
C_12194 - VZD Änderungen

Inhaltsverzeichnis

1 Änderung in gemSpec_VZD.....	2
2 Änderung in gemSpec_VZD_FHIR_Directory.....	45
3 Änderungen in Steckbriefen.....	73
3.1 Änderungen in gemProdT_VZD_PTV.....	73
3.2 Änderungen in gemProdT_FD_KOMLE.....	75
3.3 Änderungen in gemProdT_CM_KOMLE.....	76
3.4 Änderungen in gemProdT_VZD_FHIR.....	77

1 Änderung in gemSpec_VZD

Es wird Kapitel "3.1 IT-Sicherheit und Datenschutz" wie folgt aufgenommen

3.1 IT-Sicherheit und Datenschutz

...

TIP1-A_5555 -- VZD, SOAP-Fehlercodes

Der VZD MUSS für seine SOAP-Schnittstelle die generischen Fehlercodes

- Code 2: Verbindung zurückgewiesen
- Code 3: Nachrichtenschema fehlerhaft
- Code 4: Version Nachrichtenschema fehlerhaft
- Code 6: Protokollfehler

aus Tabelle Tab_Gen_Fehler aus [gemSpec_OM] im SOAP-Fault verwenden. Erkannte Fehler auf Transportprotokollebene müssen auf gematik SOAP Faults (Code 6 aus Tabelle Tab_Gen_Fehler aus [gemSpec_OM]) abgebildet werden.

<=

...

Es wird Kapitel "3.3 Anforderungen an VZD Clients" wie folgt aufgenommen

3.3 Anforderungen an VZD Clients

A_27744 VZD Clients - Nutzung zentraler TI-Systeme durch dezentrale Clients: Verbindungsmanagement

Dezentrale Client-Systeme MÜSSEN dafür sorgen, dass Verbindungen nur im Zusammenhang mit einem konkreten fachlichen Use Case, der die Nutzung der entsprechenden Schnittstelle zwingend erfordert, aufgebaut werden.

Verbindungsaufbauten im Rahmen eines Initialisierungsprozesses sind zu vermeiden und sind nur in Kombination mit einem wirksamen Connection-Idle-Timeout zulässig. Das Absetzen regelmäßiger Dummy-Requests zum Umgehen des Idle-Timeouts oder zu anderen Zwecken (z.B. Monitoring) ist nicht erlaubt.

Ein Client hat sicherzustellen, dass gleichzeitig maximal eine Verbindung zur VZD-Schnittstelle aufgebaut wird. Das gleichzeitige Öffnen mehrerer paralleler Verbindungen durch denselben Client ist nicht zulässig, es sei denn, ein verbindliches Maximum wird für eine Schnittstelle explizit definiert.

Im Fall des Fehlschlagens des Verbindungsaufbau MUSS eine Wartezeit bis zum nächsten Verbindungsversuch eingehalten werden (Retry-Intervall). Das Retry-Intervall ist mit zunehmender Anzahl fehlgeschlagener Verbindungsversuch bis zu einem Maximum zu erhöhen.

Verbindungen sind nach Beendigung des fachlichen Use Cases zeitnah zu schließen (5 Sek). Erfolgt dies nicht, MUSS nach Ablauf des Connection-Idle-Timeouts die Verbindung abgebaut werden.

Die maximale Bearbeitungsdauer einer Abfrage ist clientseitig per Konfiguration

festzulegen. Um potenzielle Überlastsituationen durch langlaufende Anfragen (> 30 Sekunden) zu vermeiden, durch den VZD eine Begrenzung der maximalen Bearbeitungsdauer serverseitig (TimeOut) mit Beendigung der Abfrage möglich.

<=

A_27749 VZD Client - Nutzung zentraler TI-Systeme durch dezentrale Clients: Verbindungsmanagement, Parameter

Dezentrale Client-Systeme oder Apps MÜSSEN parametrisierbar sein, d.h. folgende Parameter müssen aus der Ferne zentral angepasst werden können. Die Standardwerte (Default) MÜSSEN nach Aufforderung durch die gematik in einem [noch zu definierenden Prozess] innerhalb einer [noch festzulegenden Zeit] anpassbar sein.

Parameter	Beschreibung	Standardwerte (Default)
CONNECTION_IDLE_TIMEOUT (Hinweis: Die Parameternamen müssen ggf. produkt- oder Schnittstellenspezifisch angepasst werden)	Haltedauer der TCP-Verbindung eines Clients zu einem Dienst, in der kein Datenverkehr zwischen Client und Dienst stattfindet.	30 Sek
MAX_CONNECTION	Anzahl der pro Client maximal zulässigen gleichzeitigen Verbindungen.	2
RETRY_TIME	Mindestwartezeit nach den ersten beiden fehlgeschlagenen Verbindungsversuchen. Bei jedem weiteren Versuch nach dem 3. Versuch SOLL die Wartezeit um diesen Wert bis RETRY_TIME_MAX oder mit größer werden Abständen vergrößert werden.	5 Sek
RETRY_TIME_MAX	Maximale Wartezeit zwischen zwei Verbindungsversuchen.	5 min

<=

A_27751 VZD Client - Nutzung zentraler TI-Systeme durch dezentrale Clients: Angepasste Konfiguration und Außerbetriebnahme von Clients

Jeder Client MUSS entsprechend des tatsächlichen Bedarfs, d.h. der zu erwartenden Anwendungsfälle und deren Häufigkeit so konfiguriert werden, dass nicht notwendige Last (Anfrage- und Verbindungslast auf Systemkomponenten durch parallele Verbindungen, häufige Requests oder ineffiziente Nutzung von Schnittstellen) auf den zentralen TI-Systemen vermieden wird.

Clients, die vorübergehend oder langfristig nicht mehr genutzt werden, SOLLEN in angemessen kurzer Zeit deaktiviert werden.

<=

A_28318 VZD Client - Deaktivierung nicht genutzter Clients

VZD Clients, die vorübergehend oder langfristig nicht mehr genutzt werden, SOLLEN in angemessen kurzer Zeit deaktiviert werden.

<=

A_27752 -VZD Client - Nutzung zentraler TI-Systeme durch dezentrale Clients: Vermeidung der Gesamtauslese des VZD durch Clients

Ein Client DARF NICHT eine Gesamtauslese (systematische Abfrage aller verfügbaren Einträge über Einzelabfragen statt Nutzung dafür vorgesehener Exportmechanismen) des Verzeichnisdienstes (VZD) durchführen. Stattdessen SOLLEN die dedizierten Schnittstellen, falls vorhanden, für einen entsprechenden Export genutzt werden. Clients, bei denen durch kontinuierliche Abfragen eine unzulässige Gesamtauslese vermutet wird, werden im Zweifel gesperrt.

Zur Reduzierung der Serverlast bei aufeinanderfolgender Abfrage an der I_Directory_Query-Schnittstelle (Idap) steht den Client ein Paging gemäß RFC2696 zur Verfügung.

[<=,,]

A_27753 VZD Client - Nutzung zentraler TI-Systeme durch dezentrale Clients: Caching

Zur Lastvermeidung und Erhöhung der Ausfallsicherheit SOLLEN Client-Systeme Antworten von häufig durchgeführten Abfragen kurzzeitig (max. 5 Min.), wenn für den Anwendungsfall nicht explizit anders spezifiziert, aufbewahren (cachen).

<=

A_27755 VZD Client - Nutzung zentraler TI-Systeme durch dezentrale Clients: Fehler-Monitoring

VZD Clients SOLLEN zur frühzeitigen Erkennung von Instabilitäten im Client- oder Netzwerkbereich Metriken wie Antwortzeiten, Fehlerraten und Timeouts erfassen und bei Bedarf an ein zentrales Monitoring-System übermitteln.

<=

Es wird Kapitel "4.2 Schnittstelle I_Directory_Maintenance" gestrichen

4.2 Schnittstelle I_Directory_Maintenance

Die Schnittstelle ermöglicht die Administration der Basisdaten.

TIP1-A_5571 VZD, Schnittstelle I_Directory_Maintenance

Der VZD MUSS die Schnittstelle I_Directory_Maintenance gemäß Tabelle Tab_VZD_Schnittstelle_I_Directory_Maintenance anbieten.

Tabelle 1: Tab_VZD_Schnittstelle_I_Directory_Maintenance

Name	I_Directory_Maintenance
-------------	-------------------------

Version	wird im Produkttypsteckbrief des VZD definiert	
Operationen	Name	Kurzbeschreibung
	add_Directory_Entry	Erzeugung eines Basisdaten-Verzeichniseintrages oder Überschreiben eines bestehenden Verzeichniseintrages.
	read_Directory_Entry	Abfrage aller Basis- und Fachdaten eines Verzeichniseintrages.
	modify_Directory_Entry	Änderung eines Basisdaten-Verzeichniseintrages.
	delete_Directory_Entry	Löschung eines Verzeichniseintrages (Basisdaten und Fachdaten).

<=

TIP1-A_5572 VZD, I_Directory_Maintenance, TLS-gesicherte Verbindung

Der VZD MUSS die Schnittstelle I_Directory_Maintenance durch Verwendung von TLS mit beidseitiger Authentisierung sichern.

Der VZD muss sich mit der Identität ID.ZD.TLS-S authentisieren.

Der VZD muss das vom FAD übergebene AUT-Zertifikat C.FD.TLS-C hinsichtlich OCSP-Gültigkeit und Übereinstimmung mit einem Zertifikat eines zur Nutzung dieser Schnittstelle registrierten Fachdienstes prüfen. Bei negativem Ergebnis wird der Verbindungsaufbau abgebrochen.

<=

TIP1-A_5574 VZD und Nutzer der Schnittstelle I_Directory_Maintenance, Webservice

Der VZD und Nutzer der Schnittstelle MÜSSEN die Schnittstelle I_Directory_Maintenance als SOAP-Webservice über HTTPS implementieren. Der Webservice wird durch die Dokumente DirectoryMaintenance.wsdl und DirectoryMaintenance.xsd definiert.

<=

4.2.1 Operation add_Directory_Entry

Diese Operation legt einen neuen Basisdatensatz an oder überschreibt einen bestehenden Datensatz im LDAP Verzeichnis.

4.2.1.1 Umsetzung

TIP1-A_5575 VZD, Umsetzung add_Directory_Entry

Der VZD MUSS nach folgenden Vorgaben die Operation add_Directory_Entry implementieren:

1. Ein bereits zur Telematik-ID gehörender Basisdatensatz wird gelöscht und neu angelegt.
2. Existiert noch kein Basisdatensatz zur Telematik-ID wird ein neuer angelegt.
3. Die Daten aus dem SOAP Request bilden gemäß Tab_VZD_Daten-Transformation und Tab_VZD_Datenbeschreibung den neuen Basisdatensatz.

Es müssen die Fehlermeldungen gemäß Tab_TUC_VZD_0002 verwendet werden.

<=

In der folgenden Tabelle sind die Regeln zur Transformation von I_Directory_Maintenance-Request Elementen zu LDAP-Directory Attributen und die Regeln zur Transformation aus LDAP-Directory Attributen zu I_Directory_Maintenance-Response Elementen beschrieben.

Tabelle 2: Tab_VZD_Daten-Transformation

I_Directory_Maintenance-Request-Element	LDAP-Directory-Attribut	I_Directory_Maintenance-Response-Element	Zusatzinformation
n/a	givenname	givenname	Verwendung gemäß Tab_VZD_Datenbeschreibung
n/a	sn SMC-B: Wird vom VZD als Kopie von otherName eingetragen.	surname	Verwendung gemäß Tab_VZD_Datenbeschreibung
n/a	cn Wird vom VZD als Kopie von otherName eingetragen.	commonName	Verwendung gemäß Tab_VZD_Datenbeschreibung
n/a	displayName Wird vom VZD als Kopie von otherName eingetragen.	displayName	
streetAddress	streetAddress	streetAddress	Alias street Der Alias-Wert wird in der LDAP-Response verwendet.
postalCode	postalCode	postalCode	
localityName	localityName	localityName	Alias l Der Alias-Wert wird in der LDAP-Response verwendet.
stateOrProvinceName	stateOrProvinceName	stateOrProvinceName	Alias st Der Alias-Wert wird in der

			LDAP-Response- verwendet.
title	title	title	Verwendung gemäß- Tab_VZD_Datenbeschreib- ung
organization	organization	organization	Alias- Der Alias-Wert wird in der LDAP-Response- verwendet. Verwendung gemäß- Tab_VZD_Datenbeschreib- ung
otherName	otherName SMC-B: wird- vom VZD- zusätzlich in- displayName-, surname und- en eingetragen	otherName	Verwendung gemäß- Tab_VZD_Datenbeschreib- ung
subject	specialization	subject	Verwendung gemäß- Tab_VZD_Datenbeschreib- ung
n/a	domainID	n/a	
n/a	personalEntry	n/a	Verwendung gemäß- Tab_VZD_Datenbeschreib- ung
x509CertificateEnc	userCertificate	x509CertificateEnc	Verwendung gemäß- Tab_VZD_Datenbeschreib- ung
n/a	entryType	n/a	Verwendung gemäß- Tab_VZD_Datenbeschreib- ung
n/a	telematikID	telematikID	Verwendung gemäß- Tab_VZD_Datenbeschreib- ung
n/a	professionOID	n/a	Verwendung gemäß- Tab_VZD_Datenbeschreib- ung
n/a	description	n/a	
timestamp	n/a	timestamp	Datum und Zeit des- Requests bzw. der-

			Response
variant	n/a HBA: Wenn variant == full, dann werden givenName und sn aus dem Zertifikat in die gleichnamigen LDAP Attribute übernommen.	n/a	
givenname	n/a	n/a	
surname	n/a	n/a	
commonName	n/a	n/a	
serviceData	n/a	n/a	
n/a	n/a	status	

4.2.1.2 Nutzung

TIP1-A_5576 - Nutzer der Schnittstelle, TUC_VZD_0002 „add_Directory_Entry“

Der Nutzer der Schnittstelle MUSS den technischen Use Case TUC_VZD_0002-
„add_Directory_Entry“ gemäß Tabelle Tab_TUC_VZD_0002 umsetzen.
Der SOAP-Requests MUSS gemäß Tab_VZD_Datenbeschreibung mit der Bedeutung
entsprechenden Daten ausgefüllt sein.

Tabelle 3: Tab_TUC_VZD_0002

Name	TUC_VZD_0002 „add_Directory_Entry“	
Beschreibung	Diese Operation ermöglicht die Erzeugung von neuen Basisdaten. Bestehende Basisdaten werden überschrieben.	
Vorbedingungen	keine	
Eingangsdaten	SOAP-Request „addDirectoryEntry“	
Komponenten	Nutzer der Schnittstelle, Verzeichnisdienst	
Ausgangsdaten	SOAP-Response „VZD:responseMsg“	
Standardablauf	Aktion	Beschreibung

	Aufbau TLS-Verbindung	Wenn noch keine Verbindung besteht initiiert der Nutzer der Schnittstelle den Verbindungsaufbau. Der Nutzer der Schnittstelle authentisiert sich mit dem AUT-Zertifikat C.FD.TLS-C.
	SOAP-Request-senden	Der Nutzer der Schnittstelle ruft die SOAP-Operation VZD:addDirectoryEntry auf.
	SOAP-Response-empfangen	Die SOAP-Response VZD:responseMsg mit dem VZD:status wird empfangen.
Varianten/ Alternativen	keine	
Fehlerfälle	<p>Es werden die protokollspezifischen Fehlermeldungen verwendet (TCP, HTTP, TLS). Fehler bei der Verarbeitung des SOAP Requests werden als gematik SOAP Fault versendet: faultcode 4211, faultstring: Operation fehlerhaft ausgeführt, Basisdaten konnten nicht angelegt werden (Fehler im Verzeichnisdienst) faultcode 4202, faultstring: SOAP Request enthält Fehler faultcode 4201, faultstring: Operation enthält ungültige Daten</p> <p>Erkannte Fehler auf Transportprotokollebene müssen auf gematik SOAP Faults (Code 6 aus Tabelle Tab_Gen_Fehler aus [gemSpec_OM]) abgebildet werden. Zusätzlich müssen die generischen gematik SOAP Faults Code 2: Verbindung zurückgewiesen Code 3: Nachrichtenschema fehlerhaft Code 4: Version Nachrichtenschema fehlerhaft unterstützt werden.</p>	

<=

4.2.2 Operation read_Directory_Entry

Diese Operation liest einen vollständigen Eintrag aus dem LDAP Verzeichnis aus.

4.2.2.1 Umsetzung

TIP1-A_5577 - VZD, Umsetzung read_Directory_Entry

Der VZD MUSS nach folgenden Vorgaben die Operation I_Directory_Maintenance::read_Directory_Entry implementieren:

1. Der zur Telematik-ID gehörende Eintrag wird im LDAP Directory ermittelt.
2. Es wird eine SOAP Response VZD:readResponseMsg aus dem kompletten Eintrag (Basisdaten + Fachdaten) gemäß Tab_VZD_Daten-Transformation und Tab_VZD_Datenbeschreibung erzeugt.

Es müssen die Fehlermeldungen gemäß Tab_TUC_VZD_0003 verwendet werden.

4.2.2.2 Nutzung

TIP1-A_5578 – Nutzer der Schnittstelle, TUC_VZD_0003 „read_Directory_Entry“

Der Nutzer der Schnittstelle MUSS den technischen Use Case TUC_VZD_0003 „read_Directory_Entry“ gemäß Tabelle Tab_TUC_VZD_0003 umsetzen. Der Webservice wird durch die Dokumente DirectoryMaintenance.wsdl und DirectoryMaintenance.xsd definiert.

Die SOAP-Response ist gemäß Tabelle Tab_VZD_Datenbeschreibung mit den zur Telematik-ID gehörenden Daten aus dem VZD ausgefüllt.

Tabelle 4: Tab_TUC_VZD_0003

Name	TUC_VZD_0003 „read_Directory_Entry“	
Beschreibung	Diese Operation liest einen vollständigen Eintrag aus dem VZD aus.	
Vorbedingungen	Keine	
Eingangsdaten	SOAP-Request „readDirectoryEntry“	
Komponenten	Nutzer der Schnittstelle, Verzeichnisdienst	
Ausgangsdaten	SOAP-Response „readResponseMsg“	
Standardablauf	Aktion	Beschreibung
	Aufbau-TLS-Verbindung	Wenn noch keine Verbindung besteht initiiert der Nutzer der Schnittstelle den Verbindungsaufbau. Der Nutzer der Schnittstelle authentisiert sich mit dem AUT-Zertifikat C.FD.TLS-C.
	SOAP-Request-senden	Der Nutzer der Schnittstelle ruft die SOAP-Operation VZD:readDirectoryEntry auf.
	SOAP-Response-empfangen	Die SOAP-Response VZD:readResponseMsg mit allen Basisdaten wird empfangen.
Varianten/ Alternativen	keine	
Fehlerfälle	Es werden die protokollspezifischen Fehlermeldungen verwendet (TCP, HTTP, TLS) Fehler bei der Verarbeitung des SOAP Requests werden als gematik SOAP-Fault versendet: faultcode4221, faultstring: Operation fehlerhaft ausgeführt,	

	<p>Basisdaten konnten nicht gelesen werden (Fehler im Verzeichnisdienst)</p> <p>faultcode 4312, faultstring: Basisdaten konnten nicht gefunden werden</p> <p>faultcode 4202, faultstring: SOAP Request enthält Fehler</p> <p>Erkannte Fehler auf Transportprotokollebene müssen auf gematik SOAP Faults (Code 6 aus Tabelle Tab_Gen_Fehler aus [gemSpec_OM]) abgebildet werden. Zusätzlich müssen die generischen gematik SOAP Faults</p> <p>Code 2: Verbindung zurückgewiesen</p> <p>Code 3: Nachrichtenschema fehlerhaft</p> <p>Code 4: Version Nachrichtenschema fehlerhaft unterstützt werden.</p>
--	--

<=

4.2.3 Operation modify_Directory_Entry

Diese Operation ändert die Daten eines bestehenden Basisdatensatzes im LDAP Verzeichnis.

4.2.3.1 Umsetzung

TIP1-A_5579 – VZD, Umsetzung modify_Directory_Entry

Der VZD MUSS nach folgenden Vorgaben die Operation modify_Directory_Entry implementieren:

1. Der zur Telematik-ID gehörende Basisdatensatz wird im LDAP Directory ermittelt.
2. Die Daten im Basisdatensatz werden durch die Daten aus dem SOAP Request gemäß Tab_VZD_Daten-Transformation und Tab_VZD_Datenbeschreibung geändert.

Es müssen die Fehlermeldungen gemäß Tab_TUC_VZD_0004 verwendet werden.

<=

4.2.3.2 Nutzung

TIP1-A_5580 – Nutzer der Schnittstelle, TUC_VZD_0004 „modify_Directory_Entry“

Der Nutzer der Schnittstelle MUSS den technischen Use Case TUC_VZD_0004 „modify_Directory_Entry“ gemäß Tabelle Tab_TUC_VZD_0004 umsetzen. Der Webservice wird durch die Dokumente DirectoryMaintenance.wsdl und DirectoryMaintenance.xsd definiert.

Der SOAP Requests MUSS gemäß Tabelle VZD_TAB_modifyDirectoryEntry_Mapping mit der Bedeutung entsprechenden Daten ausgefüllt sein.

Tabelle 5: Tab_TUC_VZD_0004

Name	TUC_VZD_0004 „modify_Directory_Entry“
Beschreibung	Diese Operation ermöglicht die Änderung von Basisdaten.
Vorbedingungen	keine

Eingangsdaten	SOAP-Request „modifyDirectoryEntry“	
Komponenten	Nutzer der Schnittstelle, Verzeichnisdienst	
Ausgangsdaten	SOAP-Response „responseMsg“	
Standardablauf	Aktion	Beschreibung
	Aufbau-TLS-Verbindung	Wenn noch keine Verbindung besteht initiiert der Nutzer der Schnittstelle den Verbindungsaufbau. Der Nutzer der Schnittstelle authentisiert sich mit dem AUT-Zertifikat C.FD.TLS-C.
	SOAP-Request-senden	Der Nutzer der Schnittstelle ruft die SOAP-Operation VZD:modifyDirectoryEntry auf.
	SOAP-Response-empfangen	Die SOAP-Response VZD:responseMsg mit dem VZD:status wird empfangen.
Varianten/Alternativen	keine	
Fehlerfälle	<p>Es werden die protokollspezifischen Fehlermeldungen verwendet (TCP, HTTP, TLS)</p> <p>Fehler bei der Verarbeitung des SOAP Requests werden als gematik SOAP-Fault versendet:</p> <p>faultcode 4231, faultstring: Operation fehlerhaft ausgeführt, Basisdaten konnten nicht modifiziert werden (Fehler im Verzeichnisdienst)</p> <p>faultcode 4312, faultstring: Basisdaten konnten nicht gefunden werden</p> <p>faultcode 4202, faultstring: SOAP-Request enthält Fehler</p> <p>Erkannte Fehler auf Transportprotokollebene müssen auf gematik SOAP-Faults (Code 6 aus Tabelle Tab_Gen_Fehler aus [gemSpec_OM]) abgebildet werden. Zusätzlich müssen die generischen gematik SOAP-Faults</p> <p>Code 2: Verbindung zurückgewiesen</p> <p>Code 3: Nachrichtenschema fehlerhaft</p> <p>Code 4: Version Nachrichtenschema fehlerhaft unterstützt werden.</p>	

<=

4.2.4 Operation delete_Directory_Entry

Diese Operation löscht einen bestehenden Datensatz im LDAP-Verzeichnis.

4.2.4.1 Umsetzung

TIP1-A_5581 -- VZD, Umsetzung delete_Directory_Entry

Der VZD MUSS nach folgenden Vorgaben die Operation
I_Directory_Maintenance::delete_Directory_Entry implementieren:

1. Ein zur Telematik-ID gehörender vollständiger Eintrag gelöscht.

Es müssen die Fehlermeldungen gemäß Tab_TUC_VZD_0005 verwendet werden.

<=

4.2.4.2 Nutzung**TIP1-A_5582 -- Nutzer der Schnittstelle, TUC_VZD_0005 „delete_Directory_Entry“**

Der Nutzer der Schnittstelle MUSS den technischen Use Case TUC_VZD_0005-
„delete_Directory_Entry“ gemäß Tabelle Tab_TUC_VZD_0005 umsetzen. Der Webservice
wird durch die Dokumente DirectoryMaintenance.wsdl und DirectoryMaintenance.xsd
definiert.

Tabelle 6: Tab_TUC_VZD_0005

Name	TUC_VZD_0005 „delete_Directory_Entry“	
Beschreibung	Diese Operation ermöglicht die Löschung von Basisdaten inkl. der zugehörigen Fachdaten.	
Vorbedingungen	keine	
Eingangsdaten	SOAP-Request „deleteDirectoryEntry“	
Komponenten	Nutzer der Schnittstelle, Verzeichnisdienst	
Ausgangsdaten	SOAP-Response „responseMsg“	
Standardablauf	Aktion	Beschreibung
	Aufbau-TLS-Verbindung	Wenn noch keine Verbindung besteht, initiiert der Nutzer der Schnittstelle den Verbindungsaufbau. Der Nutzer der Schnittstelle authentisiert sich mit dem AUT-Zertifikat C.FD.TLS-C.
	SOAP-Request senden	Der Nutzer der Schnittstelle ruft die SOAP-Operation VZD:deleteDirectoryEntry auf.

	SOAP-Response-empfangen	Die SOAP-Response VZD:responseMsg mit dem VZD:status wird empfangen.
Varianten/ Alternativen	keine	
Fehlerfälle	<p>Es werden die protokollspezifischen Fehlermeldungen verwendet (TCP, HTTP, TLS)</p> <p>Fehler bei der Verarbeitung des SOAP Requests werden als gematik SOAP-Fault versendet:</p> <p>faultcode 4241, faultstring: Operation fehlerhaft ausgeführt, Basisdaten konnten nicht gelöscht werden (Fehler im Verzeichnisdienst)</p> <p>faultcode 4312, faultstring: Basisdaten konnten nicht gefunden werden</p> <p>faultcode 4202, faultstring: SOAP Request enthält Fehler</p> <p>Erkannte Fehler auf Transportprotokollebene müssen auf gematik SOAP Faults (Code 6 aus Tabelle Tab_Gen_Fehler aus [gemSpec_OM]) abgebildet werden. Zusätzlich müssen die generischen gematik SOAP Faults</p> <p>Code 2: Verbindung zurückgewiesen</p> <p>Code 3: Nachrichtenschema fehlerhaft</p> <p>Code 4: Version Nachrichtenschema fehlerhaft unterstützt werden.</p>	

<=

Es wird Kapitel "4.3 Schnittstelle I_Directory_Application_Maintenance" wie folgt angepasst

4.3 Schnittstelle I_Directory_Application_Maintenance

Die Schnittstelle ermöglicht die Administration der Fachdaten.

Der VZD stellt diese Schnittstelle als REST SchnittstelleLDAPv3 und Webservice (SOAP und REST) bereit. Deshalb sind die Unterkapitel „Nutzung“ und „Umsetzung“ jeweils für LDAPv3 und Webservice (SOAP und REST) vorhanden.

...

TIP1-A_5586-02 -VZD, I_Directory_Application_Maintenance, Webservice

Der VZD MUSS die Schnittstelle I_Directory_Application_Maintenance als REST Webservice Webservice (SOAP und REST über HTTPS) und als LDAPv3 über LDAPS implementieren. Der Webservice (SOAP) wird durch die Dokumente DirectoryApplicationMaintenance.wsdl und DirectoryApplicationMaintenance.xsd definiert. Der Webservice (REST) wird durch die [Directory_Application_Maintenance.yaml] Datei definiert. Die LDAPv3 Attribute sind in

dem Informationsmodell Abb_VZD_logisches_Datenmodell beschrieben.
[<=, Verzeichnisdienst, funkt. Eignung: Test Produkt/FA]

TIP1-A_5587 - VZD, Implementierung der LDAPv3 Schnittstelle

Der VZD MUSS die Schnittstelle I_Directory_Application_Maintenance gemäß den LDAPv3-Standards [RFC4510], [RFC4511], [RFC4512], [RFC4513], [RFC4514], [RFC4515], [RFC4516], [RFC4517], [RFC4518], [RFC4519], [RFC4520], [RFC4522] und [RFC4523] implementieren.

<=

TIP1-A_5588-01 -FAD, I_Directory_Application_Maintenance, Nutzung Webservice

Ein FAD, der Fachdaten im VZD verwalten will, MUSS entweder die Webservice- oder die LDAPv3-Schnittstelle (REST) nutzen.

[<=, KOM-LE FD, funkt. Eignung: Herstellererklärung]

TIP1-A_5589 - FAD, Implementierung der LDAPv3 Schnittstelle

Der FAD, der die LDAPv3-Schnittstelle I_Directory_Application_Maintenance des VZD nutzt, MUSS diese Schnittstelle gemäß den LDAPv3-Standards [RFC4510], [RFC4511], [RFC4512], [RFC4513], [RFC4514], [RFC4515], [RFC4516], [RFC4517], [RFC4518], [RFC4519], [RFC4520], [RFC4522] und [RFC4523] implementieren. Die LDAPv3-Attribute sind in dem Informationsmodell Abb_VZD_logisches_Datenmodell beschrieben.

<=

A_23728-01 - VZD, I_Directory_Application_Maintenance, Aktualisierung zulässiger Anwendungskennzeichen

Der VZD MUSS täglich um 4:00 Uhr das FHIR CodeSystems mit den Anwendungskennzeichen aus Simplifier ([https://simplifier.net/app-transport-framework/app-tags-cs/\\$download?format=json](https://simplifier.net/app-transport-framework/app-tags-cs/$download?format=json)) aktualisieren und

<=

Es werden Kapitel 4.3.2.1, 4.3.2.2, 4.3.2.3 und 4.3.2.4 gestrichen

4.3.2.1 Umsetzung SOAP

TIP1-A_5590 - VZD, Umsetzung add_Directory_FA-Attributes (SOAP)

Der VZD MUSS nach folgenden Vorgaben die Operation add_Directory_FA-Attributes implementieren:

1. Wenn kein zur Telematik-ID gehörender Basisdatensatz gefunden wurde, wird der Request mit einem gematik SOAP-Fault beendet:
faultcode: 4312,
faultstring: Basisdaten konnten nicht gefunden werden.
2. Ein bereits zur Telematik-ID gehörender Fachdatensatz wird gelöscht und neu angelegt.
3. Ein noch nicht existierender Fachdatensatz zur Telematik-ID wird im LDAP Directory neu angelegt.
4. Die Daten aus dem SOAP Request werden gemäß VZD_TAB_I_Directory_Application_Maintenance_Add_Mapping zum Basisdatensatz hinzugefügt.

Tabelle 7: VZD_TAB_I_Directory_Application_Maintenance_Add_Mapping

SOAP-Request Element	LDAP-Directory Basisdatensatz Attribut
VZD:timestamp	wird nicht in das LDAP-Directory eingetragen
VZD:Telematik-ID	
<FA-Attributes>	fachdienstspezifische Attribute. Die SOAP-Request-Elemente werden namensgleich als LDAP-Attribute übernommen.

Es müssen die Fehlermeldungen gemäß Tab_TUC_VZD_0006 verwendet werden.

<=

4.3.2.2 Nutzung SOAP

TIP1-A_5591 -- FAD, TUC_VZD_0006 "add_Directory_FA_Attributes (SOAP)"

Der FAD MUSS den technischen Use Case TUC_VZD_0006 "add_Directory_FA_Attributes" gemäß Tabelle Tab_TUC_VZD_0006 umsetzen.

Tabelle 8: Tab_TUC_VZD_0006

Name	add_Directory_FA_Attributes	
Beschreibung	Mit dieser Operation werden Fachdaten zu einem bestehenden Basisdaten-Eintrag zugefügt.	
Vorbedingungen	Keine.	
Eingangsdaten	SOAP-Request „addDirectoryFAAttributes“	
Komponenten	VZD, FAD	
Ausgangsdaten	SOAP-Response „responseMsg“	
Standardablauf	Aktion	Beschreibung
	Aufbau-TLS-Verbindung	Falls noch keine TLS-Verbindung besteht, wird eine aufgebaut. Der FAD authentisiert sich mit ID.FD.TLS-C.
	SOAP-Request senden	Der FAD ruft die SOAP-Operation VZD:addDirectoryFAAttributes auf.
	SOAP-Response empfangen	Die SOAP-Response VZD:responseMsg enthält den vzd:status. Im Fehlerfall wird eine gematik SOAP-Fault-

	Response empfangen
Fehlerfälle	<p>Es werden die protokollspezifischen Fehlermeldungen verwendet (TCP, HTTP, TLS):</p> <p>Fehler bei der Verarbeitung des SOAP Requests werden als gematik SOAP-Fault versendet:</p> <p>faultcode 4311, faultstring: Operation fehlerhaft ausgeführt, Fachdaten konnten nicht angelegt werden (Fehler im Verzeichnisdienst)</p> <p>faultcode 4312, faultstring: Basisdaten konnten nicht gefunden werden</p> <p>faultcode 4202, faultstring: SOAP Request enthält Fehler</p>

<=

TIP1-A_5592-03 - FAD, KOM-LE_FA_Add_Attributes

Der FAD MUSS für die FA KOM-LE die Fachdaten nach VZD_TAB_KOM-LE_Add_Attributes administrieren.

Tabelle 9: VZD_TAB_KOM-LE_Attributes

SOAP-Request-Element	LDAP-Directory Basisdatensatz Attribut
VZD:timestamp	wird nicht in das LDAP-Directory eingetragen
VZD:telematikID	
VZD:KOM-LE-EMail-Address	mail
VZD:version	KOM-LE-Version

<=

4.3.2.3 Umsetzung LDAPv3

TIP1-A_5593 - VZD, Umsetzung add_Directory_FA_Attributes (LDAPv3)

Der VZD MUSS nach folgenden Vorgaben die Operation add_Directory_FA_Attributes implementieren:

1. Wenn kein zur Telematik-ID gehörender Basisdatensatz gefunden wurde, wird der Request mit einer Fehlermeldung beendet.
2. Ein noch nicht existierender Fachdatensatz zur Telematik-ID wird im VZD neu angelegt.
3. Der FAD darf nur die zu seinem Dienst gehörenden Fachdaten schreiben.

Es müssen die Fehlermeldungen gemäß Tab_TUC_VZD_0007 verwendet werden.

<=

4.3.2.4 Nutzung LDAPv3

TIP1-A_5594 -- FAD, TUC_VZD_0007 "add_Directory_FA_Attributes (LDAPv3)"

Der FAD MUSS den technischen Use Case TUC_VZD_0007 „add_Directory_FA_Attributes(LDAPv3)“ gemäß Tabelle Tab_TUC_VZD_0007 unterstützen.

Tabelle 10: Tab_TUC_VZD_0007

Name	add_Directory_FA_Attributes(LDAPv3)	
Beschreibung	Mit dieser Operation werden Fachdaten zu einem bestehenden Eintrag zugefügt.	
Vorbedingungen	Der LDAPS-Verbindungsaufbau muss erfolgreich durchgeführt sein.	
Eingangsdaten	Add-Request gemäß [RFC4511]#4.7 und Informationsmodell (Abb_VZD_logisches_Datenmodell)	
Komponenten	LDAP-Client des FAD, Verzeichnisdienst	
Ausgangsdaten	gemäß [RFC4511]#4.7	
Standardablauf	Aktion	Beschreibung
	Add-Request senden	Der LDAP-Client des FAD sendet den Add-Request gemäß [RFC4511]#4.7 an den VZD. Die RFCs [RFC4510], [RFC4511], [RFC4513], [RFC4514], [RFC4515], [RFC4516], [RFC4519] und [RFC4522] müssen unterstützt werden.
	Add-Response empfangen	Der LDAP-Client empfängt das Ergebnis der Operation gemäß [RFC4511]#4.7.
Varianten/Alternativen	keine	
Zustand nach erfolgreichem Ablauf	Das Ergebnis der Operation liegt im LDAP-Client des FAD vor.	
Fehlerfälle	Zur Behandlung auftretender Fehlerfälle werden Fehlermeldungen gemäß [RFC4511]#Appendix A verwendet.	

<=

A_21834 - VZD, I_Directory_Application_Maintenance, KOM-LE_Version_Prüfung_LDAP

Der VZD MUSS bei Änderungen an KOM-LE-Fachdaten mit den Operationen "add_Directory_FA_Attributes (LDAPv3)" und "modify_Directory_FA_Attributes (LDAPv3)" den Inhalt von Parameter KOM-LE_Version des Operation Requests gegen die Liste der gültigen Werte prüfen. Im Falle von ungültigen Werten MUSS der VZD mit LDAP Result Code constraintViolation (19) antworten und darf die Operation nicht ausführen. Der VZD MUSS die Liste der gültigen Werte von Attribut KOM-LE_Version konfigurierbar realisieren und der gematik Änderungsmöglichkeiten über einen Service Request bieten.

<=

A_21835 - VZD, I_Directory_Application_Maintenance, Eindeutige Zuordnung von KOM-LE Adressen zu VZD-Einträgen LDAP

Der VZD MUSS sicherstellen, dass jede KOM-LE-Adresse mit den Operationen "add_Directory_FA_Attributes (LDAPv3)" und "modify_Directory_FA_Attributes (LDAPv3)" nur an maximal einen VZD-Eintrag angehängt wird. Hierzu MUSS er vor einer Eintragung einer KOM-LE-Adresse prüfen, ob diese bereits im VZD hinterlegt ist. Ist sie bereits hinterlegt, MUSS der VZD mit LDAP Result Code attributeOrValueExists (20) antworten und darf die Operation nicht ausführen.

<=

A_23729 - VZD, I_Directory_Application_Maintenance, Anwendungskennzeichen-Prüfung LDAP

Der VZD MUSS bei Änderungen an KOM-LE-Fachdaten mit den Operationen "add_Directory_FA_Attributes (LDAPv3)" und "modify_Directory_FA_Attributes (LDAPv3)" den Inhalt von Parameter Anwendungskennzeichen (appTags) des Operation Requests gegen die Liste der gültigen Werte prüfen. Im Falle von ungültigen Werten MUSS der VZD mit LDAP Result Code constraintViolation (19) antworten und darf die Operation nicht ausführen.

<=

Es werden Kapitel 4.3.3.1, 4.3.3.2, 4.3.3.3 und 4.3.3.4 gestrichen

4.3.3.1 Umsetzung SOAP

TIP1-A_5595 - VZD, Umsetzung delete_Directory_FA_Attributes

Der VZD MUSS nach folgenden Vorgaben die Operation delete_Directory_FA_Attributes implementieren:

1. Wenn kein zur Telematik-ID gehörender Basisdatensatz gefunden wurde, wird der Request mit einem gematik SOAP-Fault beendet:
faultcode: 4312,
faultstring: Basisdaten konnten nicht gefunden werden.
2. Ein zur Telematik-ID gehörender Fachdatensatz wird gelöscht.
3. Ein nicht existierender Fachdatensatz zur Telematik-ID führt zu keiner Aktion.

Es müssen die Fehlermeldungen gemäß Tab_TUC_VZD_0008 verwendet werden.

<=

4.3.3.2 Nutzung SOAP

TIP1-A_5596 -- FAD, TUC_VZD_0008 "delete_Directory_FA-Attributes (SOAP)"

Der FAD MUSS den technischen Use Case TUC_VZD_0008 "delete_Directory_FA-Attributes" gemäß Tabelle Tab_TUC_VZD_0008 umsetzen.

Tabelle 11: Tab_TUC_VZD_0008

Name	delete_Directory_FA-Attributes	
Beschreibung	Mit dieser Operation wird ein Fachdaten-Eintrag gelöscht.	
Vorbedingungen	Keine.	
Eingangsdaten	SOAP-Request „deleteDirectoryFAAttributes“	
Komponenten	VZD, FAD	
Ausgangsdaten	SOAP-Response „responseMsg“	
Standardablauf	Aktion	Beschreibung
	Aufbau TLS-Verbindung	Falls noch keine TLS-Verbindung besteht, wird eine aufgebaut. Der FAD authentisiert sich mit ID.FD.TLS-C.
	SOAP-Request senden	Der FAD ruft die SOAP-Operation VZD:deleteDirectoryFAAttributes auf.
	SOAP-Response empfangen	Die SOAP-Response VZD:responseMsg enthält den vzd:status. Im Fehlerfall wird eine gematik SOAP Fault-Response empfangen
Fehlerfälle	<p>Es werden die protokollspezifischen Fehlermeldungen verwendet (TCP, HTTP, TLS):</p> <p>Fehler bei der Verarbeitung des SOAP Requests werden als gematik SOAP-Fault versendet:</p> <p>faultcode 4321, faultstring: Operation fehlerhaft ausgeführt, Fachdaten konnten nicht gelöscht werden (Fehler im Verzeichnisdienst)</p> <p>faultcode 4312, faultstring: Basisdaten konnten nicht gefunden werden</p> <p>faultcode 4202, faultstring: SOAP Request enthält Fehler</p>	

<=

4.3.3.3 Umsetzung LDAPv3

TIP1-A_5597 -- VZD, Umsetzung delete_Directory_FA-Attributes (LDAPv3)

Der VZD MUSS nach folgenden Vorgaben die Operation delete_Directory_FA Attributes implementieren:

1. Wenn kein zur Telematik-ID gehörender Basisdatensatz gefunden wurde, wird der Request beendet.
2. Ein zur Telematik-ID gehörender Fachdatensatz wird gelöscht.
3. Ein nicht existierender Fachdatensatz zur Telematik-ID führt zu keiner Aktion.
4. Der FAD darf nur die zu seinem Dienst gehörenden Fachdaten löschen.

Es müssen die Fehlermeldungen gemäß Tab_TUC_VZD_0009 verwendet werden.

<=

4.3.3.4 Nutzung LDAPv3

TIP1-A_5598 - FAD, TUC_VZD_0009 "delete_Directory_FA Attributes (LDAPv3)"

Der FAD MUSS den technischen Use Case TUC_VZD_0009 „delete_Directory_FA Attributes (LDAPv3)“ gemäß Tabelle Tab_TUC_VZD_0009 unterstützen.

Tabelle 12: Tab_TUC_VZD_0009

Name	delete_Directory_FA Attributes (LDAPv3)	
Beschreibung	Mit dieser Operation werden alle Fachdaten zu einem bestehenden Eintrag gelöscht.	
Vorbedingungen	Der LDAPS-Verbindungsaufbau muss erfolgreich durchgeführt sein.	
Eingangsdaten	Delete-Request gemäß [RFC4511]#4.8 und Informationsmodell (Abb_VZD_logisches_Datenmodell)	
Komponenten	LDAP-Client des FAD, Verzeichnisdienst	
Ausgangsdaten	gemäß [RFC4511]#4.8	
Standardablauf	Aktion	Beschreibung
	Delete-Request senden	Der LDAP-Client des FAD sendet den delete-Request gemäß [RFC4511]#4.8 an den VZD. Die RFCs [RFC4510], [RFC4511], [RFC4513], [RFC4514], [RFC4515], [RFC4516], [RFC4519] und [RFC4522] müssen unterstützt werden.

	Delete-Response-empfangen	Der LDAP Client empfängt das Ergebnis der Operation gemäß [RFC4511]#4.8.
Varianten/Alternativen	keine	
Zustand nach erfolgreichem Ablauf	Das Ergebnis der Operation liegt im LDAP Client des FAD vor.	
Fehlerfälle	Zur Behandlung auftretender Fehlerfälle werden Fehlermeldungen gemäß [RFC4511]#Appendix A verwendet.	

<=

Es wird Kapitel "4.3.3.5 Umsetzung REST" wie folgt angepasst

4.3.3.5 Umsetzung REST

A_21460-01 -VZD, Umsetzung delete_Directory_FA-Attributes (REST)

Der VZD MUSS nach folgenden Vorgaben die Operation delete_Directory_FA-Attributes implementieren:

1. Wenn kein zur Telematik-ID gehörender Basisdatensatz gefunden wurde, wird der Request mit einem HTTP-Statuscode beendet:
HTTP-Statuscode: 404
2. Ein zur Telematik-ID gehörender Fachdatensatz wird gelöscht.
3. Ein nicht existierender Fachdatensatz zur Telematik-ID führt zu keiner Aktion und HTTP-Statuscode: 404 200 im Response.

[<=,Verzeichnisdienst,funkt. Eignung: Test Produkt/FA]

Es werden Kapitel 4.3.4.1, 4.3.4.2, 4.3.4.3 und 4.3.4.4 gestrichen

4.3.4.1 Umsetzung SOAP

TIP1-A_5599-01 - VZD, Umsetzung modify_Directory_FA-Attributes

Der VZD MUSS nach folgenden Vorgaben die Operation modify_Directory_FA-Attributes implementieren:

1. Wenn kein zur Telematik-ID gehörender Basisdatensatz gefunden wurde, wird der Request mit einem gematik SOAP-Fault beendet:
faultcode: 4312,
faultstring: Basisdaten konnten nicht gefunden werden.
2. Ein bereits zur Telematik-ID gehörender Fachdatensatz wird überschrieben.
3. Die Daten aus dem SOAP Request werden gemäß VZD_TAB_I_Directory_Application_Maintenance_Modify_Mapping zum Basisdatensatz hinzugefügt.
4. Für die Koexistenz dieser Operation mit den Erweiterungen für das Anwendungskennzeichen MÜSSEN folgende Vorgaben umgesetzt werden:

- Beim Aufruf von `modify_Directory_FA_Attributes` wird das Attribut "Mail" übergeben. KimData MUSS basierend auf der übergebenen Mail-Adresse gefüllt werden, wobei die Subattribute "Version" und "AppTags" (falls vorhanden) erhalten bleiben.
- Wenn das KimData-Attribut für eine Mail-Adresse vor dem Aufruf von `modify_Directory_FA_Attributes` gepflegt ist, das KomLeData-Attribut jedoch leer ist, DÜRFEN keine Änderungen an den Attributen KomLeData und KimData für diese Mail-Adresse vorgenommen werden.
- Bestehende KimData-Einträge DÜRFEN durch `modifyDirectoryFAAttributes` NICHT entfernt werden.

Tabelle 13: VZD_TAB_I_Directory_Application_Maintenance_Modify_Mapping

SOAP-Request Element	LDAP-Directory Basisdatensatz Attribut
VZD:timestamp	wird nicht in das LDAP-Directory eingetragen
VZD:Telematik-ID	
<FA-Attributes>	fachdienstspezifische Attribute. Die SOAP-Request-Elemente werden namensgleich als LDAP-Attribute übernommen.

Es müssen die Fehlermeldungen gemäß Tab_TUC_VZD_0010 verwendet werden.

<=>

4.3.4.2 Nutzung SOAP

TIP1-A_5600 - FAD, TUC_VZD_0010 "modify_Directory_FA_Attributes (SOAP)"

Der FAD MUSS den technischen Use Case TUC_VZD_0010 "modify_Directory_FA_Attributes" gemäß Tabelle Tab_TUC_VZD_0010 umsetzen.

Tabelle 14: Tab_TUC_VZD_0010

Name	<code>modify_Directory_FA_Attributes</code>
Beschreibung	Mit dieser Operation werden Fachdaten geändert.
Vorbedingungen	Keine.
Eingangsdaten	SOAP-Request „ <code>modifyDirectoryFAAttributes</code> “
Komponenten	VZD, FAD
Ausgangsdaten	SOAP-Response „ <code>responseMsg</code> “

Standardablauf	Aktion	Beschreibung
	Aufbau-TLS-Verbindung	Falls noch keine TLS-Verbindung besteht, wird eine aufgebaut. Der FAD authentisiert sich mit ID.FD.TLS-C.
	SOAP-Request senden	Der FAD ruft die SOAP-Operation VZD:modifyDirectoryFAAttributes auf.
	SOAP-Response empfangen	Die SOAP-Response VZD:responseMsg enthält den vzd:status. Im Fehlerfall wird eine gematik SOAP-Fault-Response empfangen
Fehlerfälle	Es werden die protokollspezifischen Fehlermeldungen verwendet (TCP, HTTP, TLS). Fehler bei der Verarbeitung des SOAP-Requests werden als gematik SOAP-Fault versendet: faultcode 4331, faultstring: Operation fehlerhaft ausgeführt, Fachdaten konnten nicht geändert werden (Fehler im Verzeichnisdienst) faultcode 4312, faultstring: Basisdaten konnten nicht gefunden werden faultcode 4202, faultstring: SOAP-Request enthält Fehler	

<=

TIP1-A_5601-03 -- FAD, KOM-LE_FA_Modify_Attributes

Der FAD MUSS für die FA KOM-LE die Fachdaten nach VZD_TAB_KOM-LE_Modify_Attributes administrieren.

Tabelle 15: VZD_TAB_KOM-LE_Attributes

SOAP-Request Element	LDAP-Directory Basisdatensatz Attribut
VZD:timestamp	wird nicht in das LDAP-Directory eingetragen
VZD:telematikID	
VZD:KOM-LE-EMail-Address	mail
VZD:version	KOM-LE-Version

<=

4.3.4.3 Umsetzung LDAPv3

TIP1-A_5602 -- VZD, Umsetzung modify_Directory_FA_Attributes (LDAPv3)

Der VZD MUSS nach folgenden Vorgaben die Operation modify_Directory_FA_Attributes implementieren:

1. Wenn kein zur Telematik-ID gehörender Basisdatensatz gefunden wurde, wird der Request beendet.
2. Ein bereits zur Telematik-ID gehörender Fachdatensatz wird geändert.
3. Der FAD darf nur die zu seinem Dienst gehörenden Fachdaten ändern.

Es müssen die Fehlermeldungen gemäß Tab_TUC_VZD_0011 verwendet werden.

<=

4.3.4.4 Nutzung LDAPv3

TIP1-A_5603 -- FAD, TUC_VZD_0011 "modify_Directory_FA_Attributes (LDAPv3)"

Der FAD MUSS den technischen Use Case TUC_VZD_0011 „modify_Directory_FA_Attributes(LDAPv3)“ gemäß Tabelle Tab_TUC_VZD_0011 unterstützen.

Tabelle 16: Tab_TUC_VZD_0011

Name	modify_Directory_FA_Attributes(LDAPv3)	
Beschreibung	Mit dieser Operation werden Fachdaten zu einem bestehenden Eintrag geändert.	
Vorbedingungen	Der LDAPS-Verbindungsaufbau muss erfolgreich durchgeführt sein.	
Eingangsdaten	Modify-Request gemäß [RFC4511]#4.6 und Informationsmodell (Abb_VZD_logisches_Datenmodell)	
Komponenten	LDAP-Client des FAD, Verzeichnisdienst	
Ausgangsdaten	gemäß [RFC4511]#4.6	
Standardablauf	Aktion	Beschreibung
	Modify-Request-senden	Der LDAP-Client des FAD sendet den modify-Request gemäß [RFC4511]#4.6 an den VZD. Die RFCs [RFC4510], [RFC4511], [RFC4513], [RFC4514], [RFC4515], [RFC4516], [RFC4519] und [RFC4522] müssen unterstützt werden.
	Modify-Response-empfangen	Der LDAP-Client empfängt das Ergebnis der Operation gemäß [RFC4511]#4.6.
Varianten/Alternativen	keine	

Zustand nach erfolgreichem Ablauf	Das Ergebnis der Operation liegt im LDAP-Client des FAD vor.
Fehlerfälle	Zur Behandlung auftretender Fehlerfälle werden Fehlermeldungen gemäß [RFC4511]#Appendix A verwendet.

<=

Es wird Kapitel "4.3.7 Operation search_Directory_FA-Attributes" wie folgt angepasst

Die Anwendungsdaten können mit der im Folgenden beschriebenen Operation eingesehen werden.

4.3.7.1 Umsetzung REST

A_27223 -VZD, I_Directory_Application_Maintenance, search_Directory_FA-Attributes

Der VZD MUSS die Operation „search_Directory_FA-Attributes“ gemäß Tabelle Tab_VZD „search_Directory_FA-Attributes“ umsetzen.

Tabelle 17: Tab_VZD „search_Directory_FA-Attributes“

Name	search_Directory_FA-Attributes	
Beschreibung	Diese Operation ermöglicht die Suche und das Lesen von Anwendungsdaten.	
Eingangsdaten	REST-Request GET /DirectoryEntries/KOM-LE_Fachdaten operationId: search_Directory_FA-Attributes (siehe DirectoryApplicationMaintenance.yaml)	
	Parameter	Beschreibung
	Parameter zur Selektion der Anwendungsdaten	Siehe DirectoryApplicationMaintenance.yaml
Komponenten	Nutzer der Schnittstelle, Verzeichnisdienst	
Ausgangsdaten	REST-Response mit allen zu den Filter-Parametern passenden Anwendungsdaten.	
Ablauf	Der VZD sucht im LDAP-Verzeichnis die zu den Such-Parametern passenden Anwendungsdaten. Bei mehr als 100 gefundenen Einträgen werden nur 100 gefundene Einträge zurückgegeben.	
Fehlerfälle	Es werden die protokollspezifischen Fehlermeldungen verwendet (TCP, HTTP, TLS) und in DirectoryApplicationMaintenance.yaml mit spezifischen Fehlerbeschreibungen ergänzt.	

[<=, Verzeichnisdienst, funkt. Eignung: Herstellererklärung]

4.3.7.2 Nutzung REST

A_28423 -FAD, TUC_VZD_0017 "search_Directory_FA-Attributes (REST)"

Der FAD KANN den technischen Use Case TUC_VZD_0017 "TUC_VZD_0017" gemäß Tabelle Tab_TUC_VZD_0017 umsetzen.

Tabelle 18: Tab_TUC_VZD_0017

Name	search_Directory_FA-Attributes	
Beschreibung	Mit dieser Operation kann Anhand der Anwendungsdaten im VZD gesucht werden.	
Vorbedingungen	Keine.	
Eingangsdaten	REST-Request „search_Directory_FA-Attributes“	
Komponenten	VZD, FAD	
Ausgangsdaten	REST-Response mit den gefundenen VZD Einträgen	
Standardablauf	Aktion	Beschreibung
	Aufbau TLS-Verbindung	Falls noch keine TLS-Verbindung besteht, wird eine aufgebaut. Der FAD authentisiert sich mit ID.FD.TLS-C.
	REST-Request senden	Der FAD ruft die REST-Operation search_Directory_FA-Attributes auf.
	REST-Response empfangen	Die REST-Response enthält den HTTP-Statuscode und die Liste der gefundenen VZD-Einträge. Im Fehlerfall wird ein HTTP-Statuscode empfangen.
Fehlerfälle	Es werden die protokollspezifischen Fehlermeldungen verwendet (TCP, HTTP, TLS). Fehler bei der Verarbeitung des REST Requests werden als HTTP-Statuscode versendet.	

[<=,KOM-LE FD,funkt. Eignung: Herstellererklärung]

Es wird Kapitel "4.3.8 Operation readLog" wie folgt angepasst

Die Logdaten können mit der im Folgenden beschriebenen Operation eingesehen werden.

4.3.7.1 Umsetzung REST

A_27224 -VZD, I_Directory_Application_Maintenance, readLog

Der VZD MUSS Operation „readLog“ gemäß Tabelle Tab_VZD „readLog“ umsetzen.

Tabelle 19: Tab_VZD „readLog“

Name	readLog	
Beschreibung	Diese Operation ermöglicht das Lesen von Logdaten.	
Eingangsdaten	REST-Request GET /Log operationId:readLog (siehe DirectoryApplicationMaintenance.yaml)	
	Parameter	Beschreibung
	Parameter zur Selektion der Logdaten	Siehe DirectoryApplicationMaintenance
Komponenten	Nutzer der Schnittstelle, Verzeichnisdienst	
Ausgangsdaten	REST-Response mit allen zu den Filter-Parametern passenden Anwendungsdaten.	
Ablauf	Der VZD sucht im LDAP-Verzeichnis die zu den Such-Parametern passenden Logdaten und gibt sie als Ergebnis der Operation.	
Fehlerfälle	Es werden die protokollspezifischen Fehlermeldungen verwendet (TCP, HTTP, TLS) und in DirectoryApplicationMaintenance.yaml mit spezifischen Fehlerbeschreibungen ergänzt.	

【<=,Verzeichnisdienst,funkt. Eignung: Herstellererklärung】

4.3.7.2 Nutzung REST

A 28424 -FAD, TUC_VZD_0018 “readLog (REST)”

Der FAD KANN den technischen Use Case TUC_VZD_0018 “TUC_VZD_0018” gemäß Tabelle Tab_TUC_VZD_0018 umsetzen.

Tabelle 20: Tab_TUC_VZD_0017

Name	readLog	
Beschreibung	Mit dieser Operation kann der VZD gelesen werden.	
Vorbedingungen	Keine.	
Eingangsdaten	REST-Request „readLog“	
Komponenten	VZD, FAD	
Ausgangsdaten	REST-Response mit den gefundenen VZD Log-Einträgen	
Standardablauf	Aktion	Beschreibung
	Aufbau TLS-Verbindung	Falls noch keine TLS-Verbindung besteht, wird eine aufgebaut. Der FAD authentisiert sich mit ID.FD.TLS-C.

	REST-Request senden	Der FAD ruft die REST-Operation readLog auf.
	REST-Response empfangen	Die REST-Response enthält den HTTP-Statuscode und die Liste der gefundenen Log-Einträge. Im Fehlerfall wird ein HTTP-Statuscode empfangen.
Fehlerfälle	Es werden die protokollspezifischen Fehlermeldungen verwendet (TCP, HTTP, TLS). Fehler bei der Verarbeitung des REST Requests werden als HTTP-Statuscode versendet.	

[<=,KOM-LE FD,funkt. Eignung: Herstellererklärung]

Es wird Kapitel "4.6.1 Operationen der Schnittstelle I_Directory_Administration" wie folgt angepasst

4.6.1 Operationen der Schnittstelle I_Directory_Administration

...

A_18602-01 -VZD, I_Directory_Administration, keine Datenänderung über Maintenance Schnittstelle

Der VZD MUSS Änderungen an Basisdatensätzen und Zertifikatseinträgen (Certificate in Abb_VZD_logisches_Datenmodell) über andere Schnittstellen verhindern, wenn für den jeweiligen Eintrag Daten über die Schnittstelle I_Directory_Administration eingetragen wurden (LDAP-Directory Attribut dataFromAuthority == TRUE).
Nicht erlaubte Änderungen MUSS der VZD mit ~~faultcode 4202 (faultstring: SOAP Request enthält Fehler)~~ HTTP Statuscode "400 Bad Request" ablehnen. [<=,Verzeichnisdienst,funkt. Eignung: Test Produkt/FA]

...

Es wird Kapitel "4.6.1.4 DirectoryEntry Synchronization" wie folgt angepasst

4.6.1.4 DirectoryEntry Synchronization

...

A_20402-04 -VZD, I_Directory_Administration, read_Directory_Entry_for_Sync, Paging, Berechtigung

Der VZD MUSS für den Paging Mechanismus von Operation „read_Directory_Entry_for_Sync“ sicherstellen:

- Die pagingSize darf die Maximalgröße entsprechend [TIP1-A_5552] nicht überschreiten.
- Die Suchparameter dürfen sich während eines Pagings (mit mehreren Request/Response Sequenzen) nicht ändern (nur das "cookie" ändert sich).

~~Bei Abweichungen von diesen Festlegungen MUSS der VZD mit einem Fehler (HTTP-Status-Code 403) antworten.~~

Bei Abweichungen von der Maximalgröße der pagingSize MUSS der VZD mit einem Fehler (HTTP-Status-Code 403) antworten.

Bei geänderten Suchparametern MUSS der VZD die Anfrage als neue Suchanfrage behandeln und den "cookie" ignorieren (HTTP-Status-Code 200).

[<=,Verzeichnisdienst,funkt. Eignung: Test Produkt/FA]

...

Es wird Kapitel "5 Datenmodell" wie folgt angepasst

TIP1-A_5607-13 -VZD, logisches Datenmodell

Der VZD MUSS das logische Datenmodell nach Abb_VZD_logisches_Datenmodell und Tab_VZD_Datenbeschreibung implementieren. Es wird keine Vorgabe an die technische Ausprägung des Datenmodells gemacht.

Der VZD MUSS sicherstellen, dass ein Eintrag nur Zertifikate aus dem Vertrauensraum der TI mit gleicher Telematik-ID enthält.

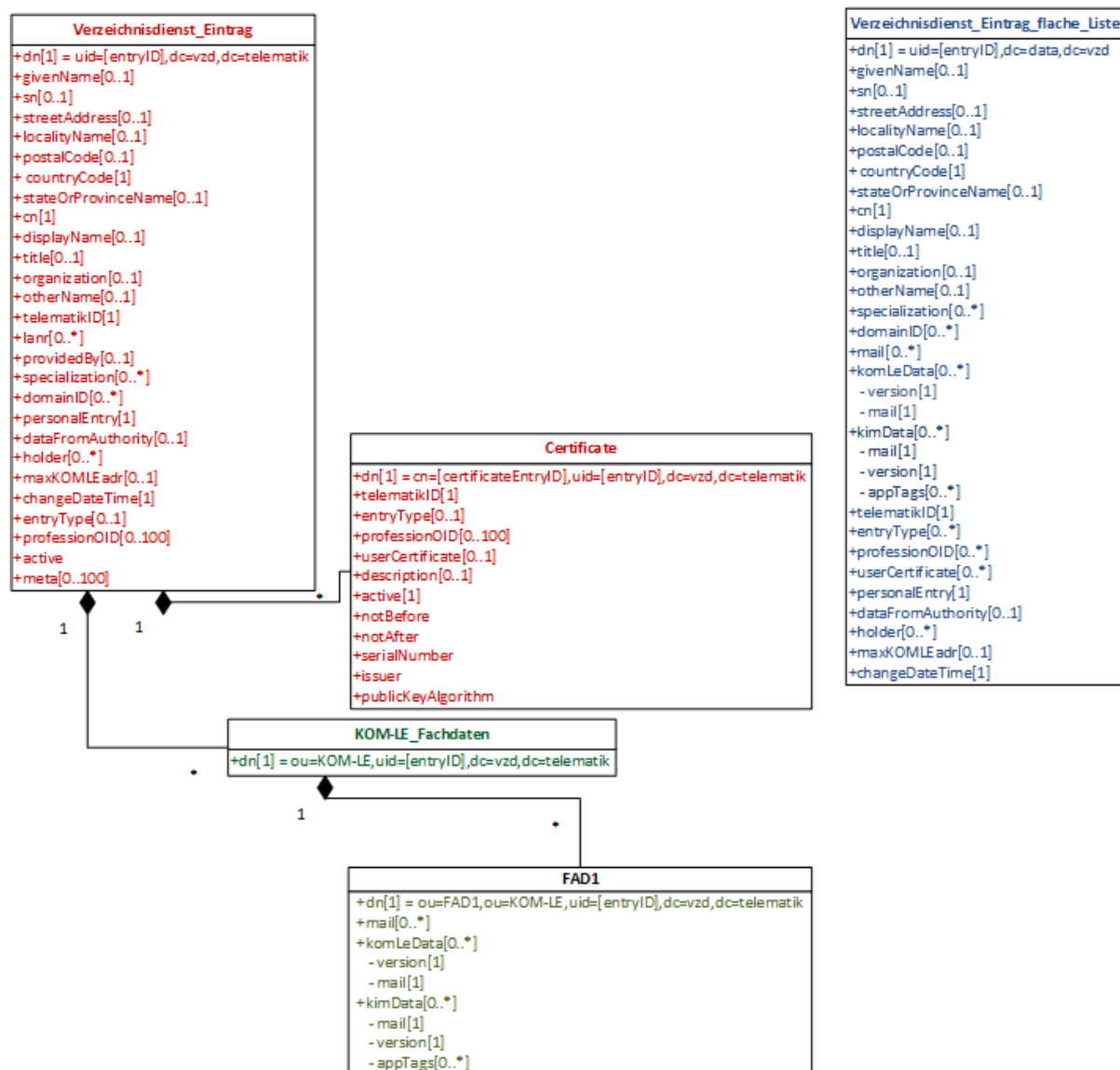


Abbildung 1: Abb_VZD_logisches_Datenmodell

Tabelle 21: Tab_VZD_Datenbeschreibung

LDAP-Directory Attribut	Pflichtfeld?	Erläuterung

givenName	optional	<p>HBA-Eintrag: Bezeichner: Vorname, Wird vom VZD aus dem Zertifikatsattribut givenName übernommen, wenn der Client von Schnittstelle I_Directory_Administration keinen Wert angibt. Wird über die Schreiboperationen von Schnittstelle I_Directory_Administration für givenName ein Inhalt geliefert, so wird dieser Wert für das Attribut gesetzt.</p> <p>Wird dem Verzeichniseintrag ein neues Zertifikat hinzu gefügt, wird der aktuelle Wert des Attributs durch der Wert aus Zertifikatsattribut givenName überschrieben.</p> <p>SMC-B-Eintrag: wird nicht verwendet</p>
sn	optional	<p>Wird von E-Mail-Clients für die Suche nach Einträgen und die Anzeige von gefundenen Einträgen verwendet.</p> <p>HBA-Eintrag: Bezeichner: Nachname Verhalten der Befüllung des Attributs bei Nutzung der Operationen</p> <ul style="list-style-type: none"> • add_Directory_Entry: <ul style="list-style-type: none"> • Wird sn als Parameter übergeben, wird der angegebene Wert übernommen. • Wird sn nicht als Parameter übergeben, wird sn als Kopie von Parameter displayName gesetzt. • Wird sn und displayName nicht als Parameter übergeben und ein Zertifikat übergeben, wird sn mit dem Inhalt von Attribut surName aus dem Zertifikat gefüllt. • modify_Directory_Entry: <ul style="list-style-type: none"> • Wird sn als Parameter übergeben, wird der angegebene Wert übernommen. • Wird sn nicht als Parameter übergeben, wird sn als Kopie von Parameter displayName gesetzt. • add_Directory_Entry_Certificate <ul style="list-style-type: none"> • Bei dem Hinzufügen eines Zertifikats wird sn mit dem Inhalt von Attribut surName aus dem Zertifikat gefüllt/überschrieben. <p>SMC-B Eintrag: Verhalten der Befüllung des Attributs bei Nutzung der Operationen</p> <ul style="list-style-type: none"> • add_Directory_Entry: <ul style="list-style-type: none"> • Wird sn als Parameter übergeben, wird der angegebene Wert übernommen. • Wird sn nicht als Parameter übergeben, wird sn als Kopie von Parameter displayName gesetzt. • Wird sn und displayName nicht als Parameter übergeben, wird sn auf einen leeren Wert gesetzt ("-" im LDAP-View). • modify_Directory_Entry: <ul style="list-style-type: none"> • Wird sn als Parameter übergeben, wird der angegebene Wert übernommen. • Wird sn nicht als Parameter übergeben, wird sn gelöscht ("-" im LDAP-View).

		<ul style="list-style-type: none"> add_Directory_Entry_Certificate Hat keine Auswirkungen auf das sn Attribut.
cn	obligatorisch	<p>Wird von E-Mail Clients für die Suche nach Einträgen und die Anzeige von gefundenen Einträgen verwendet</p> <p>HBA: Eintrag: Bezeichner: Nachname, Vorname</p> <p>SMC-B Eintrag: Bezeichner: Name</p> <p>Unabhängig vom Kartentyp wird bei Nutzung der Schreiboperationen von Schnittstelle I_Directory_Administration cn als Kopie von Attribut displayName gesetzt, wenn cn nicht als Parameter übergeben wird. Wird cn als Parameter übergeben, wird der angegebene Wert übernommen.</p>
displayName	optional	<p>Bezeichner: Anzeigename, Name, nach dem der Eintrag von Nutzern gesucht wird, und unter dem gefundene Einträge angezeigt werden.</p> <p>HBA: Konvention für HBA Einträge: Name, Vorname Dieses Attribut wird genutzt, um den Namen der Person gegenüber dem Anwender darzustellen (Verwendung als Filter-Attribut, um die Suche einzuschränken, und bei der Darstellung des Ergebnisses).</p> <p>SMC-B: Dieses Attribut wird genutzt, um den Namen der Betriebsstätte gegenüber dem Anwender darzustellen (Verwendung als Filter-Attribut, um die Suche einzuschränken, und bei der Darstellung des Ergebnisses).</p> <p>Unabhängig vom Kartentyp: Dieses Attribut wird durch den VZD nicht automatisch aus dem Zertifikat ermittelt. Es kann über die Schreiboperationen von Schnittstelle I_Directory_Administration gesetzt werden. Wird über die Operation add_Directory_Entry von Schnittstelle I_Directory_Administration für displayName kein Inhalt geliefert, so wird in displayName der Wert "-" gesetzt.</p>
streetAddress	optional	<p>Bezeichner: Straße und Hausnummer</p> <p>Alias: street (wird vom VZD in der Response zu einer LDAP Query verwendet)</p>
postalCode	optional	Bezeichner: Postleitzahl
countryCode	optional obligatorisch	<p>Kann beim Anlegen des Datensatzes und beim Ändern gesetzt werden (falls nicht gesetzt, ergänzt der VZD den Defaultwert für Deutschland). Bei der Anlieferung einer PLZ, StateOrProvince, City, Straße muss ein CountryCode obligatorisch gesetzt werden. Nicht-Anlieferung führt zu einem "Bad Request"-Fehler (Fehlercode 400).</p>
localityName	optional	<p>Bezeichner: Ort</p> <p>Alias: l (wird vom VZD in der Response zu einer LDAP Query verwendet)</p>

stateOrProvinceName	optional	Bezeichner: Bundesland oder Region Alias: st (wird vom VZD in der Response zu einer LDAP Query verwendet)
title	optional	HBA: Bezeichner: Titel SMC-B: nicht verwendet
organization	optional	HBA: Bezeichner: Name der Organisation oder Name der Betriebsstätte SMC-B: Alternativer Name, nach dem der Eintrag von Nutzern gesucht wird, und unter dem gefundene Einträge angezeigt werden
otherName	optional	Bezeichner: Anderer Name Veraltet: Wird für die Suche nach Einträgen und die Anzeige von gefundenen Einträgen nicht benötigt (siehe displayName und organization)
specialization	optional	<p>Bezeichner: Fachgebiet Kann mehrfach vorkommen (1..100).</p> <p>Für Einträge der Leistungserbringerorganisationen außer Apotheken (SMC-B Eintrag) Der Wertebereich entspricht den in hl7 definierten und für ePA festgelegten Werten(https://wiki.hl7.de/index.php?title=IG:Value_Sets_f%C3%BCr_XDS#DocumentEntry.practiceSettingCode). urn:psc:<OID Codesystem:Code> Beispiel für Allgemeinmedizin: urn:psc:1.3.6.1.4.1.19376.3.276.1.5.4:ALLG Beispiel für Zahnmedizin: urn:psc:1.3.6.1.4.1.19376.3.276.1.5.4:MKZH Beispiel für Zahnmedizin: urn:psc:1.3.6.1.4.1.19376.3.276.1.5.4:MZKH Beispiel für Krankenhaus: urn:psc:1.3.6.1.4.1.19376.3.276.1.5.4:GESU</p> <p>Für Einträge der Apotheken (SMC-B Eintrag) Im Attribut specialization werden die Apothekentypen (OffizinApo, Versand etc) erfasst. Hierfür wird das dafür definierten CodeSysteme PharmacyTypeCS (https://simplifier.net/vzd-fhir-directory/pharmacytypecs) genutzt. Default für das Attribut ist LEER. LEER wird in der eRezept Anwendung gleich behandelt wie "Sonstige_offen".</p> <p>Für Einträge der Leistungserbringer (HBA-Eintrag) Der Wertebereich entspricht den in hl7 definierten Werten (https://wiki.hl7.de/index.php?title=IG:Value_Sets_f%C3%BCr_XDS#DocumentEntry.authorSpecialty). urn:as:<OID Codesystem:Code> Psychologischer Psychotherapeut: urn:as:1.3.6.1.4.1.19376.3.276.1.5.11:82 Psychotherapeut: urn:as:1.3.6.1.4.1.19376.3.276.1.5.11:183 Fachpsychotherapeut für Kinder und Jugendliche: urn:as:1.3.6.1.4.1.19376.3.276.1.5.11:184 Fachpsychotherapeut für Erwachsene: urn:as:1.3.6.1.4.1.19376.3.276.1.5.11:185 Beispiel für FA Allgemeinmedizin: urn:as:1.2.276.0.76.5.514:011001 Beispiel für Zahnarzt: urn:as:1.2.276.0.76.5.492:1</p>

domainID	optional	Bezeichner: domänenspezifisches Kennzeichen des Eintrags. kann mehrfach vorkommen (0..100)
holder	optional	Legt fest, wer Änderungen an den Basisdaten des Eintrags vornehmen darf. Hat keinen Einfluss auf Fachdaten und Zertifikatsdaten.
maxKOMLEader	optional	Maximale Anzahl von mail Adressen in den KOM-LE-Fachdaten. Falls kein Wert eingetragen wurde, können beliebig viele mail Adressen in den KOM-LE Fachdaten eingetragen werden. Falls ein Wert eingetragen wurde, können maximal so viele mail Adressen in den KOM-LE Fachdaten eingetragen werden.
personalEntry	obligatorisch	Wird vom VZD eingetragen Wert == TRUE, wenn baseDirectoryEntry.entryType 1 hat (Berufsgruppe), Wert == FALSE sonst. Nach Löschung aller Zertifikate bleibt der Wert dieses Attributs `personalEntry` erhalten.
dataFromAuthority	optional	Wird vom VZD eingetragen Wert == TRUE, wenn der Verzeichnisdienst_Eintrag von dem Kartenherausgeber geschrieben wurde, Wert == FALSE sonst
active	obligatorisch	Mit diesem Attribut im Basiseintrag (Verzeichnisdienst_Eintrag in Abb_VZD_logisches_Datenmodell) kann der Client (Kartenherausgeber, TSP) die Aufnahme des VZD-Eintrags in die flache Liste steuern. Wenn das Attribut beim Anlegen eines VZD-Eintrags mit Zertifikat nicht angegeben wird, setzt der VZD das Attribut active auf TRUE (Default-Wert). Bei FALSE wird der Eintrag vom VZD aus der flachen Liste entfernt bzw. nicht übertragen. Dieses Attribut ist nicht in der flachen Liste enthalten. Wenn der VZD beim zeitlichen Ablauf des letzten Zertifikats einen VZD-Eintrag aus der flachen Liste entfernt, bleibt das Attribut active unverändert. Beim erneuten Hinzufügen eines Zertifikats wird der VZD-Eintrag also wieder in die flache Liste übernommen, wenn dieses Attribut den Wert "true" enthält.
meta	optional	Kann von den pflegenden Clients zur Abstimmung der Prozesse zwischen z. B. Kartenherausgeber und TSP genutzt werden. Dieses Attribut wird durch den VZD nicht ausgewertet. Die Werte für dieses Attribut müssen von den pflegenden Organisationen festgelegt und abgestimmt werden. Array von Strings (wird in LDAP auf <String, String> gemappt). Dieses Attribut ist nicht in der flachen Liste enthalten. Kann mehrfach vorkommen (0..100).
userCertificate	optional	Bezeichner: Enc-Zertifikat kann mehrfach vorkommen (0..50) Das Zertifikat wird gelöscht, wenn es ungültig geworden ist. Wenn kein Zertifikat vorliegt, dann kann der Eintrag nicht mittels LDAP-Abfrage gefunden werden. Format: DER, Base64-kodiert
notBefore	obligatorisch	Wird vom VZD bei Eintrag eines Zertifikats aus dem Zertifikat entnommen und ist nicht änderbar. Wird vom VZD zur Ermittlung der zeitlich gültigen Zertifikate

		genutzt. Dieses Attribut ist nicht in der flachen Liste enthalten.
userCertificate.active	obligatorisch	Wird vom VZD eingetragen. Wert == TRUE, wenn das userCertificate gemäß OCSP gültig ist (OCSP Response Status "good"), Wert == FALSE bei Zertifikaten von noch nicht freigeschalteten Karten (OCSP Response Status "unknown"). Wenn das Attribut den Wert FALSE enthält, wird der Zertifikatseintrag nicht in die flache Liste übernommen.
notAfter	obligatorisch	Wird vom VZD bei Eintrag eines Zertifikats aus dem Zertifikat entnommen und ist nicht änderbar. Wird vom VZD zur Ermittlung der zeitlich gültigen Zertifikate genutzt. Dieses Attribut ist nicht in der flachen Liste enthalten.
serialNumber	obligatorisch	Wird vom VZD bei Eintrag eines Zertifikats aus dem Zertifikat entnommen und ist nicht änderbar. Kann zur Suche nach Zertifikaten genutzt werden. Dieses Attribut ist nicht in der flachen Liste enthalten.
issuer	obligatorisch	Wird vom VZD bei Eintrag eines Zertifikats aus dem Zertifikat entnommen und ist nicht änderbar. Kann zur Suche nach Zertifikaten genutzt werden. Dieses Attribut ist nicht in der flachen Liste enthalten.
publicKeyAlgorithm	obligatorisch	Wird vom VZD bei Eintrag eines Zertifikats aus dem Zertifikat entnommen und ist nicht änderbar. Kann zur Suche nach Zertifikaten genutzt werden. Dieses Attribut ist nicht in der flachen Liste enthalten.
entryType	optional	Bezeichner: Eintragstyp Wird vom VZD anhand der im Zertifikat enthaltenen OID (Extension Admission, Attribut ProfessionOID) und der Spalte Eintragstyp in Tab_VZD_Mapping_Eintragstyp_und_ProfessionOID automatisch eingetragen. Siehe auch [gemSpecOID]# Tab_PKI_402 und Tab_PKI_403. entryType kann über Operationen add_Directory_Entry und modify_Directory_Entry gesetzt werden. Wird in Operation add_Directory_Entry ein Zertifikat angegeben wird, muss ein eventuell angegebener Parameter entryType mit dem Wert aus dem Zertifikat übereinstimmen. Bei nicht angegebenem Parameter entryType wird das Attribut entryType entsprechend dem Zertifikat gesetzt. Mit Operation modify_Directory_Entry kann über Request Parameter entryType das Attribut im VZD geändert werden, solange kein Zertifikat im VZD enthalten ist (welches dann einen abweichenden Wert gegenüber dem Request Parameter entryType enthalten würde). Wenn mit Operation add_Directory_Entry_Certificate ein neues Zertifikat hinzugefügt wird - welches in Bezug auf Attribut entryType vom Basisdatensatz abweicht - dann führt das zum Abbruch der Operation mit einem Fehler.
telematikID	obligatorisch	Bezeichner: TelematikID Wird vom VZD anhand der im jeweiligen Zertifikat enthaltenen Telematik-ID (Feld registrationNumber der Extension Admission) übernommen. Ist in den Basisdaten und in den Zertifikatsdaten enthalten.

lanr	optional	<p>Bezeichner: LANR</p> <p>Die lebenslange Arztnummer, kurz LANR, dient der Suche nach Ärzten. Insbesondere für die Suche durch Clients, welche die TelematikID nicht vorliegen haben.</p>
providedBy	optional	<p>Zusammenhängende Einträge können über das Attribut providedBy gekennzeichnet werden. Siehe Kapitel 4.6.3 Zusammenführung mehrerer TelematikID's zu einer Organisation</p>
professionOID	optional	<p>Bezeichner: Profession OID</p> <p>Wird vom VZD anhand der im Zertifikat enthaltenen OID (Extension Admission, Attribut ProfessionOID) und dem Mapping in Tab_VZD_Mapping_Eintragstyp_und_ProfessionOID automatisch eingetragen. Siehe [gemSpecOID#Tab_PKI_402 und Tab_PKI_403]. kann mehrfach vorkommen (0..100)</p>
description	optional	<p>Bezeichner: Beschreibung</p> <p>Dieses Attribut ermöglicht das Zertifikat zu beschreiben, um die Administration des VZD-Eintrags zu vereinfachen.</p> <p>Hinweis: wird aktuell nicht verwendet.</p>
mail	optional	<p>Bezeichner: KOM-LE-Mail-Adresse</p> <p>kann mehrfach vorkommen (0..1000)</p> <p>Wird vom KOM-LE-Fachdienst-Anbieter eingetragen.</p>
komLeData	optional	<p>Bezeichner: komLeData</p> <p>kann mehrfach vorkommen (0..1000)</p> <p>Enthält die KOM-LE-Version des Clientmoduls der angegebenen "mail" Adresse im Attribut "version". Anhand dieser Version erkennt das sendende Clientmodul, welche KOM-LE-Version vom Empfänger-Clientmodul unterstützt wird und in welchem Format die Mail an diesen Empfänger versandt wird.</p> <p>Wenn zu einer KOM-LE-Mail-Adresse aus Attribut Mail kein korrespondierender Eintrag (mit gleicher KOM-LE-Mail-Adresse) im komLeData Attribut enthalten ist, muss KOM-LE-Version 1.0 angenommen werden.</p> <p>Jeder Datensatz - bestehend aus Version und KOM-LE-Mail-Adresse - muss vollständig sein (beide Attribute sind obligatorisch).</p> <p>Zu beachten ist bei der Auswertung bzw. Pflege dieser Daten:</p> <ul style="list-style-type: none"> • Ein komLeData Eintrag setzt sich zusammen aus der Mail Adresse (Attribut "mail") und der zugehörigen KOM-LE Version (Attribut "version"). • Für jede Mail Adresse aus dem "mail" Attribut darf es nur einen Eintrag in Datenstruktur komLeData geben. Es dürfen in komLeData keine Mail Adressen referenziert werden, die nicht im übergeordneten "mail" Attribut enthalten sind. • Wenn eine Mail Adresse gelöscht wird, muss auch ihr komLeData Eintrag gelöscht werden. Geschrieben wird immer die gesamte Liste. Für Änderungen muss erst der aktuelle Eintrag gelesen werden und nach Änderung in der Liste der gesamte Eintrag wieder geschrieben werden. • Beispiel für den Wert eines komLeData Eintrags in der flachen Liste (Ausgabe einer LDAP Suche): komLeData: 1.0,mc_smcb_z@dom1.komle.telematik-

		test komLeData: 1.0,mz_smcb_za@dom2.kim.telematik-test komLeData: 1.0,mz_smcb_za@dom1.kim.telematik-test komLeData: 1.0,mb_secu_sm@dom3.kim.telematik-test komLeData: 1.0,mb_secu_sm@dom4.kim.telematik-test komLeData: 1.5,ak_secu_102@dom5.kim.telematik-test
kimData	optional	<p>Bezeichner: kimData kann mehrfach vorkommen (0..1000) Enthält die KOM-LE-Version des Clientmoduls der angegebenen "mail" Adresse im Attribut "version". Zusätzlich kann zur KOM-LE-Version ein "+" angegeben sein. Anhand dieser Version erkennt das sendende Clientmodul, welche KOM-LE-Version vom Empfänger-Clientmodul unterstützt wird und in welchem Format die Mail an diesen Empfänger versandt wird. Wenn ein zusätzliches "+" angegeben ist, dann können mit dieser "mail" Adresse Nachrichten größer 15MiB verarbeitet werden.</p> <p>Jeder Datensatz MUSS die Attribute KOM-LE-Mail-Adresse und Version enthalten (beide Attribute sind obligatorisch). Wenn noch keine Version zu einer KOM-LE-Mail-Adresse angegeben wurde, dann wird vom VZD die Version 1.0 eingetragen.</p> <p>Jeder Datensatz kann zusätzlich ein oder mehrere Anwendungskennzeichen der angegebenen "mail" Adresse im Attribut "appTags" enthalten. Anhand dieser Anwendungskennzeichen erkennt das sendende Clientmodul, welche KIM Anwendungen vom Empfänger verarbeitet werden können.</p> <p>Das Attribut Anwendungskennzeichen (appTags) ist optional. Wenn zu einer KOM-LE-Mail-Adresse kein Anwendungskennzeichen enthalten ist, können alle KIM Anwendungen an diesen Empfänger versendet werden.</p> <p>Die Bestandteile KOM-LE-Mail-Adresse, KOM-LE-Version und Anwendungskennzeichen sind jeweils durch das Zeichen "," getrennt.</p> <p>Wenn mehrere Anwendungskennzeichen angegeben sind, dann sind diese durch das Zeichen " " getrennt.</p> <p>Zu beachten ist bei der Auswertung bzw. Pflege dieser Daten:</p> <ul style="list-style-type: none"> • Ein kimData Eintrag setzt sich zusammen aus der Mail Adresse (Attribut "mail"), der zugehörigen KOM-LE Version (Attribut "version") inklusive dem optionalen "+" und optional einem oder mehreren Anwendungskennzeichen (Attribut "appTags"). • Bei Angabe von mehreren Anwendungskennzeichen werden sie im LDAP Attribut durch das ' ' Zeichen

		<p>getrennt (siehe Beispiel unten).</p> <ul style="list-style-type: none"> Für jede Mail Adresse darf es nur einen Eintrag in der Datenstruktur kimData geben. Wenn eine Mail Adresse gelöscht wird, muss auch ihr kimData Eintrag gelöscht werden. Geschrieben wird immer der gesamte kimData Eintrag inklusive aller enthaltenen Attribute mit ihren Werten (für alle Mail Adressen). Für Änderungen muss erst der aktuelle Eintrag gelesen werden und nach Änderung der gesamte Eintrag wieder geschrieben werden. Beispiel für den Wert eines kimData Eintrags in der flachen Liste (Ausgabe einer LDAP Suche): kimData: mc_smcb_z@dom1.komle.telematik-test,1.0,eEB kimData: mz_smcb_z@dom2.kim.telematik-test,1.0,DALE-UV eEB kimData: mz_smcb_z@dom1.kim.telematik-test,1.0 kimData: mb_secu_sm@dom3.kim.telematik-test,1.0 kimData: mb_secu_sm@dom4.kim.telematik-test,1.0 kimData: ak_secu_102@dom5.kim.telematik-test,1.5
changeDateTime	obligatorisch	Der VZD setzt dieses Attribut bei jeder Schreiboperation für den Datensatz (Basisdaten und Zertifikate) auf die aktuelle Zeit. Format entsprechend RFC 3339, section 5.6.

【<=,Verzeichnisdienst,funkt. Eignung: Herstellererklärung】

...

Tabelle 46: Tab_VZD_Mapping_Eintragstyp_und_ProfessionOID

Eintragstyp	Eintragstyp Bedeutung	ProfessionOID (ProfessionItem)
1	Berufsgruppe	1.2.276.0.76.4.30 (Ärztin/Arzt) 1.3.6.1.4.1.24796.4.11.1 (Ärztin/Arzt)* 1.2.276.0.76.4.31 (Zahnärztin/Zahnarzt) 1.2.276.0.76.4.32 (Apotheker/-in) 1.2.276.0.76.4.33 (Apothekerassistent/-in) 1.2.276.0.76.4.34 (Pharmazieingenieur/-in) 1.2.276.0.76.4.35 (pharmazeutisch-technische/-r Assistent/-in) 1.2.276.0.76.4.36 (pharmazeutisch-kaufmännische/-r Angestellte) 1.2.276.0.76.4.37 (Apothekenhelfer/-in) 1.2.276.0.76.4.38 (Apothekenassistent/-in) 1.2.276.0.76.4.39 (Pharmazeutische/-r Assistent/-in) 1.2.276.0.76.4.40 (Apothekenfacharbeiter/-in) 1.2.276.0.76.4.41 (Pharmaziepraktikant/-in) 1.2.276.0.76.4.42 (Stud.pharm. oder

		<p>Famulant/-in)</p> <p>1.2.276.0.76.4.43 (PTA-Praktikant/-in)</p> <p>1.2.276.0.76.4.44 (PKA Auszubildende/-r)</p> <p>1.2.276.0.76.4.45 (Psychotherapeut/-in)</p> <p>1.2.276.0.76.4.46 (Psychologische/-r Psychotherapeut/-in)</p> <p>1.2.276.0.76.4.47 (Kinder- und Jugendlichenpsychotherapeut/-in)</p> <p>1.2.276.0.76.4.48 (Rettungsassistent/-in)</p> <p>1.2.276.0.76.4.178 (Notfallsanitäter/-in)</p> <p>1.2.276.0.76.4.232 (Gesundheits- und Krankenpfleger/-in, Gesundheits- und Kinderkrankenpfleger/-in)</p> <p>1.2.276.0.76.4.233 (Altenpfleger/-in)</p> <p>1.2.276.0.76.4.234 (Pflegefachfrauen und Pflegefachmänner)</p> <p>1.2.276.0.76.4.235 (Hebamme)</p> <p>1.2.276.0.76.4.236 (Physiotherapeut/-in)</p> <p>1.2.276.0.76.4.237 (Augenoptiker/-in und Optometrist/-in)</p> <p>1.2.276.0.76.4.238 (Hörakustiker/-in)</p> <p>1.2.276.0.76.4.239 (Orthopädienschuhmacher/-in)</p> <p>1.2.276.0.76.4.240 (Orthopädietechniker/-in)</p> <p>1.2.276.0.76.4.241 (Zahntechniker/-in)</p> <p>1.2.276.0.76.4.274 (Ergotherapeut/-in)</p> <p>1.2.276.0.76.4.275 (Logopäde/Logopädin)</p> <p>1.2.276.0.76.4.276 (Podologe/Podologin)</p> <p>1.2.276.0.76.4.277 (Ernährungstherapeut/-in Leistungserbringer/-in Ernährungstherapie)</p> <p>1.2.276.0.76.4.305 (Orthopädienschuhmacher/-in und Orthopädietechniker/-in)</p> <p>1.2.276.0.76.4.308 (Augenoptiker/-in, Optometrist/-in und Hörakustiker/-in)</p> <p>1.2.276.0.76.4.312 Hilfsmittelerbringer/-in (Hinweis: Berufsgruppen der Hilfsmittelerbringer/-innen, die nicht den Gesundheitshandwerken zugeordnet sind)</p> <p>1.2.276.0.76.4.313 Frisör/-in</p> <p>1.2.276.0.76.4.315 Masseur/-in und medizinische/-r Bademeister/-in</p> <p>1.2.276.0.76.4.316 Leistungserbringer/-in Soziotherapie</p> <p>1.2.276.0.76.4.318 Leistungserbringer/in Stimm-, Sprech-, Sprach- und Schluck-Therapie</p> <p>1.2.276.0.76.4.319 Diätassistent/-in</p>
2	Versicherte/-r	1.2.276.0.76.4.49 (Versicherte/-r)
3	Leistungserbringer - institution	<p>1.2.276.0.76.4.50 (Betriebsstätte Arzt)</p> <p>1.2.276.0.76.4.51 (Zahnarztpraxis)</p>

		1.2.276.0.76.4.52 (Betriebsstätte Psychotherapeut) 1.2.276.0.76.4.53 (Krankenhaus) 1.2.276.0.76.4.54 (Öffentliche Apotheke) 1.2.276.0.76.4.55 (Krankenhausapotheke) 1.2.276.0.76.4.56 (Bundeswehraphotheke) 1.2.276.0.76.4.57 (Betriebsstätte Mobile Einrichtung Rettungsdienst) 1.2.276.0.76.4.245 (Betriebsstätte Gesundheits-, Kranken- und Altenpflege) 1.2.276.0.76.4.246 (Betriebsstätte Geburtshilfe) 1.2.276.0.76.4.247 (Betriebsstätte Physiotherapie) 1.2.276.0.76.4.248 (Betriebsstätte Augenoptiker) 1.2.276.0.76.4.249 (Betriebsstätte Hörakustiker) 1.2.276.0.76.4.250 (Betriebsstätte Orthopädienschuhmacher) 1.2.276.0.76.4.251 (Betriebsstätte Orthopädietechniker) 1.2.276.0.76.4.252 (Betriebsstätte Zahntechniker) 1.2.276.0.76.4.253 (Rettungsleitstelle) 1.2.276.0.76.4.254 (Betriebsstätte Sanitätsdienst Bundeswehr) 1.2.276.0.76.4.255 (Betriebsstätte Öffentlicher Gesundheitsdienst) 1.2.276.0.76.4.256 (Betriebsstätte Arbeitsmedizin) 1.2.276.0.76.4.257 (Betriebsstätte Vorsorge- und Rehabilitation) 1.2.276.0.76.4.278 (Ergotherapiepraxis) 1.2.276.0.76.4.279 (Logopaedische Praxis) 1.2.276.0.76.4.280 (Podologiepraxis) 1.2.276.0.76.4.281 (Ernährungstherapeutische Praxis) 1.2.276.0.76.4.304 (Betriebsstätte Augenoptiker und Hörakustiker) 1.2.276.0.76.4.306 (Betriebsstätte Orthopädienschuhmacher und Orthopädietechniker) 1.2.276.0.76.4.311 Betriebsstätte Hilfsmittelerbringer (Hinweis: Betriebsstätten der Hilfsmittelerbringer, welche nicht den Gesundheitshandwerken zugeordnet sind) 1.2.276.0.76.4.314 Betriebsstätte Frisör 1.2.276.0.76.4.317 Betriebsstätte Soziotherapie
4	Organisation	1.2.276.0.76.4.187 (Betriebsstätte Leistungserbringerorganisation Vertragszahnärzte)

		1.2.276.0.76.4.58 (Betriebsstätte gematik) 1.2.276.0.76.4.190 (AdV-Umgebung bei Kostenträger) 1.2.276.0.76.4.210 (Betriebsstätte Leistungserbringerorganisation Kassenärztliche Vereinigung) 1.2.276.0.76.4.223 (Betriebsstätte GKV-Spitzenverband) 1.2.276.0.76.4.226 (Betriebsstätte Mitgliedsverband der Krankenhäuser) 1.2.276.0.76.4.227 (Betriebsstätte der Deutsche Krankenhaus TrustCenter und Informationsverarbeitung GmbH) 1.2.276.0.76.4.228 (Betriebsstätte der Deutschen Krankenhausgesellschaft) 1.2.276.0.76.4.224 (Betriebsstätte Apothekerverband) 1.2.276.0.76.4.225 (Betriebsstätte Deutscher Apothekerverband) 1.2.276.0.76.4.229 (Betriebsstätte der Bundesärztekammer) 1.2.276.0.76.4.230 (Betriebsstätte einer Ärztekammer) 1.2.276.0.76.4.231 (Betriebsstätte einer Zahnärztekammer) 1.2.276.0.76.4.242 (Betriebsstätte der Kassenärztlichen Bundesvereinigung) 1.2.276.0.76.4.243 (Betriebsstätte der Bundeszahnärztekammer) 1.2.276.0.76.4.244 (Betriebsstätte der Kassenzahnärztlichen Bundesvereinigung) 1.2.276.0.76.4.262 (Betriebsstätte Pflegeberatung nach § 7a SGB XI) 1.2.276.0.76.4.263 (Betriebsstätte Psychotherapeutenkammer) 1.2.276.0.76.4.264 (Betriebsstätte Bundespsychotherapeutenkammer) 1.2.276.0.76.4.265 (Betriebsstätte Landesapothekerkammer) 1.2.276.0.76.4.266 (Betriebsstätte Bundesapothekerkammer) 1.2.276.0.76.4.267 (Betriebsstätte elektronisches Gesundheitsberuferegister) 1.2.276.0.76.4.268 (Betriebsstätte Handwerkskammer) 1.2.276.0.76.4.269 (Betriebsstätte Register für Gesundheitsdaten) 1.2.276.0.76.4.270 (Betriebsstätte Abrechnungsdienstleister) 1.2.276.0.76.4.271 (Betriebsstätte PKV-Verband) 1.2.276.0.76.4.284 (Betriebsstätte Weitere Kostenträger im Gesundheitswesen) 1.2.276.0.76.4.285 (Weitere Organisationen der Gesundheitsversorgung)
--	--	--

		1.2.276.0.76.4.292 (NCPeH Fachdienst)
5	Krankenkasse	1.2.276.0.76.4.59 (Betriebsstätte Kostenträger)
6	Krankenkasse ePA	1.2.276.0.76.4.273 (ePA-KTR-Zugriffsautorisierung)
7	KIM	1.2.276.0.76.4.286 (KIM-Hersteller und -Anbieter)
8	TIM	1.2.276.0.76.4.295 (TIM-Hersteller und -Anbieter)
9	DiGA	1.2.276.0.76.4.282 (DiGA-Hersteller und Anbieter)
10	Ombudsstelle	1.2.276.0.76.4.303 (Ombudsstelle eines Kostenträgers)

...

2 Änderung in gemSpec_VZD_FHIR_Directory

Es wird Kapitel "4.2.1.2" wie folgt angepasst

4.2.1.2 FHIR Schnittstelle für TI-Messenger-Nutzer FHIRDirectorySearchAPI

...

Das search-access_token enthält folgende Attribute:

```
{
  "iss": "https://fhir-directory-test.vzd.ti-dienste.de/tim-
authenticate",
  "sub": "@usr02:matrix.dev.service-ti.de",
  "aud": [
    "https://fhir-directory.vzd.ti-dienste.de/search",
    "https://fhir-directory.vzd.ti-dienste.de/certificates"
  ],
  "exp": 1759841621,
  "scope": "search:read certificate:read",
  "iat": 1759755221
}
```

Das Attribut "iss" enthält die URL des Endpunktes für die Authentisierung in der jeweiligen Umgebung RU, TU oder PU.

Das Attribut "aud" enthält die URL des der Endpunktes in der jeweiligen Umgebung RU, TU oder PU.

Das Attribut "sub" enthält die TI-Messenger Adresse des authentifizierten Nutzers.

Die zeitliche Gültigkeit des search-access_tokens beträgt 24 Stunden.

...

Es wird Kapitel "4.2.1.3" wie folgt angepasst

4.2.1.3 FHIR-Schnittstelle für Besitzer FHIRDirectoryOwnerAPI

Die Schnittstelle ermöglicht es den Besitzern einer Telematik-ID, ihren Eintrag im VZD-FHIR-Directory zu ändern. Im bei der Authentifizierung verwendeten Accesstoken ist die Telematik-ID des Nutzers enthalten. Nur der Eintrag (PractitionerDirectory oder OrganizationDirectory) mit der eigenen Telematik-ID darf verändert werden. Dabei dürfen nur die Attribute verändert werden, die nicht vom VZD-LDAP-Directory synchronisiert werden.

Holder können diese Schnittstelle ebenfalls zur Bearbeitung aller FHIR VZD Einträge in ihrer Zuständigkeit (sie sind als Holder im Datensatz eingetragen) nutzen. Die änderbaren Attribute für Holder werden schrittweise ausgebaut. Aktuell können die "Mehrwertdaten" von Apotheken und NCPeH Attribute - die nicht über den LDAP VZD gepflegt werden können - administriert werden. FHIR VZD Datensätze ohne gesetztes Holder Attribut

können nicht durch Holder im FHIR VZD gepflegt werden. Dazu muss erst das Holder Attribut des Datensatzes gesetzt werden. Das kann über den LDAP VZD oder durch einen FHIR VZD Super-Administrator erfolgen.

Endpunkte für das Ändern von eigenen Einträgen im VZD-FHIR-Directory durch TI-Messenger Clients und Org-Admin-Clients

In der Produktionsumgebung (PU) ist die URL:

<https://fhir-directory.vzd.ti-dienste.de/owner>

In der Referenzumgebung (RU) ist die URL:

<https://fhir-directory-ref.vzd.ti-dienste.de/owner>

In der Testumgebung (TU) ist die URL: <https://fhir-directory-tu.vzd.ti-dienste.de/owner>

Authentisierung

Um die Schnittstelle nutzen zu können, MÜSSEN sich die Clients mit einem gültigen Accesstoken authentisieren, das vom FHIR-Proxy ausgestellt wurde. Wenn kein gültiges Accesstoken im Client vorhanden ist, dann muss sich der Client an einem IDP der TI-IDP-Föderation authentisieren.

Nur der eigene Eintrag mit einem Identifier passend zur Telematik-ID aus dem Accesstoken KANN bearbeitet werden. Für einen eigenen OrganizationDirectory-Eintrag KÖNNEN weitere HealthcareService-Einträge erstellt und mit dem eigenen OrganizationDirectory-Eintrag verlinkt werden.

Das Accesstoken enthält folgende Attribute:

```
{
  "iss": "https://fhir-directory.vzd.ti-dienste.de/owner-
authenticate",
  "sub": "<telematikID>",
  "aud": [
    "https://fhir-directory-ref.vzd.ti-dienste.de/owner",
    "https://fhir-directory-ref.vzd.ti-dienste.de/search",
    "https://fhir-directory-ref.vzd.ti-dienste.de/PersonInstitutionLin
k",
    "https://fhir-directory-ref.vzd.ti-dienste.de/certificates",
    "https://fhir-directory-ref.vzd.ti-dienste.de/fachliches-log"
  ],
  "iat": 1630306800,
  "exp": 1630393200
  "scope": "owner:read owner:write search:read link:suggest
link:approve
link:deny link:read certificate:read log:read"
}
```

...

Das Holder-Access-Token enthält folgende Attribute:

```
{
  "scope": "search:read owner:read owner:write link:read link:deny
certificate:read
log:read",
}
```

```
"iss": "https://fhir-directory.vzd.ti-dienste.de/holder-
authenticate",
"aud": [
  "https://fhir-directory.vzd.ti-dienste.de/holder-services",
  "https://fhir-directory.vzd.ti-dienste.de/owner",
  "https://fhir-directory.vzd.ti-dienste.de/search",
  "https://fhir-directory.vzd.ti-dienste.de/PersonInstitutionLink",
  "https://fhir-directory.vzd.ti-dienste.de/certificates",
  "https://fhir-directory.vzd.ti-dienste.de/fachliches-log"
],
"iat": 1759753474,
"exp": 1759839874,
"sub": null,
"clientId": "<Die ClientID des authentifizierten Holders>",
"holderId": "<Die HolderID>"
}
```

...

Endpunkte für die Authentisierung

In der Produktionsumgebung (PU) ist die URL:

<https://fhir-directory.vzd.ti-dienste.de/owner-authenticate>

In der Referenzumgebung (RU) ist die

URL: <https://fhir-directory-ref.vzd.ti-dienste.de/owner-authenticate>

In der Testumgebung (TU) ist die URL: <https://fhir-directory-tu.vzd.ti-dienste.de/owner-authenticate>

FHIR VZD Endpunkte für die Authentisierung mit dem SmartcardIDP

In der Produktionsumgebung (PU) ist die URL:

<https://fhir-directory.vzd.ti-dienste.de/signin-gematik-idp-dienst>

In der Referenzumgebung (RU) ist die

URL: <https://fhir-directory-ref.vzd.ti-dienste.de/signin-gematik-idp-dienst>

In der Testumgebung (TU) ist die URL: <https://fhir-directory-test.vzd.ti-dienste.de/signin-gematik-idp-dienst>

FHIR-VZD-Endpunkte für die Authentisierung mit dem gematik Authenticator und Polling Endpunkt

In der Produktionsumgebung (PU) sind die URLs:

- <https://fhir-directory.vzd.ti-dienste.de/owner-authenticate-decoupled>
- <https://fhir-directory.vzd.ti-dienste.de/owner-authenticate-poll>
- <https://fhir-directory.vzd.ti-dienste.de/signin-gematik-idp-dienst-decoupled>

In der Referenzumgebung (RU) sind die URLs:

- <https://fhir-directory-ref.vzd.ti-dienste.de/owner-authenticate-decoupled>
- <https://fhir-directory-ref.vzd.ti-dienste.de/owner-authenticate-poll>
- <https://fhir-directory-ref.vzd.ti-dienste.de/signin-gematik-idp-dienst-decoupled>

In der Testumgebung (TU) sind die URLs:

- <https://fhir-directory-tu.vzd.ti-dienste.de/owner-authenticate-decoupled>

- <https://fhir-directory-tu.vzd.ti-dienste.de/owner-authenticate-poll>
- <https://fhir-directory-tu.vzd.ti-dienste.de/signin-gematik-idp-dienst-decoupled>

FHIR-VZD-Endpunkte für die Holder Authentisierung (Keycloak-AccessToken) mit Client Credentials

- In der Produktionsumgebung (PU) ist die URL:
<https://auth.vzd.ti-dienste.de:9443/auth/realms/RSDirectoryAdministration/protocol/openid-connect/token>
- In der Referenzumgebung (RU) ist die URL:
<https://auth-ref.vzd.ti-dienste.de:9443/auth/realms/RSDirectoryAdministration/protocol/openid-connect/token>
- In der Testumgebung (TU) ist die URL:
<https://auth-test.vzd.ti-dienste.de:9443/auth/realms/RSDirectoryAdministration/protocol/openid-connect/token>

FHIR-VZD-Endpunkte für den Tausch des Keycloak-AccessTokens gegen das Holder-AccessToken

- In der Produktionsumgebung (PU) ist die URL:
<https://fhir-directory.vzd.ti-dienste.de/holder-authenticate>
- In der Referenzumgebung (RU) ist die URL:
<https://fhir-directory-ref.vzd.ti-dienste.de/holder-authenticate>
- In der Testumgebung (TU) ist die URL:
<https://fhir-directory-tu.vzd.ti-dienste.de/holder-authenticate>

Operationen

Die FHIR-Operationen für das Ändern von eigenen Einträgen im VZD-FHIR-Directory sind in der HL7-FHIR-Spezifikation (<https://www.hl7.org/fhir/http.html>) festgelegt.

Daten

Das VZD-FHIR-Directory Datenmodell wird in Simplifier beschrieben [Simplifier-FHIR-VZD].

Für TI-Anwendungen werden die Kommunikationsadressen in den FHIR Endpoint eingetragen:

Tabelle 22: Tab_VZD_TI-Anwendungen_Endpoint

TI-Anwendung	Endpoint.connectionType code	Endpoint.payloadType code	Endpoint.address
TI Messenger	tim	tim-chat	<p>Format (MXID in URL Form) für User entsprechend [matrix-uri-scheme]:</p> <p>matrix:u/localpart:domainpart</p> <p>Beispiel MatrixID: @1-1tst-auto-ts-ow2:tim.test.gematik.de MatrixID im URL Format in Endpoint.address:</p>

			matrix:u/1-1tst-auto-ts- ow2: tim.test.gematik.de
--	--	--	--

Es wird Kapitel "4.2.1.4" wie folgt angepasst

4.2.1.4 Schnittstelle FHIRDirectoryTIMProviderAPI (I_VZD_TIM_Provider_Services.yaml)

...

Das provider-accesstoken enthält folgende Attribute:

```
{
  "iss": "https://fhir-directory.vzd.ti-dienste.de/ti-provider-authenticate",
  "sub": "<client_id>",
  "aud": [
    "https://fhir-directory-ref.vzd.ti-dienste.de/tim-provider-services",
    "https://fhir-directory-ref.vzd.ti-dienste.de/certificates"
  ],
  "scope": "federation:read federation:write",
  "iat": 1630306800,
  "exp": 1630308600,
  "clientId": "<client_id>"
}
```

Das Attribut "iss" enthält die URL des Endpunktes für die Authentisierung in der jeweiligen Umgebung RU, TU oder PU.

Das Attribut "aud" enthält die URL des Endpunktes in der jeweiligen Umgebung RU, TU oder PU.

Das Attribut "scope" enthält die Berechtigungen.

Die zeitliche Gültigkeit des provider-accesstokens beträgt 24 Stunden.

...

Es wird Kapitel "4.2.1.5" wie folgt angepasst

4.2.1.5 FHIR Schnittstelle für Versicherte FHIRDirectoryFdvSearchAPI

...

~~Das search-access_token (Fachdienste) enthält folgende Attribute:~~

Das search-access_token enthält - bei Authentisierung über Client Credentials (Fachdienste und Versicherte) - folgende Attribute:

```
{
  "sub": "<ClientID>",
  "scope": "certificate:read fdv_search:readsearch:read",
  "iss": "https://fhir-directory.vzd.ti-dienste.de/service-authenticate",
  "aud": [
    "https://fhir-directory.vzd.ti-dienste.de/fdv/search",
    "https://fhir-directory.vzd.ti-dienste.de/search",
    "https://fhir-directory.vzd.ti-dienste.de/certificates"
  ]
}
```



```
],  
"iat": 1759827516,  
"exp": 1759913916  
}
```

Das search-access_token (TIM-Clients von Versicherten) enthält folgende Attribute:

```
{  
  "iss": "https://fhir-directory-test.vzd.ti-dienste.de/tim-  
authenticate",  
  "sub": "@usr02:matrix.dev.service-ti.de",  
  "aud": [  
    "https://fhir-directory.vzd.ti-dienste.de/search",  
    "https://fhir-directory.vzd.ti-dienste.de/certificates"  
  ],  
  "exp": 1759841621,  
  "scope": "search:read certificate:read",  
  "iat": 1759755221  
}
```

Das Attribut "iss" enthält die URL des Endpunktes für die Authentisierung in der jeweiligen Umgebung RU, TU oder PU.

Das Attribut "aud" enthält die URLs des der Endpunktes in der jeweiligen Umgebung RU, TU oder PU.

Das Attribut "sub" enthält die TI-Messenger Adresse des authentifizierten Nutzers bzw. die ClientID bei Authentisierung über Client Credentials.

Die zeitliche Gültigkeit des search-access_tokens beträgt 24 Stunden.

...

Es wird Kapitel "4.2.1.7" wie folgt eingefügt

4.2.1.7 Schnittstelle zum Lesen der fachlichen Logs I_FHIR_VZD_Fachliches_Log

Berechtigte Nutzer (Owner oder Holder) können per Schnittstellenabfrage relevante Informationen aus dem fachlichen Log erhalten.

Die Schnittstelle ist in I_FHIR_VZD_Fachliches_Log.yaml als OpenAPI RESTful Service spezifiziert:

https://github.com/gematik/api-vzd/blob/main/src/openapi/I_FHIR_VZD_Fachliches_Log.yaml

Endpunkte zum Lesen der fachlichen Logs

- In der Produktionsumgebung (PU) ist die URL:
<https://fhir-directory.vzd.ti-dienste.de/fachliches-log/log>
- In der Referenzumgebung (RU) ist die URL:
<https://fhir-directory-ref.vzd.ti-dienste.de/fachliches-log/log>

- In der Testumgebung (TU) ist die URL:
<https://fhir-directory-tu.vzd.ti-dienste.de/fachliches-log/log>

Um die Schnittstelle nutzen zu können, müssen sich die Clients mit einem gültigen Token authentisieren, das vom FHIR-Directory Auth-Service ausgestellt wurde. Akzeptiert werden die folgenden Token:

- Accesstoken von der FHIRDirectoryOwnerAPI Schnittstelle I_VZD_Owner
- Accesstoken von der FHIRDirectoryHolderAPI Schnittstelle I_VZD_Holder_Authenticate_Service

Die Schnittstelle ist in I_FHIR_VZD_Fachliches_Log.yaml als OpenAPI RESTful Service spezifiziert:

https://github.com/gematik/api-vzd/blob/main/src/openapi/I_FHIR_VZD_Fachliches_Log.yaml

Tabelle 23: Tab_I_FHIR_VZD_Fachliches_Log_Operations

Operation	Beschreibung
GET /log	Log von Verzeichniseinträgen lesen

Der Inhalt des fachlichen Logs wird in Tab_I_FHIR_VZD_Fachliches_Log_Inhalt erläutert.

Tabelle 24: Tab_I_FHIR_VZD_Fachliches_Log_Inhalt

Frage	Inhalt	Ausprägung
WER	Origin	Owner-Schnittstelle (TI-FHIR-Provider): OwnerID abhängig der TelematikId (aus Token) LDAP-Synchronisation (VZD-Converter): "SYSTEM"
WANN	Zeitstempel	DateTime
OBJECTTYP	RessourceType	HealthcareService, PractitionerRole, Location, Endpoint, Organization, Practitioner
OPERATION	Durchgeführte Operation	CREATE, UPDATE, DELETE
UID	Ressource-ID	UUID (HAPI-FHIR-UUID)
TID	TelematikId	TelematikId des Ressourcenbündels (HealthcareService, Organisation, Location, Endpoint bzw. PractitionerRole, Practitioner, Location, Endpoint). Die ID befindet sich in dem Telematik-Identifizier der jeweiligen Organisation bzw. Practitioner-Ressource.
Sync-Quelle	LDAP-uid	String entsprechend LDAP-uid

Es wird Kapitel "4.3.1" wie folgt angepasst

...

TIP1-A 5548-01 -VZD, Protokollierung der Änderungsoperationen

Der VZD MUSS Änderungen der Verzeichnisdiensteinträge protokollieren und muss sie **24 Monate** zur Verfügung halten.

[<=,VZD_FHIR, Verzeichnisdienst,Sich.techn. Eignung: Gutachten]

...

GS-A 5567-01 -Nutzung Zentraler Dienste der TI nur durch bestätigte Anwendungen

Ein Anbieter ~~weiterer Anwendungen mit Beeinträchtigung der TI~~ MUSS durch technisch-organisatorische Maßnahmen gewährleisten, dass ausschließlich die bestätigten Anwendungen bestimmte, festgelegte Zentrale Dienste der TI nutzen können.

[<=,extZug_VZD, Anb_VZD_FHIR,Sich.techn. Eignung: Anbietererklärung, funkt. Eignung: Anbietererklärung]

GS-A 5568-01 -Keine Weitergabe von Daten Zentraler Dienste der TI an nicht bestätigte oder zugelassene Anwendungen

Der Anbieter ~~weiterer Anwendungen mit Beeinträchtigung der TI~~ MUSS durch technisch-organisatorische Maßnahmen gewährleisten, dass von Zentralen Diensten der TI zur Verfügung gestellte personenbezogene Daten weder unverändert noch geändert an nicht bestätigte oder nicht zugelassene Anwendungen weitergegeben werden.

[<=,extZug_VZD,Sich.techn. Eignung: Anbietererklärung]

...

Es wird Kapitel "4.3.4 Anforderungen an VZD Clients" wie folgt aufgenommen

4.3.4 Anforderungen an VZD Clients

A_27744 -VZD Clients - Nutzung zentraler TI-Systeme durch dezentrale Clients: Verbindungsmanagement

Dezentrale Client-Systeme MÜSSEN dafür sorgen, dass Verbindungen nur im Zusammenhang mit einem konkreten fachlichen Use Case, der die Nutzung der entsprechenden Schnittstelle zwingend erfordert, aufgebaut werden.

Verbindungsaufbauten im Rahmen eines Initialisierungsprozesses sind zu vermeiden und sind nur in Kombination mit einem wirksamen Connection-Idle-Timeout zulässig. Das Absetzen regelmäßiger Dummy-Requests zum Umgehen des Idle-Timeouts oder zu anderen Zwecken (z.B. Monitoring) ist nicht erlaubt.

Ein Client hat sicherzustellen, dass gleichzeitig maximal eine Verbindung zur VZD-Schnittstelle aufgebaut wird. Das gleichzeitige Öffnen mehrerer paralleler Verbindungen durch denselben Client ist nicht zulässig, es sei denn, ein verbindliches Maximum wird für eine Schnittstelle explizit definiert.

Im Fall des Fehlschlages des Verbindungsaufbau MUSS eine Wartezeit bis zum nächsten Verbindungsversuch eingehalten werden (Retry-Intervall). Das Retry-Intervall ist mit zunehmender Anzahl fehlgeschlagener Verbindungsversuch bis zu einem Maximum zu erhöhen.

Verbindungen sind nach Beendigung des fachlichen Use Cases zeitnah zu schließen (5 Sek). Erfolgt dies nicht, MUSS nach Ablauf des Connection-Idle-Timeouts die Verbindung abgebaut werden.

Die maximale Bearbeitungsdauer einer Abfrage ist clientseitig per Konfiguration festzulegen. Um potenzielle Überlastsituationen durch langlaufende Anfragen (> 30 Sekunden) zu vermeiden, durch den VZD eine Begrenzung der maximalen Bearbeitungsdauer serverseitig (TimeOut) mit Beendigung der Abfrage möglich. [≤, „]

A_27749 -VZD Client - Nutzung zentraler TI-Systeme durch dezentrale Clients: Verbindungsmanagement, Parameter

Dezentrale Client-Systeme oder Apps MÜSSEN parametrisierbar sein, d. h. folgende Parameter müssen aus der Ferne zentral angepasst werden können. Die Standardwerte (Default) MÜSSEN nach Aufforderung durch die gematik in einem [noch zu definierenden] Prozess innerhalb einer [noch festzulegenden Zeit] anpassbar sein.

Parameter	Beschreibung	Standardwerte (Default)
CONNECTION_IDLE_TIMEOUT (Hinweis: Die Parameternamen müssen ggf. produkt-oder schnittstellenspezifisch angepasst werden)	Haltedauer der TCP-Verbindung eines Clients zu einem Dienst, in der kein Datenverkehr zwischen Client und Dienst stattfindet.	30 Sek
MAX_CONNECTION	Anzahl der pro Client maximal zulässigen gleichzeitigen Verbindungen.	2
RETRY_TIME	Mindestwartezeit nach den ersten beiden fehlgeschlagenen Verbindungsversuchen. Bei jedem weiteren Versuch nach dem 3. Versuch SOLL die Wartezeit um diesen Wert bis RETRY_TIME_MAX oder mit größer werdenden Abständen vergrößert werden.	5 Sek
RETRY_TIME_MAX	Maximale Wartezeit zwischen zwei Verbindungsversuchen.	5 min

[≤, „]

A_27751 -VZD Client - Nutzung zentraler TI-Systeme durch dezentrale Clients: Angepasste Konfiguration und Außerbetriebnahme von Clients

Jeder Client MUSS entsprechend des tatsächlichen Bedarfs, d. h. der zu erwartenden Anwendungsfälle und deren Häufigkeit so konfiguriert werden, dass nicht notwendige

Last (Anfrage- und Verbindungslast auf Systemkomponenten durch parallele Verbindungen, häufige Requests oder ineffiziente Nutzung von Schnittstellen) auf den zentralen TI-Systemen vermieden wird.

[<=,,]

A_28318 -VZD Client - Deaktivierung nicht genutzter Clients

VZD Clients, die vorübergehend oder langfristig nicht mehr genutzt werden, SOLLEN in angemessen kurzer Zeit deaktiviert werden. [<=,,]

A_27752 VZD Client - Nutzung zentraler TI-Systeme durch dezentrale Clients: Vermeidung der Gesamtauslese des VZD durch Clients

Ein Client DARF NICHT eine Gesamtauslese (systematische Abfrage aller verfügbaren Einträge über Einzelabfragen statt Nutzung dafürvorgesehener Exportmechanismen) des Verzeichnisdienstes (VZD) durchführen. Stattdessen SOLLEN die dedizierten Schnittstellen, falls vorhanden, für einen entsprechenden Export genutzt werden. Clients, bei denen durch kontinuierliche Abfragen eine unzulässige Gesamtauslese vermutet wird, KÖNNEN im Zweifel gesperrt werden.

<=

A_27753 -VZD Client - Nutzung zentraler TI-Systeme durch dezentrale Clients: Caching

Zur Lastvermeidung und Erhöhung der Ausfallsicherheit SOLLEN Client-Systeme Antworten von häufig durchgeführten Abfragen kurzzeitig (max. 5 Min.), wenn für den Anwendungsfall nicht explizit anders spezifiziert, aufbewahren (cachen).

[<=,,]

A_27754 -VZD Client - Nutzung zentraler TI-Systeme durch dezentrale Clients: Effiziente Gestaltung von FHIR-Suchanfragen

Aus Effizienzgründen SOLLEN dezentrale Clients FHIR-Suchanfragen so kurz und zielgerichtet wie möglich gestalten, da jede Anfrage zu einer direkten Datenbankabfrage führt. Eine ineffiziente Gestaltung von Suchanfragen kann zu unnötiger Systemlast und Verbindungsengpässen führen.

Zur Performanceoptimierung SOLLEN Clients folgende Maßnahmen umsetzen:

- Verwendung des `_text`-Suchparameters zur gezielten Volltextsuche
- Ergänzende Nutzung von geographischen Suchparametern (z. B. `address` oder `location`) zur klaren Unterscheidung semantischer Suchkontexte (z. B. zwischen „Suche nach einem Arzt in Berlin“ und „Suche nach Dr. Berlin“)
- Bei Bedarf: gezieltes Einbinden abhängiger Sub-Ressourcen mittels `_include`, um Mehrfachanfragen zu vermeiden und Netzwerkverkehr zu reduzieren

[<=,,]

Beispielhafte Abfrage zur effizienten Arztsuche:

https://fhir-directory-tu.vzd.ti-dienste.de/fdv/search/HealthcareService?organization.active=true &_text=Mustermann&_include=HealthcareService%3Aorganization &_include=HealthcareService%3Alocation

Diese Abfrage kombiniert Volltextsuche mit gezieltem Einbinden abhängiger Ressourcen in einer einzigen Anfrage und reduziert dadurch zusätzliche Roundtrips zur FHIR-Schnittstelle.

A_27755 -VZD Client - Nutzung zentraler TI-Systeme durch dezentrale Clients: Fehler-Monitoring

VZD Clients SOLLEN zur frühzeitigen Erkennung von Instabilitäten im Client- oder Netzwerkbereich Metriken wie Antwortzeiten, Fehlerraten und Timeouts erfassen und bei Bedarf an ein zentrales Monitoring-System übermitteln. [≤,,]

Es wird Kapitel "5.1" wie folgt angepasst

AF_10036-04 -Nutzer sucht Einträge im FHIR-Directory

Attribute	Bemerkung
Akteure	<ul style="list-style-type: none"> • Mitarbeiter im Gesundheitswesen • Versicherte
Beschreibung	<p>Nutzer können im FHIR-Directory über die Einstiegspunkte HealthcareServiceDirectory-, PractitionerRoleDirectory- und EndpointDirectory-Einträgen nach allen FHIR VZD Ressourcen suchen.</p> <p>Für die Suche von TI-Messenger Nutzern im FHIR-Directory ist eine Authentisierung am FHIR-Directory Auth-Service erforderlich. Hier ist die Authentisierung mit TI-Messenger-Clients beschrieben.</p> <ol style="list-style-type: none"> 1. Der TIM-Client des Nutzers prüft, ob er ein gültiges search-access_token vom FHIR VZD Auth-Service vorliegen hat. [1] 2. Wenn dem TIM-Client kein gültiges search-access_token vorliegt, fragt er bei seinem Matrix-Homeserver ein Matrix-OpenID-Token ab. [2-4] 3. Abruf search-access_token [5-1314] <ul style="list-style-type: none"> Der TIM-Client tauscht das Matrix-OpenID-Token gegen ein search-access_token ein. Der FHIR-Directory Auth-Service <ol style="list-style-type: none"> a. prüft ob das Matrix-OpenID-Token von einem Matrix-Homeserver aus der TI-Föderation stammt [6] b. ermittelt den Port unter dem der Userinfo Endpunkt des Matrix-Homeservers zu erreichen ist [7] c. validiert die Gültigkeit des Matrix-OpenID-Token mit Hilfe des Matrix-Homeserver [8-9] d. ermittelt den handelnden Akteur anhand des Status von isInsurance in der Föderationsliste für den Matrix-Homeserver[10] <ol style="list-style-type: none"> i. bei isInsurance=false(Mitarbeiter im Gesundheitswesen) wird ein search-access_token mit aud:https://fhir-directory.vzd.ti-dienste.de/search erzeugt [11] ii. bei isInsurance=true(Versicherter) wird ein search-access_token mit aud:https://fhir-directory.vzd.ti-

	dienste.de/fdv/search erzeugt [12] e. erzeugt und übermittelt das search-access_token an den Client [13-14]
Vorbedingung	Der Nutzer ist an seinem Homeserver registriert.
Nachbedingung	Der TI-Messenger-Client hat alle gefundenen Einträge empfangen.

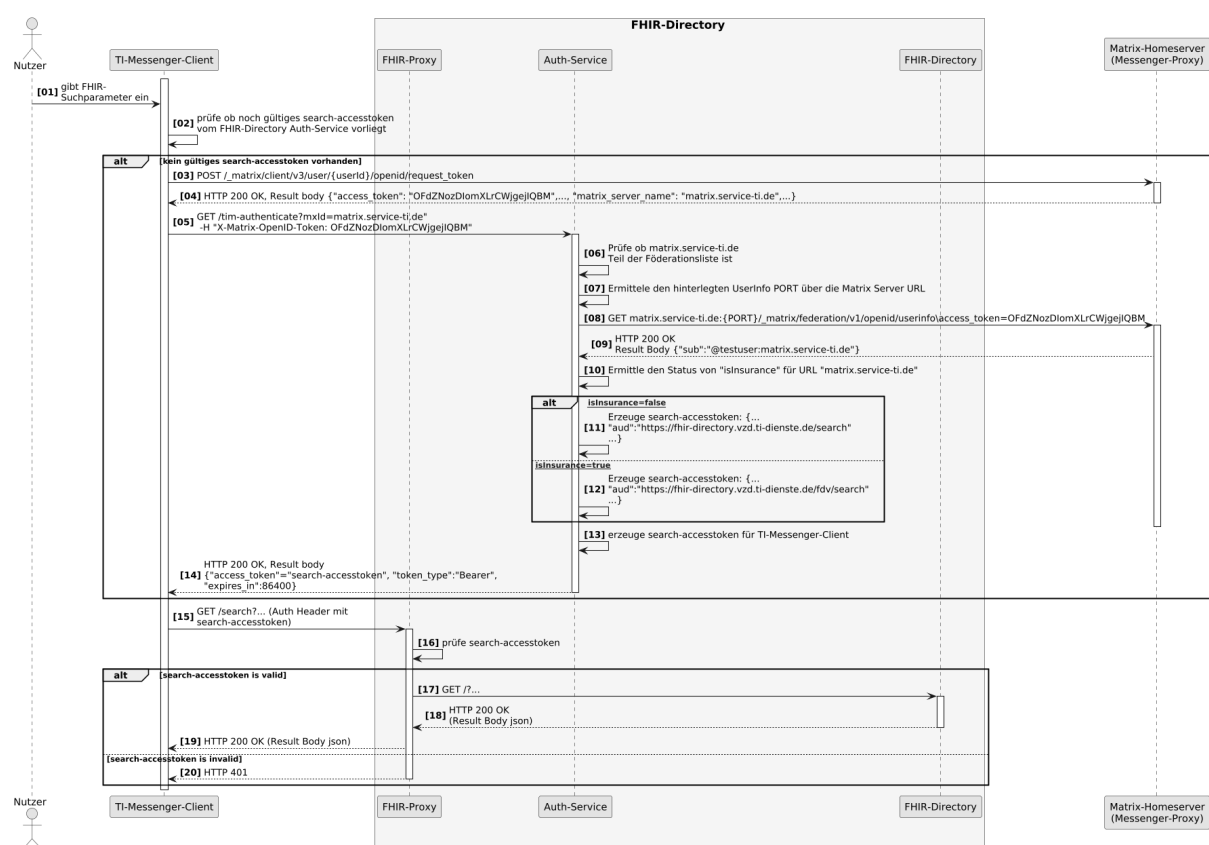


Abbildung 2: Sequence diagram /search

[<=,TI-M_Client_Basis, VZD_FHIR, TIM_FD, TI-M_FD_Basis, TIM_Client,funkt. Eignung: Herstellererklärung, funkt. Eignung: Test Produkt/FA]

Es wird Kapitel "5.2" wie folgt angepasst

AF_10037-04 -Einträge im VZD-FHIR-Directory ändern und suchen

Attribute	Bemerkung
Beschreibung	Über die Authentisierung mit HBA/SM(C)-B erfolgt die Authentisierung für die VZD-FHIR-Directory Schnittstellen /owner und /search

	<p>Änderung von eigenen Daten im VZD-FHIR-Directory</p> <p>Organisationen können ihren Eintrag im VZD-FHIR-Directory an die eigenen Strukturen anpassen. Leistungserbringer können z. B. die TI-Messenger-Adresse in ihrem Eintrag hinzufügen. Der Basiseintrag einer Organisation oder eines Leistungserbringers wird wie bisher durch die Kartenherausgeber erstellt. Die Organisation KANN eigene mit dem Basiseintrag verlinkte FHIR-Ressourcen erstellen, um die Struktur der Organisation abzubilden. Zum Beispiel können Krankenhäuser ihre Fachabteilungen als HealthcareService-Einträge abbilden, die mit dem Organization-Eintrag verlinkt sind.</p> <p>Wenn der Org-Admin oder LE kein gültiges owner-access_token vom VZD-FHIR-Directory im Client vorliegt, muss die Authentisierung mittels OIDC an einem IDP der TI-IDP-Föderation erfolgen. Nach erfolgreicher Authentisierung ist die durch den IDP bestätigte Telematik-ID des Leistungserbringers oder der Organisation am Auth-Service bekannt. Für den Aufruf der FHIR-Operationen durch den Client stellt der Auth-Service dem Client ein owner-access_token aus, das auch die Telematik-ID des LE oder der Organisation enthält.</p> <p>Für die Änderung von Daten muss ein POST für die Owner Schnittstelle für die jeweilige Ressource genutzt werden. Zum Beispiel für einen HealthcareService</p> <p>POST {FHIR-VZD-URL}/owner/HealthcareService</p> <p>Welche Attribute für den "Owner" eines FHIR-VZD Eintrags änderbar sind, wird im FHIR VZD Datenmodell definiert:</p> <p>https://github.com/gematik/api-vzd/blob/main/docs/FHIR_VZD_HOWTO_Data.adoc</p> <p>Suche von Daten im VZD-FHIR-Directory</p> <p>Das erzeugte Token kann auch für die Suche im VZD-FHIR-Directory über die /search Schnittstelle genutzt werden.</p> <ul style="list-style-type: none"> • Für die Suche im Zusammenhang von Datenänderungen im VZD-FHIR-Directory kann die Suche in der /owner Schnittstelle genutzt werden. • Für die normale Suche MUSS der Client die VZD-FHIR-Directory Suche über die /search Schnittstelle nutzen (die /search Schnittstelle kann entsprechend der Last skaliert werden).
Vorbedingung	<p>Die Organisation oder der Leistungserbringer hat bereits einen Basiseintrag im VZD-FHIR-Directory.</p> <p>Eine Authenticator-App des IDP steht zur Verfügung, mit der die Organisations-Identität oder die Leistungserbringer-Identität bei einem IDP der TI-IDP-Föderation bestätigt werden kann.</p>

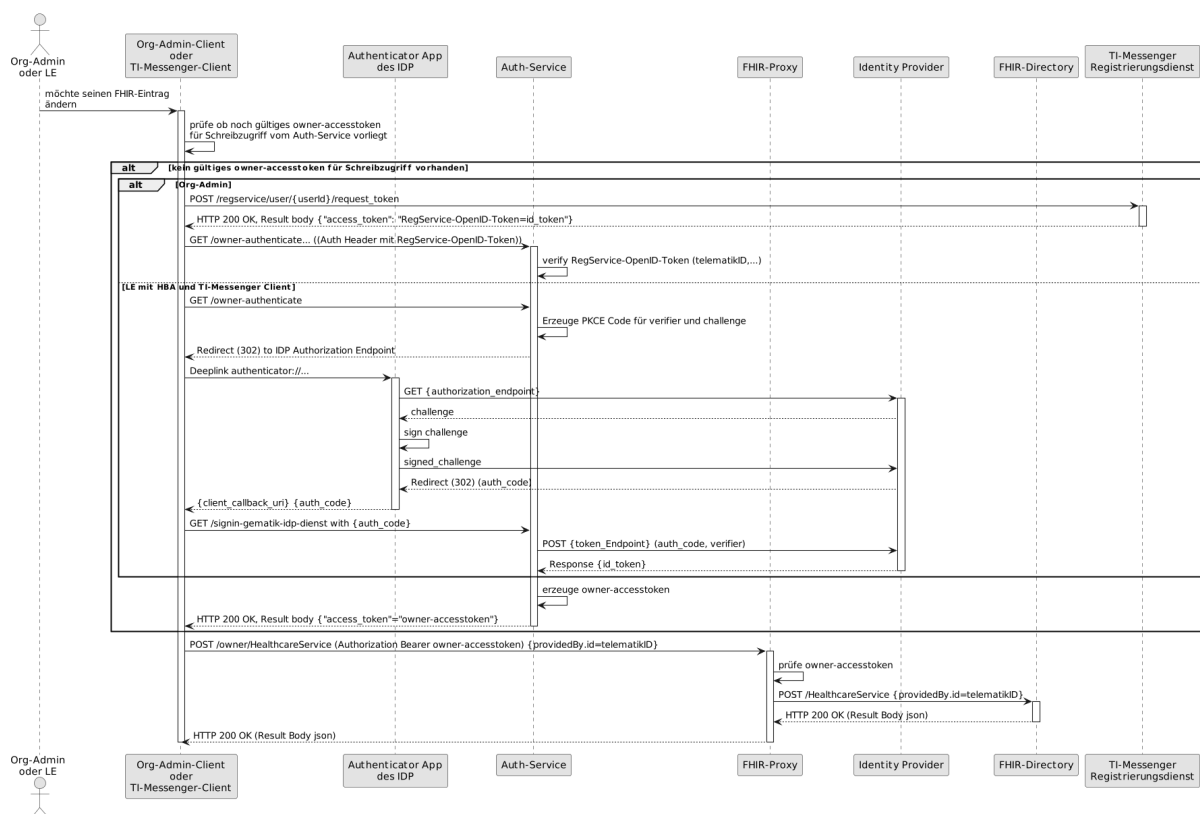


Abbildung 3: Sequenzdiagramm VZD-FHIR-Directory Änderung von eigenen OrganizationDirectory- oder PractitionerDirectory-Einträgen

[<=, TI-M_Client_Basis, VZD_FHIR, TIM_Client, funkt. Eignung: Herstellererklärung]

In Kapitel "5.2", Abschnitt "Akzeptanzkriterien für den Anwendungsfall AF_10037 OrganizationDirectory-Einträge im VZD-FHIR-Directory ändern" wird wie folgt aufgenommen

...

ML-179493 -Authentifizierung am Endpunkt /owner nur mit bekannter TelematikID (VZD-FHIR-Directory)

Bei der Authentifizierung an der VZD FHIR Owner-Schnittstelle muss überprüft werden, ob die verwendete HBA- / SMCB-Karte (Telematik-ID) dem VZD FHIR bereits bekannt ist. Damit darf sich niemand anmelden der kein Inhaber einer VZD FHIR-Ressource ist. [<=]

...

Es wird Kapitel "5.2" wie folgt angepasst

AF_10219-02 -Versicherter sucht Einträge im FHIR-Directory

Attribute	Bemerkung
-----------	-----------

Beschreibung	<p>Für die Suche von Versicherten im FHIR-Directory nach Organisationen (HealthcareServiceDirectory-Einträgen), Practitioner'n (PractitionerRoleDirectory-Einträgen) und Endpoints (EndpointDirectory-Einträgen) eine Authentisierung der Fachanwendung am Auth-Service patient-authenticate Endpunkt erforderlich. Der Ablauf entsprechend Abbildung "Sequence diagram /fdv/search":</p> <ol style="list-style-type: none"> 1. Der Client prüft, ob er ein gültiges search-access_token vom FHIR VZD Auth-Service vorliegen hat. [1] 2. Client Anfrage von search-access_token [2] Wenn im Client kein gültiges search-access_token vom FHIR VZD Auth-Service vorhanden ist, stellt der Client eine Anfrage an den Fachdienst (siehe I_FHIR_VZD_token_FD.yaml). Vor dieser Anfrage muss sich der Client des Versicherten gegenüber dem Fachdienst authentisiert haben. 3. Der Fachdienst benötigt zur Authentisierung gegenüber dem OAuth-Server Client Credentials. Diese erhält er in einem Registrierungsprozess vom Betreiber FHIR-Directory und kann sie z.B. in einem Konfigurationsfile auf dem Fachdienst ablegen. [3] 4. Authentisierung des Fachdiensts mit Client Credentials [4-6] Der Fachdienst authentisiert sich mit seinen Client Credentials und erhält nach erfolgreicher Prüfung ein service-authz-token. 5. Abruf search-access_token [7-10] Der Fachdienst tauscht das service-authz-token gegen ein search-access_token ein. 6. Cachen vom search-access_token [11] Optional kann der Fachdienst das search-access_token cachen und für Anfragen mehrerer Clients nutzen, solange die zeitliche Gültigkeit von dem search-access_token ausreicht. 7. Rückgabe von dem search-access_token an den Client [12] 8. Suche im FHIR-Directory [13-17] Mit dem search-access_token kann der Client im FHIR-Directory suchen und erhält eine Antwort mit dem Suchergebnis. Wenn das search-access_token ungültig ist (z.B. zeitlich abgelaufen), erhält er als Antwort den HTTP Status Code 401. Bei der Suche über Endpunkt HealthcareServices werden Ressourcen (HealthcareService, referenzierte Organization, referenzierte Location, ggf. referenzierte Endpoints) vom FHIR VZD aus dem Ergebnis entfernt sobald die referenzierte Organization das Flag (Extension) Organization.organizationVisibility = "hide-erezeptApp" "hide-versicherte" gesetzt hat. Bei allen Suchen über /fdv/search werden vom FHIR VZD aus dem Ergebnis die Endpoints entfernt, deren Attribut (Extension) Endpoint.extension:endpointVisibility = "hide-versicherte" gesetzt hat. Falls der Client für die interne Verarbeitung in dem fachlichen Anwendungsfall mit "hide-versicherte" markierte FHIR VZD Ressourcen benötigt, kann er diese über den FHIR VZD /search
--------------	--

	Endpunkt abfragen. Diese FHIR VZD Ressourcen dürfen für die interne Verarbeitung genutzt, dem Versicherten aber nicht direkt als Suchergebnis angezeigt werden.
Vorbedingung	Der Versicherte ist bei seiner Kasse registriert. Der Client des Versicherten hat sich gegenüber dem Fachdienst authentisiert. Der Fachdienst des Versicherten hat sich bei FHIR VZD Anbieter für Schnittstelle /fdv/search registriert und Client Credentials vorliegen.
Nachbedingung	Der Client hat alle gefundenen Einträge empfangen.

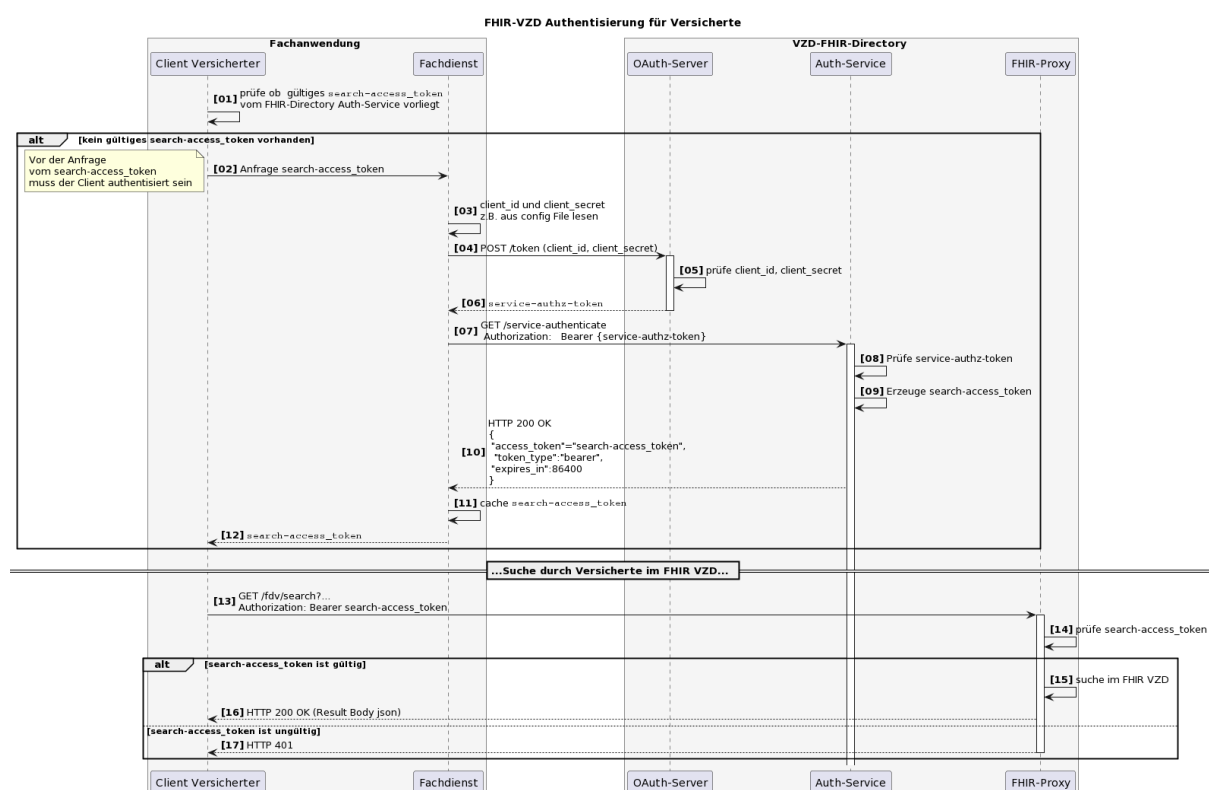


Abbildung 4: Sequence diagram /fdv/search

[<=,Aktensystem_ePA, VZD_FHIR, eRp_FdV, Frontend_Vers_ePA,funkt. Eignung: Herstellererklärung]

...

Es wird Kapitel "7 VZD Self-Service Portal" wie folgt aufgenommen

7 VZD Self-Service Portal

Das „VZD Self-Service Portal“ dient der sicheren und effizienten Verwaltung und Einsicht von Gesundheitsdaten für „Leistungserbringende“ und „leistungserbringende Institutionen“, Kartenherausgeber und der gematik. Das Portal ermöglicht es den

Nutzern, Daten zu lesen, zu ändern und zu verwalten, basierend auf den ihnen zugewiesenen Berechtigungen und Zuständigkeiten.

7.1 Akteure

Zielgruppen des VZD Self-Service Portals sind

- **HBA-Inhaber:**
 - Einsicht in die FHIR VZD Daten.
- **Organisationen des Gesundheitswesens (SMC-B Inhaber):**
 - Einsicht in die FHIR VZD Daten.
 - Für definierte Sektoren des Medizinwesens die Möglichkeit, eigene definierte "Mehrwertdaten" zu ändern.
- **Kartenherausgeber:**
 - Einsicht in die FHIR VZD Daten.
 - Änderbarkeit aller Daten ihrer Karteninfrastruktur.
- **gematik:**
 - Einsicht in die FHIR VZD Daten.
 - Mit Beauftragung durch Kartenherausgeber und bei TI-Störungen Änderbarkeit aller FHIR VZD Daten.

7.2 Funktionale Anforderungen

7.2.1 Architektur des VZD Self-Service Portals

Das VZD Self-Service Portal muss aus folgenden Komponenten bestehen:

- **Zentrale Komponente (Server-Seite):** Ein zentraler Server (Web-Server), der die gesamte Logik, Verbindungen und Kommunikation mit den Clients und dem FHIR VZD übernimmt.
- **Client-Seite:** Web-Browser, die keine zusätzliche Installation benötigen. Das Vorhandensein des gematik Authenticators darf für die Kommunikation mit den Karten vorausgesetzt werden. Wenn der gematik Authenticator auf der Client-Seite nicht vorhanden ist, müssen die Authentisierungsverfahren ohne Karten nutzbar sein.

Browser und Auflösung

Es sollen die aktuellen modernen Webbrowser unterstützt werden. Der Nachweis der korrekten Umsetzung erfolgt mit dem aktuellen Google Chrome-Browser unter Windows.

Das VZD Self-Service Portal muss mit einer Bildschirm Auflösung von $\geq 1024\text{px}$ Breite x 800px Höhe nutzbar sein.

7.2.1. Benutzerverwaltung, Authentisierung und Berechtigungen

Im VZD Self-Service Portal müssen folgende Benutzergruppen unterstützt werden:

Karteninhaber (Owner)

- Die Anmeldung erfolgt mittels SMC-B- oder HBA-Karte.
- Die Identifikation des Owners erfolgt über die der Karte zugeordnete Telematik-ID.
- Karteninhaber können bestimmte Informationen einsehen und unter definierten Bedingungen bearbeiten.

- Für Karteninhaber erfolgt die Benutzerverwaltung über ihre Karten und die Gültigkeit dieser Karten. Mit einem gültigen - und dem FHIR VZD bekannten - HBA bzw. SMC-B muss die Authentisierung am VZD Self-Service Portal möglich sein. Die Anmeldung mit allen anderen Karten muss abgelehnt werden, auch wenn ein IDP für diese Karten Token ausstellt.

Einfache Benutzer mit Lese-Berechtigung

- Anmeldung per Benutzername und Passwort.
- Die Benutzerverwaltung muss über die Registrierung bei der gematik und Verwaltung des Benutzeraccounts bei dem VZD Betreiber erfolgen.
- Diese Benutzer verfügen über das Standardrecht und haben ausschließlich lesenden Zugriff auf die freigegebenen Informationen.

Administrativer Benutzer mit erweiterten Rechten

- Anmeldung ebenfalls per Benutzername und Passwort.
- Die Benutzerverwaltung muss über die Registrierung bei der gematik und Verwaltung des Benutzeraccounts bei dem VZD Betreiber erfolgen.
- Diese können zusätzlich zu den Leseoperationen definierte Inhalte bearbeiten.

Kartenherausgeber (Holder)

- Auch hier erfolgt die Anmeldung per Benutzername und Passwort.
- Die Benutzerverwaltung muss über die Registrierung bei der gematik und Verwaltung des Benutzeraccounts bei dem VZD Betreiber erfolgen.
- Besitzen das Recht, das erweiterte administrative Zugriffe ermöglicht.

Alle übertragenen Daten müssen Ende-zu-Ende verschlüsselt werden, um den Schutz der Daten während der Übertragung zu gewährleisten.

Das Portal muss alle relevanten Datenschutzbestimmungen, insbesondere die Datenschutz-Grundverordnung (DSGVO), einhalten.

7.2.1.1. Funktionsspezifische Unterschiede

Je nach Rolle unterscheiden sich die zur Verfügung stehenden Funktionen innerhalb des Systems:

7.2.1.1.1. Suche und Anzeige

Suche und Anzeige von Detail-Informationen

Die Suchfunktion steht allen Benutzergruppen zur Verfügung. Auch die grundlegenden Detailinformationen können von allen Gruppen eingesehen werden. Unterschiede in den erweiterten Einsichts- oder Bearbeitungsrechten werden in den folgenden Abschnitten näher beschrieben.

Die Eingabe der Suchkriterien muss für den Nutzer einfach - ähnlich wie bei den aktuellen Internetsuchmaschinen - möglich sein.

Die Suche muss als Ergebnis liefern:

- Trefferliste mit Suchfeld. Treffer befinden sich in einer Tabelle, welche über die Art der Einträge "Praxis, Apotheke, Person" mittels Tabellen-Tabs gefiltert werden kann.
- Die Liste muss sowohl aktive als auch inaktive VZD-Einträge enthalten.

Durch Selektion eines VZD-Eintrags in der Trefferliste müssen die Detailinformationen dieses Eintrags dargestellt werden. In den Detailinformationen müssen die wesentlichen Attribute des VZD-Eintrags für den Anwender leicht verständlich aufbereitet dargestellt werden.

Zusätzlich zu den Detailinformationen müssen folgende Daten einsehbar sein:

Anzeige Zertifikatsinformationen

Die Zertifikatsinformationen sind mit den Einträgen verknüpft und werden unter dem Reiter "Telematik" dargestellt.

Die Zertifikatsinformationen haben einen öffentlichen Charakter und können von allen Benutzern eingesehen werden.

Anzeige Fachliches Log (VZD FHIR + VZD LDAP)

Im Reiter „Historie“ werden alle Änderungen an einem Eintrag inklusive Bearbeiter und Änderungsinhalt dokumentiert.

- **Karteninhaber (Owner)** sehen nur das Log ihrer eigenen Einträge, basierend auf der zugeordneten Telematik-ID.
- **Administrative Benutzer** und zukünftig **Kartenherausgeber (Holder)** können das Log aller Einträge einsehen.

Anzeige Rohdaten

Im Reiter „Rohdaten“ werden die zugrunde liegenden FHIR-Ressourcen im JSON-Format dargestellt.

Dies dient der technischen Nachvollziehbarkeit und ermöglicht detaillierte Prüfungen auf Datenebene.

- **Karteninhaber (Owner)** können ausschließlich die Rohdaten ihrer eigenen Einträge einsehen, basierend auf ihrer Telematik-ID.
- **Administrative Benutzer** sowie zukünftig auch **Kartenherausgeber (Holder)** erhalten Einsicht in die Rohdaten aller Einträge.

7.2.1.1.2. Datenänderung über das VZD Self-Service Portal

Änderung von Mehrwertdaten (inkl. Endpunkte)

Mehrwertdaten umfassen zusätzliche Informationen zu einem Eintrag, wie:

- Telekommunikationsdaten
- Geokoordinaten (Breiten-/Längengrad)
- Verknüpfte technische Endpunkte
- angebotene Apothekenservices
- Öffnungszeiten

Diese Daten dürfen ausschließlich von **Karteninhabern (Owner)** und **administrativen Benutzern** bearbeitet werden. Karteninhabern (Owner) dürfen nur Daten ihres eigenen VZD Eintrags bearbeiten (identifiziert über Telematik-ID), administrative Benutzer nur VZD Einträge innerhalb der eigenen Zuständigkeit (identifiziert über das Holder Attribut).

Aktuell ist eine Bearbeitung für **Karteninhaber** nur für **Apotheken**, einschließlich EU-Versandapotheken, vorgesehen. Die Erweiterung für andere Sektoren muss möglich sein.

Datenvalidierung: Daten - die geändert werden - müssen validiert werden, um sicherzustellen, dass die Qualität der Daten gewährleistet ist.

7.2.6. Benutzeroberfläche und Benutzererfahrung

Die Benutzeroberfläche muss einfach und intuitiv zu bedienen sein, um eine hohe Akzeptanz bei den Nutzern zu gewährleisten.

Benutzerfreundlichkeit (Usability):

- Die Navigation muss logisch aufgebaut und leicht verständlich sein.
- Elemente wie Schaltflächen, Menüs und Formulare müssen eindeutig beschriftet und leicht auffindbar sein.

Effizienz:

- Die Benutzeroberfläche muss es Benutzern ermöglichen, Aufgaben schnell und effizient zu erledigen.
- Kurze Reaktionszeiten, welche die VZD Antwortzeiten nicht merklich verlangsamen.
- Häufig genutzte Funktionen müssen leicht zugänglich sein und nicht durch viele Zwischenschritte erreicht werden müssen.

Konsistenz:

- Die Gestaltung und Funktionsweise verschiedener Elemente innerhalb der Benutzeroberfläche muss konsistent erfolgen.
- Gleichartige Elemente müssen immer auf die gleiche Weise dargestellt und bedient werden.

Barrierefreiheit:

- Die Benutzeroberfläche muss für Menschen mit Behinderungen zugänglich sein.
- Dies kann beispielsweise durch angepasste Farben und Schriftgrößen oder die Verwendung von Tastaturkürzeln erfolgen.

Fehlerbehandlung:

- Die Benutzeroberfläche muss Benutzer auf Fehler hinweisen.
- Fehlermeldungen müssen klar und verständlich sein und auf die Fehlerursache bzw. deren Behebung hinweisen.

7.2.8 Anwendungsfälle

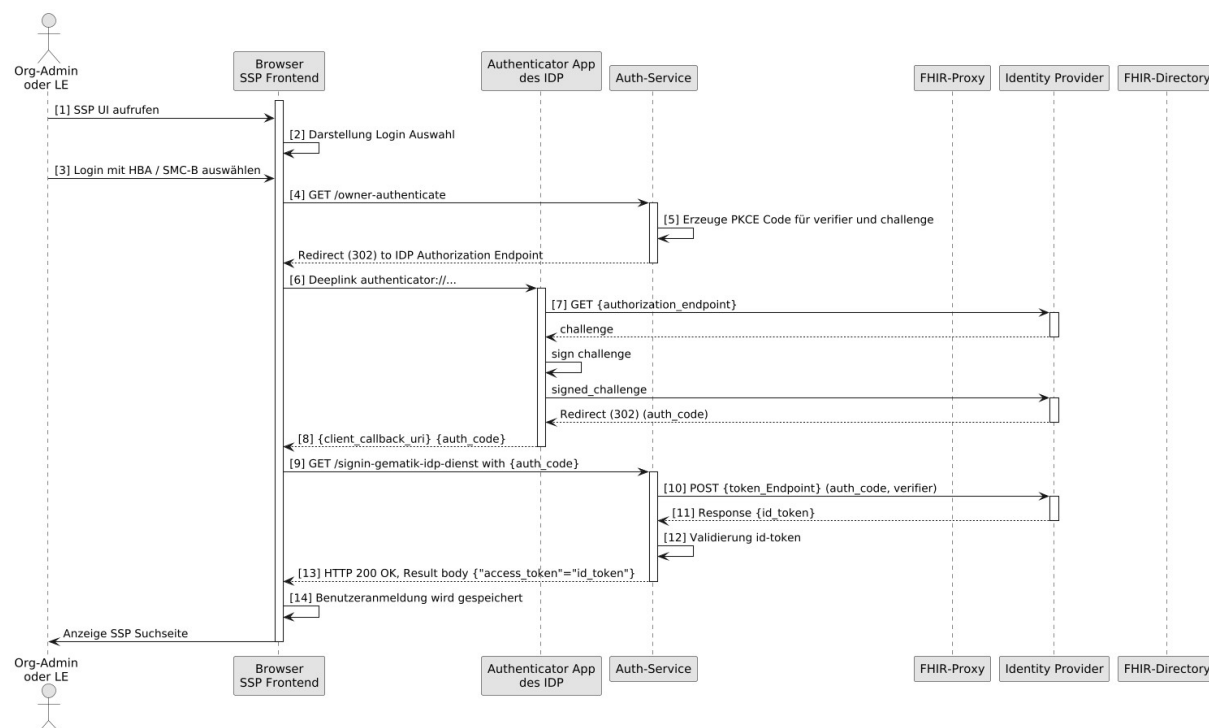
7.2.8.1 Authentisierung über HBA/SMC-B

AF_10414 -FHIR VZD Self-Service Portal - Authentisierung über HBA/SMC-B

Attribute	Bemerkung
Akteure	<ul style="list-style-type: none">• Mitarbeiter im Gesundheitswesen (Authentisierung via HBA)• Administratoren von Organisationen im Gesundheitswesen

	(Authentisierung via SMC-B)
Beschreibung	<p>Für die Nutzung des Self-Service Portals ist eine Authentisierung erforderlich. Hier erfolgt die Authentisierung über einen HBA oder eine SMC-B.</p> <ol style="list-style-type: none"> 1. Der Nutzer ruft das Self-Service Portal für die gewünschte Umgebung (RU, TU oder PU) über die jeweilige URL im Web Browser der Praxis bzw. Organisation auf. [1] 2. Das Self-Service Portal Frontend bietet die Auswahl der Authentisierungsmethode an [2]. 3. Der Nutzer wählt im Self-Service Portal die Authentisierung via HBA bzw. SMC-B. [3] 4. Das Self-Service Portal Frontend startet den Authentisierungs-Flow der Authenticator-App. [4] Dafür werden zuerst die benötigten Austauschinformationen generiert (PKCE_code_challenge, PKCE_code_verifier, state). [5] 5. Anschließend ruft der Browser die lokal-laufende Authenticator-App [6] und dieser wiederum den Gematik-IDP auf. [7] Nach einem erfolgreichen Austausch folgt die Authenticator-App der Redirect-URI. [8] 6. Das Self-Service Portal Frontend übergibt die bekannten Austauschinformationen auth_code und key_verifier an den Token-Endpunkt des Gematik-IDP. [9][10] Sind die übergebenen Informationen korrekt, erhält der Auth-Service das signierte id_token zurück. [11] Das id_token wird auf seine zeitliche Gültigkeit sowie auf die Signatur überprüft. [12] Für die Validierung der Signatur wird das öffentliche Zertifikat des Gematik-IDP benutzt. Dieses wurde zuvor von der OpenID-Konfigurations-Seite des IDP heruntergeladen. 7. Ist der id_token gültig, wird es an das SSP-Frontend weitergeleitet. [12][13] Intern wird die Benutzeranmeldung im SSP-Frontend zwischengespeichert. [14] Der Benutzer ist anschließend erfolgreich angemeldet. 8. Nach erfolgreicher Anmeldung wird dem Benutzer die Suchseite der Webanwendung angezeigt, wobei im Hintergrund die REST-Schnittstelle des SSP-Backends aufgerufen wird und ein vom SSP-selbst-signiertes AccessToken im Authorization-Header an den FHIR-VZD übertragen wird. Der VZD FHIR validiert den Token auf zeitliche Gültigkeit und seine Signatur.
Vorbedingung	<p>Die Organisation oder der Leistungserbringer hat bereits einen Basiseintrag im VZD-FHIR-Directory. Eine Authenticator-App des IDP steht zur Verfügung, mit der die Organisations-Identität oder die Leistungserbringer-Identität bei einem</p>

	IDP der TI-IDP-Föderation bestätigt werden kann.
Nachbedingung	Die Organisation oder der Leistungserbringer sind authentisiert und können das Self-Service Portal nutzen.



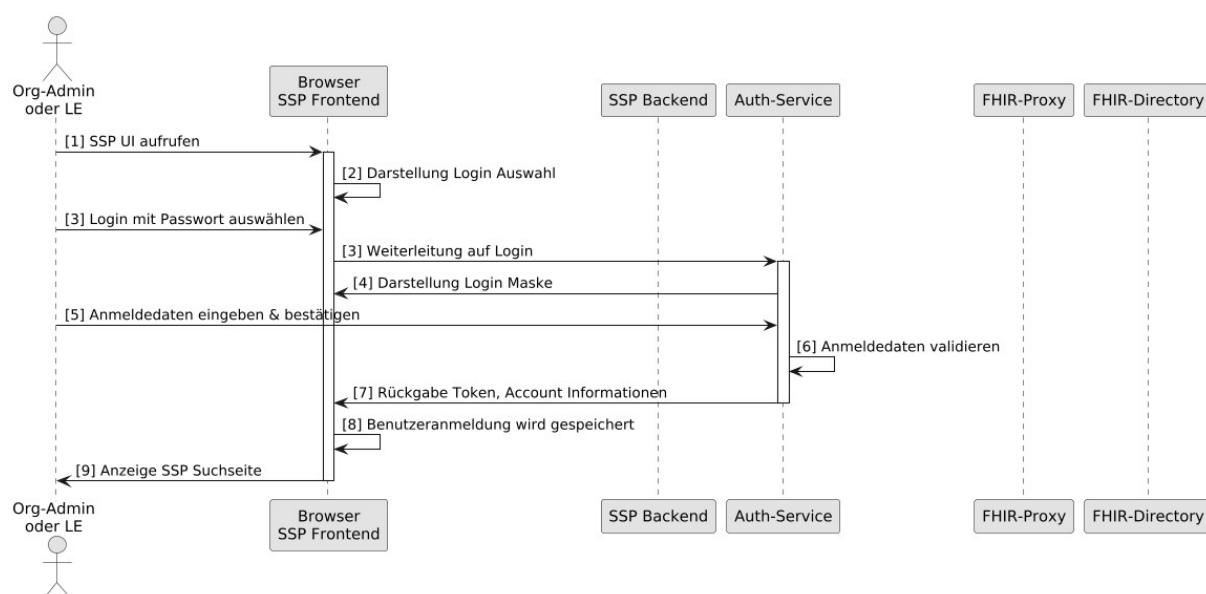
【<=,VZD_FHIR,funkt. Eignung: Herstellererklärung】

7.2.8.2 Authentisierung von administrativen Nutzern

AF_10415 -FHIR VZD Self-Service Portal - Authentisierung über Passwort

Attribute	Bemerkung
Akteure	Administrative Nutzer im Gesundheitswesen (Authentisierung via Passwort), z.B. Kartenherausgeber, gematik.
Beschreibung	<p>Für die Nutzung des Self-Service Portals ist eine Authentisierung erforderlich. Hier erfolgt die Authentisierung über Credentials (Username/Passwort).</p> <ol style="list-style-type: none"> Der Nutzer ruft das Self-Service Portal für die gewünschte Umgebung (RU, TU oder PU) über die jeweilige URL im Web Browser auf. [1] Das Self-Service Portal Frontend bietet die Auswahl der Authentisierungsmethode an [2]. Der Nutzer wählt im Self-Service Portal die Authentisierung via Passwort. [3] Das Self-Service Portal Frontend zeigt die Login Maske für die

	<p>Eingabe der Credentials an. [4]</p> <p>5. Der Nutzer gibt die Credentials im Self-Service Portal Frontend (Browser) ein und bestätigt sie [5].</p> <p>6. Der FHIR VZD Auth-Service validiert die eingegebenen Credentials. [6]</p> <p>7. Sind die eingegebenen Credentials gültig, wird ein Token erzeugt und zusammen mit den Account Informationen an das SSP-Frontend weitergeleitet. [7]</p> <p>8. Intern wird die Benutzeranmeldung im SSP-Frontend zwischengespeichert. [8] Der Benutzer ist anschließend erfolgreich angemeldet.</p> <p>9. Nach erfolgreicher Anmeldung wird dem Nutzer die Suchseite der Webanwendung angezeigt, wobei im Hintergrund die REST-Schnittstelle des SSP-Backends aufgerufen wird und ein vom SSP-selbst-signiertes AccessToken im Authorization-Header an den FHIR-VZD übertragen wird. [9] Der VZD FHIR validiert den Token auf zeitliche Gültigkeit und seine Signatur.</p>
Vorbedingung	Der Administrative Nutzer ist bei der gematik und dem Self-Service Portal Betreiber registriert und hat seine Credentials erhalten.
Nachbedingung	Der Administrative Nutzer ist authentisiert und kann das Self-Service Portal nutzen.



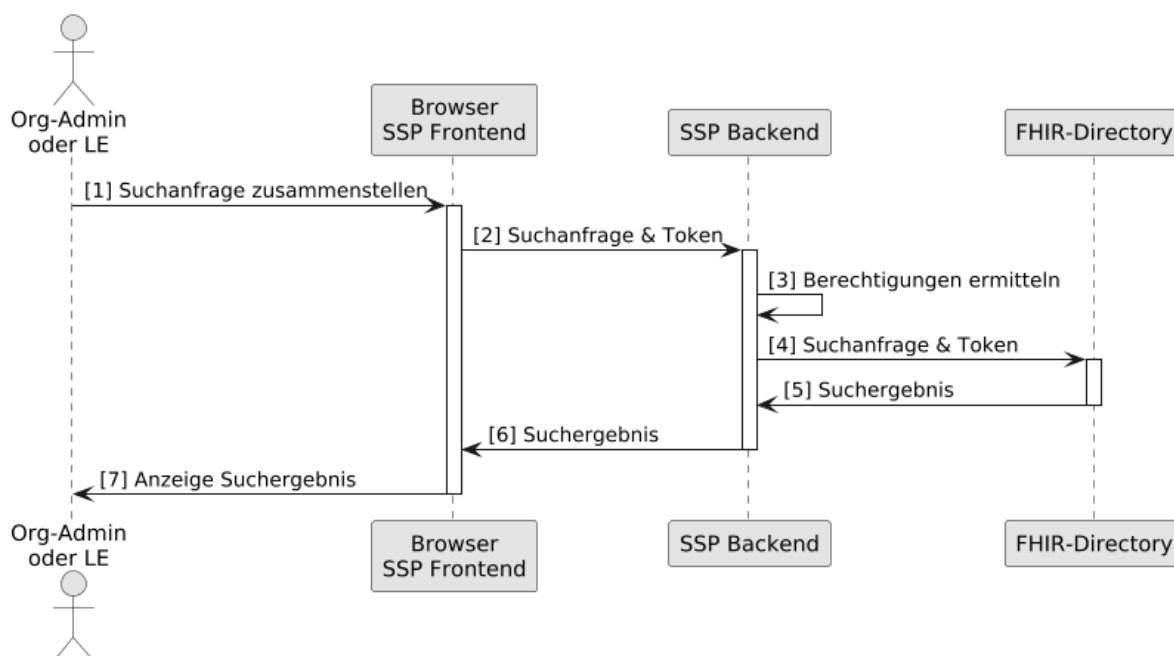
【<=,VZD_FHIR,funkt. Eignung: Herstellererklärung】

7.2.8.3 Suche und Anzeige von FHIR VZD Einträgen

AF_10416 -FHIR VZD Self-Service Portal - Suche und Anzeige von Einträgen

Attribute	Bemerkung
-----------	-----------

Akteure	<ul style="list-style-type: none"> Mitarbeiter im Gesundheitswesen Administratoren von Organisationen im Gesundheitswesen Administrative Nutzer im Gesundheitswesen
Beschreibung	<ol style="list-style-type: none"> Der Benutzer formuliert im SSP Frontend/Browser seine Suchanfrage. [1] Das SSP Frontend sendet die Suchanfrage zusammen mit dem vorliegenden Token an das SSP Backend. [2] Das SSP Backend validiert das Token & ermittelt die Berechtigungen. [3] Das SSP Backend leitet die Suchanfrage zusammen mit dem Token an das FHIR-Directory weiter. [4] Die FHIR-Directory Antwort wird über SSP Backend und SSP Frontend zurückgegeben. [5,6] Das SSP Frontend stellt dem Benutzer das Suchergebnis dar. [7]
Vorbedingung	Der Benutzer wurde authentisiert und die erforderlichen Nutzerdaten liegen im SSP Frontend vor.
Nachbedingung	Dem Benutzer liegt die Antwort auf seine Suchanfrage vor.



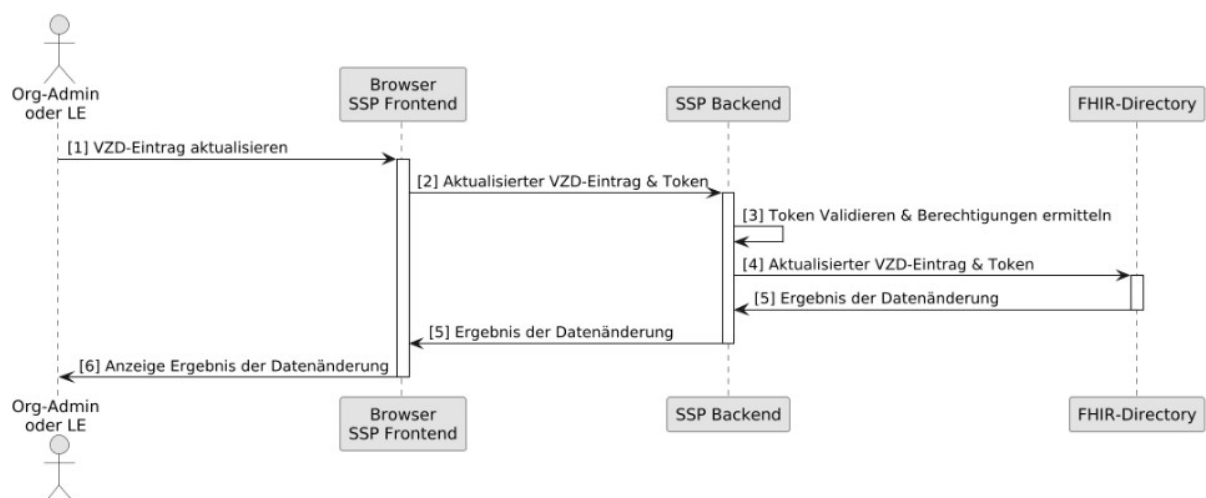
[<=,VZD_FHIR,funkt. Eignung: Herstellererklärung]

7.2.8.4 Änderung von FHIR VZD Einträgen

AF_10417 -FHIR VZD Self-Service Portal - Suche und Änderung von Einträgen

Attribute	Bemerkung
-----------	-----------

Akteure	<ul style="list-style-type: none"> Mitarbeiter im Gesundheitswesen Administratoren von Organisationen im Gesundheitswesen Administrative Nutzer im Gesundheitswesen
Beschreibung	<ol style="list-style-type: none"> Der Benutzer ändert den VZD-Eintrag. [1] Das SSP Frontend sendet den aktualisierten VZD-Eintrag zusammen mit dem vorliegenden Token an das SSP Backend. [2] Das SSP Backend validiert das Token und ermittelt die Berechtigungen. [3] Das SSP Backend übergibt den aktualisierten VZD-Eintrag zusammen mit dem SSP Backend Token an das FHIR-Directory. [4] Das Ergebnis der Datenänderung wird vom FHIR-Directory über FHIR-Proxy, SSP Backend und SSP Frontend zurückgegeben. [5] Das SSP Frontend stellt dem Benutzer das Ergebnis der Datenänderung dar. [6]
Vorbedingung	Der Benutzer wurde authentisiert und die erforderlichen Nutzerdaten liegen im SSP Frontend vor. Der Benutzer hat eine Suche nach dem zu ändernden VZD Datensatz durchgeführt und das Suchergebnis liegt im SSP Frontend vor.
Nachbedingung	Dem Benutzer wird das Ergebnis der Datenänderung dargestellt.



【<=,VZD_FHIR,funkt. Eignung: Herstellererklärung】

Es wird Kapitel "7.5.2" wie folgt angepasst

8.5.2 Weitere Dokumente

...

Mitgeltende Dokumente und Web-Inhalte

Quelle	Herausgeber: Bezeichnung / URL	Version Branch / Tag
[VZD-FHIR- PACKAGE- DIRECTORY]	https://simplifier.net/packages/de.gematik.fhir.directory/0.10.25 https://simplifier.net/packages/de.gematik.fhir.directory/1.0.0	0.11.24 1.0.0

Es wird Kapitel "7.6" wie folgt angepasst

8.6 Versionierung Datenmodell

Folgende Versionen der Datenmodell Ressourcen (<https://simplifier.net/vzd-fhir-directory/>) sind für die vorliegende Spezifikation relevant:

- [de.gematik.fhir.directory/0.11.25](https://simplifier.net/packages/de.gematik.fhir.directory/0.11.25)
- [de.gematik.fhir.directory/1.0.0](https://simplifier.net/packages/de.gematik.fhir.directory/1.0.0)

3 Änderungen in Steckbriefen

3.1 Änderungen in gemProdT_VZD_PTV

Anmerkung: Die Anforderungen der folgenden Tabelle stellen einen Auszug dar und verteilen sich innerhalb der Tabelle des Originaldokuments [gemProdT_VZD_PTV]. Alle Anforderungen der Tabelle des Orig

inaldokuments, die in der folgenden Tabelle nicht ausgewiesen sind, bleiben unverändert bestehenden.

Tabelle 25: Festlegungen zur funktionalen Eignung "Produkttest/Produktübergreifender Test"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
TIP1-A_5555	VZD, SOAP-Fehlercodes	gemSpec_VZD
TIP1-A_5572	VZD, I_Directory_Maintenance, TLS-gesicherte-Verbindung	gemSpec_VZD
TIP1-A_5574	VZD und Nutzer der Schnittstelle I_Directory_Maintenance, WebService	gemSpec_VZD
TIP1-A_5575	VZD, Umsetzung add_Directory_Entry	gemSpec_VZD
TIP1-A_5576	Nutzer der Schnittstelle, TUC_VZD_0002-„add_Directory_Entry“	gemSpec_VZD
TIP1-A_5577	VZD, Umsetzung read_Directory_Entry	gemSpec_VZD
TIP1-A_5578	Nutzer der Schnittstelle, TUC_VZD_0003-„read_Directory_Entry“	gemSpec_VZD
TIP1-A_5579	VZD, Umsetzung modify_Directory_Entry	gemSpec_VZD
TIP1-A_5580	Nutzer der Schnittstelle, TUC_VZD_0004-„modify_Directory_Entry“	gemSpec_VZD
TIP1-A_5581	VZD, Umsetzung delete_Directory_Entry	gemSpec_VZD
TIP1-A_5582	Nutzer der Schnittstelle, TUC_VZD_0005-„delete_Directory_Entry“	gemSpec_VZD
TIP1-A_5586-02	VZD, I_Directory_Application_Maintenance, Webservice und LDAPv3	gemSpec_VZD

TIP1-A_5587	VZD, Implementierung der LDAPv3 Schnittstelle	gemSpec_VZD
TIP1-A_5590	VZD, Umsetzung add_Directory_FA-Attributes (SOAP)	gemSpec_VZD
TIP1-A_5591	FAD, TUC_VZD_0006 "add_Directory_FA-Attributes (SOAP)"	gemSpec_VZD
TIP1-A_5592-03	FAD, KOM-LE_FA_Add_Attributes	gemSpec_VZD
TIP1-A_5593	VZD, Umsetzung add_Directory_FA-Attributes (LDAPv3)	gemSpec_VZD
TIP1-A_5594	FAD, TUC_VZD_0007 "add_Directory_FA-Attributes (LDAPv3)"	gemSpec_VZD
A_21834	VZD, I_Directory_Application_Maintenance, KOM-LE_Version-Prüfung LDAP	gemSpec_VZD
A_21835	VZD, I_Directory_Application_Maintenance, Eindeutige Zuordnung von KOM-LE-Adressen zu VZD-Einträgen LDAP	gemSpec_VZD
A_23729	VZD, I_Directory_Application_Maintenance, Anwendungskennzeichen-Prüfung LDAP	gemSpec_VZD
TIP1-A_5595	VZD, Umsetzung delete_Directory_FA-Attributes	gemSpec_VZD
TIP1-A_5596	FAD, TUC_VZD_0008 "delete_Directory_FA-Attributes (SOAP)"	gemSpec_VZD
TIP1-A_5597	VZD, Umsetzung delete_Directory_FA-Attributes (LDAPv3)	gemSpec_VZD
TIP1-A_5598	FAD, TUC_VZD_0009 "delete_Directory_FA-Attributes (LDAPv3)"	gemSpec_VZD
A_21460-01	VZD, Umsetzung delete_Directory_FA-Attributes (REST)	gemSpec_VZD
TIP1-A_5599-01	VZD, Umsetzung modify_Directory_FA-Attributes	gemSpec_VZD
TIP1-A_5600	FAD, TUC_VZD_0010 "modify_Directory_FA-Attributes (SOAP)"	gemSpec_VZD
TIP1-A_5601-03	FAD, KOM-LE_FA_Modify_Attributes	gemSpec_VZD
TIP1-A_5602	VZD, Umsetzung modify_Directory_FA-Attributes	gemSpec_VZD

	(LDAPv3)	
TIP1-A_5603	FAD, TUC_VZD_0011 "modify_Directory_FA-Attributes (LDAPv3)"	gemSpec_VZD
A_18602-01	VZD, I_Directory_Administration, keine Datenänderung über Maintenance Schnittstelle	gemSpec_VZD
A_20402-04	VZD, I_Directory_Administration, read_Directory_Entry_for_Sync, Paging, Berechtigung	gemSpec_VZD

Tabelle 26: Festlegungen zur funktionalen Eignung "Herstellererklärung"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
TIP1-A_5571	VZD, Schnittstelle I_Directory_Maintenance	gemSpec_VZD
A_23728-01	VZD, I_Directory_Application_Maintenance, Aktualisierung zulässiger Anwendungskennzeichen	gemSpec_VZD
TIP1-A_5607-13	VZD, logisches Datenmodell	gemSpec_VZD

Tabelle 27: Festlegungen zur funktionalen Eignung "Sich.techn Eignung: Gutachten"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
TIP1-A_5548-01	VZD, Protokollierung der Änderungsoperationen	gemSpec_VZD

3.2 Änderungen in gemProdT_FD_KOMLE

Anmerkung: Die Anforderungen der folgenden Tabelle stellen einen Auszug dar und verteilen sich innerhalb der Tabelle des Originaldokuments [gemProdT_FD_KOMLE]. Alle Anforderungen der Tabelle des Orig

inaldokuments, die in der folgenden Tabelle nicht ausgewiesen sind, bleiben unverändert bestehenden.

Tabelle 28: Festlegungen zur funktionalen Eignung "Herstellererklärung"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
TIP1-A_5588-01	FAD, I_Directory_Application_Maintenance,	gemSpec_VZD

	Nutzung Webservice	
A_28423	FAD, TUC_VZD_0017 "search_Directory_FA-Attributes (REST)"	gemSpec_VZD
A_28424	FAD, TUC_VZD_0018 "readLog (REST)"	gemSpec_VZD
TIP1-A_5589	FAD, Implementierung der LDAPv3-Schnittstelle	gemSpec_VZD
TIP1-A_5591	FAD, TUC_VZD_0006 "add_Directory_FA-Attributes (SOAP)"	gemSpec_VZD
TIP1-A_5592-03	FAD, KOM-LE_FA_Add_Attributes	gemSpec_VZD
TIP1-A_5594	FAD, TUC_VZD_0007 "add_Directory_FA-Attributes (LDAPv3)"	gemSpec_VZD
TIP1-A_5596	FAD, TUC_VZD_0008 "delete_Directory_FA-Attributes (SOAP)"	gemSpec_VZD
TIP1-A_5598	FAD, TUC_VZD_0009 "delete_Directory_FA-Attributes (LDAPv3)"	gemSpec_VZD
TIP1-A_5600	FAD, TUC_VZD_0010 "modify_Directory_FA-Attributes (SOAP)"	gemSpec_VZD
TIP1-A_5601-03	FAD, KOM-LE_FA_Modify_Attributes	gemSpec_VZD
TIP1-A_5603	FAD, TUC_VZD_0011 "modify_Directory_FA-Attributes (LDAPv3)"	gemSpec_VZD
A_28423	FAD, TUC_VZD_0017 "search_Directory_FA-Attributes (REST)"	gemSpec_VZD
A_28424	FAD, TUC_VZD_0018 "readLog (REST)"	gemSpec_VZD

3.3 Änderungen in gemProdT_CM_KOMLE

Anmerkung: Die Anforderungen der folgenden Tabelle stellen einen Auszug dar und verteilen sich innerhalb der Tabelle des Originaldokuments [gemProdT_CM_KOMLE]. Alle Anforderungen der Tabelle des Originaldokuments, die in der folgenden Tabelle nicht ausgewiesen sind, bleiben unverändert bestehenden.

Tabelle 29: Festlegungen zur funktionalen Eignung "Herstellererklärung"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
--------	-----------------	-------------------

A_27744	VZD Clients - Nutzung zentraler TI-Systeme durch dezentrale Clients: Verbindungsmanagement	gemSpec_VZD
A_27749	VZD Client - Nutzung zentraler TI-Systeme durch dezentrale Clients: Verbindungsmanagement, Parameter	gemSpec_VZD
A_27751	VZD Client - Nutzung zentraler TI-Systeme durch dezentrale Clients: Angepasste Konfiguration und Außerbetriebnahme von Clients	gemSpec_VZD
A_28318	VZD Client - Deaktivierung nicht genutzter Clients	gemSpec_VZD
A_27752	VZD Client - Nutzung zentraler TI-Systeme durch dezentrale Clients: Vermeidung der Gesamtauslese des VZD durch Clients	gemSpec_VZD
A_27753	VZD Client - Nutzung zentraler TI-Systeme durch dezentrale Clients: Caching	gemSpec_VZD
A_27754	VZD Client - Nutzung zentraler TI-Systeme durch dezentrale Clients: Effiziente Gestaltung von FHIR-Suchanfragen	gemSpec_VZD
A_27755	VZD Client - Nutzung zentraler TI-Systeme durch dezentrale Clients: Fehler-Monitoring	gemSpec_VZD

3.4 Änderungen in gemProdT_VZD_FHIR

Anmerkung: Die Anforderungen der folgenden Tabelle stellen einen Auszug dar und verteilen sich innerhalb der Tabelle des Originaldokuments [gemProdT_VZD_FHIR]. Alle Anforderungen der Tabelle des Originaldokuments, die in der folgenden Tabelle nicht ausgewiesen sind, bleiben unverändert bestehenden.

Tabelle 30: Festlegungen zur funktionalen Eignung "Herstellererklärung"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
AF_10036-04	Nutzer sucht Einträge im FHIR-Directory	gemSpec_VZD_FHIR_Directory
AF_10037-04	Einträge im VZD-FHIR-Directory ändern und suchen	gemSpec_VZD_FHIR_Directory
AF_10219-02	Versicherter sucht Einträge im FHIR-Directory	gemSpec_VZD_FHIR_Directory

AF_10414	FHIR VZD Self-Service Portal - Authentisierung über HBA/SMC-B	gemSpec_VZD_FHIR_Directory
AF_10415	FHIR VZD Self-Service Portal - Authentisierung über Passwort	gemSpec_VZD_FHIR_Directory
AF_10416	FHIR VZD Self-Service Portal - Suche und Anzeige von Einträgen	gemSpec_VZD_FHIR_Directory
AF_10417	FHIR VZD Self-Service Portal - Suche und Änderung von Einträgen	gemSpec_VZD_FHIR_Directory

Tabelle 31: Festlegungen zur funktionalen Eignung "Sich.techn Eignung: Gutachten"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
TIP1- A_5548-01	VZD, Protokollierung der Änderungsoperationen	gemSpec_VZD_FHIR_Directory