Beim vorliegenden Dokument handelt es sich um einen Entwurf der gematik in Vorbereitung auf zukünftige normative Festlegungen als Grundlage entsprechender Zulassungs- und Bestätigungsverfahren. Die gematik veröffentlicht diesen Entwurf mit dem Ziel, dass sich Interessierte bereits frühzeitig einen Überblick über die mögliche Weiterentwicklung der Telematikinfrastruktur verschaffen können. Die gematik übernimmt keine Gewähr für die Aktualität, Richtigkeit und Vollständigkeit dieses Entwurfes und behält sich das Recht vor, ohne vorherige Ankündigung Änderungen oder Ergänzungen vorzunehmen oder von den Regelungen insgesamt bzw. teilweise Abstand zu nehmen.

Elektronische Gesundheitskarte und Telematikinfrastruktur

Spezifikation Verzeichnisdienst

ENTWURF

Version:	1.~~9~~10.0 CC
Revision:	~~192694~~230780
Stand:	~~02.10.2019~~30.04.2020
Status:	zur Abstimmung freigegeben
Klassifizierung:	öffentlich_Entwurf
Referenzierung:	gemSpec_VZD

Dokumentinformationen

Änderungen zur Vorversion

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

Dokumentenhistorie

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
1.2.0	17.07.15		Nutzer der Schnittstelle I_Directory_Maintenance geändert	gematik
1.3.0	24.08.16		Anpassungen zum Online-Produktivbetrieb (Stufe 1)	gematik
1.4.0	28.10.16		Einarbeitung lt. Änderungsliste	gematik
1.5.0	19.04.17		Anpassung nach Änderungsliste	gematik
1.6.0	14.05.18		Anpassung nach Änderungslisten P15.2, 15.4 und 15.5	gematik
1.7.0	15.05.19		Einarbeitung der Änderungen gemäß P18.1	gematik
1.8.0	28.06.19		Einarbeitung der Änderungen gemäß P19.1	gematik
1.9.0	02.10.19		Einarbeitung der Änderungen gemäß P20.1 und P16.1/2	gematik
1.~~9~~10.0	30.04.20~~02.10.19~~		~~freigegeben~~Anpassungen gemäß Änderungsliste P22.1 und Scope-Themen aus Systemdesign R4.0.0	gematik

ENTWURF

Inhaltsverzeichnis

ENTWURF

ENTWURF

ENTWURF

ENTWURF

1 Einordnung des Dokumentes

1.1 Zielsetzung

Die Spezifikation des Verzeichnisdienstes (VZD) enthält die Definition der Funktionalität, der Prozesse und der Schnittstellen sowie das Informationsmodell des VZD.

Der VZD ist ein zentraler Dienst der TI-Plattform.

Das Informationsmodell des VZD ist erweiterbar.

Die vorliegende Spezifikation definiert die Anforderungen zu Herstellung, Test, Betrieb, Datenschutz und Informationssicherheit des Produkttyps VZD.

1.2 Zielgruppe

Das Dokument ist maßgeblich für Anbieter und Hersteller von Verzeichnisdiensten

1.3 Geltungsbereich

Dieses Dokument enthält normative Festlegungen zur Telematikinfrastruktur des Deutschen Gesundheitswesens. Der Gültigkeitszeitraum der vorliegenden Version und deren Anwendung in Zulassungs- oder Abnahmeverfahren wird durch die gematik mbH in gesonderten Dokumenten (z.B. Dokumentenlandkarte, Produkttypsteckbrief, Leistungsbeschreibung) festgelegt und bekannt gegeben.

Schutzrechts-/Patentrechtshinweis

Die nachfolgende Spezifikation ist von der gematik allein unter technischen Gesichtspunkten erstellt worden. Im Einzelfall kann nicht ausgeschlossen werden, dass die Implementierung der Spezifikation in technische Schutzrechte Dritter eingreift. Es ist allein Sache des Anbieters oder Herstellers, durch geeignete Maßnahmen dafür Sorge zu tragen, dass von ihm aufgrund der Spezifikation angebotene Produkte und/oder Leistungen nicht gegen Schutzrechte Dritter verstoßen und sich ggf. die erforderlichen Erlaubnisse/Lizenzen von den betroffenen Schutzrechtsinhabern einzuholen. Die gematik mbH übernimmt insofern keinerlei Gewährleistungen.

1.4 Abgrenzungen

Spezifiziert werden in dem Dokument die von dem Produkttyp bereitgestellten (angebotenen) Schnittstellen. Benutzte Schnittstellen werden hingegen in der Spezifikation desjenigen Produkttypen beschrieben, der diese Schnittstelle bereitstellt. Auf die entsprechenden Dokumente wird verwiesen (siehe auch 6- Anhang A – Verzeichnisse).

ENTWURF

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

Nicht Bestandteil des vorliegenden Dokumentes sind die Festlegungen zum Themenbereich

- Werkzeuge für Fachdienstanbieter, die die Administration von fachdienstspezifischen Daten unterstützen.

1.5 Methodik

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

Sie werden im Dokument wie folgt dargestellt:

<AFO-ID> - <Titel der Afo>
Text / Beschreibung
[<=]

Dabei umfasst die Anforderung sämtliche innerhalb der Afo-ID und der Textmarke angeführten Inhalte.

Für die Erzeugung der Abbildungen und Informationsmodelle wird das Tool „Enterprise Architect" verwendet.

ENTWURF

2 Systemüberblick

Der VZD ist ein Produkttyp der TI gemäß [gemKPT_Arch_TIP].

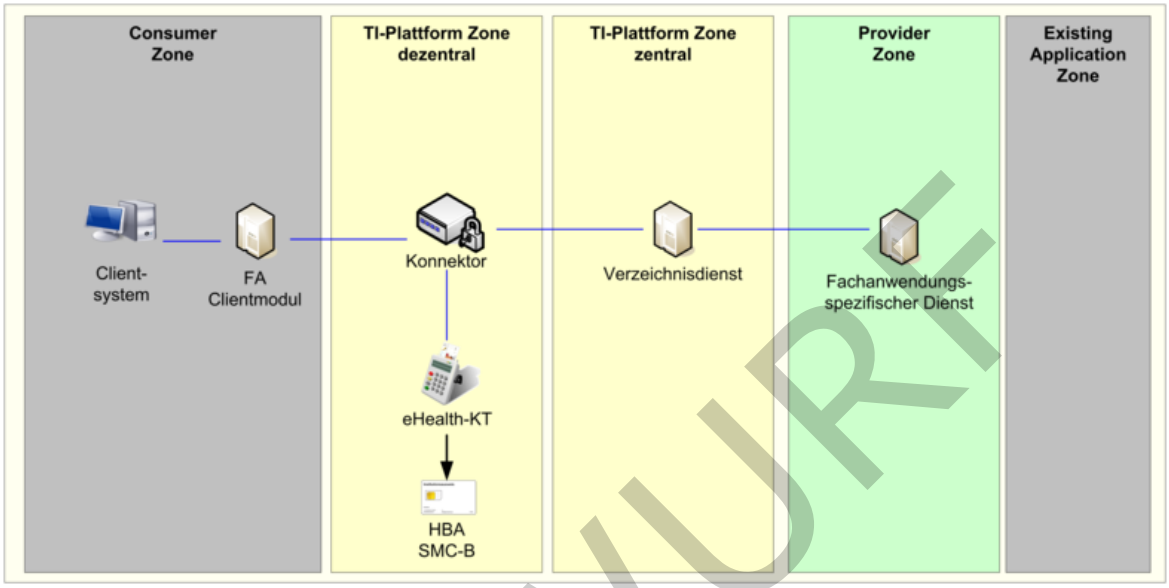


Abbildung 1: Einordnung des VZD in die TI

Der VZD befindet sich in der zentralen Zone der TI-Plattform.

Die Dateneinträge werden erstellt und gepflegt:

1. per Basisdatenadministration durch berechtigte Benutzer (Kartenherausgeber oder von ihnen berechtigte Organisationen sowie von KOM-LE-Anbietern mittels KOM-LE-Fachdienst, wenn für bestimmte LE noch keine Basisdaten eingetragen sind)
2. durch fachanwendungsspezifische Dienste (FAD), die fachanwendungsspezifische Daten (Fachdaten) zu bereits bestehenden Basisdaten zufügen.

Der VZD kann durch LDAP-Clients abgefragt werden.

ENTWURF

3 Übergreifende Festlegungen

3.1 IT-Sicherheit und Datenschutz

TIP1-A_5546 - VZD, Integritäts- u. Authentizitätsschutz
Der Anbieter des VZD MUSS die Integrität und Authentizität der im VZD gespeicherten Daten gemäß den Richtlinien des Bundesamtes für Sicherheit in der Informationstechnik für allgemeine Verzeichnisdienste, [BSI-AllVZD], implementieren.
[<=]

TIP1-A_5547 - VZD, Löschen ungültiger Zertifikate
Der VZD MUSS täglich die gespeicherten Zertifikate nach Ablaufdatum (TUC_PKI_002 „Gültigkeitsprüfung des Zertifikats“) und Status (TUC_PKI_006 "OCSP-Abfrage) prüfen. Ungültige Zertifikate werden sofort gelöscht. Ein Eintrag ohne gültige Zertifikate wird nach einem Jahr gelöscht und darf nicht durch eine Anfrage über die Operation search_Directory der Schnittstelle I_Directory_Query gefunden werden.
[<=]

TIP1-A_5548 - VZD, Protokollierung der Änderungsoperationen
Der VZD MUSS Änderungen der Verzeichnisdiensteinträge protokollieren und muss sie 6 Monate zur Verfügung halten.
[<=]

6 Monate ist die maximale Nachweistiefe ohne in den Bereich der Vorratsdatenspeicherung zu kommen.

TIP1-A_5549 - VZD, Keine Leseprofilbildung
Der VZD DARF Suchanfragen NICHT speichern oder protokollieren.
[<=]

TIP1-A_5550 - VZD, Keine Kopien von gelöschten Daten
Der VZD DARF von gelöschten Daten KEINE Kopien speichern.
[<=]

TIP1-A_5551 - VZD, Sicher gegen Datenverlust
Der Anbieter des VZD MUSS den Dienst gegen Datenverlust absichern.
[<=]

TIP1-A_5552 - VZD, Begrenzung der Suchergebnisse
Der VZD MUSS die Ergebnisliste einer Suchanfrage auf 100 Suchergebnisse begrenzen.
[<=]

TIP1-A_5553 - VZD, Private Schlüssel sicher speichern
Der VZD MUSS seine privaten Schlüssel sicher speichern und ihr Auslesen verhindern um Manipulationen zu verhindern.
[<=]

TIP1-A_5554 - VZD, Registrierungsdaten sicher speichern
Der VZD MUSS die Integrität und Authentizität der gespeicherten Registrierungsdaten der FAD gewährleisten.
[<=]

TIP1-A_5555 - VZD, SOAP-Fehlercodes
Der VZD MUSS für seine SOAP-Schnittstelle die generischen Fehlercodes

- Code 2: Verbindung zurückgewiesen

ENTWURF

- 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.

[<=]

TIP1-A_5556 - VZD, Fehler Logging
Der VZD MUSS lokal und remote erkannte Fehler in seinem lokalen Speicher protokollieren.
[<=]

TIP1-A_5557 - VZD, Unterstützung IPv4 und IPv6
Der VZD MUSS IPv4 und IPv6 für alle seine IP-Schnittstellen im Dual-Stack-Mode unterstützen.
[<=]

TIP1-A_5558 - VZD, Sicheres Speichern der TSL
Der VZD MUSS die Inhalte der TSL in einem lokalen Trust Store sicher speichern und für X.509-Zertifikatsprüfungen lokal zugreifbar halten.
[<=]

TIP1-A_5611 - VZD, Widerspruch der Einwilligung
Der Anbieter des VZD MUSS die Daten des Leistungserbringers unverzüglich vom Verzeichnisdienst löschen, sobald ihm der Widerruf der Einwilligung durch den Leistungserbringer bekannt wird.
Wenn ein Eintrag aufgrund des Widerspruchs des Leistungserbringers gelöscht wurde, MUSS der Anbieter des VZD den Ersteller des Eintrages innerhalb von 5 Werktagen darüber informieren.
[<=]

3.2 Fachliche Anforderungen

TIP1-A_5560 - VZD, Erweiterbarkeit für neue Fachdaten
Der Anbieter des VZD MUSS die Erweiterbarkeit des VZD für die Aufnahme der Fachdaten neuer Fachanwendungen gewährleisten.
[<=]

TIP1-A_5561 - VZD, DNS-SD
Der Anbieter des VZD MUSS alle erforderlichen Einträge zur Dienstlokalisierung der Außenschnittstellen gemäß [RFC6763] beginnend mit folgenden PTR Resource Record-Bezeichnern im Namensdienst der TI-Plattform anlegen:

- für den Zugriff auf die Schnittstelle I_Directory_Query: _ldap._tcp.vzd.telematik.
- für den Zugriff auf die Schnittstelle I_Directory_Maintenance: _vzd-bd._tcp.vzd.telematik.
- für den Zugriff auf die Schnittstelle I_Directory_Application_Maintenance: _vzd-fd._tcp.vzd.telematik.

[<=]

ENTWURF

TIP1-A_5562 - VZD, Parallele Zugriffe
Der Betreiber des VZD MUSS sicherstellen, dass Benutzer gleichzeitig auf den VZD zugreifen können. Dies umfasst alle technischen Schnittstellen. In [gemSpec_Perf] ist die Anzahl der parallelen Zugriffe definiert.
[<=]

TIP1-A_5563 - VZD, Erhöhung der Anzahl der Einträge
Der Anbieter des VZD MUSS sicherstellen das 500 000 Einträge gespeichert werden können.
[<=]

TIP1-A_5620 - VZD, Nicht-Speicherung von Leading und Trailing Spaces
Der Anbieter des VZD MUSS Leading und Trailing Spaces abschneiden.
[<=]

ENTWURF

4 Funktionsmerkmale

Der VZD beinhaltet alle serverseitigen Anteile des Basisdienstes Verzeichnis_Identitäten gemäß [gemKPT_Arch_TIP]. Dazu zählen die Speicherung der Einträge von Leistungserbringern und Institutionen mit allen definierten Attributen sowie die Speicherung von Fachdaten durch FAD. Mit einer LDAP-Suchanfrage können Clients und FAD Basis- und Fachdaten abfragen (z. B. X.509-Zertifikate).

Einträge des VZD werden durch berechtigte Benutzer sowie durch berechtigte FAD erstellt und gepflegt.

TIP1-A_5564 - VZD, Festlegung der Schnittstellen
Der VZD MUSS die Schnittstellen gemäß Tabelle Tab_PT_VZD_Schnittstellen implementieren („bereitgestellte" Schnittstellen) und nutzen („benötigte" Schnittstellen).

Tabelle 1: Tab_PT_VZD_Schnittstellen

Schnittstelle	bereitgestellt / benötigt	Bemerkung
I_Directory_Query	bereitgestellt	
I_Directory_Maintenance	bereitgestellt	
I_Directory_Application_Maintenance	bereitgestellt	
I_Directory_Administration	bereitgestellt	
I_IP_Transport	benötigt	Definition in [gemSpec_Net]
I_DNS_Name_Resolution	benötigt	Definition in [gemSpec_Net]
I_NTP_Time_Information	benötigt	Definition in [gemSpec_Net]
I_OCSP_Status_Information	benötigt	Definition in [gemSpec_PKI]
I_TSL_Download	benötigt	Definition in [gemSpec_TSL]

[<=]

4.1 Schnittstelle I_Directory_Query

Die Schnittstelle ermöglicht LDAPv3-Clients die Suche nach Daten im VZD gemäß der im Informationsmodell (siehe Kapitel 5) definierten Attribute.

TIP1-A_5565 - VZD, Schnittstelle I_Directory_Query
Der VZD MUSS für LDAP Clients die Schnittstelle I_Directory_Query gemäß Tabelle Tab_VZD_Schnittstelle_I_Directory_Query anbieten.

Tabelle 2: Tab_VZD_Schnittstelle_I_Directory_Query

Name	I_Directory_Query

ENTWURF

Version	wird im Produkttypsteckbrief des VZD definiert	
Operationen	Name	Kurzbeschreibung
	search_Directory	Abfragen von Daten des VZD gemäß LDAPv3 Protokoll. Der Base DN für die LDAP Suche ist dc=data,dc=vzd.

[<=]

4.1.1 Operation search_Directory

TIP1-A_5566 - LDAP Client, LDAPS
Der LDAP Client MUSS die Verbindung zum VZD mittels LDAPS sichern.
Der LDAP Client muss das Zertifikat des VZD C.ZD.TLS-S gemäß TUC_PKI_018 "Zertifikatsprüfung in der TI" und die Rolle (zulässig ist oid_vzd_ti) prüfen. LDAP Clients der Anbieter von aAdG und aAdG-NetG-TI sind davon ausgenommen.
Der LDAP Client authentisiert sich nicht.
[<=]

TIP1-A_5567 - VZD, LDAPS bei search_Directory
Der VZD MUSS sicherstellen, dass die Operation search_Directory nur über eine bestehende LDAPS -Verbindung ausgeführt werden kann.
Der VZD muss die TLS-Verbindung 15 Minuten nach dem letzten Meldungsverkehr abbauen, falls sie noch besteht.
[<=]

TIP1-A_5568 - VZD und LDAP Client, Implementierung der LDAPv3 search Operation
Der VZD und die LDAP-Clients MÜSSEN die search Operation gemäß den LDAPv3 Standards [RFC4510], [RFC4511], [RFC4512], [RFC4513], [RFC4514], [RFC4515], [RFC4516], [RFC4517], [RFC4518], [RFC4519], [RFC4520], [RFC4522] und [RFC4523] implementieren.
[<=]

A_17794 - VZD, Testunterstützung
Der VZD MUSS für die Schnittstelle I_Directory_Query einen technischen User in RU/TU bereitstellen, über den eine unlimitierte Abfrage der Daten des Verzeichnisdienstes (searchView) möglich ist.
[<=]

4.1.1.1 Umsetzung

TIP1-A_5569 - VZD, search_Directory, Suche nach definierten Attributen
Der VZD MUSS die enthaltenen Daten so strukturiert haben, dass mit einer einzigen LDAPv3-Suche alle einer Telematik-ID zugeordneten Attribute (Basisdaten und Fachdaten) in Form einer flachen Liste von Attributen ohne ou-Unterstruktur abgefragt werden können.
Die abgefragten Attribute MÜSSEN durch marktübliche E-Mail Clients nutzbar sein.
[<=]

4.1.1.2 Nutzung

TIP1-A_5570 - LDAP Client, TUC_VZD_0001 „search_Directory"
Der Anbieter des VZD MUSS für die Nutzung durch LDAP Clients den technischen Use Case TUC_VZD_0001 „search_Directory" gemäß Tabelle Tab_TUC_VZD_0001

ENTWURF

403 unterstützen.
404

405 **Tabelle 3: Tab_TUC_VZD_0001**

Name	TUC_VZD_0001 "search_Directory"	
Beschreibung	Diese Operation ermöglicht die Suche nach den im VZD gespeicherten Daten.	
Vorbedingungen	Der LDAPS-Verbindungsaufbau muss erfolgreich durchgeführt sein.	
Eingangsdaten	Search Request gemäß [RFC4511]#4.5.1 und Informationsmodell (Abb_VZD_logisches_Datenmodell)	
Komponenten	LDAP Client, Verzeichnisdienst	
Ausgangsdaten	gemäß [RFC4511]#4.5.2	
Standardablauf	Aktion	Beschreibung
	Search Request senden	Der LDAP Client sendet eine Suchanfrage gemäß [RFC4511]#4.5.1 an die Schnittstelle I_Directory_Query des VZD. Die RFCs [RFC4510], [RFC4511], [RFC4513], [RFC4514], [RFC4515], [RFC4516], [RFC4519] und [RFC4522] müssen unterstützt werden. Der Base DN für die LDAP Suche ist dc=data,dc=vzd.
	Search Response empfangen	Der LDAP Client empfängt das Ergebnis der Suche gemäß [RFC4511]#4.5.2.
Varianten/Alternativen	keine	
Zustand nach erfolgreichem Ablauf	Die Ergebnisse der Suche liegen im LDAP Client vor.	
Fehlerfälle	Zur Behandlung auftretender Fehlerfälle werden Fehlermeldungen gemäß [RFC4511]#Appendix A verwendet.	

406 **[<=]**

ENTWURF

407 4.2 Schnittstelle I_Directory_Maintenance

408 Die Schnittstelle ermöglicht die Administration der Basisdaten.

409 **TIP1-A_5571 - VZD, Schnittstelle I_Directory_Maintenance**
410 Der VZD MUSS die Schnittstelle I_Directory_Maintenance gemäß Tabelle
411 Tab_VZD_Schnittstelle_I_Directory_Maintenance anbieten.
412

413 **Tabelle 4: 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.
[<=]

ENTWURF

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

448

449 **Tabelle 5: 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	surname	Verwendung gemäß Tab_VZD_Datenbeschreibung
n/a	cn	commonName	Verwendung gemäß Tab_VZD_Datenbeschreibung
displayName	displayName	displayName	
streetAddress	streetAddress	streetAddress	
postalCode	postalCode	postalCode	
localityName	localityName	localityName	
stateOrProvinceName	stateOrProvinceName	stateOrProvinceName	
title	title	title	Verwendung gemäß Tab_VZD_Datenbeschreibung
organization	organization	organization	Verwendung gemäß Tab_VZD_Datenbeschreibung
otherName	otherName	otherName	Verwendung gemäß Tab_VZD_Datenbeschreibung
subject	specialization	subject	Verwendung gemäß Tab_VZD_Datenbeschreibung

ENTWURF

n/a	domainID	n/a	
n/a	personalEntry	n/a	Verwendung gemäß Tab_VZD_Datenbeschreibung
x509CertificateEnc	userCertificate	x509CertificateEnc	
n/a	entryType	n/a	Verwendung gemäß Tab_VZD_Datenbeschreibung
n/a	telematikID	telematikID	Verwendung gemäß Tab_VZD_Datenbeschreibung
n/a	professionOID	n/a	Verwendung gemäß Tab_VZD_Datenbeschreibung
n/a	usage	n/a	Wenn der Eintrag von einem KOM-LE Fachdienst erzeugt oder geändert wird, dann muss das Attribut usage den Wert "KOM-LE" erhalten.
n/a	description	n/a	
timestamp	n/a	timestamp	Datum und Zeit des Requests bzw. der Response
variant	n/a	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	

ENTWURF

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.

454 Der SOAP-Requests MUSS gemäß Tab_VZD_Datenbeschreibung mit der Bedeutung
455 entsprechenden Daten ausgefüllt sein.
456

457 **Tabelle 6: 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	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 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.	

458 **[<=]**

ENTWURF

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) gemäßTab_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 7: 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.

ENTWURF

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: faultcode 4221, faultstring: Operation fehlerhaft ausgeführt, Basisdaten konnten nicht gelesen werden (Fehler im Verzeichnisdienst) faultcode 4312, faultstring: Basisdaten konnten nicht gefunden werden faultcode 4202, faultstring: SOAP Request enthält Fehler 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.	

[<=]

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.

ENTWURF

504

505 **Tabelle 8: 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	Es werden die protokollspezifischen Fehlermeldungen verwendet (TCP, HTTP, TLS) Fehler bei der Verarbeitung des SOAP Requests werden als gematik SOAP-Fault versendet: faultcode 4231, faultstring: Operation fehlerhaft ausgeführt, Basisdaten konnten nicht modifiziert werden (Fehler im Verzeichnisdienst) faultcode 4312, faultstring: Basisdaten konnten nicht gefunden werden faultcode 4202, faultstring: SOAP Request enthält Fehler 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.	

506 **[<=]**

507 4.2.4 Operation delete_Directory_Entry

508 Diese Operation löscht einen bestehenden Datensatz im LDAP Verzeichnis.

ENTWURF

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 9: 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.

ENTWURF

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: faultcode 4241, faultstring: Operation fehlerhaft ausgeführt, Basisdaten konnten nicht gelöscht werden (Fehler im Verzeichnisdienst) faultcode 4312, faultstring: Basisdaten konnten nicht gefunden werden faultcode 4202, faultstring: SOAP Request enthält Fehler 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.	

[<=]

4.3 Schnittstelle I_Directory_Application_Maintenance

Die Schnittstelle ermöglicht die Administration der Fachdaten.

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

TIP1-A_5583 - VZD, Schnittstelle I_Directory_Application_Maintenance
Der VZD MUSS für FADs I_Directory_Maintenance gemäß Tabelle Tab_VZD_Schnittstelle_I_Directory_Application_Maintenance anbieten.

Tabelle 10: Tab_VZD_Schnittstelle_I_Directory_Application_Maintenance

Name	I_Directory_Application_Maintenance	
Version	wird im Produkttypsteckbrief des VZD definiert	
Operationen	Operation	Kurzbeschreibung
	add_Directory_FA-Attributes	Erzeugung eines Fachdaten-Eintrags
	delete_Directory_FA-Attributes	Löschen von einzelnen oder allen zu einem FAD gehörenden Fachdaten eines Eintrags.
	modify_Directory_FA-Attributes	Ändern fachspezifischer Attribute

[<=]

ENTWURF

TIP1-A_5584 - VZD, Änderung nur durch registrierte FAD
Der Anbieter des VZD MUSS sicherstellen, dass Fachdaten eines Dienstes nur durch einen beim VZD für diesen Dienst registrierten Fachdienst erzeugt, gelöscht und geändert werden können.
[<=]

TIP1-A_5585 - VZD, I_Directory_Application_Maintenance, TLS-gesicherte Verbindung
Der VZD MUSS die Schnittstelle I_Directory_Application_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_5586 - VZD, I_Directory_Application_Maintenance, Webservice und LDAPv3
Der VZD MUSS die Schnittstelle I_Directory_Application_Maintenance als Webservice (SOAP über HTTPS) und als LDPv3 über LDAPS implementieren. Der Webservice wird durch die Dokumente DirectoryApplicationMaintenance.wsdl und DirectoryApplicationMaintenance.xsd definiert. Die LDAPv3-Attribute sind in dem Informationsmodell Abb_VZD_logisches_Datenmodell beschrieben.
[<=]

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 - FAD, I_Directory_Application_Maintenance, Nutzung LDAP v3 oder Webservice
Ein FAD, der Fachdaten im VZD verwalten will, MUSS entweder die Webservice- oder die LDAPv3-Schnittstelle nutzen.
[<=]

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.
[<=]

4.3.1 Operation add_Directory_FA-Attributes

Diese Operation legt einen neuen Fachdatensatz an oder überschreibt einen bestehenden fachdienstspezifischen Datensatz.

Voraussetzung: Die Fachdaten müssen einem Basisdateneintrag zuordenbar sein.

ENTWURF

4.3.1.1 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 11: 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.
[<=]

4.3.1.2 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 12: 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

ENTWURF

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

[<=]

TIP1-A_5592-01~~TIP1-A_5592~~ - 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 13: 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	version

[<=]

4.3.1.3 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.
[<=]

ENTWURF

4.3.1.4 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 14: 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.	

[<=]

4.3.2 Operation delete_Directory_FA-Attributes

Diese Operation löscht einen Fachdatensatz.

4.3.2.1 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:

ENTWURF

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.
[<=]

4.3.2.2 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 15: 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	Es werden die protokollspezifischen Fehlermeldungen verwendet (TCP, HTTP, TLS). Fehler bei der Verarbeitung des SOAP Requests werden als gematik SOAP-Fault versendet: faultcode 4321, faultstring: Operation fehlerhaft ausgeführt, Fachdaten konnten nicht gelöscht werden (Fehler im Verzeichnisdienst) faultcode 4312, faultstring: Basisdaten konnten nicht gefunden werden faultcode 4202, faultstring: SOAP Request enthält Fehler	

[<=]

ENTWURF

4.3.2.3 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.
[<=]

4.3.2.4 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 16: 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.	

ENTWURF

Fehlerfälle	Zur Behandlung auftretender Fehlerfälle werden Fehlermeldungen gemäß [RFC4511]#Appendix A verwendet.

[<=]

4.3.3 Operation modify_Directory_FA-Attributes

Diese Operation überschreibt einen Fachdatensatz.

4.3.3.1 Umsetzung SOAP

TIP1-A_5599 - 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.

Tabelle 17: 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.**[<=]**

4.3.3.2 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 18: Tab_TUC_VZD_0010

Name	modify_Directory_FA-Attributes
Beschreibung	Mit dieser Operation werden Fachdaten geändert.
Vorbedingungen	Keine.
Eingangsdaten	SOAP-Request „modifyDirectoryFAAttributes"

ENTWURF

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: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_5601-01~~TIP1-A_5601~~ - 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 19: 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	version

[<=]

4.3.3.3 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:

ENTWURF

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.
[<=]

4.3.3.4 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 20: 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.	

[<=]

ENTWURF

4.4 Prozessschnittstelle P_Directory_Application_Registration (Provided)

TIP1-A_5604 - VZD, Registrierung FADs
Der Anbieter des VZD MUSS einen Registrierungsprozess für FAD implementieren. Der Anbieter des VZD MUSS dazu überprüfen:

- Gültigkeit des TLS-Client-Zertifikat des FADs C.FD.TLS-C (Prüfschritte wie in TUC_PKI_018 und mit admission gemäß vom GTI vorgegebener OID-Liste),
- Name der Fachanwendung (z.B. KOM-LE),
- Name des Fachdienstbetreibers.

Der VZD-Anbieter dokumentiert den Prozess und legt ihn dem GTI zur Freigabe vor.
Der Anbieter des VZD informiert alle FAD-Anbieter darüber, wie der Prozess genutzt wird.
[<=]

TIP1-A_5605 - VZD, De-Registrierung FADs
Der Anbieter des VZD MUSS einen Deregistrierungsprozess für FAD implementieren.
Der VZD MUSS alle verbliebenen Fachdaten eines deregistrierten FAD löschen.
Der VZD-Anbieter dokumentiert den Prozess und legt ihn dem GTI zur Freigabe vor.
Der Anbieter des VZD informiert alle FAD-Anbieter wie der Prozess genutzt wird.
[<=]

4.5 Prozessschnittstelle P_Directory_Maintenance (Provided)

TIP1-A_5606 - VZD, Mandat zur Löschung von Einträgen.
Der Anbieter des VZD MUSS einen Prozess implementieren, der es LE ermöglicht ihren Eintrag im VZD ohne zugehörige Smartcard zu löschen.
Der Anbieter des VZD MUSS vom LE einen Nachweis fordern und prüfen, dass die zu löschenden Daten dem LE gehören. Erst nach positivem Ergebnis der Prüfung darf gelöscht werden.
Der VZD-Anbieter dokumentiert den Prozess und legt ihn dem GTI zur Freigabe vor.
[<=]

4.6 Schnittstelle I_Directory_Administration

Der Verzeichnisdienst (VZD) stellt ein Verzeichnis von Leistungserbringern und Organisationen/Institutionen mit den definierten Attributen für die Anwendungen der TI bereit. Zum Füllen und Administrieren dieser Daten durch die Kartenherausgeber wird die Schnittstelle I_Directory_Administration definiert.

Über diese Schnittstelle können Verzeichniseinträge inklusive Untereinträge für Zertifikate erzeugt, aktualisiert und gelöscht werden. Die Administration von Fachdaten erfolgt über die Schnittstelle I_Directory_Application_Maintenance und wird durch die Fachanwendungen durchgeführt. Operation getDirectoryEntries ermöglicht in der Schnittstelle I_Directory_Administration das Lesen eines gesamten Verzeichniseintrags inklusive Zertifikaten und Fachdaten.

Als Clients dieser Schnittstelle sind nur Systeme der TI-Kartenherausgeber und von ihnen berechtigte Organisationen (z.B. TSPs) zulässig. Sie dürfen alle Operationen zur Administration der Verzeichniseinträge nutzen.

ENTWURF

Das AccessToken enthält im "sub" claim den Identifier des Clients, der auf die Einträge zugreift. Dieser Identifier wird im Log abgelegt, welcher die Zugriffe über diese Schnittstelle protokolliert.

4.6.1 Operationen der Schnittstelle I_ Directory_Administration

Die – über diese REST Schnittstelle administrierten – Ressourcen werden entsprechend dem logischen Datenmodell des VZD (siehe Abb_VZD_logisches_Datenmodell) in DirectoryAdministration.yaml definiert.

A_18371 - VZD, Schnittstelle I_Directory_Administration
Der VZD MUSS die Schnittstelle I_Directory_Administration gemäß Tabelle Tab_VZD_Schnittstelle_I_Directory_Administration im Internet anbieten.

Tabelle 21: Tab_VZD_Schnittstelle_I_Directory_Administration

Name	**I_Directory_Administration**	
Version	wird im Produkttypsteckbrief des VZD definiert	
Operationen	Resource: DirectoryEntry	
	Name	Kurzbeschreibung
	POST	Hinzufügen eines Verzeichniseintrages inklusive dazugehörendem Zertifikat.
	GET	Abfrage aller Daten von Verzeichniseinträgen.
	PUT	Änderung eines Basisdaten-Verzeichniseintrages.
	DELETE	Löschung eines Verzeichniseintrages (kompletter Datensatz inklusive aller Zertifikate und Fachdaten).
	Resource: Certificate	
	Name	Kurzbeschreibung
	POST	Hinzufügen eines Zertifikatseintrags zu einem Verzeichniseintrag.
	GET	Abfrage von Zertifikatseinträgen.
	PUT	Änderung eines Zertifikatseintrags.
	DELETE	Löschung eines Zertifikatseintrags.

[<=]

A_18373 - VZD, Schnittstelle I_Directory_Administration
Der VZD MUSS die Schnittstelle I_Directory_Administration als REST-Webservice über HTTPS implementieren. Der Webservice wird durch das Dokument DirectoryAdministration.yaml definiert.
[<=]

ENTWURF

A_18408 - VZD, I_Directory_Administration, Registrierung
Der VZD-Anbieter MUSS für Clients der Schnittstelle I_Directory_Administration einen Registrierungsprozess bereitstellen. Während der Registrierung muss die Berechtigung des Antragstellers (Clients) zur Nutzung von Schnittstelle I_Directory_Administration durch den VZD-Anbieter geprüft und durch die gematik bestätigt werden. Nach erfolgreicher Registrierung MÜSSEN dem Antragsteller alle nötigen Daten - inklusive OAuth Client Credentials, CA-Zertifikat (welches zur Prüfung des Serverzertifikats durch den Client benötigt wird), VZD-Serverzertifikat - zur Nutzung der Schnittstelle bereitgestellt werden.
Der VZD-Anbieter MUSS die erfolgreich registrierten Clients immer mit aktuellen Zertifikaten versorgen.
[<=]

A_18470 - VZD, I_Directory_Administration, Client Secret Qualität
Der VZD-Anbieter MUSS bei der Erzeugung der OAuth client_secret‘s 128 Bit Zufall aus einer Zufallsquelle gemäß GS-A_4367 [gemSpec_Krypt] verwenden.
[<=]

A_18409 - VZD, I_Directory_Administration, Sperrung OAuth Client Credentials
Der VZD-Anbieter MUSS – für die gematik und den Client-Betreiber selbst - einen Service zur Sperrung der OAuth Client Credentials anbieten.
[<=]

A_18372 - VZD, I_Directory_Administration, TLS-gesicherte Verbindung
Der VZD MUSS die Schnittstelle I_Directory_Administration durch Verwendung von TLS mit serverseitiger Authentisierung sichern.
Der VZD MUSS für diese TLS-Verbindungen öffentliche Zertifikate nutzen (keine TI-Zertifikate).
Der VZD MUSS sich mit der Server-Identität von Schnittstelle I_Directory_Administration authentisieren.
[<=]

Die Prüfung der öffentliche TLS-Server Zertifikate muss gemäß GS-A_5581 [gemSpec_Krypt] erfolgen. Dabei müssen in (1) von GS-A_5581 statt der "Komponenten-CA-Zertifikate der TI" die CA-Zertifikate der Schnittstelle I_Directory_Administration genutzt werden.

A_18374 - VZD, I_Directory_Administration, Redirect
Der VZD MUSS für die Schnittstelle I_Directory_Administration Anfragen der Clients – welche kein AccessToken entsprechend [RFC 6750] enthalten – durch ein Redirect zu dem OAuth2-Authentifizierungsdienst weiterleiten. **[<=]**

A_18375 - VZD, I_Directory_Administration, OAuth2 Dienst
Der VZD MUSS einen OAuth2-Dienst bereitstellen. Dieser Dienst MUSS die Clients der Schnittstelle I_Directory_Administration anhand ihrer Client Credentials authentisieren und ihnen ein AccessToken entsprechend [RFC 6750] ausstellen. Das AccessToken muss im "sub" claim den Identifier des Clients enthalten. Die Anfrage des Clients MUSS nach erfolgreicher Authentisierung durch ein Redirect wieder zur VZD I_Directory_Administration Schnittstelle weitergeleitet werden.
[<=]

A_18376 - VZD, I_Directory_Administration, Prüfung AccessToken
Der VZD MUSS das vom Client übergebene AccessToken auf Gültigkeit für Schnittstelle I_Directory_Administration prüfen. Bei negativem Ergebnis muss die Operation mit HTTP Fehler 401 Unauthorized abgebrochen werden.
[<=]

A_18471-01~~A_18471~~ - VZD, I_Directory_Administration, Datenquelle
Der VZD MUSS bei den Operationen ~~createDirectoryEntry~~ add_Directory_Entry und ~~updateBaseDirectoryEntry~~modify_Directory_Entry das LDAP-Directory-Attribut

ENTWURF

dataFromAuthority auf den Wert TRUE setzen und bei allen anderen Operationen unverändert belassen.
[<=]

A_18735 - VZD, Disable I_Directory_Maintenance, wenn dataFromAuthority TRUE
Der VZD DARF Änderungen an VZD-Einträgen über die Schnittstelle I_Directory_Maintenance NICHT zulassen, wenn an dem betroffenen VZD-Eintrag das Attribut dataFromAuthority auf TRUE gesetzt ist.
[<=]

A_18472-01~~A_18472~~ - VZD, I_Directory_Administration, Doubletten
Der VZD MUSS bei den Operationen ~~createDirectoryEntry~~ add_Directory_Entry und ~~updateBaseDirectoryEntry~~ modify_Directory_Entry prüfen, ob die Operation eine Doublette im LDAP-Verzeichnis erzeugt und in diesem Fall die Operation mit HTTP-Fehlercode "400 Bad Request" ablehnen. Zur Prüfung auf eine potentielle Dublette MUSS der VZD alle LDAP-Directory-Attribute des zu erzeugenden Basisdatensatzes (Verzeichnisdienst_Eintrag ohne Certificate und Fachdaten) jedoch ohne den Distinguished Name heranziehen.
[<=]

A_18602 - 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) ablehnen.**[<=]**

4.6.1.1 DirectoryEntry Administration

Die Pflege der Basiseinträge (Verzeichnisdienst_Eintrag) erfolgt mit den im Folgenden beschriebenen Operationen.

4.6.1.1.1 POST

Diese Operation legt einen neuen Eintrag im LDAP-Verzeichnis an.

A_18448 - VZD, I_Directory_Administration, add_Directory_Entry
Der VZD MUSS Operation „add_Directory_Entry" gemäß Tabelle Tab_VZD „add_Directory_Entry" umsetzen.

Tabelle 22: Tab_VZD „add_Directory_Entry"

Name	add_Directory_Entry	
Beschreibung	Diese Operation ermöglicht die Erzeugung eines neuen Eintrags im LDAP-Verzeichnis.	
Eingangsdaten	REST-Request POST /DirectoryEntries operationId: add_Directory_Entry (siehe DirectoryAdministration.yaml)	
	Parameter	Beschreibung

ENTWURF

	Verzeichnisdienst_Eintrag	Siehe Abb_VZD_logisches_Datenmodell und Tab_VZD_Datenbeschreibung. Der Distinguished Name wird vom VZD belegt. Der VZD übernimmt entsprechend Tab_VZD_Datenbeschreibung eine Reihe von Attributen aus dem Zertifikat.
	Certificate	Kann optional belegt werden. Siehe Abb_VZD_logisches_Datenmodell und Tab_VZD_Datenbeschreibung. Der Distinguished Name wird vom VZD belegt. Der VZD übernimmt entsprechend Tab_VZD_Datenbeschreibung eine Reihe von Attributen aus dem Zertifikat.
Komponenten	Nutzer der Schnittstelle, Verzeichnisdienst	
Ausgangsdaten	REST-Response mit dem Distinguished Name (dn) von dem Verzeichnisdienst_Eintrag.	
Ablauf	Der VZD übernimmt entsprechend Tab_VZD_Datenbeschreibung Attribute aus dem Zertifikat und trägt die übergebenen Parameter in den Verzeichniseintrag ein. Der VZD setzt das LDAP-Directory-Attribut dataFromAuthority auf den Wert TRUE.	
Fehlerfälle	Es werden die protokollspezifischen Fehlermeldungen verwendet (TCP, HTTP, TLS) und in DirectoryAdministration.yaml mit spezifischen Fehlerbeschreibungen ergänzt.	

[<=]

4.6.1.1.2 GET

Diese Operation liest Verzeichniseinträge aus dem LDAP-Verzeichnis.

A_18449 - VZD, I_Directory_Administration, read_Directory_Entry
Der VZD MUSS Operation „read_Directory_Entry" gemäß Tabelle Tab_VZD „read_Directory_Entry" umsetzen.

Tabelle 23: Tab_VZD „read_Directory_Entry"

Name	read_Directory_Entry	
Beschreibung	Diese Operation ermöglicht die Suche und Lesen von Verzeichniseinträgen im LDAP-Verzeichnis. Diese Operation liefert (im Gegensatz zu TIP1-A_5547/search_Directory) auch Einträge, die ohne gültige Zertifikate sind.	
Eingangsdaten	REST-Request GET /DirectoryEntries operationId: read_Directory_Entry (siehe DirectoryAdministration.yaml)	
	Parameter	Beschreibung

ENTWURF

	Parameter zur Selektion der Verzeichniseinträge	Alle im Datenmodell aufgeführten Felder des Basiseintrags - insbesondere auch dataFromAuthority - können zur Suche genutzt werden. Die angegebenen Parameter werden zur Suche mit einem logischen UND verknüpft.
Komponenten	Nutzer der Schnittstelle, Verzeichnisdienst	
Ausgangsdaten	REST-Response mit allen zu den Filterparametern passenden Verzeichniseinträgen. Die Verzeichniseinträge werden inklusive Zertifikatseinträgen und Fachdaten geliefert.	
Ablauf	Der VZD sucht im LDAP-Verzeichnis die zu den Suchparametern passenden Verzeichniseinträge. Bei mehr als 100 gefundenen Einträgen wird der Request mit Fehler „400 Bad Request" beantwortet.	
Fehlerfälle	Es werden die protokollspezifischen Fehlermeldungen verwendet (TCP, HTTP, TLS) und in DirectoryAdministration.yaml mit spezifischen Fehlerbeschreibungen ergänzt.	

[<=]

4.6.1.1.3 PUT

Diese Operation aktualisiert den Verzeichniseintrag (ohne Zertifikate und Fachdaten) mit den übergebenen Daten im LDAP-Verzeichnis.

A_18450 - VZD, I_Directory_Administration, modify_Directory_Entry
Der VZD MUSS Operation „modify_Directory_Entry" gemäß Tabelle Tab_VZD „modify_Directory_Entry" umsetzen.

Tabelle 24: Tab_VZD „modify_Directory_Entry"

Name	modify_Directory_Entry	
Beschreibung	Diese Operation ermöglicht die Aktualisierung von Verzeichniseinträgen im LDAP-Verzeichnis.	
Eingangsdaten	REST-Request PUT /DirectoryEntries/{uid}/baseDirectoryEntries operationId: modify_Directory_Entry (siehe DirectoryAdministration.yaml)	
	Parameter	Beschreibung
	uid	Die „uid" identifiziert den Verzeichnisdienst_Eintrag (Abb_VZD_logisches_Datenmodell) welcher aktualisiert wird.
	displayName	Kann optional angegeben werden und überschreibt den Wert im selektierten Verzeichniseintrag.

ENTWURF

	otherName	Kann optional angegeben werden und überschreibt den Wert im selektierten Verzeichniseintrag.
	streetAddress	Kann optional angegeben werden und überschreibt den Wert im selektierten Verzeichniseintrag.
	postalCode	Kann optional angegeben werden und überschreibt den Wert im selektierten Verzeichniseintrag.
	localityName	Kann optional angegeben werden und überschreibt den Wert im selektierten Verzeichniseintrag.
	stateOrProvienceName	Kann optional angegeben werden und überschreibt den Wert im selektierten Verzeichniseintrag.
	title	Kann optional angegeben werden und überschreibt den Wert im selektierten Verzeichniseintrag.
	organization	Kann optional angegeben werden und überschreibt den Wert im selektierten Verzeichniseintrag.
	specialization	Kann optional angegeben werden und überschreibt den Wert im selektierten Verzeichniseintrag.
	domainID	Kann optional angegeben werden und überschreibt den Wert im selektierten Verzeichniseintrag.
Komponenten	Nutzer der Schnittstelle, Verzeichnisdienst	
Ausgangsdaten	REST-Response mit dem Distinguished Name (dn) von dem aktualisierten Verzeichnisdienst_Eintrag.	
Ablauf	Der VZD aktualisiert im LDAP-Verzeichnis den über Parameter „uid" identifizierten Verzeichniseintrag mit den übergebenen Parametern. Der VZD setzt das LDAP-Directory-Attribut dataFromAuthority auf den Wert TRUE.	
Fehlerfälle	Es werden die protokollspezifischen Fehlermeldungen verwendet (TCP, HTTP, TLS) und in DirectoryAdministration.yaml mit spezifischen Fehlerbeschreibungen ergänzt.	

ENTWURF

[<=]

4.6.1.1.4 DELETE

Diese Operation löscht den gesamten Verzeichniseintrag (inklusive Zertifikaten und Fachdaten).

A_18451 - VZD, I_Directory_Administration, delete_Directory_Entry
Der VZD MUSS Operation „delete_Directory_Entry" gemäß Tabelle Tab_VZD „delete_Directory_Entry" umsetzen.

Tabelle 25: Tab_VZD „delete_Directory_Entry"

Name	delete_Directory_Entry	
Beschreibung	Diese Operation ermöglicht die Löschung von kompletten Verzeichniseinträgen (inklusive Zertifikaten und Fachdaten) im LDAP-Verzeichnis.	
Eingangsdaten	REST-Request DELETE /DirectoryEntries/{uid} operationId: delete_Directory_Entry (siehe DirectoryAdministration.yaml)	
	Parameter	Beschreibung
	uid	Die „uid" identifiziert den Verzeichnisdienst_Eintrag (Abb_VZD_logisches_Datenmodell) welcher inklusive der dazu gehörenden Zertifikate und Fachdaten gelöscht wird.
Komponenten	Nutzer der Schnittstelle, Verzeichnisdienst	
Ausgangsdaten	REST-Response.	
Ablauf	Der VZD löscht im LDAP-Verzeichnis den über Parameter „uid" identifizierten Verzeichniseintrag inklusive der dazu gehörenden Zertifikate und Fachdaten.	
Fehlerfälle	Es werden die protokollspezifischen Fehlermeldungen verwendet (TCP, HTTP, TLS) und in DirectoryAdministration.yaml mit spezifischen Fehlerbeschreibungen ergänzt.	

[<=]

4.6.1.2 Certificate Administration

Die Pflege der Zertifikatseinträge (Certificate in Abb_VZD_logisches_Datenmodell) erfolgt mit den im Folgenden beschriebenen Operationen.

4.6.1.2.1 POST

Diese Operation fügt einem existierenden Basisdatensatz einen Zertifikatseintrag im LDAP-Verzeichnis an.

A_18452 - VZD, I_Directory_Administration, add_Directory_Entry_Certificate
Der VZD MUSS Operation „add_Directory_Entry_Certificate" gemäß Tabelle Tab_VZD „add_Directory_Entry_Certificate" umsetzen.

ENTWURF

Tabelle 26: Tab_VZD „add_Directory_Entry_Certificate"

Name	add_Directory_Entry_Certificate	
Beschreibung	Diese Operation fügt einem existierenden Basisdatensatz einen Zertifikatseintrag im LDAP-Verzeichnis an.	
Eingangsdaten	REST-Request POST /DirectoryEntries/{uid}/Certificates operationId: add_Directory_Entry_Certificate (siehe DirectoryAdministration.yaml)	
	Parameter	Beschreibung
	uid	Die „uid" identifiziert den Verzeichnisdienst_Eintrag (Abb_VZD_logisches_Datenmodell) an welchen der Zertifikatseintrag angehangen wird.
	userCertificate	Muss angegeben werden und enthält das Zertifikat.
	usage	Kann optional belegt werden.
	description	Kann optional belegt werden.
Komponenten	Nutzer der Schnittstelle, Verzeichnisdienst	
Ausgangsdaten	REST-Response mit dem Distinguished Name (dn) von dem erzeugten Certificate-Eintrag.	
Ablauf	Der VZD übernimmt entsprechend Tab_VZD_Datenbeschreibung Attribute aus dem Zertifikat und trägt die übergebenen Parameter in den Zertifikatseintrag ein. Der Distinguished Name (dn) von dem erzeugten Certificate wird vom Verzeichnisdienst gefüllt und über dn.uid mit dem übergeordneten Verzeichnisdienst_Eintrag verknüpft.	
Fehlerfälle	Es werden die protokollspezifischen Fehlermeldungen verwendet (TCP, HTTP, TLS) und in DirectoryAdministration.yaml mit spezifischen Fehlerbeschreibungen ergänzt.	

[<=]

4.6.1.2.2 GET

Diese Operation liest Zertifikatseinträge aus dem LDAP-Verzeichnis.

A_18453 - VZD, I_Directory_Administration, read_Directory_Certificates
Der VZD MUSS Operation „read_Directory_Certificates" gemäß Tabelle Tab_VZD „read_Directory_Certificates" umsetzen.

Tabelle 27: Tab_VZD „read_Directory_Certificates"

Name	read_Directory_Certificates
Beschreibung	Diese Operation ermöglicht die Suche und das Lesen von Zertifikatseinträgen (Certificate in Abb_VZD_logisches_Datenmodell) im LDAP-Verzeichnis.

ENTWURF

Eingangsdaten	REST-Request GET /DirectoryEntries/Certificates operationId: read_Directory_Certificates (siehe DirectoryAdministration.yaml) Mindestens ein Filterparameter muss angegeben werden.	
	Parameter	Beschreibung
	uid	Optionaler Parameter. Die „uid" identifiziert einen Verzeichnisdienst_Eintrag (Abb_VZD_logisches_Datenmodell). Dieser Parameter selektiert alle Zertifikatseinträge dieses Verzeichnisdiensteintrags.
	certificateEntryID	Optionaler Parameter. Dieser Parameter identifiziert einen Zertifikatseintrag (Abb_VZD_logisches_Datenmodell dn.cn von Certificate).
	telematikID	Optionaler Parameter. Dieser Parameter selektiert alle Zertifikatseinträge mit dieser TeleamtikID.
Komponenten	Nutzer der Schnittstelle, Verzeichnisdienst	
Ausgangsdaten	REST-Response mit allen zu den Filter Parametern passenden Zertifikatseinträgen.	
Ablauf	Der VZD sucht im LDAP Verzeichnis die zu den Such-Parametern passenden Zertifikatseinträge. Bei mehr als 100 gefundenen Einträgen wird der Request mit Fehler „400 Bad Request" beantwortet.	
Fehlerfälle	Es werden die protokollspezifischen Fehlermeldungen verwendet (TCP, HTTP, TLS) und in DirectoryAdministration.yaml mit spezifischen Fehlerbeschreibungen ergänzt.	

[<=]

4.6.1.2.3 PUT

Diese Operation aktualisiert den Zertifikatseintrag mit den übergebenen Daten im LDAP-Verzeichnis.

A_18454 - VZD, I_Directory_Administration, modify_Directory_Entry_Certificate
Der VZD MUSS Operation „modify_Directory_Entry_Certificate" gemäß Tabelle Tab_VZD „modify_Directory_Entry" umsetzen.

ENTWURF

922 **Tabelle 28: Tab_VZD „modify_Directory_Entry_Certificate"**

Name	modify_Directory_Entry_Certificate	
Beschreibung	Diese Operation ermöglicht die Aktualisierung von Zertifikatseinträgen (Certificate in Abb_VZD_logisches_Datenmodell) im LDAP-Verzeichnis. Modifiziert werden können die Attribute "usage" und "description".	
Eingangsdaten	REST-Request PUT /DirectoryEntries/{uid}/Certificates/{certificateEntryID} operationId: modify_Directory_Entry_Certificate (siehe DirectoryAdministration.yaml)	
	Parameter	Beschreibung
	uid	Pflichtparameter. Die „uid" identifiziert den Verzeichnisdienst_Eintrag (Abb_VZD_logisches_Datenmodell) zu dem der Zertifikatseintrag gehört.
	certificateEntryID	Pflichtparameter. Dieser Parameter identifiziert einen Zertifikatseintrag (Abb_VZD_logisches_Datenmodell dn.cn von Certificate).
	usage	Kann optional angegeben werden und überschreibt den Wert im selektierten Verzeichniseintrag. Zum Aktualisieren eines Werts muss mit read_Directory_Certificates der aktuelle Inhalt des Attributs gelesen werden. Der Client aktualisiert das Attribut dann durch Hinzufügen, Ersetzen oder Löschen von Werten. modify_Directory_Entry_Certificate überschreibt dann das Attribut im Verzeichnisdienst mit dem übergebenen Wert.
	description	Kann optional angegeben werden und überschreibt den Wert im selektierten Verzeichniseintrag. Bei einem nicht angegebenen Wert wird der Wert im selektierten Verzeichniseintrag gelöscht.
	userCertificate	Pflichtparameter. Muss unverändert gegenüber dem Zertifikat im VZD sein (kann nicht modifiziert werden).
Komponenten	Nutzer der Schnittstelle, Verzeichnisdienst	
Ausgangsdaten	REST-Response mit dem Distinguished Name (dn) von dem aktualisierten Zertifikatseintrag (Certificate in Abb_VZD_logisches_Datenmodell).	

ENTWURF

Ablauf	Der VZD aktualisiert im LDAP Verzeichnis den über Parameter „certificateEntryID" identifizierten Zertifikatseintrag mit den übergebenen Parametern. Falls das übergebene userCertificate nicht mit dem Wert im LDAP-Verzeichnis übereinstimmt wird mit Fehler 400 Bad Request abgebrochen.
Fehlerfälle	Es werden die protokollspezifischen Fehlermeldungen verwendet (TCP, HTTP, TLS) und in DirectoryAdministration.yaml mit spezifischen Fehlerbeschreibungen ergänzt.

[<=]

4.6.1.2.4 DELETE

Diese Operation löscht einen Zertifikatseintrag.

A_18455 - VZD, I_Directory_Administration, delete_Directory_Entry_Certificate
Der VZD MUSS Operation „delete_Directory_Entry_Certificate" gemäß Tabelle Tab_VZD „delete_Directory_Entry_Certificate" umsetzen.

Tabelle 29: Tab_VZD „delete_Directory_Entry_Certificate"

<table>
<tr><td>Name</td><td colspan="2">delete_Directory_Entry_Certificate</td></tr>
<tr><td>Beschreibung</td><td colspan="2">Diese Operation ermöglicht die Löschung eines Zertifikatsseintrags im LDAP-Verzeichnis.</td></tr>
<tr><td>Eingangsdaten</td><td colspan="2">REST-Request
DELETE /DirectoryEntries/{uid}/Certificates/{certificateEntryID}

operationId: delete_Directory_Entry_Certificate (siehe DirectoryAdministration.yaml)</td></tr>
<tr><td></td><td>Parameter</td><td>Beschreibung</td></tr>
<tr><td></td><td>uid</td><td>Pflichtparameter.
Die „uid" identifiziert den Verzeichnisdienst_Eintrag (Abb_VZD_logisches_Datenmodell) zu dem der Zertifikatseintrag gehört.</td></tr>
<tr><td></td><td>certificateEntryID</td><td>Pflichtparameter.
Dieser Parameter identifiziert einen Zertifikatseintrag (Abb_VZD_logisches_Datenmodell dn.cn von Certificate).</td></tr>
<tr><td>Komponenten</td><td colspan="2">Nutzer der Schnittstelle, Verzeichnisdienst</td></tr>
<tr><td>Ausgangsdaten</td><td colspan="2">REST-Response.</td></tr>
<tr><td>Ablauf</td><td colspan="2">Der VZD löscht im LDAP-Verzeichnis den über die Parameter „uid" und „certificateEntryID" identifizierten Zertifikatseintrag.</td></tr>
<tr><td>Fehlerfälle</td><td colspan="2">Es werden die protokollspezifischen Fehlermeldungen verwendet (TCP, HTTP, TLS) und in DirectoryAdministration.yaml mit spezifischen Fehlerbeschreibungen ergänzt.</td></tr>
</table>

ENTWURF

[<=]

4.6.2 Nutzung der Schnittstelle I_Directory_Administration

Der Client der Schnittstelle I_Directory_Administration muss eine TLS-Verbindung mit serverseitiger Authentisierung nutzen. Dabei muss er das Serverzertifikat des VZD prüfen. Bei negativem Ergebnis muss der Verbindungsaufbau abgebrochen werden.

Mit Hilfe der Operationen der Schnittstelle muss der Client die Verzeichniseinträge eintragen und pflegen.

Beispielablauf:

Falls die „uid" des Verzeichniseintrags nicht bekannt ist erfolgt die Suche nach einem vorhandenen Verzeichniseintrag mit der telematikID (operationId read_Directory_Certificates mit Parameter telematikID)

a. Falls ein Eintrag gefunden wurde:

1. Lesen des Basis-Verzeichniseintrags (operationId read_Directory_Entry mit Parameter „uid" aus dem read_Directory_Certificates Response)

2. Aktualisieren des Verzeichniseintrags und (je nach Bedarf) der dazugehörigen Zertifikatseinträge (operationId's: modify_Directory_Entry, delete_Directory_Entry, modify_Directory_Entry_Certificate, delete_Directory_Entry_Certificate)

b. Falls kein Eintrag gefunden wurde:

1. Erzeugen des Verzeichniseintrags und (je nach Bedarf) anhängen zusätzlicher Zertifikatseinträge (operationId's: add_Directory_Entry, add_Directory_Entry_Certificate). Der erste Zertifikatseintrag wird mit Operation add_Directory_Entry erzeugt da jeder Verzeichniseintrag mindestens einen Zertifikatseintrag enthalten muss. Zusätzliche Zertifikatseinträge können mit Operation add_Directory_Entry_Certificate hinzugefügt werden.

4.7 ~~Datenmodell~~Schnittstelle I_Directory_Search

Der Verzeichnisdienst (VZD) stellt ein Verzeichnis von Leistungserbringern und Organisationen/Institutionen mit den definierten Attributen für die Anwendungen der TI bereit. Zur Nutzung dieser Daten wird die Schnittstelle I_Directory_Search definiert.

Über diese Schnittstelle können Verzeichniseinträge aus dem Verzeichnisdienst ausgelesen werden.

A_20062 - VZD, Schnittstelle I_Directory_Search, Verwaltung Resource Records FQDN

Der VZD MUSS im Namensraum Internet die Resource Records gemäß nachstehender Tabelle verwalten.

Tabelle 30: Tab_VZD_Schnittstelle_I_Directory_Search_FQDN

Resource Record Typ	Beschreibung

ENTWURF

FQDN	A Resource Records zur Namensauflösung von FQDN der VZD I_Directory_Search Schnittstelle mit dem FQDN directory.vzd.ti-dienste.de in IP-Adressen.

[<=]

4.7.1 Operationen der Schnittstelle I_ Directory_Search

Die – über diese REST Schnittstelle gelieferten – Ressourcen werden entsprechend dem logischen HL7 FHIR [HL7FHIR] Datenmodell in DirectorySearch.yaml definiert.

A_19505 - VZD, Schnittstelle I_Directory_Search
Der VZD MUSS die Schnittstelle I_Directory_Search gemäß Tabelle Tab_VZD_Schnittstelle_I_Directory_Search im Internet anbieten.

Tabelle 31: Tab_VZD_Schnittstelle_I_Directory_Search

Name	**I_Directory_Search**	
Version	wird im Produkttypsteckbrief des VZD definiert	
Operationen	Resource: DirectoryEntry	
	Name	**Kurzbeschreibung**
	GET	Abfrage aller Daten von Verzeichniseinträgen.

[<=]

A_19506 - VZD, Schnittstelle Search
Der VZD MUSS die Schnittstelle I_Directory_Search als REST-Webservice über HTTPS implementieren. Der Webservice wird durch das Dokument DirectorySearch.yaml definiert.
[<=]

A_19507 - VZD, I_Directory_Search, TLS-gesicherte Verbindung
Der VZD MUSS die Schnittstelle I_Directory_Search durch Verwendung von TLS mit serverseitiger Authentisierung sichern.
Der VZD MUSS für diese TLS-Verbindungen öffentliche Extended-Validation-X.509-Zertifikate nutzen (keine TI-Zertifikate).
Der VZD MUSS sich mit der Server-Identität von Schnittstelle I_Directory_Search authentisieren.
[<=]

Die Prüfung der öffentlichen TLS-Server-Zertifikate muss gemäß GS-A_5581 [gemSpec_Krypt] erfolgen. Dabei müssen in (1) von GS-A_5581 statt der "Komponenten-CA-Zertifikate der TI" die CA-Zertifikate der Schnittstelle I_Directory_Search genutzt werden.

A_20016 - VZD, I_Directory_Search, Registrierung beim IdP als Relying Party
Der Anbieter des VZD MUSS sich über einen organisatorischen Prozess beim IdentityProvider (IdP) der Telematikinfrastruktur als Relying Party registrieren und die

ENTWURF

Bereitstellung der folgenden Claims in für Nutzer ausgestellte ACCESS_TOKEN mit dem IdP vereinbaren:

- `professionOID`
- `acr`

damit der VZD die Fachlogik der Autorisierung auf diesen Attributen umsetzen kann.**[<=]**

A_19509 - VZD, I_Directory_Search, Authentifizierung erforderlich
Der VZD MUSS alle eingehenden HTTP-Requests mit dem HTTP-Fehlercode 401 und dem HTTP-Response-Header "`WWW-Authenticate: Bearer realm='vzd.telematik'`" abweisen, die kein IdentityToken als JSON-Web-Token-Format gemäß [JWT] im HTTP-Request-Header "Authorization" bereitstellen, damit ausschließlich Nutzer in der Rolle Versicherter Zugriff auf die I_Directory_Search HTTP-Schnittstelle des VZD erhalten. **[<=]**

A_19510 - VZD, I_Directory_Search, Authentifizierung abgelaufen
Der VZD MUSS alle eingehenden HTTP-Requests mit dem HTTP-Fehlercode 401 und dem HTTP-Response-Header "`WWW-Authenticate: Bearer realm='vzd.telematik', error='invalid_token'`"abweisen, die ein unsigniertes, ungültiges oder zeitlich abgelaufenes IdentityToken im HTTP-Request-Header "Authorization" bereitstellen, damit ausschließlich authentifizierte Nutzer Zugriff auf die I_Directory_Search HTTP-Schnittstelle des VZD erhalten.**[<=]**

A_19511 - VZD, I_Directory_Search, Authentifizierung Signaturprüfung
Der VZD MUSS die Signatur jedes im HTTP-Header "Authorization" eines eingehenden HTTP-Requests übergebenen JSON-Web-Tokens gemäß [JWS] prüfen und bei Ungültigkeit oder bei Signatur durch einen IdentityProvider, bei dem der VZD nicht als Relying Party registriert ist, den HTTP-Request mit dem HTTP-Fehlercode 401 abweisen.**[<=]**

A_19885 - VZD, I_Directory_Search, Authentifizierung Nutzerrolle
Der VZD MUSS die fachliche Rolle eines Nutzers in jedem Operationsaufruf anhand des Attributs professionOID im übergebenen IdP-Token im HTTP-Header "Authorization" feststellen und für die nachfolgende Rollenprüfung je Operationsaufruf verwenden.**[<=]**

A_19890 - VZD, I_Directory_Search, Rollenprüfung
Der VZD MUSS beim Aufruf der HTTP-GET-Operation auf den Endpunkt I_Directory_Search sicherstellen, dass ausschließlich Nutzer in der Rolle

- oid_versicherter

die Operation aufrufen dürfen.**[<=]**

A_19888 - VZD, I_Directory_Search, Authentifizierung Authentifizierungsstärke
Der VZD MUSS die Authentifizierungsstärke des übergebenen IdP-Token anhand des Attributs `acr` im übergebenen IdP-Token im HTTP-Header "Authorization" feststellen und einen anderen Wert als bzw. ein Authentifizierungsniveau unterhalb von "`http://eidas.europa.eu/LoA/low`" mit dem HTTP-Status-Code 401 ablehnen. **[<=]**

A_19889 - VZD, I_Directory_Search, Authentifizierung Registrierter Endpunkt
Der Anbieter des VZDs MUSS den Schnittstellenendpunkt I_Directory_Search beim Identity Provider registrieren.**[<=]**

ENTWURF

A_19732 - VZD, I_Directory_Search, Aufrufe pro Zeiteinheit
Der VZD MUSS die Anzahl der Operationen an der Schnittstelle I_Directory_Search pro Versicherten-Session und Minute auf einen - durch den Betreiber im Wertebereich 1 bis 15 - konfigurierbaren Wert beschränken. Der Defaultwert für diese Konfigurationsparameter MUSS 10 betragen. Wird diese Anzahl überschritten, MUSS ein HTTP-Response mit HTTP-Statuscode 429 entsprechend RFC6585 Kapitel 4 "429 Too Many Requests" an den Client zurückgegeben werden.
[<=]

4.7.1.1 GET

Diese Operation liest Verzeichniseinträge aus dem Verzeichnisdienst.

A_19512 - VZD, I_Directory_Search, search_Directory_Entry
Der VZD MUSS die Operation „search_Directory_Entry" gemäß Tabelle Tab_VZD „search_Directory_Entry" umsetzen.

Tabelle 32: Tab_VZD „search_Directory_Entry

Name	search_Directory_Entry	
Beschreibung	Diese Operation ermöglicht die Suche und das Lesen von Verzeichniseinträgen im LDAP-Verzeichnis.	
Eingangsdaten	REST-Request GET /v1.0/Organization operationId: search_Directory_Entry (siehe DirectorySearch.yaml)	
	Parameter	Beschreibung
	Parameter zur Selektion der Verzeichniseinträge	Alle im DirectorySearch.yaml aufgeführten Felder der GET-Operation können zur Suche genutzt werden. Die Suchparameter entsprechen den relevanten Parametern der FHIR-Spezifikation für die Resource Organization [HL7FHIR] und https://www.hl7.org/fhir/search.html. Die angegebenen Parameter werden zur Suche mit einem logischen UND verknüpft.
Komponenten	Nutzer der Schnittstelle, Verzeichnisdienst	
Ausgangsdaten	REST-Response mit allen zu den Suchparametern passenden Verzeichniseinträgen entsprechend DirectorySearch.yaml und [HL7FHIR] Resource Bundle.	
Ablauf	Der VZD sucht im LDAP-Verzeichnis die zu den Suchparametern passenden Verzeichniseinträge. Bei mehr als 100 gefundenen Einträgen wird der Request mit Fehler „400 Bad Request" beantwortet.	
Fehlerfälle	Es werden die protokollspezifischen Fehlermeldungen verwendet (TCP, HTTP, TLS) und in DirectorySearch.yaml mit spezifischen Fehlerbeschreibungen ergänzt.	

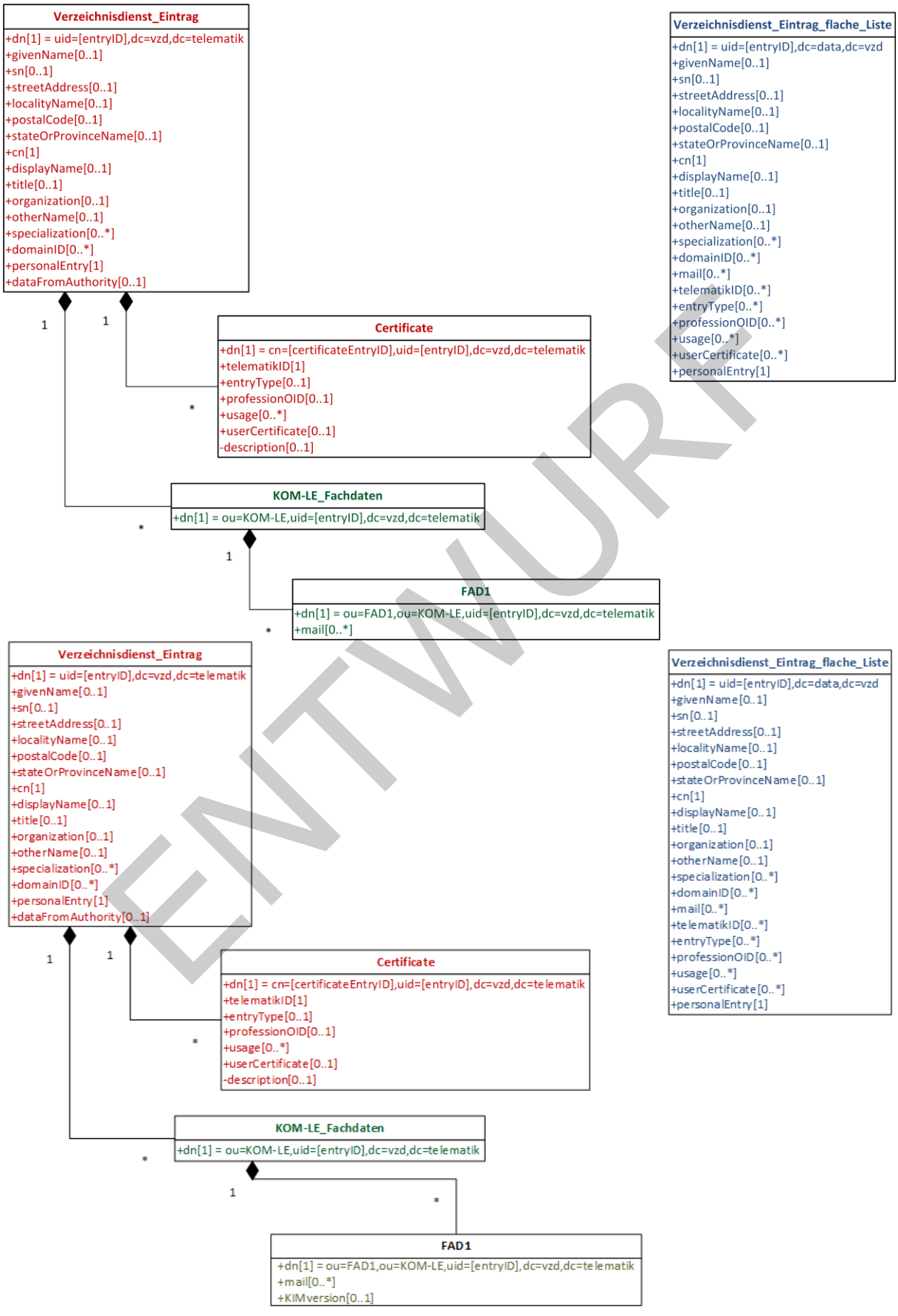
[<=]

ENTWURF

5 Datenmodell

TIP1-A_5607 - 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.

ENTWURF


Verzeichnisdienst_Eintrag
+dn[1] = uid=[entryID],dc=vzd,dc=telematik
+givenName[0..1]
+sn[0..1]
+streetAddress[0..1]
+localityName[0..1]
+postalCode[0..1]
+stateOrProvinceName[0..1]
+cn[1]
+displayName[0..1]
+title[0..1]
+organization[0..1]
+otherName[0..1]
+specialization[0..*]
+domainID[0..*]
+personalEntry[1]
+dataFromAuthority[0..1]
Verzeichnisdienst_Eintrag_flache_Liste
+dn[1] = uid=[entryID],dc=data,dc=vzd
+givenName[0..1]
+sn[0..1]
+streetAddress[0..1]
+localityName[0..1]
+postalCode[0..1]
+stateOrProvinceName[0..1]
+cn[1]
+displayName[0..1]
+title[0..1]
+organization[0..1]
+otherName[0..1]
+specialization[0..*]
+domainID[0..*]
+mail[0..*]
+telematikID[0..*]
+entryType[0..*]
+professionOID[0..*]
+usage[0..*]
+userCertificate[0..*]
+personalEntry[1]
Certificate
+dn[1] = cn=[certificateEntryID],uid=[entryID],dc=vzd,dc=telematik
+telematikID[1]
+entryType[0..1]
+professionOID[0..1]
+usage[0..*]
+userCertificate[0..1]
-description[0..1]
KOM-LE_Fachdaten
+dn[1] = ou=KOM-LE,uid=[entryID],dc=vzd,dc=telematik
FAD1
+dn[1] = ou=FAD1,ou=KOM-LE,uid=[entryID],dc=vzd,dc=telematik
+mail[0..*]
+KIMversion[0..1]
1
*

ENTWURF

1071 **Abbildung 2: Abb_VZD_logisches_Datenmodell**

1072 **Tabelle 33: Tab_VZD_Datenbeschreibung**

LDAP-Directory Attribut	Pflichtfeld?	Erläuterung
givenName	optional	HBA: Bezeichner: Vorname, obligatorisch, wird vom VZD aus dem Zertifikat übernommen SMC-B: nicht verwendet
sn	optional	HBA: Bezeichner: Name, obligatorisch, wird vom VZD aus dem Zertifikat übernommen SMC-B: nicht verwendet
cn	obligatorisch	HBA: Bezeichner: Vorname und Nachname SMC-B: Bezeichner: Name Wird vom VZD aus dem Zertifikatsattribut commonName übernommen. veraltet: Wird für die Suche nach Einträgen und die Anzeige von gefundenen Einträgen nicht benötigt (siehe displayName und organization)
displayName	optional	Bezeichner: Anzeigename, Name nach dem der Eintrag von Nutzern gesucht wird und unter dem gefundene Einträge angezeigt werden
streetAddress	optional	Bezeichner: Straße und Hausnummer
postalCode	optional	Bezeichner: Postleitzahl
localityName	optional	Bezeichner: Ort
stateOrProvinceName	optional	Bezeichner: Bundesland
title	optional	HBA: Bezeichner: Titel, optional SMC-B: nicht verwendet
organization	optional	HBA: Bezeichner: Name der Organisation, optional SMC-B: Alternativer Name nach dem der Eintrag von Nutzern gesucht wird und unter dem gefundene Einträge angezeigt werden

ENTWURF

otherName	optional	Bezeichner: Anderer Name Wird vom VZD aus dem Zertifikatsattribut otherName übernommen. veraltet: Wird für die Suche nach Einträgen und die Anzeige von gefundenen Einträgen nicht benötigt (siehe displayName und organization)
specialization	optional	HBA: Bezeichner: medizinisches Fachgebiet SMC-B: Bezeichner: Fachgebiet, optional kann mehrfach vorkommen (0..100)
domainID	optional	Bezeichner: domänenspezifisches Kennzeichen des Eintrags kann mehrfach vorkommen (0..100)
personalEntry	obligatorisch	wird vom VZD eingetragen Wert == TRUE, wenn alle Zertifikate den entryType 1 haben (Berufsgruppe), Wert == FALSE sonst
dataFromAuthority	optional	wird vom VZD eingetragen Wert == TRUE, wenn der Verzeichnisdienst_Eintrag von dem Kartenherausgeber geschrieben wurde, Wert == FALSE sonst
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
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.
telematikID	obligatorisch	Bezeichner: TelematikID Wird vom VZD anhand der im jeweiligen Zertifikat enthaltenen Telematik-ID (Feld registrationNumber der Extension Admission) übernommen.
professionOID	optional	Bezeichner: Profession OID 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)

ENTWURF

usage	optional	Bezeichner: Nutzungskennzeichnung kann pro Zertifikat mehrfach (0..100) vergeben werden vorgegebener Wertebereich [KOM-LE, ePA, eFA] Hinweis: wird aktuell für ePA und KOM-LE nicht verwendet.
description	optional	Bezeichner: Beschreibung Dieses Attribut ermöglicht das Zertifikat zu beschreiben, um die Administration des VZD-Eintrags zu vereinfachen. Hinweis: wird aktuell nicht verwendet
mail	optional	Bezeichner: KOM-LE E-Mail-Adresse kann mehrfach vorkommen (0..100)
version	optional	Bezeichner: Version Enthält die KOM-LE-Version von dem Client der angegebenen "mail" Adresse. Anhand dieser Version entscheidet der Versender einer Mail (bzw. das Clientmodul), in welchem Format die Mail an diesen Empfänger versandt wird. Wenn nicht angegeben, wird Version 1.0 angenommen.

[<=]

Die Abbildung Abb_VZD_logisches_Datenmodell stellt die Datenstruktur des Verzeichnisdienstes als UML-Klassendiagramm dar. Die Basisdaten sind rot, die Fachdaten grün und die als Ergebnis der LDAP-Suche in Form einer flachen Liste gefundenen Einträge sind blau dargestellt. Zu jedem Attribut ist die Kardinalität in eckigen Klammern angegeben.

Unter dem Begriff SMC-B sind alle Ausprägungen zusammengefasst (SMC-B ORG, SMC-B KTR). Wenn eine Differenzierung erforderlich ist, wird die spezifische Ausprägung der SMC-B explizit beschrieben.

In der folgenden Tabelle wird der Wertebereich für das Attribut Eintragstyp (in LDAP == entryType) sowie das Mapping auf die ProfessionOID festgelegt.

Tabelle 34: Tab_VZD_Mapping_Eintragstyp_und_ProfessionOID

Eintragstyp	Eintragstyp Bedeutung	ProfessionOID (ProfessionItem)
1	**Berufsgruppe**	1.2.276.0.76.4.30 (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)

ENTWURF

		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 Famulant/-in) 1.2.276.0.76.4.43 (PTA-Praktikant/-in) 1.2.276.0.76.4.44 (PKA Auszubildende/-r) 1.2.276.0.76.4.45 (Psychotherapeut/-in) 1.2.276.0.76.4.46 (Psychologische/-r Psychotherapeut/-in) 1.2.276.0.76.4.47 (Kinder- und Jugendlichenpsychotherapeut/-in) 1.2.276.0.76.4.48 (Rettungsassistent/-in) 1.2.276.0.76.4.178 (Notfallsanitäter/-in)
2	**Versicherte/-r**	1.2.276.0.76.4.49 (Versicherte/-r)
3	**Leistungserbringer Institution**	1.2.276.0.76.4.50 (Betriebsstätte Arzt) 1.2.276.0.76.4.51 (Zahnarztpraxis) 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 (Bundeswehrapotheke) 1.2.276.0.76.4.57 (Betriebsstätte Mobile Einrichtung Rettungsdienst)
4	**Organisation**	1.2.276.0.76.4.187 (Betriebsstätte Leistungserbringerorganisation Vertragszahnärzte)
5	**Krankenkasse**	1.2.276.0.76.4.59 (Betriebsstätte Kostenträger)

1087

ENTWURF

~~5~~6 Anhang A – Verzeichnisse

~~5.1~~6.1 Abkürzungen

Kürzel	Erläuterung
aAdG	andere Anwendungen des Gesundheitswesens (mit Zugriff auf Dienste der TI)
aAdG-NetG-TI	andere Anwendungen des Gesundheitswesens mit Zugriff auf Dienste der TI aus angeschlossenen Netzen des Gesundheitswesens
C.FD.TLS-C	Client-Zertifikat (öffentlicher Schlüssel) eines fachanwendungsspezifischen Dienstes für TLS Verbindungen
C.ZD.TLS-S	Server-Zertifikat (öffentlicher Schlüssel) eines zentralen Dienstes der TI-Plattform für TLS Verbindungen
DNS-SD	Domain Name System Service Discovery
DNSSEC	Domain Name System Security Extensions
FAD	fachanwendungsspezifischer Dienst
FQDN	Full Qualified Domain Name
GTI	Gesamtbetriebsverantwortlicher der TI
HBA	Heilberufsausweis
http	hypertext transport protocol
ID.FD.TLS-C	Client-Identität (privater und öffentlicher Schlüssel) eines fachanwendungsspezifischen Dienstes für TLS Verbindungen
ID.ZD.TLS-S	Server-Identität (privater und öffentlicher Schlüssel) eines zentralen Dienstes der TI-Plattform für TLS Verbindungen
KOM-LE	Kommunikation für Leistungserbringer (Fachanwendung)
LDAP	Lightweight Directory Access Protocol
LE	Leistungserbringer
OCSP	Online Certificate Status Protocol

ENTWURF

PKI	Public Key Infrastructure
PTR Resource Record	Domain Name System Pointer Resource Record
SMC	Secure Module Card
SOAP	Simple Object Access Protocol
TCP	Transmission Control Protocol
TI	Telematikinfrastruktur
TIP	Telematikinfrastruktur-Plattform
TLS	Transport Layer Security
TUC	Technischer Use Case
URL	Uniform Resource Locator
VZD	Verzeichnisdienst
XML	Extensible Markup Language

~~5.2~~6.2 Glossar

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

~~5.3~~6.3 Abbildungsverzeichnis

~~5.4~~6.4 Tabellenverzeichnis

ENTWURF

ENTWURF

ENTWURF

~~5.5~~6.5 Referenzierte Dokumente

~~5.5.1~~6.5.1 Dokumente der gematik

Die nachfolgende Tabelle enthält die Bezeichnung der in dem vorliegenden Dokument referenzierten Dokumente der gematik zur Telematikinfrastruktur. Der mit der vorliegenden Version korrelierende Entwicklungsstand dieser Konzepte und

Spezifikationen wird pro Release in einer Dokumentenlandkarte definiert; Version und Stand der referenzierten Dokumente sind daher in der nachfolgenden Tabelle nicht aufgeführt. Deren zu diesem Dokument jeweils gültige Versionsnummern sind in der aktuellen, von der gematik veröffentlichten Dokumentenlandkarte enthalten, in der die vorliegende Version aufgeführt wird.

[Quelle]	Herausgeber: Titel
[gemGlossar]	gematik: Glossar der Telematikinfrastruktur
[gemKPT_Arch_TIP]	gematik: Konzept Architektur der TI-Plattform
[gemKPT_PKI_TIP]	gematik: Konzept PKI der TI-Plattform
[gemKPT_DS_TIP]	gematik: Datenschutzkonzept TI-Plattform
[gemKPT_Sich_TIP]	gematik: Spezifisches Sicherheitskonzept TI-Plattform
[gemSpec_Net]	gematik: Spezifikation Netzwerk
[gemSpec_OM]	gematik: Operations und Maintenance Spezifikation
[gemSpec_OID]	gematik: Spezifikation Festlegung von OIDs
[gemSpec_PKI]	gematik: Spezifikation PKI
[gemSpec_Perf]	gematik: Performance und Mengengerüst TI-Plattform
[gemSpec_TSL]	gematik: Spezifikation TSL-Dienst

~~5.5.2~~6.5.2 Weitere Dokumente

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[BSI-AllVZD]	Bundesamt für Sicherheit in der Informationstechnik: B 5.15 Allgemeiner Verzeichnisdienst, https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge /Inhalt/_content/baust/b05/b05015.html
[BSI-SiGw]	Bundesamt für Sicherheit in der Informationstechnik (o.J.): Konzeption von Sicherheitsgateways, Version 1.0

ENTWURF

[HL7FHIR]	FHIR Specification https://www.hl7.org/fhir/
[RFC2119]	RFC 2119 (March 1997): Key words for use in RFCs to Indicate Requirement Levels http://www.rfc-editor.org/rfc/rfc2119.txt
[RFC4510]	RFC 4510 (June 2006): Lightweight Directory Access Protocol (LDAP): Technical Specification Road Map, http://www.ietf.org/rfc/rfc4510.txt
[RFC4511]	RFC 4511 (June 2006): Lightweight Directory Access Protocol (LDAP): The Protocol, http://www.ietf.org/rfc/rfc4511.txt
[RFC4512]	RFC 4512 (June 2006): Lightweight Directory Access Protocol (LDAP): Directory Information Models http://www.rfc-editor.org/rfc/rfc4512.txt
[RFC4513]	RFC 4513 (June 2006): Lightweight Directory Access Protocol (LDAP): Authentication Methods and Security Mechanisms http://www.rfc-editor.org/rfc/rfc4513.txt
[RFC4514]	RFC 4514 (June 2006): Lightweight Directory Access Protocol (LDAP): String Representation of Distinguished Names http://www.rfc-editor.org/rfc/rfc4514.txt
[RFC4515]	RFC 4515 (June 2006): Lightweight Directory Access Protocol (LDAP): String Representation of Search Filters http://www.rfc-editor.org/rfc/rfc4515.txt
[RFC4516]	RFC 4516 (June 2006): Lightweight Directory Access Protocol (LDAP): Uniform Resource Locator http://www.rfc-editor.org/rfc/rfc4516.txt
[RFC4517]	RFC 4517 (June 2006): Lightweight Directory Access Protocol (LDAP): Syntaxes and Matching Rules

ENTWURF

	http://www.rfc-editor.org/rfc/rfc4515.txt
[RFC4519]	RFC 4519 (June 2006): Lightweight Directory Access Protocol (LDAP): Schema for User Applications http://www.rfc-editor.org/rfc/rfc4519.txt
[RFC4522]	RFC 4522 (June 2006): Lightweight Directory Access Protocol (LDAP): The Binary Encoding Option http://www.rfc-editor.org/rfc/rfc4522.txt
[RFC4523]	RFC 4523 (June 2006): Lightweight Directory Access Protocol (LDAP) Schema Definitions for X.509 Certificates http://www.rfc-editor.org/rfc/rfc4523.txt
[RFC 6750]	The OAuth 2.0 Authorization Framework: Bearer Token Usage
[RFC6763]	RFC 6763 (February 2013): DNS-Based Service Discovery http://www.rfc-editor.org/rfc/rfc6763.txt

1182

ENTWURF