

**Elektronische Gesundheitskarte und Telematikinfrastruktur**

# Spezifikation Verzeichnisdienst

Version: 1.7.0  
Revision: 109011  
Stand: 15.05.2019  
Status: freigegeben  
Klassifizierung: öffentlich  
Referenzierung: gemSpec\_VZD

## Dokumentinformationen

### Änderungen zur Vorversion

Änderungen gemäß P18.1, die Änderungen sind gelb markiert.

### Dokumentenhistorie

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
0.0.7	24.10.13		initiale Version	gematik
0.1.0	08.11.13		internes Review durchgeführt	gematik
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	
1.5.0	19.04.17		Anpassung nach Änderungsliste	gematik
			Anpassung nach Änderungslisten P15.2, 15.4 und 15.5	
1.6.0	14.05.18		freigegeben	gematik
			Einarbeitung der Änderungen gemäß P18.1	
1.7.0	15.05.2019		freigegeben	gematik

## Inhaltsverzeichnis

<b>1</b>	<b>Einordnung des Dokumentes .....</b>	<b>5</b>
1.1	Zielsetzung .....	5
1.2	Zielgruppe .....	5
1.3	Geltungsbereich .....	5
1.4	Abgrenzungen .....	5
1.5	Methodik.....	6
<b>2</b>	<b>Systemüberblick .....</b>	<b>7</b>
<b>3</b>	<b>Übergreifende Festlegungen .....</b>	<b>8</b>
3.1	IT-Sicherheit und Datenschutz .....	8
3.2	Fachliche Anforderungen .....	9
<b>4</b>	<b>Funktionsmerkmale.....</b>	<b>11</b>
4.1	<b>Schnittstelle I_Directory_Query.....</b>	<b>11</b>
4.1.1	Operation search_Directory .....	12
4.1.1.1	Umsetzung .....	12
4.1.1.2	Nutzung.....	12
4.2	<b>Schnittstelle I_Directory_Maintenance .....</b>	<b>13</b>
4.2.1	Operation add_Directory_Entry .....	14
4.2.1.1	Umsetzung .....	14
4.2.1.2	Nutzung.....	15
4.2.2	Operation read_Directory_Entry .....	16
4.2.2.1	Umsetzung .....	16
4.2.2.2	Nutzung.....	18
4.2.3	Operation modify_Directory_Entry .....	19
4.2.3.1	Umsetzung .....	19
4.2.3.2	Nutzung.....	20
4.2.4	Operation delete_Directory_Entry .....	21
4.2.4.1	Umsetzung .....	21
4.2.4.2	Nutzung.....	21
4.3	<b>Schnittstelle I_Directory_Application_Maintenance .....</b>	<b>23</b>
4.3.1	Operation add_Directory_FA-Attributes .....	24
4.3.1.1	Umsetzung SOAP .....	24
4.3.1.2	Nutzung SOAP .....	25
4.3.1.3	Umsetzung LDAPv3 .....	26
4.3.1.4	Nutzung LDAPv3.....	26
4.3.2	Operation delete_Directory_FA-Attributes .....	27
4.3.2.1	Umsetzung SOAP .....	27
4.3.2.2	Nutzung SOAP .....	27
4.3.2.3	Umsetzung LDAPv3 .....	28
4.3.2.4	Nutzung LDAPv3.....	28
4.3.3	Operation modify_Directory_FA-Attributes.....	29

4.3.3.1	Umsetzung SOAP .....	29
4.3.3.2	Nutzung SOAP .....	30
4.3.3.3	Umsetzung LDAPv3 .....	31
4.3.3.4	Nutzung LDAPv3 .....	31
4.4	Prozessschnittstelle P_Directory_Application_Registration (Provided) ....	32
4.5	Prozessschnittstelle P_Directory_Maintenance (Provided).....	32
5	Datenmodell .....	33
6	Anhang A – Verzeichnisse .....	39
6.1	Abkürzungen.....	39
6.2	Glossar .....	40
6.3	Abbildungsverzeichnis.....	40
6.4	Tabellenverzeichnis.....	40
6.5	Referenzierte Dokumente.....	41
6.5.1	Dokumente der gematik.....	41
6.5.2	Weitere Dokumente .....	42

---

# 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).

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

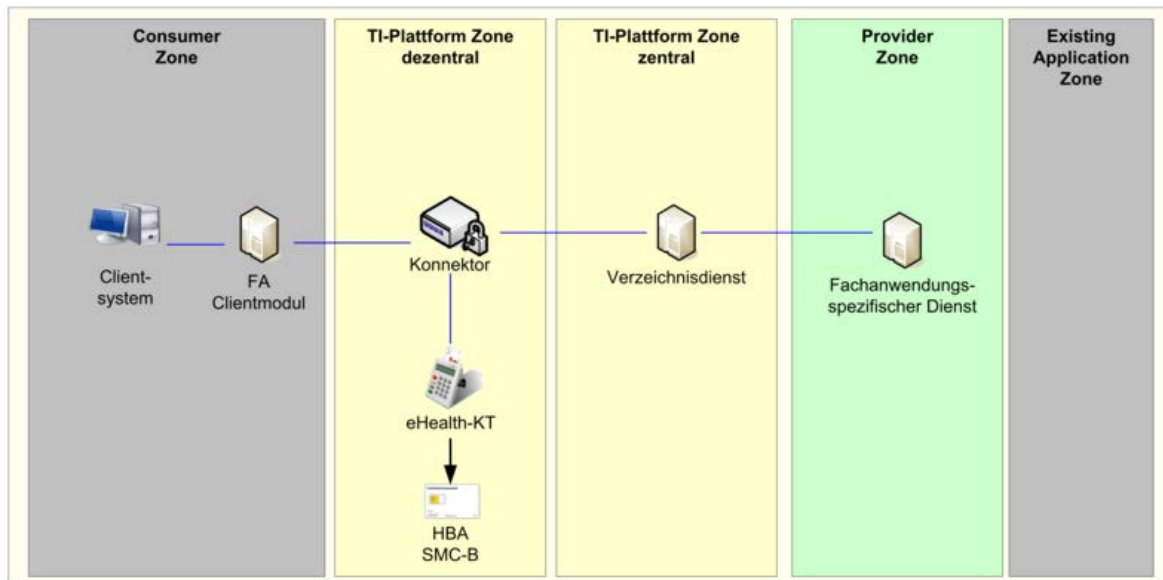
[<=]

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.

## 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
2. durch fachanwendungsspezifische Dienste (FAD), die fachanwendungsspezifische Daten (Fachdaten) zu bereits bestehenden Basisdaten zufügen.

Der VZD kann durch LDAP Clients abgefragt werden.

---

## 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
- 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.

[<=]

## **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-Bezeichnungen 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.

[<=]

#### **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.

[<=]

## 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_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**

<b>Name</b>	I_Directory_Query	
<b>Version</b>	wird im Produktypsteckbrief des VZD definiert	
<b>Operationen</b>	Name	Kurzbeschreibung

	search_Directory	Abfragen von Daten des VZD gemäß LDAPv3 Protokoll. Der Base DN für die LDAP Suche ist dc=data,dc=vzd
--	------------------	--

[&lt;=]

#### 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.

[&lt;=]

##### 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.

[&lt;=]

##### 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.

[&lt;=]

#### 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. Als Filter für die Suche sind alle Attribute außer der Telematik-ID möglich.

Die Telematik-ID darf nicht als Ergebnis geliefert werden.

Die abgefragten Attribute MÜSSEN durch marktübliche E-Mail Clients nutzbar sein.

[&lt;=]

#### 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 unterstützen.

Tabelle 3: Tab\_TUC\_VZD\_0001

<b>Name</b>	TUC_VZD_0001 "search_Directory"	
<b>Beschreibung</b>	Diese Operation ermöglicht die Suche nach den im VZD gespeicherten Daten.	
<b>Vorbedingungen</b>	Der LDAPS-Verbindungs Aufbau muss erfolgreich durchgeführt sein.	
<b>Eingangsdaten</b>	Search Request gemäß [RFC4511]#4.5.1 und Informationsmodell (Abb_VZD_logisches_Datenmodell)	
<b>Komponenten</b>	LDAP Client, Verzeichnisdienst	
<b>Ausgangsdaten</b>	gemäß [RFC4511]#4.5.2	
<b>Standardablauf</b>	<b>Aktion</b>	<b>Beschreibung</b>
	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.
<b>Varianten/Alternativen</b>	keine	
<b>Zustand nach erfolgreichem Ablauf</b>	Die Ergebnisse der Suche liegen im LDAP Client vor.	
<b>Fehlerfälle</b>	Zur Behandlung auftretender Fehlerfälle werden Fehlermeldungen gemäß [RFC4511]#Appendix A verwendet.	

[&lt;=]

## 4.2 Schnittstelle I\_Directory\_Maintenance

Die Schnittstelle ermöglicht die Administration der Basisdaten.

### TIP1-A\_5571 - VZD, Schnittstelle I\_Directory\_Maintenance

Der VZD MUSS die Schnittstelle I\_Directory\_Maintenance gemäß Tabelle Tab\_VZD\_Schnittstelle\_I\_Directory\_Maintenance anbieten.

Tabelle 4: Tab\_VZD\_Schnittstelle\_I\_Directory\_Maintenance

<b>Name</b>	I_Directory_Maintenance	
<b>Version</b>	wird im Produkttypsteckbrief des VZD definiert	
<b>Operationen</b>	<b>Name</b>	<b>Kurzbeschreibung</b>
	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).

[&lt;=]

**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.

[&lt;=]

**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.

[&lt;=]

**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 **VZD\_TAB\_addDirectoryEntry\_Mapping Tab\_VZD\_Datenbeschreibung** den neuen Basisdatensatz.

**Tabelle 5: VZD\_TAB\_addDirectoryEntry\_Mapping**

SMC-B-Daten	HBA-Daten	SOAP-Request Element	LDAP-Directory Basisdatensatz Attribut	Beschreibung
		VZD:timestamp	wird nicht in das LDAP-Directory	

		VZD:variant	eingetragen	
ENC-Zertifikat	ENC-Zertifikat	VZD:x509CertificateEnc	userCertificate	Das ENC-Zertifikat der Smartcard im DER-Format
aus-ENC-Zertifikat: Subject/commonName	aus-ENC-Zertifikat: Subject/commonName		cn	Diese Werte werden dem in VZD:x509CertificateEnc enthaltenen Zertifikat entnommen.
	aus-ENC-Zertifikat: Subject/givenName		givenName	Die Werte werden eingetragen, wenn VZD:variant == „full“
aus-ENC-Zertifikat: Subject/organizationName	aus-ENC-Zertifikat: Subject/surname		sn	Wenn VZD:variant == „minimal“ werden die Werte nicht in das LDAP-Directory eingetragen.
aus-ENC-Zertifikat: Subject/organizationName	aus-ENC-Zertifikat: Subject/surname, Subject/givenName		displayName	
		VZD:title	title	Wenn im SOAP Request vorhanden, wird das entsprechende Attribut im Verzeichnis angelegt.
		VZD:organization	organization	Ein Attribut wird im Verzeichnis nicht angelegt, wenn das entsprechende SOAP-Request Element eine leere Zeichenfolge enthält.
		VZD:streetAddress	streetAddress	
		VZD:postalCode	postalCode	
		VZD:localityName	localityName	Das Attribut subject bezeichnet das Fachgebiet des LE.
		VZD:stateOrProvinceName	stateOrProvinceName	Das Attribut otherName ermöglicht die Speicherung von überlangen Namen.
		VZD:subject	subject	
		VZD:otherName	otherName	

Es müssen die Fehlermeldungen gemäß Tab\_TUC\_VZD\_0002 verwendet werden.

[<=]

#### 4.2.1.2 Nutzung

##### TIP1-A\_5576 - Nutzer der Schnittstelle, TUC\_VZD\_0002 „add\_Directory\_Entry“

Der Nutzer der Schnittstelle MUSS den technischen Use Case TUC\_VZD\_0002

„add\_Directory\_Entry“ gemäß Tabelle Tab\_TUC\_VZD\_0002 umsetzen.

Der SOAP-Requests MUSS gemäß Tabelle VZD\_TAB\_addDirectoryEntry\_Mapping mit

der Bedeutung entsprechenden Daten ausgefüllt sein.

**Tabelle 6: Tab\_TUC\_VZD\_0002**

<b>Name</b>	TUC_VZD_0002 „add_Directory_Entry“	
<b>Beschreibung</b>	Diese Operation ermöglicht die Erzeugung von neuen Basisdaten. Bestehende Basisdaten werden überschrieben.	
<b>Vorbedingungen</b>	keine	
<b>Eingangsdaten</b>	SOAP-Request „addDirectoryEntry“	
<b>Komponenten</b>	Nutzer der Schnittstelle, Verzeichnisdienst	
<b>Ausgangsdaten</b>	SOAP-Response „VZD:responseMsg“	
<b>Standardablauf</b>	<b>Aktion</b>	<b>Beschreibung</b>
	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.
<b>Varianten/Alternativen</b>	keine	
<b>Fehlerfälle</b>	<p>Es werden die protokollspezifischen Fehlermeldungen verwendet (TCP, HTTP, TLS).</p> <p>Fehler bei der Verarbeitung des SOAP Requests werden als gematik SOAP-Fault versendet:</p> <p>faultcode 4211, faultstring: Operation fehlerhaft ausgeführt, Basisdaten konnten nicht angelegt werden (Fehler im Verzeichnisdienst)</p> <p>faultcode 4202, faultstring: SOAP Request enthält Fehler</p> <p>faultcode 4201, faultstring: Operation enthält ungültige Daten</p> <p>Erkannte Fehler auf Transportprotokollebene müssen auf gematik SOAP Faults (Code 6 aus Tabelle Tab_Gen_Fehler aus [gemSpec_OM]) abgebildet werden. Zusätzlich müssen die generischen gematik SOAP-Faults</p> <p>Code 2: Verbindung zurückgewiesen</p> <p>Code 3: Nachrichtenschema fehlerhaft</p> <p>Code 4: Version Nachrichtenschema fehlerhaft unterstützt werden.</p>	

[<=]

## 4.2.2 Operation read\_Directory\_Entry

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

### 4.2.2.1 Umsetzung

#### TIP1-A\_5577 - VZD, Umsetzung read\_Directory\_Entry



Der VZD MUSS nach folgenden Vorgaben die Operation  
 I\_Directory\_Maintenance::read\_Directory\_Entry implementieren:

4. Der zur Telematik-ID gehörende Eintrag wird im LDAP Directory ermittelt.
5. Es wird eine SOAP Response VZD:readResponseMsg aus dem kompletten Eintrag (Basisdaten + Fachdaten) gemäß  
**VZD\_TAB\_readDirectoryEntry\_Mapping** Tab\_VZD\_Datenbeschreibung erzeugt.

**Tabelle 7: VZD\_TAB\_readDirectoryEntry\_Mapping**

LDAP-Directory Basisdatensatz Attribut	SOAP-Response-Element	Beschreibung	Kardinalität
userCertificate	VZD:x509CertificateEnc	Das ENC-Zertifikat der Smartcard im DER-Format	0 bis 10
cn	VZD:commonName	aus ENC-Zertifikat: Subject/commonName	jeweils 0 bis 1
givenName	VZD:givenName	Für natürliche Personen: <alle Vornamen> Für Organisationen: n/a	
sn	VZD:surName	Für natürliche Personen: „<Nachname>“ Für Organisationen: „<organizationName>“	
displayName	VZD:displayName	Für natürliche Personen: „<Nachname>, <alle Vornamen>“ Für Organisationen: „<organizationName>“	
title	VZD:title	Titel	
organization	VZD:organization	Organisationsname	
streetAddress	VZD:streetAddress	Straße und Hausnummer	
postalCode	VZD:postalCode	PLZ	
localityName	VZD:localityName	Ort	
stateOrProvinceName	VZD:stateOrProvinceName	Bundesland	
subject	VZD:subject	Das Attribut subject bezeichnet das Fachgebiet des LE.	
otherName	VZD:otherName	Das Attribut otherName ermöglicht die Speicherung von überlangen Namen.	
serviceData	VZD:serviceData	Fachdaten	0 bis 1
	VZD:KOM-LE	Fachdaten des FD KOM-LE	0 bis 1
	VZD:providerEntry	Fachdaten eines	0 bis 1

		KOM-LE-Anbieters	unbegrenzt
	VZD:providerName (z.B. kom-le-anbieter)	Name des Anbieters	1 --- 1 bis 100
	VZD:mail (z.B. dr.mustermann@kom-le-anbieter.telematik)	E-Mail-Adresse	

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 VZD-TAB-readDirectoryEntry-Mapping Tab\_VZD\_Datenbeschreibung mit den zur Telematik-ID gehörenden Daten aus dem VZD ausgefüllt.

**Tabelle 8: Tab\_TUC\_VZD\_0003**

<b>Name</b>	TUC_VZD_0003 „read_Directory_Entry“	
<b>Beschreibung</b>	Diese Operation liest einen vollständigen Eintrag aus dem VZD aus.	
<b>Vorbedingungen</b>	Keine	
<b>Eingangsdaten</b>	SOAP-Request „readDirectoryEntry“	
<b>Komponenten</b>	Nutzer der Schnittstelle, Verzeichnisdienst	
<b>Ausgangsdaten</b>	SOAP-Response „readResponseMsg“	
<b>Standardablauf</b>	<b>Aktion</b>	<b>Beschreibung</b>
	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.
<b>Varianten/Alternativen</b>	keine	
<b>Fehlerfälle</b>	Es werden die protokollspezifischen Fehlermeldungen verwendet (TCP, HTTP, TLS) Fehler bei der Verarbeitung des SOAP Requests werden als gematik SOAP-Fault versendet: faultcode 42214311, 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.
--	---

[&lt;=]

### 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:

- Der zur Telematik-ID gehörende Basisdatensatz wird im LDAP Directory ermittelt.
- Die Daten im Basisdatensatz werden durch die Daten aus dem SOAP Request gemäß **VZD\_TAB\_modifyDirectoryEntry\_Mapping** Tab\_VZD\_Datenbeschreibung geändert.

**Tabelle 9: VZD\_TAB\_modifyDirectoryEntry\_Mapping**

SMC-B-Zertifikats-Eintrag	HBA-Zertifikats-Eintrag	SOAP-Request Element	LDAP-Directory Basisdatensatz Attribut	Beschreibung
		VZD:timestamp	wird nicht in das LDAP-Directory eingetragen	
		VZD:variant		
ENC-Zertifikat	ENC-Zertifikat	VZD:x509CertificateEnc	userCertificate	Das ENC-Zertifikat der Smartcard im DER-Format
aus-ENC-Zertifikat: Subject/commonName	aus-ENC-Zertifikat: Subject/commonName		cn	Diese Werte werden dem in VZD:x509CertificateEnc enthaltenen Zertifikat entnommen.
	aus-ENC-Zertifikat: Subject/givenName		givenName	Die Werte werden eingetragen, wenn VZD:variant == „full“
aus-ENC-Zertifikat: Subject/organisa	aus-ENC-Zertifikat: Subject/surname		sn	Wenn VZD:variant ==

tionName				„minimal“ werden die Werte nicht in das LDAP-Directory eingetragen.
aus-ENC-Zertifikat: Subject/organisationName	aus-ENC-Zertifikat: Subject/surname, Subject/givenName		displayName	
		VZD:title	title	Wenn im SOAP Request vorhanden, wird das entsprechende Attribut im Verzeichnis angelegt. Ein Attribut wird im Verzeichnis nicht angelegt, wenn das entsprechende SOAP-Request-Element eine leere Zeichenfolge enthält.
		VZD:organization	organization	
		VZD:streetAddress	streetAddress	
		VZD:postalCode	postalCode	
		VZD:localityName	localityName	Das Attribut subject bezeichnet das Fachgebiet des LE.
		VZD:stateOrProvinceName	stateOrProvinceName	
		VZD:subject	subject	Das Attribut otherName ermöglicht die Speicherung von überlangen Namen.
		VZD:otherName	otherName	

Es müssen die Fehlermeldungen gemäß Tab\_TUC\_VZD\_0004 verwendet werden.

[<=]

#### 4.2.3.2 Nutzung

##### TIP1-A\_5580 - Nutzer der Schnittstelle, TUC\_VZD\_0004 „modify\_Directory\_Entry“

Der Nutzer der Schnittstelle MUSS den technischen Use Case TUC\_VZD\_0004 „modify\_Directory\_Entry“ gemäß Tabelle Tab\_TUC\_VZD\_0004 umsetzen. Der Webservice wird durch die Dokumente DirectoryMaintenance.wsdl und DirectoryMaintenance.xsd definiert.

Der SOAP-Requests MUSS gemäß Tabelle VZD\_TAB\_modifyDirectoryEntry\_Mapping mit der Bedeutung entsprechenden Daten ausgefüllt sein.

**Tabelle 10: Tab\_TUC\_VZD\_0004**

<b>Name</b>	TUC_VZD_0004 „modify_Directory_Entry“
<b>Beschreibung</b>	Diese Operation ermöglicht die Änderung Erzeugung von neuen Basisdaten. Bestehende Basisdaten werden überschrieben.
<b>Vorbedingungen</b>	keine
<b>Eingangsdaten</b>	SOAP-Request „modifyDirectoryEntry“
<b>Komponenten</b>	Nutzer der Schnittstelle, Verzeichnisdienst
<b>Ausgangsdaten</b>	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.
<b>Varianten/Alternativen</b>	keine	
<b>Fehlerfälle</b>	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.	

[&lt;=]

#### 4.2.4 Operation delete\_Directory\_Entry

Diese Operation löscht einen bestehenden Datensatz im LDAP Verzeichnis.

##### 4.2.4.1 Umsetzung

###### TIP1-A\_5581 - VZD, Umsetzung delete\_Directory\_Entry

Der VZD MUSS nach folgenden Vorgaben die Operation I\_Directory\_Maintenance::delete\_Directory\_Entry implementieren:

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

Es müssen die Fehlermeldungen gemäß Tab\_TUC\_VZD\_0005 verwendet werden.

[&lt;=]

##### 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 11: Tab\_TUC\_VZD\_0005

<b>Name</b>	TUC_VZD_0005 „delete_Directory_Entry“	
<b>Beschreibung</b>	Diese Operation ermöglicht die <b>Löschung</b> <b>Erzeugung</b> von <b>neuen</b> Basisdaten inkl. der zugehörigen Fachdaten. <b>Bestehende Basisdaten werden überschrieben.</b>	
<b>Vorbedingungen</b>	keine	
<b>Eingangsdaten</b>	SOAP-Request „deleteDirectoryEntry“	
<b>Komponenten</b>	Nutzer der Schnittstelle, Verzeichnisdienst	
<b>Ausgangsdaten</b>	SOAP-Response „responseMsg“	
<b>Standardablauf</b>	<b>Aktion</b>	<b>Beschreibung</b>
	<b>Aufbau TLS-Verbindung</b>	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.
	<b>SOAP-Request senden</b>	Der Nutzer der Schnittstelle ruft die SOAP-Operation VZD:deleteDirectoryEntry auf.
	<b>SOAP-Response empfangen</b>	Die SOAP-Response VZD:responseMsg mit dem VZD:status wird empfangen.
<b>Varianten/Alternativen</b>	keine	
<b>Fehlerfälle</b>	<p>Es werden die protokollspezifischen Fehlermeldungen verwendet (TCP, HTTP, TLS)</p> <p>Fehler bei der Verarbeitung des SOAP Requests werden als gematik SOAP-Fault versendet:</p> <p>faultcode 4241, faultstring: Operation fehlerhaft ausgeführt, Basisdaten konnten nicht gelöscht werden (Fehler im Verzeichnisdienst)</p> <p>faultcode 4312, faultstring: Basisdaten konnten nicht gefunden werden</p> <p>faultcode 4202, faultstring: SOAP Request enthält Fehler</p> <p>Erkannte Fehler auf Transportprotokollebene müssen auf gematik SOAP Faults (Code 6 aus Tabelle Tab_Gen_Fehler aus [gemSpec_OM]) abgebildet werden. Zusätzlich müssen die generischen gematik SOAP-Faults</p> <p>Code 2: Verbindung zurückgewiesen</p> <p>Code 3: Nachrichtenschema fehlerhaft</p> <p>Code 4: Version Nachrichtenschema fehlerhaft unterstützt werden.</p>	

[&lt;=]

### 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 12: Tab\_VZD\_Schnittstelle\_I\_Directory\_Application\_Maintenance**

<b>Name</b>	I_Directory_Application_Maintenance	
<b>Version</b>	wird im Produkttypsteckbrief des VZD definiert	
<b>Operationen</b>	<b>Operation</b>	<b>Kurzbeschreibung</b>
	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

[&lt;=]

#### 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.

[&lt;=]

#### 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.

[&lt;=]

#### 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 LDAPv3 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.

#### **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:

2. 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.
3. Ein bereits zur Telematik-ID gehörender Fachdatensatz wird gelöscht und neu angelegt.
4. Ein noch nicht existierender Fachdatensatz zur Telematik-ID wird im LDAP Directory neu angelegt.
5. Die Daten aus dem SOAP Request werden gemäß VZD\_TAB\_I\_Directory\_Application\_Maintenance\_Add\_Mapping zum Basisdatensatz hinzugefügt.

**Tabelle 13: 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 14: Tab\_TUC\_VZD\_0006**

<b>Name</b>	add_Directory_FA-Attributes	
<b>Beschreibung</b>	Mit dieser Operation werden Fachdaten zu einem bestehenden Basisdaten-Eintrag zugefügt.	
<b>Vorbedingungen</b>	Keine.	
<b>Eingangsdaten</b>	SOAP-Request „addDirectoryFAAttributes“	
<b>Komponenten</b>	VZD, FAD	
<b>Ausgangsdaten</b>	SOAP-Response „responseMsg“	
<b>Standardablauf</b>	<b>Aktion</b>	<b>Beschreibung</b>
	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
<b>Fehlerfälle</b>	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 - 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 15: VZD\_TAB\_KOM-LE\_Attributes

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

[&lt;=]

#### 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.

[&lt;=]

#### 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 16: Tab\_TUC\_VZD\_0007

<b>Name</b>	add_Directory_FA-Attributes(LDAPv3)	
<b>Beschreibung</b>	Mit dieser Operation werden Fachdaten zu einem bestehenden Eintrag zugefügt.	
<b>Vorbedingungen</b>	Der LDAPS-Verbindungsaufbau muss erfolgreich durchgeführt sein.	
<b>Eingangsdaten</b>	Add-Request gemäß [RFC4511]#4.7 und Informationsmodell (Abb_VZD_logisches_Datenmodell)	
<b>Komponenten</b>	LDAP Client des FAD, Verzeichnisdienst	
<b>Ausgangsdaten</b>	gemäß [RFC4511]#4.7	
<b>Standardablauf</b>	<b>Aktion</b>	<b>Beschreibung</b>
	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.

<b>Varianten/Alternativen</b>	keine	
<b>Zustand nach erfolgreichem Ablauf</b>	Das Ergebnis der Operation liegt im LDAP Client des FAD vor.	
<b>Fehlerfälle</b>	Zur Behandlung auftretender Fehlerfälle werden Fehlermeldungen gemäß [RFC4511]#Appendix A verwendet.	

[&lt;=]

#### 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:

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.

[&lt;=]

##### 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 17: Tab\_TUC\_VZD\_0008**

<b>Name</b>	delete_Directory_FA-Attributes	
<b>Beschreibung</b>	Mit dieser Operation wird ein Fachdaten-Eintrag gelöscht.	
<b>Vorbedingungen</b>	Keine.	
<b>Eingangsdaten</b>	SOAP-Request „deleteDirectoryFAAttributes“	
<b>Komponenten</b>	VZD, FAD	
<b>Ausgangsdaten</b>	SOAP-Response „responseMsg“	
<b>Standardablauf</b>	<b>Aktion</b>	<b>Beschreibung</b>
	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
<b>Fehlerfälle</b>	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	

[&lt;=]

#### 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.

[&lt;=]

#### 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 18: Tab\_TUC\_VZD\_0009**

<b>Name</b>	delete_Directory_FA-Attributes(LDAPv3)	
<b>Beschreibung</b>	Mit dieser Operation werden alle Fachdaten zu einem bestehenden Eintrag gelöscht.	
<b>Vorbedingungen</b>	Der LDAPS-Verbindungsaufbau muss erfolgreich durchgeführt sein.	
<b>Eingangsdaten</b>	Delete-Request gemäß [RFC4511]#4.8 und Informationsmodell (Abb_VZD_logisches_Datenmodell)	
<b>Komponenten</b>	LDAP Client des FAD, Verzeichnisdienst	
<b>Ausgangsdaten</b>	gemäß [RFC4511]#4.8	
<b>Standardablauf</b>	Aktion	Beschreibung
	Delete	Der LDAP Client des FAD sendet den delete-Request

	Request senden	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.
<b>Varianten/Alternativen</b>	keine	
<b>Zustand nach erfolgreichem Ablauf</b>	Das Ergebnis der Operation liegt im LDAP Client des FAD vor.	
<b>Fehlerfälle</b>	Zur Behandlung auftretender Fehlerfälle werden Fehlermeldungen gemäß [RFC4511]#Appendix A verwendet.	

[&lt;=]

### 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 19: 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.

[&lt;=]

#### 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 20: Tab\_TUC\_VZD\_0010**

<b>Name</b>	modify_Directory_FA-Attributes	
<b>Beschreibung</b>	Mit dieser Operation werden Fachdaten geändert.	
<b>Vorbedingungen</b>	Keine.	
<b>Eingangsdaten</b>	SOAP-Request „modifyDirectoryFAAttributes“	
<b>Komponenten</b>	VZD, FAD	
<b>Ausgangsdaten</b>	SOAP-Response „responseMsg“	
<b>Standardablauf</b>	<b>Aktion</b>	<b>Beschreibung</b>
	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
<b>Fehlerfälle</b>	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 - 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 21: 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
--------------------------	------

[&lt;=]

#### 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:

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.

[&lt;=]

#### 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 22: Tab\_TUC\_VZD\_0011

<b>Name</b>	modify_Directory_FA-Attributes(LDAPv3)	
<b>Beschreibung</b>	Mit dieser Operation werden Fachdaten zu einem bestehenden Eintrag geändert.	
<b>Vorbedingungen</b>	Der LDAPS-Verbindungsaufbau muss erfolgreich durchgeführt sein.	
<b>Eingangsdaten</b>	Modify-Request gemäß [RFC4511]#4.6 und Informationsmodell (Abb_VZD_logisches_Datenmodell)	
<b>Komponenten</b>	LDAP Client des FAD, Verzeichnisdienst	
<b>Ausgangsdaten</b>	gemäß [RFC4511]#4.6	
<b>Standardablauf</b>	<b>Aktion</b>	<b>Beschreibung</b>
	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.
<b>Varianten/Alternativen</b>	keine	
<b>Zustand nach erfolgreichem Ablauf</b>	Das Ergebnis der Operation liegt im LDAP Client des FAD vor.	
<b>Fehlerfälle</b>	Zur Behandlung auftretender Fehlerfälle werden Fehlermeldungen gemäß [RFC4511]#Appendix A verwendet.	

[&lt;=]

#### 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 GBV** vorgegebener OID-Liste),
- Name der Fachanwendung (z.B. KOM-LE),
- Name des Fachdienstbetreibers.

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

[&lt;=]

##### TIP1-A\_5605 - VZD, De-Registrierung FADs

Der Anbieter des VZD MUSS einen De-Registrierungsprozess für FAD implementieren.

Der VZD MUSS alle verbliebenen Fachdaten eines deregistrierten FAD löschen.

Der VZD-Anbieter dokumentiert den Prozess und legt ihn dem **GTI GBV** zur Freigabe vor.

Der Anbieter des VZD informiert alle FAD-Anbieter wie der Prozess genutzt wird.

[&lt;=]

#### 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 GBV** zur Freigabe vor.

[&lt;=]



## 5 Datenmodell

### TIP1-A\_5607 - VZD, logisches Datenmodell

Der VZD MUSS das logische Datenmodell nach Abb\_VZD\_logisches\_Datenmodell und Tab\_VZD\_Datenbeschreibungmodell implementieren. Es wird keine Vorgabe an die technische Ausprägung des Datenmodells gemacht.

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

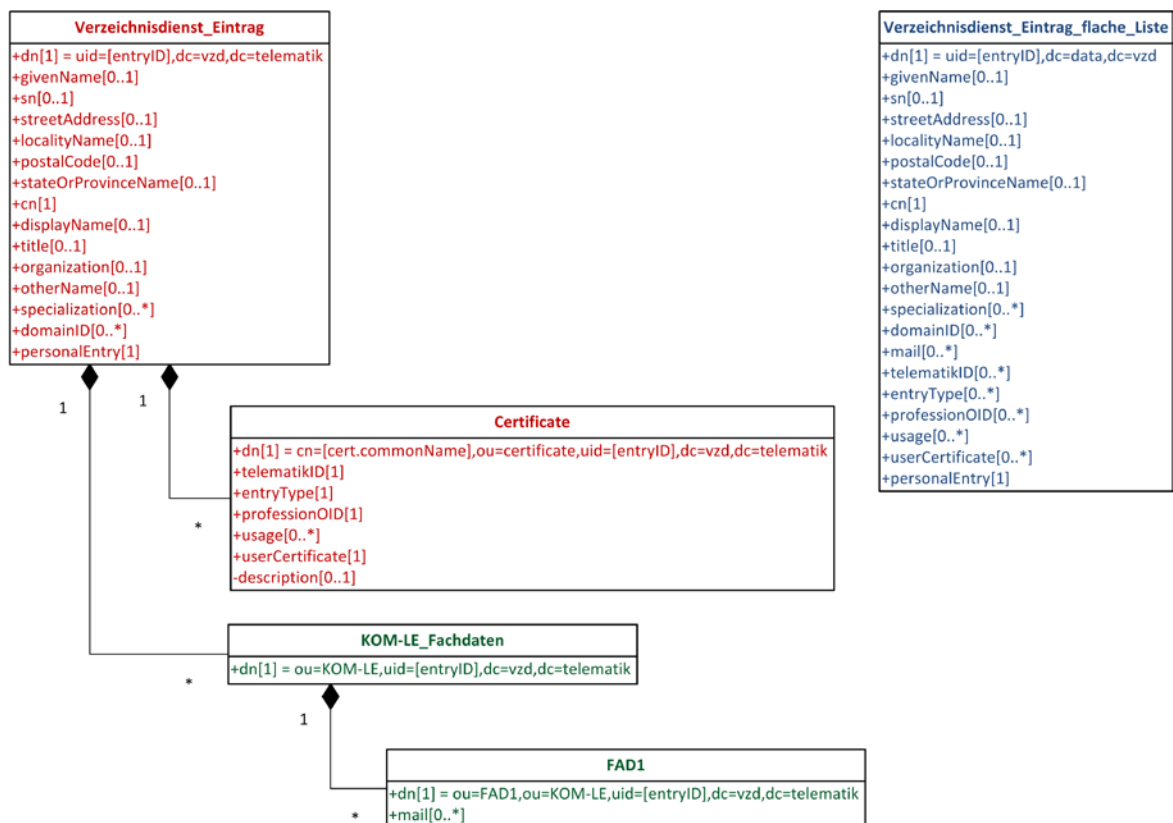


Abbildung 2: Abb\_VZD\_logisches\_Datenmodell

Tabelle 23 Tab\_VZD\_Datenbeschreibungmodell

Bezeichner	LDAP-Directory Attribut	Pflichtfeld ?	Erläuterung Zusatzinformationen
Vorname	gn givenName	ja optional	HBA: Bezeichner: Vorname, obligatorisch, wird aus dem Zertifikat übernommen SMC-B: nicht verwendet
Name	sn	ja optional	HBA: Bezeichner: Name, obligatorisch, wird aus dem Zertifikat übernommen SMC-B: nicht verwendet
Vorname und	cn	optional obligatorisch	HBA: Bezeichner: Vorname und Nachname SMC-B: Bezeichner Bezeichner: Name

<b>Nachname</b>		ch	Wird vom VZD aus dem Zertifikatsattribut commonName übernommen.
<b>Angezeigter Name</b>	displayName	optional	Bezeichner: Anzeigenname kann geändert werden HBA: voreingestellter Wert == givenName + sn SMC-B: voreingestellter Wert == organization SMC-B für Zahnärzte == cn (ProfessionOID 1.2.276.0.76.4.51 (Zahnarztpraxis))
<b>Straße Hausnummer</b>	streetAddress	ja optional	Bezeichner: Straße und Hausnummer
<b>Postleitzahl</b>	postalCode	ja optional	Bezeichner: Postleitzahl
<b>Ort</b>	localityName	ja optional	Bezeichner: Ort
<b>Bundesland</b>	stateOrProvinceName	optional optional	Bezeichner: Bundesland
<b>Titel</b>	title	optional	HBA: Bezeichner: Titel, optional SMC-B: nicht verwendet
<b>Organisation</b>	organization	optional	Wenn vorhanden, dann wird das Zertifikatsattribut organizationName eingetragen, sonst cn kann geändert werden HBA: Bezeichner: Organisation, optional SMC-B: Bezeichner: Organisation, optional SMC-B KTR: Bezeichner: Betriebsnummer (BBNR)
<b>Anderer Name</b>	otherName	optional	Bezeichner: Anderer Name Wird vom VZD aus dem Zertifikatsattribut otherName übernommen.
	specialization	optional	HBA: Bezeichner: medizinisches Fachgebiet SMC-B: Bezeichner: Fachgebiet SMC-B KTR: nicht verwendet kann mehrfach vorkommen (0..100)
	domainID	optional	kann geändert werden Ärzte: Bezeichner: Betriebsstättennummer Zahnärzte: Bezeichner: Abrechnungsnummer inkl. vorangestellter 2-stelliger KZV-Nr. KTR: Bezeichner: Institutionskennzeichen kann mehrfach vorkommen (0..100)
<b>Fachgebiet</b>	subject	optional	gehört zu Basisdaten

	personalEntry	obligatorisch	Wird vom VZD eingetragen Wert == TRUE, wenn alle Zertifikate den entryType 1 haben (Berufsgruppe), Wert == FALSE sonst
<b>Zertifikat</b>	userCertificate	optional	Bezeichner: Zertifikat kann mehrfach vorkommen (0..4 50) Neue Einträge können nur mit Zertifikat angelegt werden. Das Zertifikat wird jedoch gelöscht, wenn es ungültig geworden ist. Wenn kein Zertifikat vorliegt, dann kann der Eintrag nicht mittels LDAP-Abfrage gefunden werden. Über die Schnittstelle I_Directory_Maintenance können <del>weiterhin</del> Zertifikate hinzugefügt werden. Format: DER, Base64 kodiert
	entryType	optional	Bezeichner: Eintragstyp Wird vom VZD anhand der in den Zertifikaten enthaltenen OIDs (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 <del>Wird beim Anlegen des Eintrags im VZD aus dem Zertifikat übernommen (Feld registrationNumber der Extension Admission).</del> 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 in den Zertifikaten enthaltenen OIDs (Extension Admission, Attribut ProfessionOID) und dem Mapping in ab_VZD_Mapping_Eintragstyp_und_ProfessionOID automatisch eingetragen. Siehe [gemSpecOID]# Tab_PKI_402 und Tab_PKI_403. kann mehrfach vorkommen (0..100)
	usage	optional	Bezeichner: Nutzungskennzeichnung kann pro Zertifikat mehrfach (0..100) vergeben werden vorgegebener Wertebereich [KOM-LE, ePA]
	description	optional	Bezeichner: Beschreibung Dieses Attribut ermöglicht das Zertifikat zu beschreiben, um die Administration des VZD Eintrags zu vereinfachen.

<b>E-Mail-Adresse</b>	mail	optional	<b>Bezeichner: E-Mail-Adresse</b> kann mehrfach vorkommen (0..100)
-----------------------	------	----------	---

[&lt;=]

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 24: Tab\_VZD\_Mapping\_Eintragstyp\_und\_ProfessionOID

Eintragstyp	Eintragstyp Bedeutung	ProfessionOID (ProfessionItem)
<b>1</b>	<b>Berufsgruppe</b>	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) 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)
<b>2</b>	<b>Versicherte/-r</b>	1.2.276.0.76.4.49 (Versicherte/-r)

<b>3</b>	<b>Leistungserbringer Institution</b>	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 (Krankenhausapotheken) 1.2.276.0.76.4.56 (Bundeswehrapotheke) 1.2.276.0.76.4.57 (Betriebsstätte Mobile Einrichtung Rettungsdienst)
<b>4</b>	<b>Organisation</b>	1.2.276.0.76.4.187 (Betriebsstätte Leistungserbringerorganisation Vertragszahnärzte)
<b>5</b>	<b>Krankenkasse</b>	1.2.276.0.76.4.59 (Betriebsstätte Kostenträger)

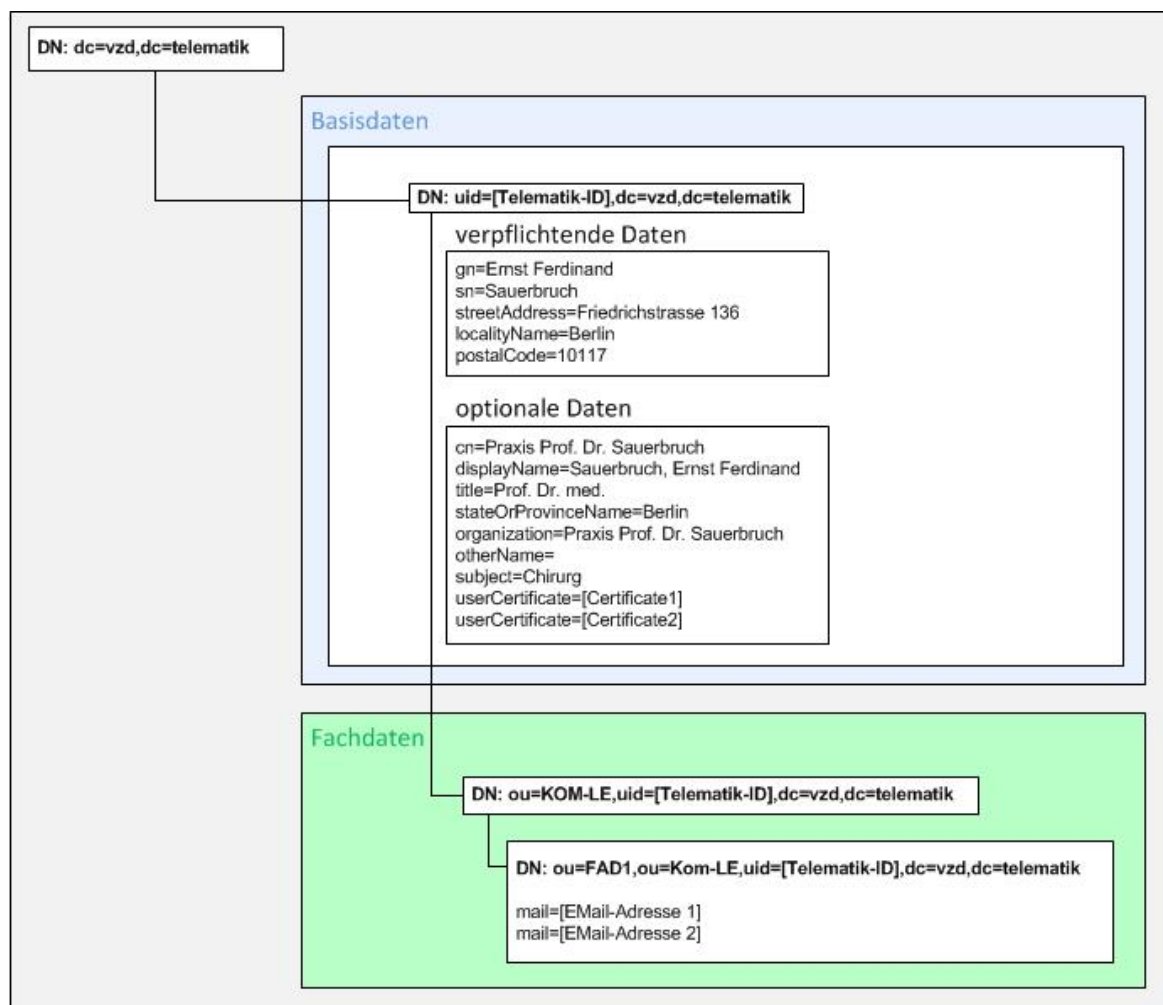


Abbildung 3: Abb\_VZD\_logisches\_Datenmodell

## TIP1-A\_5608 - VZD, Ordnungskriterium Datenmodell Verzeichnisdienst

~~Der VZD MUSS die Telematik-ID als Ordnungskriterium für das Datenmodell verwenden. Die Telematik-ID ist in den zu einem Basisdatensatz gehörenden Zertifikaten (im Feld registrationNumber der Extension Admission) enthalten.~~  
[<=]

## 6 Anhang A – Verzeichnisse

### 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
<b>GTI</b>	<b>Gesamtbetriebsverantwortlicher der TI</b>
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
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

## 6.2 Glossar

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

## 6.3 Abbildungsverzeichnis

Abbildung 1: Einordnung des VZD in die TI .....	7
Abbildung 2: Abb_VZD_logisches_Datenmodell .....	33
Abbildung 3: Abb_VZD_logisches_Datenmodell .....	37

## 6.4 Tabellenverzeichnis

Tabelle 1: Tab_PT_VZD_Schnittstellen .....	11
Tabelle 2: Tab_VZD_Schnittstelle_I_Directory_Query .....	11
Tabelle 3: Tab_TUC_VZD_0001 .....	13
Tabelle 4: Tab_VZD_Schnittstelle_I_Directory_Maintenance .....	13



Tabelle 5: VZD_TAB_addDirectoryEntry_Mapping .....	14
Tabelle 6: Tab_TUC_VZD_0002.....	16
Tabelle 7: VZD_TAB_readDirectoryEntry_Mapping .....	17
Tabelle 8: Tab_TUC_VZD_0003.....	18
Tabelle 9: VZD_TAB_modifyDirectoryEntry_Mapping.....	19
Tabelle 10: Tab_TUC_VZD_0004.....	20
Tabelle 11: Tab_TUC_VZD_0005.....	22
Tabelle 12: Tab_VZD_Schnittstelle_I_Directory_Application_Maintenance .....	23
Tabelle 13: VZD_TAB_I_Directory_Application_Maintenance_Add_Mapping.....	24
Tabelle 14: Tab_TUC_VZD_0006.....	25
Tabelle 15: VZD_TAB_KOM-LE_Attributes.....	26
Tabelle 16: Tab_TUC_VZD_0007.....	26
Tabelle 17: Tab_TUC_VZD_0008.....	27
Tabelle 18: Tab_TUC_VZD_0009.....	28
Tabelle 19: VZD_TAB_I_Directory_Application_Maintenance_Modify_Mapping.....	29
Tabelle 20: Tab_TUC_VZD_0010.....	30
Tabelle 21: VZD_TAB_KOM-LE_Attributes.....	30
Tabelle 22: Tab_TUC_VZD_0011.....	31
Tabelle 23 Tab_VZD_Datenbeschreibungmodell.....	33
Tabelle 24: Tab_VZD_Mapping_Eintragstyp_und_ProfessionOID.....	36

## 6.5 Referenzierte Dokumente

### 6.5.1 Dokumente der gematik

Die nachfolgende Tabelle enthält die Bezeichnung der in dem vorliegenden Dokument referenzierten Dokumente der gematik zur Telematikinfrastuktur. 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 Telematikinfrastuktur

[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

### 6.5.2 Weitere Dokumente

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[BSI-AIVZD]	Bundesamt für Sicherheit in der Informationstechnik: B 5.15 Allgemeiner Verzeichnisdienst, <a href="https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/content/baust/b05/b05015.html">https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/content/baust/b05/b05015.html</a>
[BSI-SiGw]	Bundesamt für Sicherheit in der Informationstechnik (o.J.): Konzeption von Sicherheitsgateways, Version 1.0
[RFC2119]	RFC 2119 (March 1997): Key words for use in RFCs to Indicate Requirement Levels <a href="http://www.rfc-editor.org/rfc/rfc2119.txt">http://www.rfc-editor.org/rfc/rfc2119.txt</a>
[RFC4510]	RFC 4510 (June 2006): Lightweight Directory Access Protocol (LDAP): Technical Specification Road Map, <a href="http://www.ietf.org/rfc/rfc4510.txt">http://www.ietf.org/rfc/rfc4510.txt</a>
[RFC4511]	RFC 4511 (June 2006): Lightweight Directory Access Protocol (LDAP): The Protocol, <a href="http://www.ietf.org/rfc/rfc4511.txt">http://www.ietf.org/rfc/rfc4511.txt</a>

[RFC4512]	RFC 4512 (June 2006): Lightweight Directory Access Protocol (LDAP): Directory Information Models <a href="http://www.rfc-editor.org/rfc/rfc4512.txt">http://www.rfc-editor.org/rfc/rfc4512.txt</a>
[RFC4513]	RFC 4513 (June 2006): Lightweight Directory Access Protocol (LDAP): Authentication Methods and Security Mechanisms <a href="http://www.rfc-editor.org/rfc/rfc4513.txt">http://www.rfc-editor.org/rfc/rfc4513.txt</a>
[RFC4514]	RFC 4514 (June 2006): Lightweight Directory Access Protocol (LDAP): String Representation of Distinguished Names <a href="http://www.rfc-editor.org/rfc/rfc4514.txt">http://www.rfc-editor.org/rfc/rfc4514.txt</a>
[RFC4515]	RFC 4515 (June 2006): Lightweight Directory Access Protocol (LDAP): String Representation of Search Filters <a href="http://www.rfc-editor.org/rfc/rfc4515.txt">http://www.rfc-editor.org/rfc/rfc4515.txt</a>
[RFC4516]	RFC 4516 (June 2006): Lightweight Directory Access Protocol (LDAP): Uniform Resource Locator <a href="http://www.rfc-editor.org/rfc/rfc4516.txt">http://www.rfc-editor.org/rfc/rfc4516.txt</a>
[RFC4517]	RFC 4517 (June 2006): Lightweight Directory Access Protocol (LDAP): Syntaxes and Matching Rules <a href="http://www.rfc-editor.org/rfc/rfc4515.txt">http://www.rfc-editor.org/rfc/rfc4515.txt</a>
[RFC4519]	RFC 4519 (June 2006): Lightweight Directory Access Protocol (LDAP): Schema for User Applications <a href="http://www.rfc-editor.org/rfc/rfc4519.txt">http://www.rfc-editor.org/rfc/rfc4519.txt</a>
[RFC4522]	RFC 4522 (June 2006): Lightweight Directory Access Protocol (LDAP): The Binary Encoding Option <a href="http://www.rfc-editor.org/rfc/rfc4522.txt">http://www.rfc-editor.org/rfc/rfc4522.txt</a>
[RFC4523]	RFC 4523 (June 2006): Lightweight Directory Access Protocol (LDAP) Schema Definitions for X.509 Certificates <a href="http://www.rfc-editor.org/rfc/rfc4523.txt">http://www.rfc-editor.org/rfc/rfc4523.txt</a>
[RFC6763]	RFC 6763 (February 2013): DNS-Based Service Discovery <a href="http://www.rfc-editor.org/rfc/rfc6763.txt">http://www.rfc-editor.org/rfc/rfc6763.txt</a>