzen, oder eine neue Föderationsliste, sofern eine aktuellere Version vorliegt.
Ausgangsdaten	<ul style="list-style-type: none"> • status • Föderationsliste • x5c-Zertifikatsliste (enthält mindestens das Signaturzertifikat als erstes Element)

Die folgende Abbildung beschreibt, wie der Messenger-Proxy seine lokal vorgehaltene Föderationsliste aktualisiert. Für die Aktualisierung der Föderationsliste muss der Messenger-Proxy diese beim Registrierungs-Dienst seines TI-M FD anfragen. Hierbei übergibt der Messenger-Proxy die durch ihn gespeicherte Versionsnummer der Föderationsliste im Request an den Registrierungs-Dienst. Die Prüfung auf Aktualität erfolgt durch den Abgleich der Versionen der Föderationslisten. Bei Übereinstimmung der Versionsnummer wird für den Messenger-Proxy keine neue Föderationsliste durch den Registrierungs-Dienst bereitgestellt. Ist die Versionsnummer größer als die vom Messenger-Proxy übergebene, dann wird durch den Registrierungs-Dienst eine aktualisierte Föderationsliste zur Verfügung gestellt. Bei jeder Anfrage eines Messenger-Proxys beim Registrierungs-Dienst nach einer aktuellen Föderationsliste muss der Registrierungs-Dienst die Aktualität der durch ihn ausgelieferten Liste sicherstellen, indem er die von ihm gespeicherte Version der Föderationsliste im Bedarfsfall mit einer aktuelleren Version, die vom FHIR-Proxy bezogen wurde, überschreibt. Ein Download der Föderationsliste ist nur notwendig, wenn eine neuere Version auf dem FHIR-Proxy existiert. Die Struktur der Föderationsliste ist in [gemSpec_VZD_FHIR_Directory] beschrieben. Nach dem Abruf der Föderationsliste vom Registrierungs-Dienst, durch den Messenger-Proxy, muss dieser die Signatur der Föderationsliste prüfen.

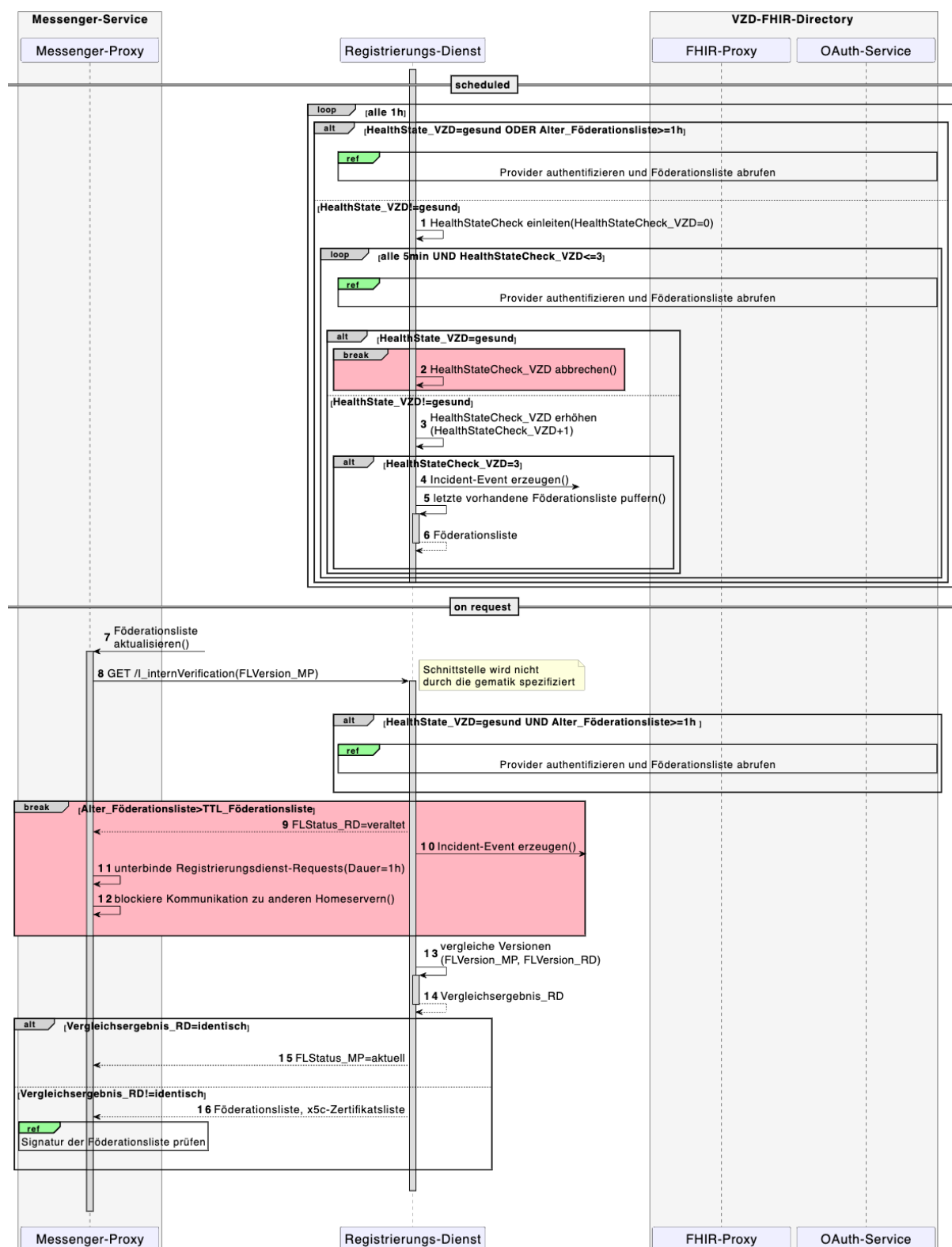


Abbildung 14: Laufzeitansicht - Aktualisierung der Föderationsliste

Das in der Abbildung "Laufzeitansicht - Aktualisierung der Föderationsliste" referenzierte Sequenzdiagramm "Provider authentifizieren und Föderationsliste abrufen":

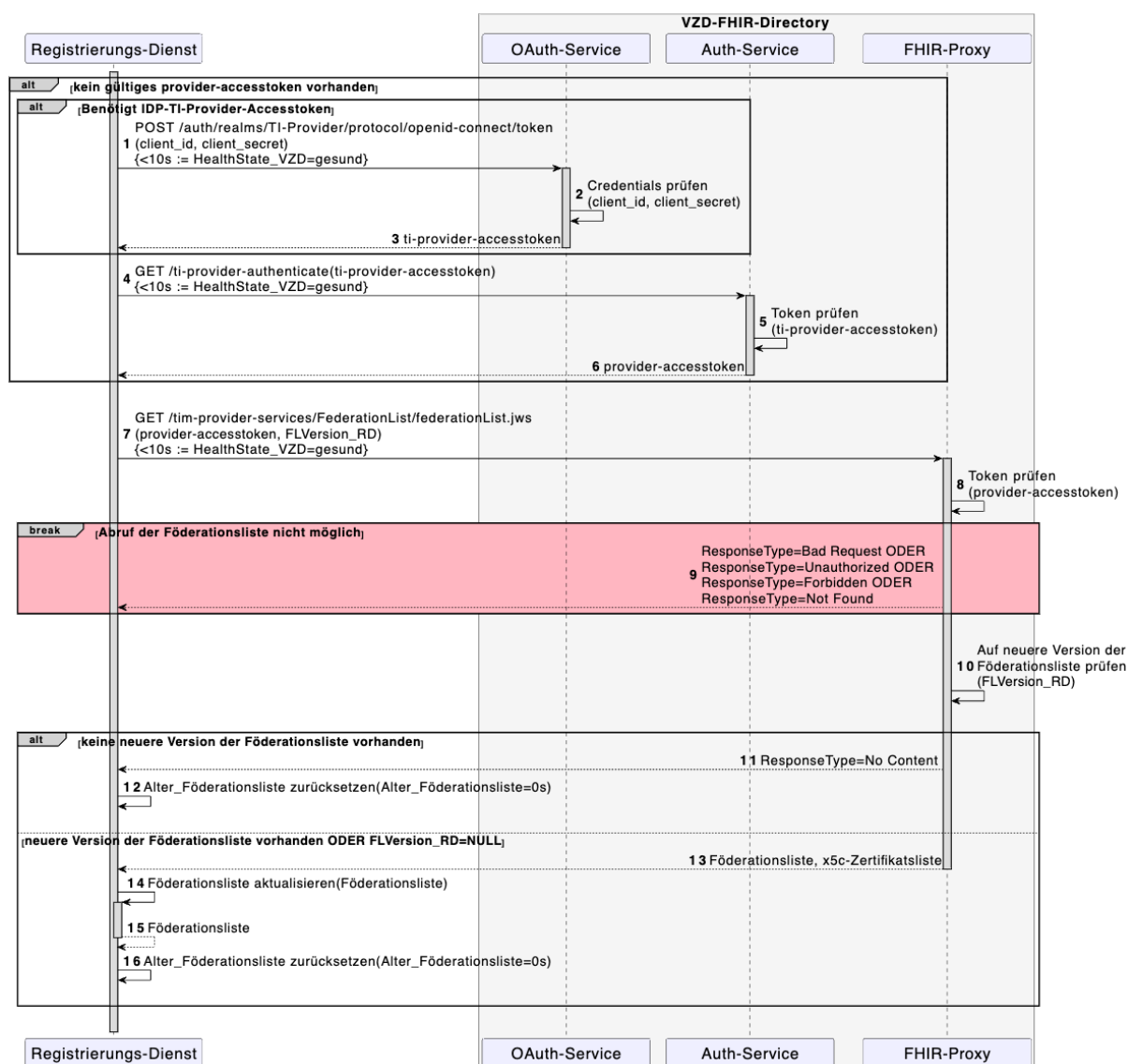


Abbildung 15: Provider authentifizieren und Föderationsliste abrufen

Das in der Abbildung "Laufzeitansicht - Aktualisierung der Föderationsliste" referenzierte Sequenzdiagramm "Signatur der Föderationsliste prüfen":



Abbildung 16: Signatur der Föderationsliste prüfen

[<=]

A_25637-01 -Aktualisierung der Föderationsliste

Der Registrierungs-Dienst MUSS die Föderationsliste stündlich abfragen. Die Prüfung auf Aktualität der Föderationsliste des Registrierungs-Dienstes MUSS zusätzlich bei jeder Anfrage durch einen Messenger-Proxy zur Bereitstellung der Föderationsliste über eine Abfrage beim FHIR-Proxy des VZD-FHIR-Directory erfolgen, sofern die durch den Registrierungs-Dienst vorgehaltene Föderationsliste älter als eine Stunde ist. [<=]

A_26413 -Attribute des Registrierungsdienstes für Aktualisierungsfunktionalität der Föderationsliste

Der Registrierungs-Dienst MUSS folgende Attribute und ihre Typen definieren und vorhalten:

Tabelle 11: Spezifische Attribute für das Handling der Föderationsliste am Registrierungs-Dienst

Attribut	Typ	Beschreibung	Wertebereich
HealthState_VZD	Zustand	Typ hält Gesundheitszustand von Komponenten des VZD-FHIR-Directorys auf Basis ihres Antwortverhaltens vor.	gesund, ungesund
HealthStateCheck_VZD	hochzählen der Iterator	Typ hält die Menge der Wiederholungsversuche der Prüfung des Gesundheitszustand es des VZD-FHIR-Directory vor.	$0 \leq \text{HealthStateCheck_VZD} \leq 3$

Alter_Föderationsliste	hochzählen der Zeitzähler	Typ hält das aktuelle Alter der Föderationsliste ab dem Zeitpunkt der letzten Aktualisierung vor.	min: 0s
TTL_Föderationsliste	Lebensdauer	Typ beschreibt den oberen Grenzwert, den eine Föderationsliste alt sein darf.	Konstanter Wert: 72h

[<=]

A_26415 -Abfrage der Föderationsliste am VZD-FHIR-Directory

Der Registrierungs-Dienst MUSS die aktuelle TI-M Föderationsliste anhand eines gültigen provider-accesstoken am VZD-FHIR-Directory abrufen und an der internen Schnittstelle I_internVerification bereitstellen. Für den Abruf MUSS die am FHIR-Proxy des VZD-FHIR-Directory bereitgestellte Operation getFederationList (GET /tim-provider-services/FederationList/federationList.jws) aufgerufen werden.[<=]

A_25638 -Caching der Föderationsliste nach Abfrage beim VZD-FHIR-Directory

Der Registrierungs-Dienst MUSS die Föderationsliste für Abfragen der Messenger-Proxies cachen, um nicht bei jeder Anfrage eines Proxies eine Anfrage an das VZD-FHIR-Directory zu stellen.[<=]

A_26417 -Prüfung des HealthState und Änderung der Vorhaltezeit der Föderationsliste

Der Registrierungs-Dienst MUSS seine eigene Vorhaltezeit der Föderationsliste auf einen festgelegten Wert von 72 Stunden (TTL_Föderationsliste) verlängern, sofern das VZD-FHIR-Directory nicht innerhalb einer definierten Antwortzeit erreichbar und weitere Aktualisierungsversuche erfolglos bleiben (HealthState_VZD und HealthStateCheck_VZD).[<=]

A_25636 -Maximale Alter der Föderationsliste

Der Messenger-Proxy MUSS die Kommunikation zu anderen Matrix-Homeservern einstellen, wenn Alter_Föderationsliste den Wert von TTL_Föderationsliste erreicht.[<=]

Hinweis: Die Vorhaltung einer aktuellen Föderationsliste ist aus sicherheitstechnischer Perspektive sinnvoll, um das Zeitfenster klein zu halten, in welchem ein Fachdienst "unwissentlich" mit einem anderen Fachdienst interagiert, der nicht mehr Teil der Föderation 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 andere Kommunikationsdienste innerhalb der TI eingeräumt werden.

A_26418 -Prüfung des HealthState der Föderationsliste und Auslösen eines Incidents

Der Registrierungs-Dienst MUSS ein Incident-Event erzeugen, welches durch ein Drittsystem aufgefangen werden kann (z. B. ein ITSM-System) und es MUSS ein Incident beim VZD-FHIR-Directory-Anbieter eingestellt werden, sofern das VZD-FHIR-Directory nicht innerhalb einer definierten Antwortzeit erreichbar und weitere Aktualisierungsversuche erfolglos bleiben (HealthState_VZD und HealthStateCheck_VZD).[<=]

A_26419 -Weiternutzung einer vorgehaltenen Föderationsliste im Falle eines Incidents

Der Registrierungs-Dienst MUSS die vorgehaltene Föderationsliste weiterhin bereitstellen, bis zur Behebung eines Aktualisierungsstörfalls bzw. -incidents, aber höchstens bis zum Erreichen der festgelegten Vorhaltezeit (TTL_Föderationsliste).[<=]

A_26421 -Prüfung der Signatur der Föderationsliste durch Messenger-Proxy

Der Messenger-Proxy MUSS sicherstellen, dass seine lokale Kopie der Föderationsliste nur dann aktualisiert wird, wenn die Signatur der Föderationsliste anhand des Signaturzertifikats gültig ist.[<=]

5.2 Berechtigungsmanagement

Das Berechtigungsmanagement sieht 2 Stufen der Prüfung vor. Zuerst erfolgt eine Prüfung der Föderationszugehörigkeit bei ein- und ausgehender Kommunikation und anschließend eine Prüfung der akteurspezifische Berechtigungskonfiguration auf Empfängerseite. Beide Stufen werden vom TI-M Fachdienst durchgesetzt.

5.2.1 Prüfung der Föderationszugehörigkeit

Die Zugehörigkeit zur Föderation wird durch Abgleich von Matrix Servernamen (siehe [Matrix Appendices/#server-name]) gegen die Föderationsliste geprüft. Bei Fehlschlag wird die Föderationsliste zunächst aktualisiert bevor anschließend eine neuerliche Prüfung durchgeführt wird. Schlägt auch diese Prüfung fehl, so wird die Anfrage abgelehnt.

A_25537-01 -Aktualisierung der Föderationsliste bei fehlgeschlagener Föderationsprüfung

Kann ein zu prüfender Servername nicht in der Föderationsliste gefunden werden, so MUSS der TI-M Fachdienst zunächst bei seinem Registrierungs-Dienst eine neue Version abrufen.[<=]

A_25534-01 -Fehlschlag der Föderationsprüfung nach Aktualisierung

Kann nach Aktualisierung der Föderationsliste ein Servername weiterhin nicht in der Liste gefunden werden, so MUSS der TI-M Fachdienst die Anfrage mit HTTP 403 und dem FehlercodeM_FORBIDDEN ablehnen.[<=]

5.2.1.1 Client-Server Prüfungen

A_25368-01 -Maximal eine Einladung in /createRoom

Der TI-M Fachdienst MUSS beim Anlegen eines Raumes mittels /createRoom sicherstellen, dass der Parameter invite mit maximal einer MXID befüllt ist und die Anfrage andernfalls mit HTTP 400 und dem FehlercodeM_FORBIDDEN ablehnen.[<=]

A_25532-01 -Föderationsprüfung von Einladungen

Der TI-M Fachdienst MUSS bei Einladung per /invite oder /createRoom die eingeladene MXID auf Föderationszugehörigkeit prüfen.[<=]

A_26328-01 -Föderationsprüfung eingehender Medienanfragen

Der TI-M Fachdienst MUSS bei eingehender Kommunikation auf folgenden Endpunkten die Pfadkomponente {serverName} auf Föderationszugehörigkeit prüfen:

- GET /_matrix/media/v3/download/{serverName}/{mediaId}
- GET /_matrix/media/v3/download/{serverName}/{mediaId}/{fileName}

- GET /_matrix/media/v3/thumbnail/{serverName}/{mediaId}

[<=]

5.2.1.2 Server-Server Prüfungen

A_25540-02 -Föderationsprüfung eingehender authentifzierter Kommunikation

Ist auf einem eingehenden Request im Authorization-Header das Attribut origin¹ gesetzt, so MUSS der TI-M Fachdienst den enthaltenen Servernamen auf Föderationszugehörigkeit prüfen.

¹ [Server-Server API/#request-authentication][<=]

A_25541-02 -Föderationsprüfung ausgehender authentifzierter Kommunikation

Ist auf einem ausgehenden Request im Authorization-Header das Attribut destination¹ gesetzt, so MUSS der TI-M Fachdienst den enthaltenen Servernamen auf Föderationszugehörigkeit prüfen.

¹ [Server-Server API/#request-authentication][<=]

A_26329-01 -Föderationsprüfung ausgehender .well-known Anfragen

Der TI-M Fachdienst MUSS bei ausgehender Kommunikation zum Endpunkt /.well-known/matrix/server den im Host-Header enthaltenen Servernamen auf Föderationszugehörigkeit prüfen.[<=]

A_26341-01 -Föderationsprüfung ausgehender Medienanfragen

Der TI-M Fachdienst MUSS bei ausgehender Kommunikation auf folgenden Endpunkten die Pfadkomponente {serverName} auf Föderationszugehörigkeit prüfen:

- GET /_matrix/media/v3/download/{serverName}/{mediaId}
- GET /_matrix/media/v3/download/{serverName}/{mediaId}/{fileName}
- GET /_matrix/media/v3/thumbnail/{serverName}/{mediaId}

[<=]

5.2.2 Akteursspezifische Berechtigungskonfiguration

Neben der Föderationszugehörigkeitsprüfung, soll der TI-Messenger Akteur steuern können, wer ihn zum Chat in neue Räume einladen darf, damit er selbst die Kontrolle über sein Chataufkommen erhält. Hierbei werden u. a. folgende Funktionen abgedeckt:

- Jeder andere TI-Messenger Akteur darf einladen.
- Nur interne TI-Messenger Akteure (gleiche Organisation) dürfen einladen.
- Nur TI-Messenger Akteure auf einer Allow-List dürfen einladen.
- Alle TI-Messenger Akteure außer solche auf einer Block-List dürfen einladen.

5.2.2.1 Berechtigungen setzen

Die folgenden Grafiken illustrieren den Vorgang zum Setzen der Berechtigungen.

TI-Messenger

Wer darf mich kontaktieren?

☒ Jeder

☐ Niemand

Ausnahmen

Server: gematik.de -

MXID:@DrMeier:mypraxis.de -

+ Weitere Kategorie hinzufügen

Abbildung 17: Beispielhaftes UI zum Setzen der Berechtigungen

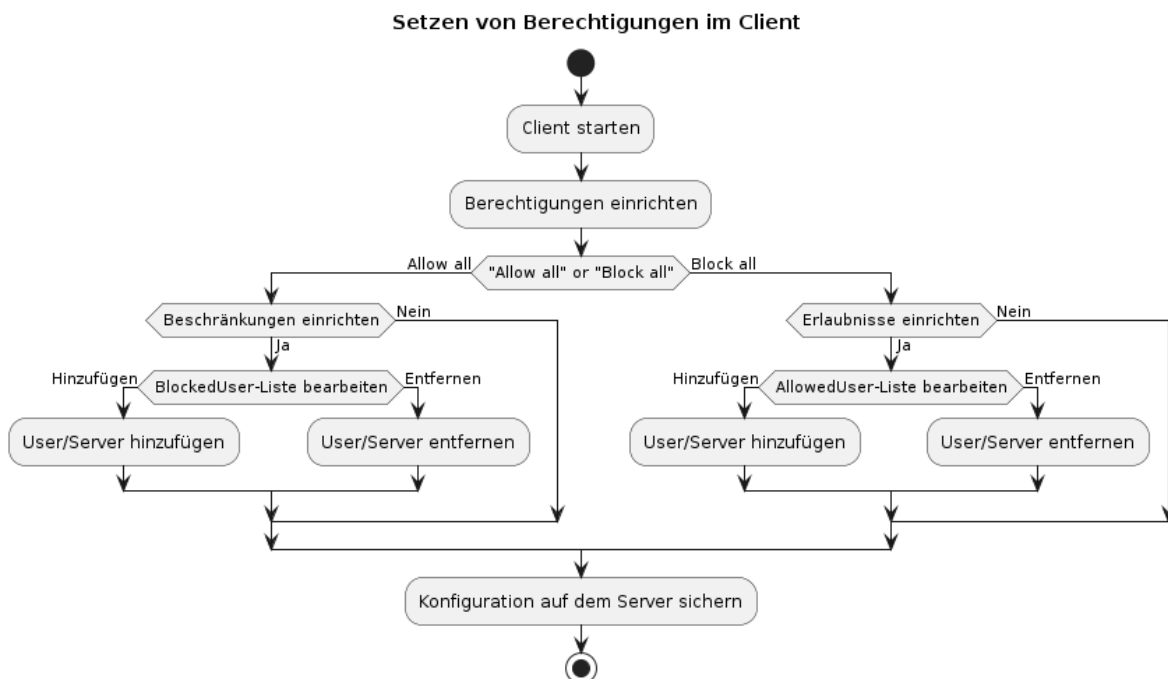


Abbildung 18: Logischer Ablauf beim Setzen der Berechtigungen

Die Berechtigungskonfiguration soll so aufgesetzt werden, dass diese in der Zukunft erweitert werden kann. Durch die TI-Messenger Basisspezifikation werden die folgenden Einstellungen unterstützt:

- Aufnahme einzelner MXID der Akteure
- Aufnahme einzelner Servernamen (siehe [Matrix Appendices/#server-name])

A_25045-02 -Funktionsumfang der Berechtigungskonfiguration im User Interface

Der TI-M Client MUSS in seinem UI für die Konfiguration der Berechtigungen folgende Varianten unterstützen:

1. Basiseinstellung ist "allow all" und der Akteur pflegt eine Block-List.
2. Basiseinstellung ist "block all" und der Akteur pflegt eine Allow-List.

Auf der Block- bzw. Allow-List MÜSSEN mindestens einzelne User eingetragen werden können. [≤]

A_26016 -Basiseinstellung vorgeben

Der TI-M Client MUSS ermöglichen, dass ein TI-Messenger-Anbieter die Basiseinstellung der Berechtigungskonfiguration vordefinieren kann. [≤]

A_25043 -Berechtigungskonfiguration in Accountdaten speichern

Der TI-M Client MUSS die Berechtigungskonfiguration aus den Accountdaten des Matrix-Homeservers [Client-Server API/#client-config] beziehen und Änderungen an der Berechtigungskonfiguration in den Accountdaten des Matrix-Homeservers speichern. [≤]

5.2.3 Berechtigungsprüfung

Die akteurspezifische Berechtigungskonfiguration wird durch den TI-M Fachdienst durchgesetzt. Hierfür prüft der Fachdienst eingehende Invites gegen die hinterlegte Konfiguration. Ist eine Einladung nicht erlaubt, lehnt der Fachdienst sie ohne Weiterleitung zum Akteur ab.

A_26021-01 -Durchsetzung der akteurspezifischen Berechtigungskonfiguration

Der TI-M Fachdienst MUSS eingehende Einladungen gegen die vom Akteur hinterlegte Berechtigungskonfiguration prüfen und nicht erlaubte Einladungen mit HTTP 403 und dem Fehlercode M_FORBIDDEN ablehnen. [≤]

5.3 Push-Benachrichtigungen

In den folgenden Kapiteln wird dargestellt, wie im Kontext vom TI-Messenger Push-Benachrichtigungen realisiert werden. Die Kapitel beschreiben exemplarisch die Einrichtung und den Empfang von Push-Benachrichtigungen. Im Anschluss wird in den einzelnen Kapiteln auf die Anforderungen an die beteiligten Komponenten eingegangen.

5.3.1 Push-Konfiguration

Die folgende Grafik verdeutlicht beispielhaft den Ablauf zur Einrichtung der Push-Konfiguration an Gateway und Homeserver.

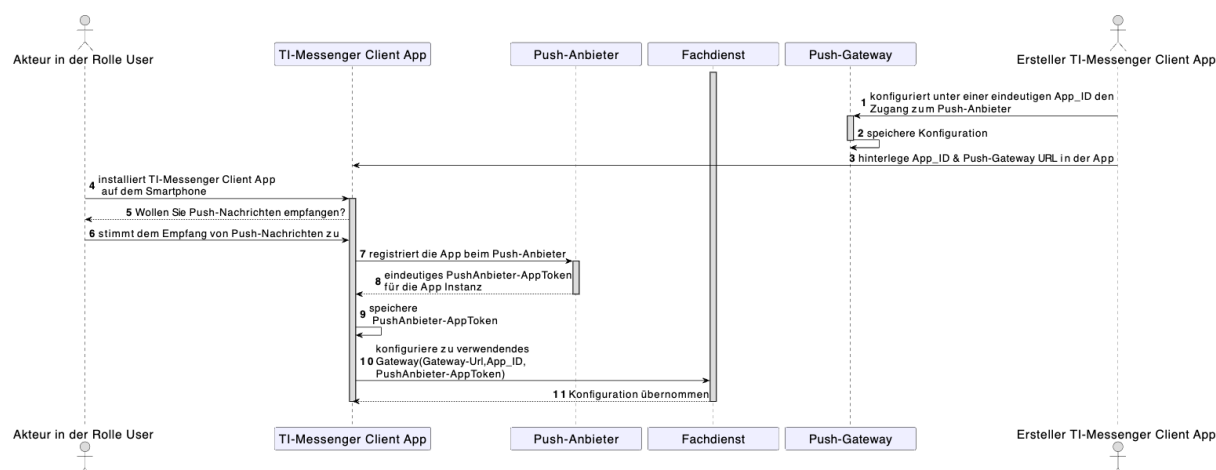


Abbildung 19: Push-Konfiguration

- Der Ersteller der TI-Messenger Client App hinterlegt unter einer eindeutigen App-ID die Zugangsinformationen für den jeweiligen Push-Anbieter. Z. B. unter einer ID die Zugangsdaten zu FCM, um Android-Geräte mit Benachrichtigungen versorgen zu können und unter einer anderen ID die Zugangsdaten zu APN, um IOS-Geräte beliefern zu können.
- Der Ersteller der TI-Messenger Client App hinterlegt in der App die gerade angelegte App-ID und die Push-Gateway URL
- Ein Akteur in der Rolle "User" installiert einen TI-Messenger Client auf seinem Endgerät
- Der Akteur stimmt dem Nutzen von Push-Nachrichten zu
- Die App registriert sich beim Push-Anbieter und erhält ein PushAnbieter-AppToken über das sich die App eindeutig identifizieren lässt.
- Die App konfiguriert am Homeserver das zu verwendende Push-Gateway u.a. über die Parameter Gateway-Url, die App_ID und den PushAnbieter-AppToken

Hinweis: Zur besseren Übersichtlichkeit wurden nicht alle Parameter im Diagramm aufgeführt, die an den APIs notwendig wären.

Hinweis: Der datenschutzrechtlich Verantwortliche für die TI-M Clients hat vor und während der Verwendung von Push-Anbietern zu prüfen ob diese eine rechtmäßige Datenverarbeitung erlauben. Insbesondere ist hierfür eine kontinuierliche Prüfung auf das Vorhandensein eines Angemessenheitsbeschlusses für das Zielland erforderlich.

5.3.2 Push-Zustellung

Unterschiedliche Ereignisse (Erwähnungen, Einladungen, etc.) können je nach Konfiguration dazu führen, dass eine Benachrichtigung auf dem Endgerät des Akteurs erscheinen soll. Das folgende Diagramm zeigt den exemplarischen Ablauf einer Zustellung.

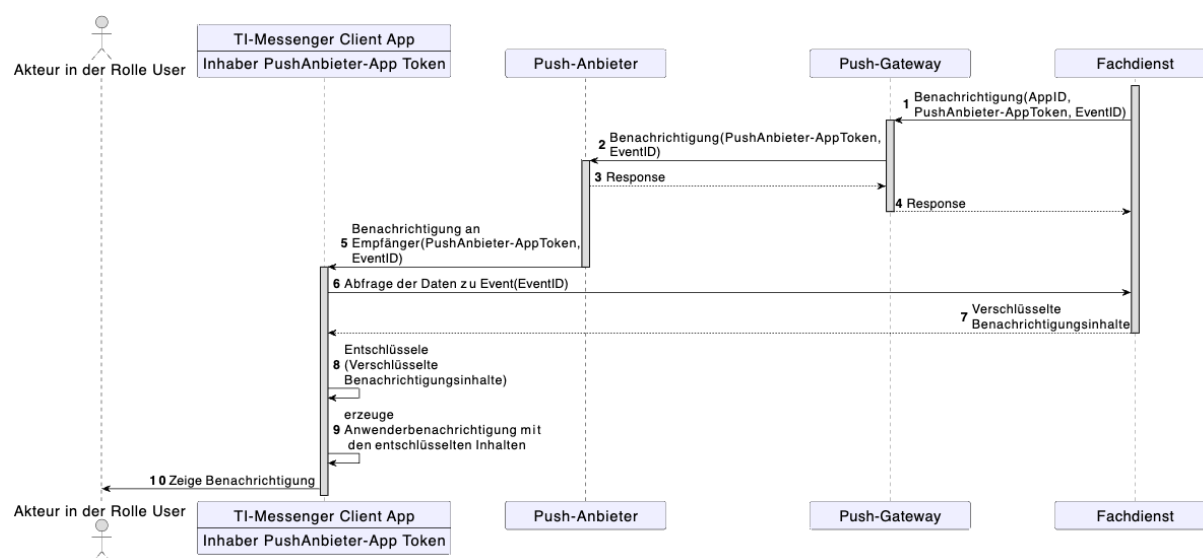


Abbildung 20: Push-Zustellung

- Durch ein Ereignis ausgelöst, weist der Fachdienst das für die App konfigurierte Push-Gateway an, eine Benachrichtigung an ein Endgerät oder mehrere Endgeräte zu senden.
- Das Push-Gateway ermittelt über die empfangene App_ID den zu verwendenden Push-Anbieter und sendet den Benachrichtigungsinhalt und den eindeutigen Push-Anbieter-AppToken an diesen.
- Der Push-Anbieter übermittelt die Benachrichtigung und den Push-Anbieter-AppToken an das passende Endgerät.
- Das Betriebssystem informiert die TI-Messenger Client App über neue Benachrichtigung
- Die TI-Messenger Client App fragt beim Homeserver die zur EventID passenden Inhalte ab
- Die TI-Messenger Client App entschlüsselt die Inhalte bei Bedarf und erzeugt eine Notification auf dem Endgerät

Hinweis: Zur besseren Übersichtlichkeit wurden nicht alle Parameter im Diagramm aufgeführt, die an den APIs notwendig wären.

5.3.3 TI-M Client App

Die TI-M Client Apps registrieren sich beim Push-Anbieter und erhalten ein PushAnbieter-AppToken. Der TI-M Client muss sicherstellen, dass das PushAnbieter-AppToken sicher auf dem Endgerät verwahrt wird und nicht missbräuchlich verwendet werden kann.

A_22965-01 -Push-Benachrichtigungen Messenger-Anbieter

TI-Messenger-Anbieter MÜSSEN sicherstellen, dass Push-Benachrichtigungen erst nach expliziter Zustimmung der Nutzer erfolgen (Opt-In) dürfen. [≤=]

5.3.4 Push-Gateway

Ein Push-Gateway wird vom Hersteller der TI-M Client App zur Verfügung gestellt und ist ein Server, der Ereignisbenachrichtigungen von Matrix-Homeservern über definierte Schnittstellen empfängt und diese an andere Push-Dienste weiterleitet.

A_25033 -Bereitstellung Push Gateway

Für TI-M Clients für mobile Szenarien MUSS ein Push-Gateway bereitgestellt werden, über welches die App mit Push-Benachrichtigungen beliefert wird. [≤]

A_25286 -Push-Gateway API

Das Push-Gateway MUSS für Homeserver eine API gemäß [Push Gateway API] bereitstellen. [≤]

5.3.5 TI-M FD

Der TI-Messenger Fachdienst ist flexibel in Bezug auf Push-Benachrichtigungen. Über eine API, kann eine TI-Messenger Client App das von Ihr gewünschte Push-Gateway konfigurieren. Neben dem Gateway kann der Akteur in der Rolle "User" über die [Client-Server API/#push-notifications] konfigurieren, für welche Ereignisse Benachrichtigungen erwünscht sind.

A_25034 -TI-M Fachdienst - Push Notifications Datenschutz

Der TI-M Fachdienst MUSS das Push-Format "event_id_only" beim Anlegen eines Pushers über die [Client-Server API/#push-notifications] durchsetzen. [≤]

A_22808-01 -Push-Benachrichtigungen Timing

Push-Nachrichten MÜSSEN vor dem Versenden um einen Zufallswert von 0-10 Sekunden verzögert werden, um timingbasierte Profilbildung zu erschweren. [≤]

5.4 Raumversionen

Raumversionen sind ein zentraler Bestandteil von Matrix und definieren strikte Regeln für erlaubte Inhalte und Operationen in Räumen. Im Folgenden sind Anforderungen an TI-M Clients und Fachdienste festgehalten, durch die sowohl Interoperabilität als auch zukünftige Erweiterungen im Zusammenhang mit Raumversionen gewährleistet werden.

A_26200 -Unterstützte Raumversionen am Client

Der TI-M Client MUSS die Raumversionen 9, 10 und 11 gemäß [Room Versions] unterstützen. [≤]

A_26201 -Unterstützte Raumversionen am Fachdienst

Der TI-M Fachdienst MUSS die Raumversionen 9, 10 und 11 gemäß [Room Versions] unterstützen. [≤]

A_26202 -Erlaubte Raumversionen beim Erstellen von Räumen

Der TI-M Fachdienst MUSS die Verwendung anderer Raumversionen als 9 und 10 beim Erstellen von Räumen verhindern, z. B. indem er entsprechende Requests an den Endpunkt /createRoom mit einer HTTP 400 Response ablehnt. [≤]

A_26248 -Default-Raumversion beim Erstellen von Räumen

Der TI-M Fachdienst MUSS beim Erstellen von Räumen standardmäßig Raumversion 10 verwenden, sofern vom TI-M Client keine andere Version angefragt wurde. [≤]

A_26203 -Erlaubte Raumversionen beim Upgrade von Räumen

Der TI-M Fachdienst MUSS Upgrades auf andere Raumversionen als 9 und 10 verhindern, z. B. indem er entsprechende Requests an den Endpunkt /rooms/{roomId}/upgrade mit einer HTTP 400 Response ablehnt. [≤]

5.5 TI-M spezifische Kommunikation

Das Matrix-Protokoll erlaubt die Definition eigener Raumtypen (*Custom Room Types*), um verschiedene Anwendungsszenarien für Räume zu unterscheiden. Der Raumtyp kann dafür bei der Erzeugung eines Raumes am `/createRoom` Endpunkt übergeben werden. Des Weiteren sieht das Matrix-Protokoll vor, bestimmte Eigenschaften von Räumen durch *State Events* wie z. B. `m.room.name` und `m.room.topic` festzulegen. Insbesondere können auch eigene *State Events* (*Custom State Events*) verwendet werden.

In der vorliegenden Spezifikation werden bereits erste *Custom Room Types* und *Custom State Events* mit von der gematik vorgegebenem *Event Type* und *Event Content* definiert. Dies ermöglicht im Kontext des TI-Messengers die Unterstützung spezieller Anwendungsfälle durch eine spezifischere, strukturiertere und gerichtete Kommunikation, als es mit Standard Matrix-Räumen möglich wäre.

Konkret wird im Folgenden zunächst ein Basis-Anwendungsfall und dessen systemseitige Implikationen beschrieben, die von jeder Produktlinie des TI-Messengers unterstützt werden müssen.

Weiterhin werden Definitionen für die föderierte und intersektorale Kommunikation eingeführt. Hierbei ist zu einem späteren Zeitpunkt vorgesehen, vordefinierte FHIR-Objekte im *Event Content* von *Custom State Events* zu hinterlegen.

5.5.1 Basis-Anwendungsfall

Um TI-M spezifische Kommunikation gezielt beschreiben zu können, werden die Standard *State Events* `m.room.name` und `m.room.topic` durch folgende *Custom State Events* ergänzt:

Custom State Event

Event type: "de.gematik.tim.room.name"
 Event state_key: <leer> (0-Längen-Zeichenkette)
 Event content: <name: festgelegter Raumname>

Custom State Event

Event type: "de.gematik.tim.room.topic"
 Event state_key: <leer> (0-Längen-Zeichenkette)
 Event content: <topic: festgelegtes Raumthema>

5.5.1.1 TI-M Client

Der TI-M Client erzeugt und verwendet die *Custom State Events* `de.gematik.tim.room.name` und `de.gematik.tim.room.topic` in dafür vorgesehenen Räumen. Die Standard *State Events* `m.room.topic` und `m.room.name` werden mit denselben Werten befüllt wie die *Custom State Events*.

Hinweis: Die Custom State Events für Raumname und Topic wurden verfrüht eingeführt und erfüllen aktuell keinen Zweck. Die Standard State Events duplikativ mit denselben Werten zu befüllen wie die Custom State Events soll die Kompatibilität erhöhen und ein zukünftiges Entfernen der Custom State Events ermöglichen.

A_26338-02 -Erzeugung und Verwendung der Custom State Events für Raumnamen und -thema

Verwendet der TI-M Client in einem Raum des Typs `de.gematik.tim.roomtype.*` die Standard *State Events* `m.room.name` oder `m.room.topic`, so MUSS er auch die *Custom State Events* `de.gematik.tim.room.name` bzw. `de.gematik.tim.room.topic` mit identischem Schema und Inhalt verwenden.【<=】

Hinweis: Die "Verwendung" der Custom State Events bezieht sich auf alle Szenarien, in denen gemäß [Matrix Specification] die Standard State Events zur Anwendung kommen. Dies schließt z. B. das in [Client-Server API/#calculating-the-display-name-for-a-room] beschriebene Verfahren zur Berechnung des Anzeigenamens eines Raumes ein.

Beispiele für die Custom State Events `de.gematik.tim.room.name` und `de.gematik.tim.room.topic`:

```
{
  "content": {
    "topic": "Ein TI-Messenger spezifisches Raumthema"
  },
  "event_id": "$143273582443PhrSn:example.org",
  "origin_server_ts": 1432735824653,
  "room_id": "!jEsUZKDJdhIrcRyVU:example.org",
  "sender": "@example:example.org",
  "state_key": "",
  "type": "de.gematik.tim.room.topic",
  "unsigned": {
    "age": 1234
  }
}
```

5.5.1.2 Matrix-Homeserver

A_25820-01 -Auswertung der Custom State Events für Raumnamen und -thema

An allen Stellen, an denen gemäß [Matrix Specification] die Standard State Events `m.room.name` und `m.room.topic` ausgewertet werden, SOLL der Matrix-Homeserver stattdessen die Inhalte der Custom State Events `de.gematik.tim.room.name` und `de.gematik.tim.room.topic` verwenden. Dies betrifft insbesondere die Zusammenstellung des Stripped State¹ von Räumen, die Replikation von State Events im Rahmen von Raum-Upgrades und die serverseitige Suche in Events.

¹ [Client-Server API/#stripped-state][<=]

5.5.2 Föderierte und intersektorale Kommunikation

Die föderierte und intersektorale Kommunikation ermöglicht es, Akteuren innerhalb des TI-Messenger Dienstes mit anderen Akteuren organisationsübergreifend und föderiert zu kommunizieren.

5.5.2.1 TI-M Client

Hierfür muss der TI-M Client während der Raumerzeugung ebenfalls den Raumtypen initialisieren und zur Initialisierungszeit mit den vorgesehenen Custom State Events füllen.

A_25426 -Verwendung des Chatroom-Typen für föderierte und intersektorale Kommunikation

Der TI-M Client MUSS den Custom Room Type `de.gematik.tim.roomtype.default.v1` für die föderierte und intersektorale Kommunikation mit Hilfe eines parametrisierten Aufrufs des `/createRoom` Endpunktes erzeugen und verwenden.[<=]

A_25814-01 -Verwendung des Raumtypen für föderierte und intersektorale Kommunikation als Standard

Der TI-M Client MUSS standardmäßig den Raumtyp `de.gematik.tim.roomtype.default.v1` verwenden, sofern nicht explizit ein anderer, von der gematik zugelassener *Custom Room Type* durch den raumerzeugenden Nutzer ausgewählt wird. [≤]

5.5.2.2 Matrix-Homeserver

A_25818-01 -Entgegennehmen von Room Types für föderierte und intersektorale Kommunikation

Der Matrix-Homeserver MUSS den Custom Room Type `de.gematik.tim.roomtype.default.v1` entgegennehmen können, ohne diesen auszuwerten, abzuweisen oder mit einer Fehlermeldung zu reagieren. [≤]

5.6 Löschen von Inhalten

5.6.1 Serverseitiges Löschen

Die Löschung von Inhalten durch TI-M Fachdienste kann sowohl aus Effizienz als auch aus Datenschutzgründen sinnvoll sein. Hierbei muss aus technischen Gründen zwischen Matrix-Events und Medien differenziert werden.

5.6.1.1 Matrix-Events

Beim serverseitigen Löschen von Matrix-Events muss es eine Unterscheidung zwischen Versicherten und Mitarbeitern des Gesundheitswesens geben. Das Zielverhalten und die dafür notwendigen Anforderungen finden sich in den gleichnamigen Kapiteln der Spezifikationen [gemSpec_TI-M_ePA] und [gemSpec_TI-M_Pro].

5.6.1.2 Medien

Für Medien wäre eigentlich ein Verhalten analog zu Events wünschenswert. Hierbei gibt es allerdings zwei technologische Hindernisse:

- Events lassen sich in Matrix nur im unverschlüsselten Zustand (also nur auf Clients) mit Medien verknüpfen.
- Es gibt in Matrix keine API zum Löschen von Medien, die ein Client benutzen könnte.

Das bedeutet Fachdienste haben abgesehen vom Zeitpunkt des letzten Downloads, keine Information darüber ob Medien obsolet sind oder nicht. Clients wiederum haben keine Möglichkeit Medien selbst zu löschen oder als obsolet zu kennzeichnen. Eine dauerhafte und anlasslose Speicherung von Daten, egal ob verschlüsselt oder nicht, ist nach DSGVO aber nicht zulässig. Hieraus resultiert, dass Fachdienste Medien nach Ablauf eines Intervalls automatisch löschen müssen. Die konkrete Festlegung dieses Intervalls obliegt dabei dem Betreiber.

A_28337 -Automatische serverseitige Löschung von Medien

TI-M Fachdienste MÜSSEN Medien nach Ablauf eines konfigurierbaren Intervalls seit Empfang oder letztem Download löschen. [≤]

5.6.2 Clientseitiges Löschen

Nutzer müssen für die Organisation ihrer Unterhaltungen in die Lage versetzt werden Räume selbstständig verlassen und vom Client entfernen zu können. Hierbei ist zu

beachten, dass Matrix zwischen `/leave` und `/forget` unterscheidet. Ein Nutzer nimmt nach `/leave` nicht mehr an der weiteren Kommunikation in einem Raum teil. Er kann die bis dahin gesendeten Inhalte aber weiterhin abrufen. Erst nach `/forget` hat der Nutzer keinen Zugriff mehr auf die Raumhistorie.

Clients steht es frei nach dem Verlassen eines Raumes durch `/leave` automatisch auch ein Vergessen per `/forget` auszuführen. Tun sie das nicht, ermöglichen sie ihren Nutzern damit die Verwaltung einer Zwischenablage für historische Räume.

A_28342 -Verlassen und Vergessen von Räumen

TI-M Clients MÜSSEN Nutzern erlauben Räume über die Nutzung der APIs `/leave` und `/forget` vom Client zu löschen. Dabei können Clients diese Operationen wahlweise getrennt oder nur kombiniert auslösbar machen.【<=】

Unabhängig hiervon kann das Verlassen eines Raumes allerdings auch fremdausgelöst sein kann. Daher müssen Clients historische Räume in jedem Falle in ihrem UI zugänglich machen. Hierfür kann ein Sync-Filter mit `include_leave` verwendet werden wodurch alle verlassenen aber noch nicht vergessenen Räume mit dem Initial-Sync zurückgeliefert werden. Dabei muss allerdings beachtet werden, dass es in Matrix keinen Mechanismus zum Synchronisieren von vergessenen Räumen über mehrere Geräte eines Nutzers hinweg gibt. Sofern die gleichzeitige Anmeldung auf mehreren Geräten nicht technisch ausgeschlossen wird, empfiehlt es sich daher in gewissen Abständen einen Initial-Sync auszuführen um neu vergessene Räume einzusammeln.

A_28343 -Anzeige historischer Räume

TI-M Clients MÜSSEN Räume, die verlassen aber noch nicht mittels `/forget` vergessen wurden, per `/sync` abfragen und in ihrem UI zugänglich machen.【<=】

Damit Clients tatsächlich die Wahl haben, ob sie `/forget` automatisch ausführen oder nicht, dürfen Homeserver diesen Automatismus nicht selbst implementieren (wie es z. B. bei der `forget_rooms_on_leave` Konfiguration in Synapse passiert).

A_28344 -Keine serverseitige Kombination von /leave und /forget

TI-M Fachdienste DÜRFEN bei Aufruf der API `/leave` NICHT automatisch ein `/forget` ausführen.【<=】

Haben alle Teilnehmer eines Homeservers einen privaten Raum verlassen und per `/forget` clientseitig entfernt, so muss dieser Raum mit seinen Inhalten auch serverseitig gelöscht werden. Dies folgt direkt aus dem DSGVO-Prinzip der Datensparsamkeit und der Tatsache, dass Nutzer diese Räume nicht mehr betreten können und auch auf ihren Geräten zur Löschung freigegeben haben.

A_28345 -Serverseitiges Löschen nach /forget

TI-M Fachdienste MÜSSEN einen Raum und dessen Inhalte lokal löschen, wenn:

- der Raum privat ist (im Sinne von Join Rules und History Visibility) und
- keiner der Nutzer des Homservers im Raum die Membership `invite` oder `join` hat und
- alle Nutzer des Homeservers, deren Membership im Raum `leave` oder `ban` ist, den Raum per `/forget` von ihren Clients entfernt haben.

Diese Löschung MUSS innerhalb von 7 Tagen ab letztem `/forget` erfolgen.【<=】

5.6.3 Redactions

Die Matrix-Spezifikation ermöglicht die Selbstmoderation von Events mittels Redactions. Redactions sind eine invasive Form des Löschens da sie über die Föderation propagieren

und letztendlich zu einer irreversiblen Löschung von Inhalten auf allen beteiligten Servern und Clients führen.

Dieses Verhalten ist in bestimmten Fällen wünschenswert. Gleichzeitig können Redactions bei Fehlbenutzung aber zu einem unerwarteten Verlust von eigentlich relevanten Nachrichten für andere Gesprächsteilnehmer führen. Als Kompromiss werden Redactions daher zwar erlaubt. Sie werden aber zeitlich eingeschränkt und müssen im Client stets mit einem Warnhinweis versehen werden.

A_25575-01 -Nachrichtenbasiertes Löschen per Redaction

TI-M Clients MÜSSEN ihren Nutzern erlauben eigene Nachrichten per Redaction innerhalb von 24h ab `origin_server_ts` zu löschen.【<=】

A_28358 -Serverseitige Zeitgrenze für Redactions

TI-M Fachdienste MÜSSEN Redactions der eigenen Nachrichten eines Nutzers ablehnen wenn seit `origin_server_ts` des zu redactenden Events mehr als 24h vergangen sind. 【<=】

A_28354 -Warnhinweis beim Auslösen von Redactions

TI-M Clients MÜSSEN ihre Nutzer vor jedem Auslösen einer Redaction per Warnhinweis darauf hinweisen, dass die Nachricht irreversibel und für alle Gesprächsteilnehmer gelöscht wird.【<=】

Damit Redactions wirksam sind, müssen sie nicht nur von Fachdiensten sondern auch von Clients durchgesetzt werden. Damit für alle Gesprächsteilnehmer ersichtlich wird, dass eine Löschung stattgefunden hat, sind Nachrichten nach Redactions zudem entsprechend zu kennzeichnen.

A_25576-01 -Lokale Anwendung von Redactions

TI-M Clients MÜSSEN `m.room.redaction` Events analog zu Matrix-Homeservern anwenden und betroffene Event-Inhalte aus ihrem lokalen Speicher löschen.【<=】

A_25577-01 -Kennzeichnung von Nachrichten nach Redactions

TI-M Clients MÜSSEN von Redactions betroffene Nachrichten kennzeichnen und den löschenden Akteur sowie Datum und Uhrzeit der Löschung ersichtlich machen.【<=】

Event Replacements, also geänderte Nachrichten, stellen bei Redactions einen Sonderfall dar. Hier gilt es zu verhindern, dass durch alleinige Redaction des ursprünglichen Events losgelöste Replacements entstehen.

A_28355 -Kaskadierung von Redactions bei Event Replacements

Ist eine zu löschende Nachricht Ausgangspunkt von Event Replacements, so MÜSSEN TI-M Clients neben dem Event selbst auch alle Replacements redacten.【<=】

Unabhängig von Redactions können TI-M Clients bei Bedarf visuelles Löschen für z. B. `m.room.message` Events auch über Event Replacements implementieren, indem die Nachricht zu einem leeren Inhalt geändert wird. Diese Form des Löschens ist reversibel und transparent da Replacements separate Events sind und die gesamte Historie von Events erhalten bleibt.

6 Anhang A - Verzeichnisse

6.1 Abkürzungen

Tabelle 12: Im Dokument verwendete Abkürzungen

Kürzel	Erläuterung
API	Application Programming Interface
FD	Fachdienst
IdP	Identity Provider
KIM	Kommunikation im Medizinwesen
LDAP	Lightweight Directory Access Protocol
OSCP	Offensive Security Certified Professional
TLS	Transport Layer Security
VZD	Verzeichnisdienst

6.2 Glossar

Tabelle 13: Im Dokument verwendete Begriffe

Begriff	Erläuterung
Funktionsmerkmal	Der Begriff beschreibt eine Funktion oder auch einzelne, eine logische Einheit bildende Teilfunktionen der TI im Rahmen der funktionalen Zerlegung des Systems.

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

6.3 Abbildungsverzeichnis

Abbildung 1: Komponenten der TI-Messenger-Architektur (vereinfachte Darstellung).....	9
Abbildung 2: Systemüberblick TI-M Client.....	18
Abbildung 3: Systemüberblick TI-M FD.....	35
Abbildung 4: Übersicht der Schnittstellen am Registrierungs-Dienst.....	36

Abbildung 5: Matrix-API des Messenger-Service.....	41
Abbildung 6: Prüfungen Messenger-Proxy.....	42
Abbildung 7: Betriebsmodell TI-M Basis.....	51
Abbildung 8: Laufzeitsicht - Authentisieren einer Organisation am TI-M Dienst.....	58
Abbildung 9: Laufzeitsicht - Bereitstellung eines Messenger-Service für eine Organisation	61
Abbildung 10: Laufzeitsicht - Föderationszugehörigkeit eines Messenger-Service prüfen	63
Abbildung 11: Laufzeitsicht - Austausch von Events zwischen Akteuren innerhalb einer Organisation.....	65
Abbildung 12: Laufzeitsicht - Einladung von Akteuren außerhalb einer Organisation.....	67
Abbildung 13: Laufzeitsicht - Austausch von Events zwischen Akteuren außerhalb einer Organisation.....	69
Abbildung 14: Laufzeitansicht - Aktualisierung der Föderationsliste.....	71
Abbildung 15: Provider authentifizieren und Föderationsliste abrufen.....	72
Abbildung 16: Signatur der Föderationsliste prüfen.....	73
Abbildung 17: Beispielhaftes UI zum Setzen der Berechtigungen.....	77
Abbildung 18: Logischer Ablauf beim Setzen der Berechtigungen.....	77
Abbildung 19: Push-Konfiguration.....	79
Abbildung 20: Push-Zustellung.....	80

6.4 Tabellenverzeichnis

Tabelle 1: Akteure und Rollen.....	10
Tabelle 2: Arten von Token.....	14
Tabelle 3: Matrix Module.....	24
Tabelle 4: Tabelle : AF - Authentisieren einer Organisation am TI-M Dienst.....	56
Tabelle 5: AF - Bereitstellung eines Messenger-Service für eine Organisation.....	59
Tabelle 6: Föderationszugehörigkeit eines Messenger-Service prüfen.....	62
Tabelle 7: Austausch von Events zwischen Akteuren innerhalb einer Organisation.....	64
Tabelle 8: AF - Einladung von Akteuren außerhalb einer Organisation.....	66
Tabelle 9: AF - Austausch von Events zwischen Akteuren außerhalb einer Organisation..	68
Tabelle 10: AF - Aktualisierung der Föderationsliste.....	69
Tabelle 11: Spezifische Attribute für das Handling der Föderationsliste am Registrierungs-Dienst.....	73
Tabelle 12: Im Dokument verwendete Abkürzungen.....	88
Tabelle 13: Im Dokument verwendete Begriffe.....	88
Tabelle 14: Referenzierte Dokumente der gematik.....	90
Tabelle 15: Weitere Referenzen.....	91

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.

Tabelle 14: Referenzierte Dokumente der gematik

[Quelle]	Herausgeber: Titel
[api-messenger]	gematik: Implementierungsleitfaden zum TI-Messenger https://github.com/gematik/api-ti-messenger
[api-testtreiber]	gematik: Testtreiber-Schnittstelle https://github.com/gematik/api-ti-messenger/blob/main/src/openapi/TiMessengerTestTreiber.yaml
[api-vzd]	gematik: Verzeichnisdienst der Telematikinfrastruktur https://github.com/gematik/api-vzd
[gematik Authenticator]	gematik Authenticator https://fachportal.gematik.de/hersteller-anbieter/komponenten-dienste/authenticator
[gematik Testkonzept]	gematik: Test und Zertifizierung TI-Messenger https://github.com/gematik/api-ti-messenger/blob/main/docs/Test/Test.adoc
[gematik Testsuite]	gematik TI-Messenger Testsuite https://github.com/gematik/TI-Messenger-Testsuite
[gemGlossar]	gematik: Einführung der Gesundheitskarte – Glossar
[gemSpec_IDP_Sek]	gematik: Spezifikation Sektoraler Identity Provider
[gemKPT_Betr]	gematik: Betriebskonzept Online-Produktivbetrieb
[gemKPT_Test]	gematik: Testkonzept der TI
[gemSpec_IDP_Dienst]	gematik: Spezifikation Identity Provider-Dienst
[gemSpec_IDP_FD]	gematik: Spezifikation Identity Provider – Nutzungsspezifikation für Fachdienste
[gemSpec_Krypt]	gematik: Übergreifende Spezifikation: Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur

[gemSpec_OID]	gematik: Spezifikation Festlegung von OIDs
[gemSpec_Perf]	gematik: Übergreifende Spezifikation Performance und Mengengerüst TI-Plattform
[gemSpec_SST_LD_BD]	gematik: Spezifikation Logdaten- und Betriebsdatenerfassung
[gemSpec_TI-M_ePA]	gematik: Spezifikation TI-Messenger ePA
[gemSpec_TI-M_Pro]	gematik: Spezifikation TI-Messenger Pro
[gemSpec_VZD_FHIR_Directory]	gematik: Spezifikation Verzeichnisdienst FHIR-Directory
[OCSP-Responder]	gematik: OCSP-Responder RSA: http://download.crl.ti-dienste.de/ocsp ECC: http://download.crl.ti-dienste.de/ocsp/ec
[ROOT-CA]	ROOT-CA Download Punkt https://download.tsl.ti-dienste.de/ECC/ROOT-CA/
[ROOT-CA-JSON]	ROOT-CA Download Punkt als JSON-Datei https://download.tsl.ti-dienste.de/ECC/ROOT-CA/roots.json
[simplifier]	gematik: TI-Messenger https://simplifier.net/tim

6.5.2 Weitere Dokumente

Tabelle 15: Weitere Referenzen

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[BITV 2.0]	Verordnung zur Schaffung barrierefreier Informationstechnik nach dem Behindertengleichstellungsgesetz (Barrierefreie-Informationstechnik-Verordnung - BITV 2.0) https://www.gesetze-im-internet.de/bitv_2_0/BJNR184300011.html
[BSI 2-Faktor]	BSI 2-Faktor Authentisierung für mehr Datensicherheit https://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
[BSI ORP. 4]	BSI ORP.4: Identitäts- und Berechtigungsmanagement (Stand Februar 2021) https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompodium_Einzel_PDFs_2021/02_ORP_Organisation_und_Personal/ORP_4_Identitaets_und_Berechtigungsmanagement_Editon_2021.html

[BSI-TR-03166]	BSI TR-03166 - Technical Guideline for Biometric Authentication Components in Devices for Authentication https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TR03166/BSI-TR-03166.pdf
[Client-Server API]	Matrix Foundation: Matrix Specification - Client-Server API https://spec.matrix.org/v1.11/client-server-api
[FHIR]	HL7 FHIR Dokumentation https://www.hl7.org/fhir/documentation.html
[ISO 9241]	Ergonomics of human-system interaction https://www.iso.org
[Matrix Appendices]	Matrix Foundation: Matrix Specification - Appendices https://spec.matrix.org/v1.11/appendices
[Matrix Specification]	Matrix Foundation: Matrix Specification https://spec.matrix.org/v1.11
[MSC3814]	MSC3814: Dehydrated devices with SSSS https://github.com/matrix-org/matrix-spec-proposals/pull/3814
[OpenID]	OpenID Foundation https://openid.net/developers/specs/
[OWASP PBKDF2]	OWASP Password Storage Cheat Sheet https://cheatsheetseries.owasp.org/cheatsheets/Password_Storage_Cheat_Sheet.html#pbkdf2
[OWASP Proactive Control]	OWASP Proactive Controls https://owasp.org/www-project-proactive-controls/
[Push Gateway]	Matrix Foundation: Matrix Specification - Push Gateway API https://spec.matrix.org/v1.11/push-gateway-api

API]	
[RFC 2119]	IETF: Key words for use in RFCs to Indicate Requirement Levels https://datatracker.ietf.org/doc/html/rfc2119
[RFC 4122]	IETF: A Universally Unique Identifier (UUID) URN Namespace https://datatracker.ietf.org/doc/html/rfc4122
[Room Versions]	Matrix Foundation: Matrix Specification - Room Versions https://spec.matrix.org/v1.11/rooms/
[Server-Server API]	Matrix Foundation: Matrix Specification - Server-Server API https://spec.matrix.org/v1.11/server-server-api
[SSS S]	Matrix Foundation: Secrets Storage & Sharing https://spec.matrix.org/v1.11/client-server-api/#secrets
[Synapse]	Element: Synapse Matrix homeserver https://github.com/element-hq/synapse