

## Elektronische Gesundheitskarte und Telematikinfrastruktur

# Spezifikation Verzeichnisdienst

Version:	1. <del>11.1</del> 12.0
Revision:	<del>3092223</del> 29061
Stand:	<del>18.12.2020</del> 19.02.2021
Status:	freigegeben
Klassifizierung:	öffentlich
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
1.10.0	30.06.20		Anpassungen gemäß Änderungsliste P22.1 und Scope-Themen aus Systemdesign R4.0.0	gematik
1.11.0	12.11.20		Anpassungen gemäß Änderungsliste P22.2 und Scope-Themen aus Systemdesign R4.0.1	gematik
1.11.1	18.12.20		Einarbeitung der Änderungen gemäß P22.4	gematik
1.12.0	19.02.21		Anpassungen gemäß Änderungsliste P22.5; Korrekturen in der Beschreibung des Datenmodells sowie neue Operation zur Abfrage aller Daten über die REST-Schnittstelle.	gematik

## Inhaltsverzeichnis

<b>1 Einordnung des Dokumentes .....</b>	<b>7</b>
1.1 Zielsetzung .....	7
1.2 Zielgruppe .....	7
1.3 Geltungsbereich .....	7
1.4 Abgrenzungen .....	7
1.5 Methodik .....	8
<b>2 Systemüberblick .....</b>	<b>9</b>
<b>3 Übergreifende Festlegungen .....</b>	<b>10</b>
3.1 IT-Sicherheit und Datenschutz .....	10
3.2 Fachliche Anforderungen .....	11
<b>4 Funktionsmerkmale .....</b>	<b>13</b>
4.1 Schnittstelle I_Directory_Query .....	13
4.1.1 Operation search_Directory .....	14
4.1.1.1 Umsetzung .....	14
4.1.1.2 Nutzung .....	14
4.2 Schnittstelle I_Directory_Maintenance .....	15
4.2.1 Operation add_Directory_Entry .....	16
4.2.1.1 Umsetzung .....	16
4.2.1.2 Nutzung .....	19
4.2.2 Operation read_Directory_Entry .....	20
4.2.2.1 Umsetzung .....	20
4.2.2.2 Nutzung .....	21
4.2.3 Operation modify_Directory_Entry .....	22
4.2.3.1 Umsetzung .....	22
4.2.3.2 Nutzung .....	22
4.2.4 Operation delete_Directory_Entry .....	23
4.2.4.1 Umsetzung .....	23
4.2.4.2 Nutzung .....	23
4.3 Schnittstelle I_Directory_Application_Maintenance .....	25
4.3.1 Operation add_Directory_FA_Attributes .....	26
4.3.1.1 Umsetzung SOAP .....	26
4.3.1.2 Nutzung SOAP .....	27
4.3.1.3 Umsetzung LDAPv3 .....	28
4.3.1.4 Nutzung LDAPv3 .....	28
4.3.2 Operation delete_Directory_FA_Attributes .....	29
4.3.2.1 Umsetzung SOAP .....	29
4.3.2.2 Nutzung SOAP .....	30
4.3.2.3 Umsetzung LDAPv3 .....	30
4.3.2.4 Nutzung LDAPv3 .....	31
4.3.3 Operation modify_Directory_FA_Attributes .....	31
4.3.3.1 Umsetzung SOAP .....	32

4.3.3.2 Nutzung SOAP .....	32
4.3.3.3 Umsetzung LDAPv3 .....	33
4.3.3.4 Nutzung LDAPv3 .....	34
<b>4.4 Prozessschnittstelle P_Directory_Application_Registration (Provided) .....</b>	<b>34</b>
<b>4.5 Prozessschnittstelle P_Directory_Maintenance (Provided) .....</b>	<b>35</b>
<b>4.6 Schnittstelle I_Directory_Administration .....</b>	<b>35</b>
4.6.1 Operationen der Schnittstelle I_Directory_Administration .....	35
4.6.1.1 DirectoryEntry Administration .....	39
4.6.1.1.1 POST .....	39
4.6.1.1.2 GET .....	40
4.6.1.1.3 PUT .....	41
4.6.1.1.4 DELETE .....	44
4.6.1.2 Certificate Administration .....	45
4.6.1.2.1 POST .....	45
4.6.1.2.2 GET .....	46
4.6.2 Nutzung der Schnittstelle I_Directory_Administration .....	48
<b>4.7 Schnittstelle I_Directory_Search .....</b>	<b>49</b>
4.7.1 Operationen der Schnittstelle I_Directory_Search .....	49
4.7.1.1 GET (search_Directory_Entry) .....	51
4.7.1.2 GET (get_Directory_Entry) .....	52
<b>5 Datenmodell .....</b>	<b>54</b>
<b>6 Anhang A Verzeichnisse .....</b>	<b>61</b>
6.1 Abkürzungen .....	61
6.2 Glossar .....	62
6.3 Abbildungsverzeichnis .....	62
6.4 Tabellenverzeichnis .....	62
6.5 Referenzierte Dokumente .....	64
6.5.1 Dokumente der gematik .....	64
6.5.2 Weitere Dokumente .....	65
<b>1 Einordnung des Dokumentes .....</b>	<b>7</b>
1.1 Zielsetzung .....	7
1.2 Zielgruppe .....	7
1.3 Geltungsbereich .....	7
1.4 Abgrenzungen .....	7
1.5 Methodik .....	8
<b>2 Systemüberblick .....</b>	<b>9</b>
<b>3 Übergreifende Festlegungen .....</b>	<b>10</b>
3.1 IT-Sicherheit und Datenschutz .....	10

<b>3.2 Fachliche Anforderungen .....</b>	<b>11</b>
<b>4 Funktionsmerkmale .....</b>	<b>13</b>
<b>4.1 Schnittstelle I_Directory_Query .....</b>	<b>13</b>
4.1.1 Operation search_Directory .....	14
4.1.1.1 Umsetzung .....	14
4.1.1.2 Nutzung .....	14
<b>4.2 Schnittstelle I_Directory_Maintenance .....</b>	<b>15</b>
4.2.1 Operation add_Directory_Entry .....	16
4.2.1.1 Umsetzung .....	16
4.2.1.2 Nutzung .....	19
4.2.2 Operation read_Directory_Entry .....	20
4.2.2.1 Umsetzung .....	20
4.2.2.2 Nutzung .....	21
4.2.3 Operation modify_Directory_Entry .....	22
4.2.3.1 Umsetzung .....	22
4.2.3.2 Nutzung .....	22
4.2.4 Operation delete_Directory_Entry .....	23
4.2.4.1 Umsetzung .....	23
4.2.4.2 Nutzung .....	23
<b>4.3 Schnittstelle I_Directory_Application_Maintenance .....</b>	<b>25</b>
4.3.1 Operation add_Directory_FA-Attributes .....	26
4.3.1.1 Umsetzung SOAP .....	26
4.3.1.2 Nutzung SOAP .....	27
4.3.1.3 Umsetzung LDAPv3 .....	28
4.3.1.4 Nutzung LDAPv3 .....	28
4.3.2 Operation delete_Directory_FA-Attributes .....	29
4.3.2.1 Umsetzung SOAP .....	29
4.3.2.2 Nutzung SOAP .....	30
4.3.2.3 Umsetzung LDAPv3 .....	30
4.3.2.4 Nutzung LDAPv3 .....	31
4.3.3 Operation modify_Directory_FA-Attributes .....	31
4.3.3.1 Umsetzung SOAP .....	32
4.3.3.2 Nutzung SOAP .....	32
4.3.3.3 Umsetzung LDAPv3 .....	33
4.3.3.4 Nutzung LDAPv3 .....	34
<b>4.4 Prozessschnittstelle P_Directory_Application_Registration (Provided)...</b>	<b>34</b>
<b>4.5 Prozessschnittstelle P_Directory_Maintenance (Provided).....</b>	<b>35</b>
<b>4.6 Schnittstelle I_Directory_Administration .....</b>	<b>35</b>
4.6.1 Operationen der Schnittstelle I_Directory_Administration .....	35
4.6.1.1 DirectoryEntry Administration .....	39
4.6.1.1.1 POST .....	39
4.6.1.1.2 GET .....	40
4.6.1.1.3 PUT .....	41
4.6.1.1.4 DELETE .....	44
4.6.1.2 Certificate Administration .....	45
4.6.1.2.1 POST .....	45
4.6.1.2.2 GET .....	46

4.6.1.3 DirectoryEntry Synchronization .....	47
4.6.1.3.1 GET .....	47
4.6.2 Nutzung der Schnittstelle I_Directory_Administration .....	48
<b>5 Datenmodell .....</b>	<b>54</b>
<b>6 Anhang A – Verzeichnisse .....</b>	<b>61</b>
6.1 Abkürzungen .....	61
6.2 Glossar .....	62
6.3 Abbildungsverzeichnis .....	62
6.4 Tabellenverzeichnis .....	62
6.5 Referenzierte Dokumente .....	64
6.5.1 Dokumente der gematik .....	64
6.5.2 Weitere Dokumente .....	65

---

## 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

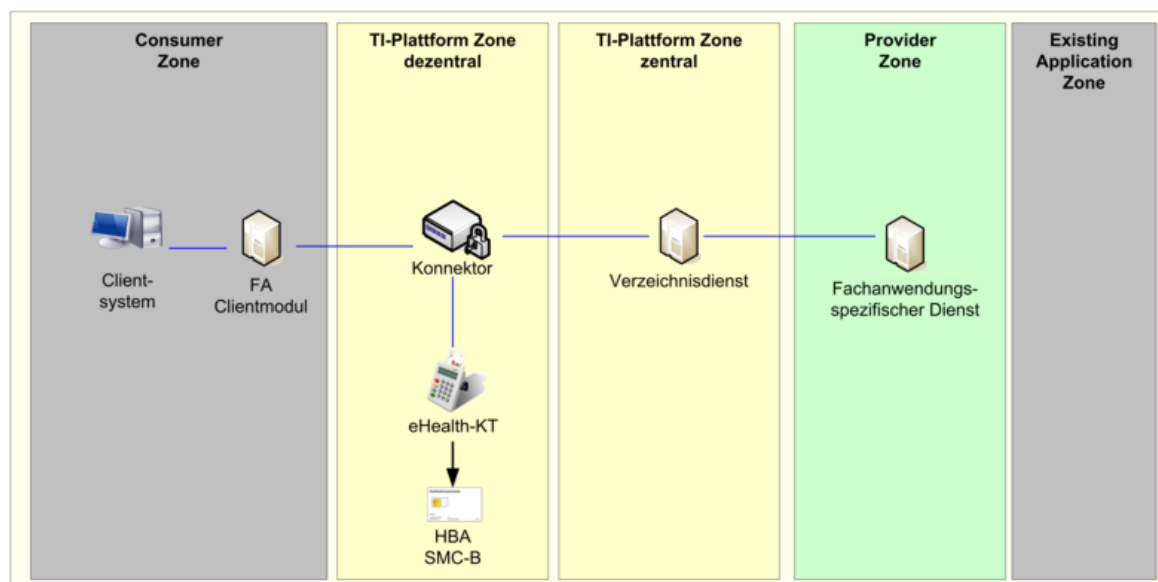
[<=]

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 (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.

---

## 3 Übergreifende Festlegungen

---

### 3.1 IT-Sicherheit und Datenschutz

#### **TIP1-A\_5546-01 - 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 APP.2.1], 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~~

~~3.2 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.~~

~~[<=]~~

### **3.3 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.

[<=]

## **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, dass 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.

[<=]

## **A\_20331 - VZD, Verhinderung LDAP Injection Attack**

Der VZD MUSS an allen Schnittstellen - welche LDAP nutzen bzw. auf LDAP abgebildet werden - LDAP Injection Attacks durch geeignete Sicherheitsprüfungen verhindern.

[<=]

## **A\_20262 - VZD, Maximale Anzahl von KOM-LE Adressen in den Fachdaten**

Der VZD MUSS bei dem Hinzufügen von KOM-LE Adressen in den Fachdaten folgende Regeln beachten:

- Wenn maxKOMLEadr im Verzeichniseintrag keinen Wert enthält, MUSS der VZD das Eintragen beliebig vieler KOM-LE Adressen in den Fachdaten erlauben.
- Wenn maxKOMLEadr im Verzeichniseintrag einen Wert enthält, MUSS der VZD das Eintragen von maximal so vielen KOM-LE Adressen in den Fachdaten erlauben.
- Wenn der Wert von maxKOMLEadr im Verzeichniseintrag gleich oder kleiner ist als die Anzahl der KOM-LE Adressen in den Fachdaten (z.B. falls der Wert herabgesetzt wurde), MUSS der VZD das Eintragen von weiteren KOM-LE Adressen in den Fachdaten ablehnen.

[<=]

## **A\_20263 - VZD, Kein automatisches Löschen von KOM-LE Adressen in den Fachdaten**

Der VZD DARF KOM-LE Adressen in den Fachdaten als Folge einer Änderung (Verkleinerung) des Attributwerts von maxKOMLEadr NICHT automatisch löschen.

[<=]

Der betroffene KOM-LE Teilnehmer muss in diesem Fall zusammen mit dem KOM-LE-Anbieter die nicht mehr benötigten KOM-LE Adressen löschen.

## 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
------	-------------------

<b>Version</b>	wird im Produkttypsteckbrief des VZD definiert	
<b>Operationen</b>	<b>Name</b>	<b>Kurzbeschreibung</b>
	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;=]

##### **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.

[&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.

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-Verbindungsaufbau 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.	

[<=]

## 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 Tab\_VZD\_Daten-Transformation und Tab\_VZD\_Datenbeschreibung den neuen Basisdatensatz.

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

[&lt;=]

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

Tabelle 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  SMC-B: Wird vom VZD als Kopie von otherName eingetragen.	surname	Verwendung gemäß Tab_VZD_Datenbeschreibung
n/a	cn  <del>SMC-B:</del> Wird vom VZD als Kopie von otherName eingetragen <del>HBA: wird vom VZD als Kopie von</del> <del>&lt;givenName&gt;</del> <del>&lt;sn&gt;</del> eingetragen.	commonName	Verwendung gemäß Tab_VZD_Datenbeschreibung
n/a	displayName  Wird vom VZD als Kopie von otherName eingetragen.	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 SMC-B: wird vom VZD zusätzlich in displayName, surname und cn eingetragen	otherName	Verwendung gemäß Tab_VZD_Datenbeschreibung
subject	specialization	subject	Verwendung gemäß Tab_VZD_Datenbeschreibung
n/a	domainID	n/a	
n/a	personalEntry	n/a	Verwendung gemäß Tab_VZD_Datenbeschreibung
x509CertificateEnc	userCertificate	x509CertificateEnc	Verwendung gemäß Tab_VZD_Datenbeschreibung
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	<del>Wenn der Eintrag von einem KOM-LE Fachdienst erzeugt oder geändert wird, dann muss das Attribut usage den Wert "KOM-LE"</del>

			erhalten-Verwendung gemäß Tab_VZD_Datenbeschreib ung
n/a	description	n/a	
timestamp	n/a	timestamp	Datum und Zeit des Requests bzw. der Response
variant	n/a HBA: Wenn variant == full, dann werden givenName und sn aus dem Zertifikat in die gleichnamigen LDAP Attribute übernommen.	n/a	
givenname	n/a	n/a	
surname	n/a	n/a	
commonName	n/a	n/a	
serviceData	n/a	n/a	
n/a	n/a	status	

#### 4.2.1.2 Nutzung

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

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

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

Der SOAP-Requests MUSS gemäß Tab\_VZD\_Datenbeschreibung mit der Bedeutung entsprechenden Daten ausgefüllt sein.

**Tabelle 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). 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>	

[&lt;=]

## 4.2.2 Operation read\_Directory\_Entry

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

### 4.2.2.1 Umsetzung

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

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

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

Es müssen die Fehlermeldungen gemäß Tab\_TUC\_VZD\_0003 verwendet werden.  
[<=]

#### 4.2.2.2 Nutzung

##### TIP1-A\_5578 - Nutzer der Schnittstelle, TUC\_VZD\_0003 „read\_Directory\_Entry“

Der Nutzer der Schnittstelle MUSS den technischen Use Case TUC\_VZD\_0003 „read\_Directory\_Entry“ gemäß Tabelle Tab\_TUC\_VZD\_0003 umsetzen. Der Webservice wird durch die Dokumente DirectoryMaintenance.wsdl und DirectoryMaintenance.xsd definiert.

Die SOAP-Response ist gemäß Tabelle Tab\_VZD\_Datenbeschreibung mit den zur Telematik-ID gehörenden Daten aus dem VZD ausgefüllt.

**Tabelle 7: 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>	<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 4221, faultstring: Operation fehlerhaft ausgeführt, Basisdaten konnten nicht gelesen werden (Fehler im Verzeichnisdienst)</p> <p>faultcode 4312, faultstring: Basisdaten konnten nicht gefunden werden</p> <p>faultcode 4202, faultstring: SOAP Request enthält Fehler</p> <p>Erkannte Fehler auf Transportprotokollebene müssen auf gematik SOAP Faults (Code 6 aus Tabelle Tab_Gen_Fehler</p>	

	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:

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.

[&lt;=]

#### 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 8: Tab\_TUC\_VZD\_0004**

<b>Name</b>	TUC_VZD_0004 „modify_Directory_Entry“	
<b>Beschreibung</b>	Diese Operation ermöglicht die Änderung von Basisdaten.	
<b>Vorbedingungen</b>	keine	
<b>Eingangsdaten</b>	SOAP-Request „modifyDirectoryEntry“	
<b>Komponenten</b>	Nutzer der Schnittstelle, Verzeichnisdienst	
<b>Ausgangsdaten</b>	SOAP-Response „responseMsg“	
<b>Standardablauf</b>	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>	<p>Es werden die protokollspezifischen Fehlermeldungen verwendet (TCP, HTTP, TLS)</p> <p>Fehler bei der Verarbeitung des SOAP Requests werden als gematik SOAP-Fault versendet:</p> <p>faultcode 4231, faultstring: Operation fehlerhaft ausgeführt, Basisdaten konnten nicht modifiziert werden (Fehler im Verzeichnisdienst)</p> <p>faultcode 4312, faultstring: Basisdaten konnten nicht gefunden werden</p> <p>faultcode 4202, faultstring: SOAP Request enthält Fehler</p> <p>Erkannte Fehler auf Transportprotokollebene müssen auf gematik SOAP Faults (Code 6 aus Tabelle Tab_Gen_Fehler aus [gemSpec_OM]) abgebildet werden. Zusätzlich müssen die generischen gematik SOAP-Faults</p> <p>Code 2: Verbindung zurückgewiesen</p> <p>Code 3: Nachrichtenschema fehlerhaft</p> <p>Code 4: Version Nachrichtenschema fehlerhaft unterstützt werden.</p>	

[&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 9: Tab\_TUC\_VZD\_0005**

<b>Name</b>	TUC_VZD_0005 „delete_Directory_Entry“	
<b>Beschreibung</b>	Diese Operation ermöglicht die Löschung von Basisdaten inkl. der zugehörigen Fachdaten.	
<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 10: 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>	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

[&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.

[<=]

#### **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 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:

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**

<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>	Aktion	Beschreibung
	Aufbau TLS-Verbindung	Falls noch keine TLS-Verbindung besteht, wird eine aufgebaut. Der FAD authentisiert sich mit ID.FD.TLS-C.
	SOAP-Request senden	Der FAD ruft die SOAP-Operation VZD:addDirectoryFAAttributes auf.

	SOAP-Response empfangen	Die SOAP-Response VZD:responseMsg enthält den vzd:status. Im Fehlerfall wird eine gematik SOAP-Fault Response empfangen
<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	

[&lt;=]

**TIP1-A\_5592-03 - FAD, KOM-LE\_FA\_Add\_Attributes**

Der FAD MUSS für die FA KOM-LE die Fachdaten nach VZD\_TAB\_KOM-LE\_Add\_Attributes administrieren.

**Tabelle 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	KOM-LE-Version

[&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 14: 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.  
[<=]

#### 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**

<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>	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
<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 4321, faultstring: Operation fehlerhaft ausgeführt, Fachdaten konnten nicht gelöscht werden (Fehler im Verzeichnisdienst)</p> <p>faultcode 4312, faultstring: Basisdaten konnten nicht gefunden werden</p> <p>faultcode 4202, faultstring: SOAP Request enthält Fehler</p>	

[<=]

#### 4.3.2.3 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**

<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>	<b>Aktion</b>	<b>Beschreibung</b>
	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.
<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.	

[<=]

#### 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**

<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>	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
<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	

[&lt;=]

**TIP1-A\_5601-03 - FAD, KOM-LE\_FA\_Modify\_Attributes**

Der FAD MUSS für die FA KOM-LE die Fachdaten nach VZD\_TAB\_KOM-LE\_Modify\_Attributes administrieren.

**Tabelle 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	KOM-LE-Version

[&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 20: 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.	

[<=]

#### 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 berechnete Organisationen (z.B. TSPs) zulässig. Sie dürfen alle Operationen zur Administration der Verzeichniseinträge nutzen.

Das ACCESS\_Token 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\_18371-02A\_18371-01 - 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**

<b>Name</b>	<b>I_Directory_Administration</b>	
<b>Version</b>	wird im Produkttypsteckbrief des VZD definiert	
<b>Operationen</b>	<b>Resource: DirectoryEntry</b>	
	<b>Name</b>	<b>Kurzbeschreibung</b>
	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).
	<b>Resource: /DirectoryEntriesSync</b>	
	<b>Name</b>	<b>Kurzbeschreibung</b>
	GET	Abfrage aller Daten von Verzeichniseinträgen zu Synchronisationszwecken.
	<b>Resource: Certificate</b>	
	<b>Name</b>	<b>Kurzbeschreibung</b>
	POST	Hinzufügen eines Zertifikatseintrags zu einem Verzeichniseintrag.
	GET	Abfrage von Zertifikatseinträgen.

[<=]

**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.

[<=]

**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\_20267 - VZD, I\_Directory\_Administration, Registrierung beim IdP als Relying Party**

Der Anbieter des VZD MUSS sich über einen organisatorischen Prozess bei einem vertrauenswürdigen Identity Provider (IDP) der Telematikinfrastruktur als Relying Party registrieren und die Bereitstellung der folgenden Claims in für Nutzer ausgestellte ACCESS\_TOKEN mit dem IDP vereinbaren:

- name
- sub
- scope
- acr

damit der VZD die Fachlogik der Autorisierung und Protokollierung auf diesen Attributen umsetzen kann.

[<=]

**A\_20268 - VZD, Authentifizierung Nutzerrolle**

Der VZD MUSS die fachliche Rolle eines Nutzers in jedem Operationsaufruf der Schnittstelle I\_Directory\_Administration anhand des Attributs "scope" im übergebenen ACCESS\_TOKEN feststellen und für die nachfolgende Rollenprüfung je Operationsaufruf verwenden. [<=]

**A\_20269 - VZD, Authentifizierung Nutzernamen**

Der VZD MUSS den Namen eines Nutzers in jedem Operationsaufruf anhand des Attributs "name" im übergebenen ACCESS\_TOKEN feststellen und für die Protokollierung des Zugriffs verwenden. [<=]

**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 - VZD, I\_Directory\_Administration, Datenquelle**

Der VZD MUSS bei den Operationen add\_Directory\_Entry und modify\_Directory\_Entry das LDAP-Directory-Attribut 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 - VZD, I\_Directory\_Administration, Doubletten**

Der VZD MUSS bei den Operationen add\_Directory\_Entry und 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“**

<b>Name</b>	add_Directory_Entry	
<b>Beschreibung</b>	Diese Operation ermöglicht die Erzeugung eines neuen Eintrags im LDAP-Verzeichnis.	
<b>Eingangsdaten</b>	REST-Request POST /DirectoryEntries operationId: add_Directory_Entry (siehe DirectoryAdministration.yaml)	
	<b>Parameter</b>	<b>Beschreibung</b>
	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.
<b>Komponenten</b>	Nutzer der Schnittstelle, Verzeichnisdienst	
<b>Ausgangsdaten</b>	REST-Response mit dem Distinguished Name (dn) von dem Verzeichnisdienst_Eintrag.	
<b>Ablauf</b>	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.	

<b>Fehlerfälle</b>	Es werden die protokollspezifischen Fehlermeldungen verwendet (TCP, HTTP, TLS) und in DirectoryAdministration.yaml mit spezifischen Fehlerbeschreibungen ergänzt.
--------------------	---

[&lt;=]

#### A\_20271-01 - VZD, I\_Directory\_Administration, add\_Directory\_Entry, holder setzen

~~A\_20271 - VZD, I\_Directory\_Administration, add\_Directory\_Entry, owner setzen~~ Der VZD MUSS bei Operation „add\_Directory\_Entry“ den Eigentümer des erzeugten Verzeichniseintrags im Attribut "ownerholder" entsprechend folgenden Vorgaben setzen:

- Ist im add\_Directory\_Entry Request das Attribut "ownerholder" nicht vorhanden oder enthält keine Werte:
  - Wird vom VZD aus dem ACCESS\_TOKEN claim scope der Wert entnommen und als "ownerholder" in dieses Attribut eingetragen.
- Ist im add\_Directory\_Entry Request das Attribut "ownerholder" vorhanden und mit Inhalten gefüllt
  - a. Ist ein Wert aus dem Request Attribut "ownerholder" nicht gültig, MUSS der VZD die Operation mit HTTP-Status-Code 422 abweisen und die weitere Verarbeitung von diesem Request abbrechen.
  - b. Sind alle Werte aus dem Request Attribut "ownerholder" gültig, MUSS der VZD die Werte aus dem Request entnehmen und sie in das "ownerholder" Attribut des Verzeichniseintrags übernehmen.

[&lt;=]

#### 4.6.1.1.2 GET

Diese Operation liest Verzeichniseinträge aus dem LDAP-Verzeichnis.

#### A\_18449-03A-18449-01 - 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“**

<b>Name</b>	read_Directory_Entry	
<b>Beschreibung</b>	Diese Operation ermöglicht die Suche und Lesen von Verzeichniseinträgen im LDAP-Verzeichnis. Diese Operation liefert ( <del>im Gegensatz zu TIP1-A_5547/search_Directory</del> ) auch Einträge, die ohne gültige Zertifikate sind.	
<b>Eingangsdaten</b>	REST-Request GET /DirectoryEntries operationId: read_Directory_Entry (siehe DirectoryAdministration.yaml)	
	<b>Parameter</b>	<b>Beschreibung</b>
	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.
<b>Komponenten</b>	Nutzer der Schnittstelle, Verzeichnisdienst
<b>Ausgangsdaten</b>	REST-Response mit allen zu den Filterparametern passenden Verzeichniseinträgen. Die Verzeichniseinträge werden <b>optional</b> inklusive Zertifikatseinträgen und Fachdaten geliefert.
<b>Ablauf</b>	Der VZD sucht im LDAP-Verzeichnis die zu den Suchparametern passenden Verzeichniseinträge. Bei mehr als 100 gefundenen Einträgen werden nur 100 gefundenen Einträge zurückgegeben.
<b>Fehlerfälle</b>	Es werden die protokollspezifischen Fehlermeldungen verwendet (TCP, HTTP, TLS) und in DirectoryAdministration.yaml mit spezifischen Fehlerbeschreibungen ergänzt.

[&lt;=]

#### ~~A\_20399 – VZD, I\_Directory\_Administration, read\_Directory\_Entry, Paging~~

~~4.6.1.1.3 Der VZD MUSS für Operation „read\_Directory\_Entry“ einen Mechanismus zum Paging von Suchergebnissen (analog zu [RFC2696]) für eigene Verzeichniseinträge bereitstellen. [<=]~~

#### ~~A\_20402 – VZD, I\_Directory\_Administration, read\_Directory\_Entry, Paging, Berechtigung~~

~~Der VZD MUSS für den Paging-Mechanismus von Operation „read\_Directory\_Entry“ sicherstellen:~~

- ~~• Der "owner"-Suchparameter muss den gleichen Wert enthalten wie der ACCESS\_TOKEN claim scope~~
- ~~• Die pagingSize darf die Maximalgröße entsprechend TIP1 A\_5552 nicht überschreiten~~
- ~~• Die Suchparameter dürfen sich während eines Pagings (mit mehreren Request/Response-Sequenzen) nicht ändern (nur das "cookie" ändert sich).~~

~~4.6.1.1.44.6.1.1.3 Bei Abweichungen von diesen Festlegungen MUSS der VZD mit einem Fehler (HTTP Status Code 403) antworten. [<=]~~

#### ~~4.6.1.1.54.6.1.1.4 PUT~~

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

#### ~~A\_18450-03A\_18450-01 - 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“

<b>Name</b>	modify_Directory_Entry	
<b>Beschreibung</b>	Diese Operation ermöglicht die Aktualisierung von Verzeichniseinträgen im LDAP-Verzeichnis.	
<b>Eingangsdaten</b>	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.
	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.
	stateOrProvinceName	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.
	ownerholder	Kann optional angegeben werden. Durch setzen des "ownerholder" kann ein Verzeichniseintrag an einen anderen Eigentümer weitergegeben werden. Die Weitergabe kann nur durch den aktuellen Eigentümer/ownerholder erfolgen.
	maxKOMLEadr	Kann optional angegeben werden. Durch setzen von "maxKOMLEadr" wird die maximale Anzahl von mail Adressen in den KOM-LE Fachdaten festgelegt.
<b>Komponenten</b>	Nutzer der Schnittstelle, Verzeichnisdienst	
<b>Ausgangsdaten</b>	REST-Response mit dem Distinguished Name (dn) von dem aktualisierten Verzeichnisdienst_Eintrag.	
<b>Ablauf</b>	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.	
<b>Fehlerfälle</b>	Es werden die protokollspezifischen Fehlermeldungen verwendet (TCP, HTTP, TLS) und in DirectoryAdministration.yaml mit spezifischen Fehlerbeschreibungen ergänzt.	

[&lt;=]

#### **A\_20272-02A\_20272 - VZD, I\_Directory\_Administration, modify\_Directory\_Entry, Zugriffsrechte**

Der VZD MUSS bei Operation „modify\_Directory\_Entry“ für den - über Parameter uid adressierten - Verzeichniseintrag das Attribut "ownerholder" im gespeicherten Verzeichniseintrag und die aktuellen Parameter ("ownerholder" und ACCESS\_TOKEN claim scope) der Operation „modify\_Directory\_Entry“ prüfen:

- Wurde im Request Parameters "ownerholder" ein Wert angegeben, der keinen aktuell gültigen Wert für Schnittstelle I\_Directory\_Administration entspricht, MUSS der VZD die Operation mit HTTP-Status-Code 422 abweisen.
- Ist im Attribut "ownerholder" im gespeicherten Verzeichniseintrags mindestens ein Wert vorhanden
  - MUSS der VZD die Operation auszuführen und die übergebenen Werte - nach Prüfung ihrer Gültigkeit - in den Verzeichniseintrag übernehmen

wenn der Wert von dem ACCESS\_TOKEN claim scope einem Wert des Attributs "ownerholder" des gespeicherten Verzeichniseintrags entspricht. Ist dies nicht der Fall, MUSS der VZD die Operation mit HTTP-Status-Code 401 abweisen.

- Ist im Attribut "ownerholder" im gespeicherten Verzeichniseintrags kein Wert vorhanden und
- in der Operation „modify\_Directory\_Entry“ wurden Werte für dieses "ownerholder" Attribut übergeben, MUSS der VZD die Operation ausführen und diese Werte - nach Prüfung ihrer Gültigkeit - in den Verzeichniseintrag übernehmen.
- in der Operation „modify\_Directory\_Entry“ wurde kein Wert für dieses "ownerholder" Attribut übergeben, MUSS der VZD die Operation ausführen und den Wert von dem ACCESS\_TOKEN claim scope in das Attribut "ownerholder" des Verzeichniseintrags übernehmen.

[<=]

#### 4.6.1.1.64.6.1.1.5 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“

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

[<=]

### **A\_20273-01A\_20273 - VZD, I\_Directory\_Administration, delete\_Directory\_Entry, Zugriffsrechte**

Der VZD MUSS bei Operation „delete\_Directory\_Entry“ für den - über Parameter uid adressierten - Verzeichniseintrag das Attribut "ownerholder" im gespeicherten Verzeichniseintrag gegen die aktuellen Parameter der Operation „delete\_Directory\_Entry“ prüfen:

- Enthalten die Werte des Attributs "ownerholder" im gespeicherten Verzeichniseintrag den Wert von dem ACCESS\_TOKEN claim scope, MUSS der VZD die Operation ausführen.
- Enthält das Attributs "ownerholder" im gespeicherten Verzeichniseintrag keine Werte, MUSS der VZD die Operation ausführen.
- Enthalten die Werte des Attributs "ownerholder" im gespeicherten Verzeichniseintrag nicht den Wert von dem ACCESS\_TOKEN claim scope, MUSS der VZD die Operation mit HTTP-Status-Code 401 abweisen.

[<=]

## **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.

**Tabelle 26: Tab\_VZD „add\_Directory\_Entry\_Certificate“**

<b>Name</b>	add_Directory_Entry_Certificate	
<b>Beschreibung</b>	Diese Operation fügt einem existierenden Basisdatensatz einen Zertifikatseintrag im LDAP-Verzeichnis an.	
<b>Eingangsdaten</b>	REST-Request POST /DirectoryEntries/{uid}/Certificates operationId: add_Directory_Entry_Certificate (siehe DirectoryAdministration.yaml)	
	<b>Parameter</b>	<b>Beschreibung</b>
	uid	Die „uid“ identifiziert den Verzeichnisdienst_Eintrag (Abb_VZD_logisches_Datenmodell) an welchen der Zertifikatseintrag angehängen wird.
	userCertificate	Muss angegeben werden und enthält das Zertifikat.
	usage	Kann optional belegt werden.
	description	Kann optional belegt werden.

<b>Komponenten</b>	Nutzer der Schnittstelle, Verzeichnisdienst
<b>Ausgangsdaten</b>	REST-Response mit dem Distinguished Name (dn) von dem erzeugten Certificate-Eintrag.
<b>Ablauf</b>	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.
<b>Fehlerfälle</b>	Es werden die protokollspezifischen Fehlermeldungen verwendet (TCP, HTTP, TLS) und in DirectoryAdministration.yaml mit spezifischen Fehlerbeschreibungen ergänzt.

[&lt;=]

#### 4.6.1.2.2 GET

Diese Operation liest Zertifikatseinträge aus dem LDAP-Verzeichnis.

#### **A\_18453-01 - 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“**

<b>Name</b>	read_Directory_Certificates	
<b>Beschreibung</b>	Diese Operation ermöglicht die Suche und das Lesen von Zertifikatseinträgen (Certificate in Abb_VZD_logisches_Datenmodell) im LDAP-Verzeichnis.	
<b>Eingangsdaten</b>	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 TelematikID.
<b>Komponenten</b>	Nutzer der Schnittstelle, Verzeichnisdienst	
<b>Ausgangsdaten</b>	REST-Response mit allen zu den Filter Parametern passenden Zertifikatseinträgen.	
<b>Ablauf</b>	Der VZD sucht im LDAP Verzeichnis die zu den Such-Parametern passenden Zertifikatseinträge. Bei mehr als 100 gefundenen Einträgen werden nur 100 gefundenen Einträge zurückgegeben.	
<b>Fehlerfälle</b>	Es werden die protokollspezifischen Fehlermeldungen verwendet (TCP, HTTP, TLS) und in DirectoryAdministration.yaml mit spezifischen Fehlerbeschreibungen ergänzt.	

[&lt;=]

#### 4.6.1.3 DirectoryEntry Synchronization

Zur Unterstützung der Pflege der Basiseinträge (Verzeichnisdienst\_Eintrag) wird die hier beschriebene Operation zur Verfügung gestellt. Sie dient der Synchronisation mit dem Datenbestand des Verzeichnisdienstes und erlaubt – im Gegensatz zur Operation „read\_Directory\_Entry“ – das Lesen beliebig vieler eigener Verzeichniseinträge.

##### 4.6.1.3.1 GET

#### A\_21230-01 - VZD, I\_Directory\_Administration, read\_Directory\_Entry\_for\_Sync

Der VZD MUSS Operation „read\_Directory\_Entry\_for\_Sync“ gemäß Tabelle Tab\_VZD „read\_Directory\_Entry\_for\_Sync“ umsetzen.

**Tabelle 28:** Tab\_VZD „read\_Directory\_Entry\_for\_Sync“

<b>Name</b>	read_Directory_Entry_for_Sync	
<b>Beschreibung</b>	Diese Operation ermöglicht die Suche und Lesen von Verzeichniseinträgen im LDAP-Verzeichnis. Diese Operation liefert auch Einträge, die ohne gültige Zertifikate sind.	
<b>Eingangsdaten</b>	REST-Request GET /DirectoryEntries operationId: read_Directory_Entry (siehe DirectoryAdministration.yaml)	
	<b>Parameter</b>	<b>Beschreibung</b>
	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.
<b>Komponenten</b>	Nutzer der Schnittstelle, Verzeichnisdienst
<b>Ausgangsdaten</b>	REST-Response mit allen zu den Filterparametern passenden Verzeichniseinträgen. Die Verzeichniseinträge werden optional inklusive Zertifikatseinträgen und Fachdaten geliefert.
<b>Ablauf</b>	Der VZD sucht im LDAP-Verzeichnis die zu den Suchparametern passenden Verzeichniseinträge. Bei mehr als 100 gefundenen Einträgen werden nur 100 gefundene Einträge zurückgegeben. Wenn über den "holder"-Suchparameter nach eigenen Verzeichniseinträgen oder Verzeichniseinträgen ohne gesetztes "holder"-Attribut gesucht wird, werden alle Suchergebnisse zurückgegeben.
<b>Fehlerfälle</b>	Es werden die protokollspezifischen Fehlermeldungen verwendet (TCP, HTTP, TLS) und in DirectoryAdministration.yaml mit spezifischen Fehlerbeschreibungen ergänzt.

[&lt;=]

#### **A\_20402-02 - VZD, I\_Directory\_Administration, read\_Directory\_Entry\_for\_Sync, Paging, Berechtigung**

Der VZD MUSS für den Paging Mechanismus von Operation „read\_Directory\_Entry\_for\_Sync“ sicherstellen:

- Der "holder" Suchparameter muss den gleichen Wert enthalten wie der ACCESS\_TOKEN claim scope.
- Die pagingSize darf die Maximalgröße entsprechend TIP1-A\_5552 nicht überschreiten.
- Die Suchparameter dürfen sich während eines Pagings (mit mehreren Request/Response Sequenzen) nicht ändern (nur das "cookie" ändert sich).

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

[&lt;=]

### **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)

- 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 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. Diese wird im Internet nach Authentifizierung des Clients bereitgestellt.

### ~~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 28: Tab\_VZD\_Schnittstelle\_I\_Directory\_Search\_FQDN**

Resource-Record Typ	Beschreibung
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 im Folgenden festgelegten Ressourcen sind 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 29: 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.

[&lt;=]

**A\_19506—VZD, Schnittstelle Search**

Der VZD MUSS die Schnittstelle I\_Directory\_Search als REST-Webservice über HTTPS implementieren. Der Webservice ist durch das Dokument DirectorySearch.yaml definiert.

[&lt;=]

**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.

[&lt;=]

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 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 ~~aer~~ im übergebenen IdP-Token im HTTP-Header "Authorization" auf dem Authentifizierungsniveau "niedrig" gemäß Verordnung (EU) Nr. 910/2014 (eIDAS-Verordnung) feststellen und einen anderen Wert, der einem Authentifizierungsniveau unterhalb von "<http://eidas.europa.eu/LoA/low>" entspricht bzw. ungültig ist, 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. [~~<=~~]

**~~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. [~~<=~~]

**~~A\_20164—VZD, I\_Directory\_Search, Organization~~**

Der VZD MUSS mit den Operationen an der Schnittstelle I\_Directory\_Search gewährleisten, dass nur Organisationen (entryType == 3 | 4 | 5) als Ergebnis geliefert werden. [~~<=~~]

**4.7.1.1 GET (search\_Directory\_Entry)**

Diese Operation sucht/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 30: Tab\_VZD „search\_Directory\_Entry

<b>Name</b>	search_Directory_Entry	
<b>Beschreibung</b>	Diese Operation ermöglicht die Suche und das Lesen von Verzeichniseinträgen im LDAP-Verzeichnis.	
<b>Eingangsdaten</b>	REST-Request GET /Organization operationId: search_Directory_Entry (siehe DirectorySearch.yaml)	
	<b>Parameter</b>	<b>Beschreibung</b>
	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 <a href="https://www.hl7.org/fhir/search.html">https://www.hl7.org/fhir/search.html</a> . Die angegebenen Parameter werden zur Suche mit einem logischen UND verknüpft.
<b>Komponenten</b>	Nutzer der Schnittstelle, Verzeichnisdienst	
<b>Ausgangsdaten</b>	REST-Response mit allen zu den Suchparametern passenden Verzeichniseinträgen entsprechend DirectorySearch.yaml und [HL7FHIR] Resource Bundle.	
<b>Ablauf</b>	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.	
<b>Fehlerfälle</b>	Es werden die protokollspezifischen Fehlermeldungen verwendet (TCP, HTTP, TLS) und in DirectorySearch.yaml mit spezifischen Fehlerbeschreibungen ergänzt.	

[&lt;=]

**4.7.1.2 GET (get\_Directory\_Entry)**

Diese Operation liest den adressierten Verzeichniseintrag aus dem Verzeichnisdienst.

**A\_20139—VZD, I\_Directory\_Search, get\_Directory\_Entry**

Der VZD MUSS die Operation „get\_Directory\_Entry“ gemäß Tabelle Tab\_VZD „get\_Directory\_Entry“ umsetzen.

Tabelle 31: Tab\_VZD „get\_Directory\_Entry

<b>Name</b>	get_Directory_Entry
-------------	---------------------

<b>Beschreibung</b>	Diese Operation ermöglicht das Lesen eines Verzeichniseintrags im LDAP-Verzeichnis.	
<b>Eingangsdaten</b>	REST-Request GET /Organization/{uid} operationId: get_Directory_Entry (siehe DirectorySearch.yaml)	
	<b>Parameter</b>	<b>Beschreibung</b>
	Parameter zur Selektion des Verzeichniseintrags	Der Verzeichniseintrag wird über den {uid}-Parameter im Pfad adressiert.
<b>Komponenten</b>	Nutzer der Schnittstelle, Verzeichnisdienst	
<b>Ausgangsdaten</b>	REST-Response mit dem über die {uid}-adressierten Verzeichniseintrag entsprechend DirectorySearch.yaml.	
<b>Ablauf</b>	Der VZD gibt aus dem LDAP-Verzeichnis den über die {uid}-adressierten Verzeichniseintrag zurück.	
<b>Fehlerfälle</b>	Es werden die protokollspezifischen Fehlermeldungen verwendet (TCP, HTTP, TLS) und in DirectorySearch.yaml mit spezifischen Fehlerbeschreibungen ergänzt.	

{&lt;=}

---

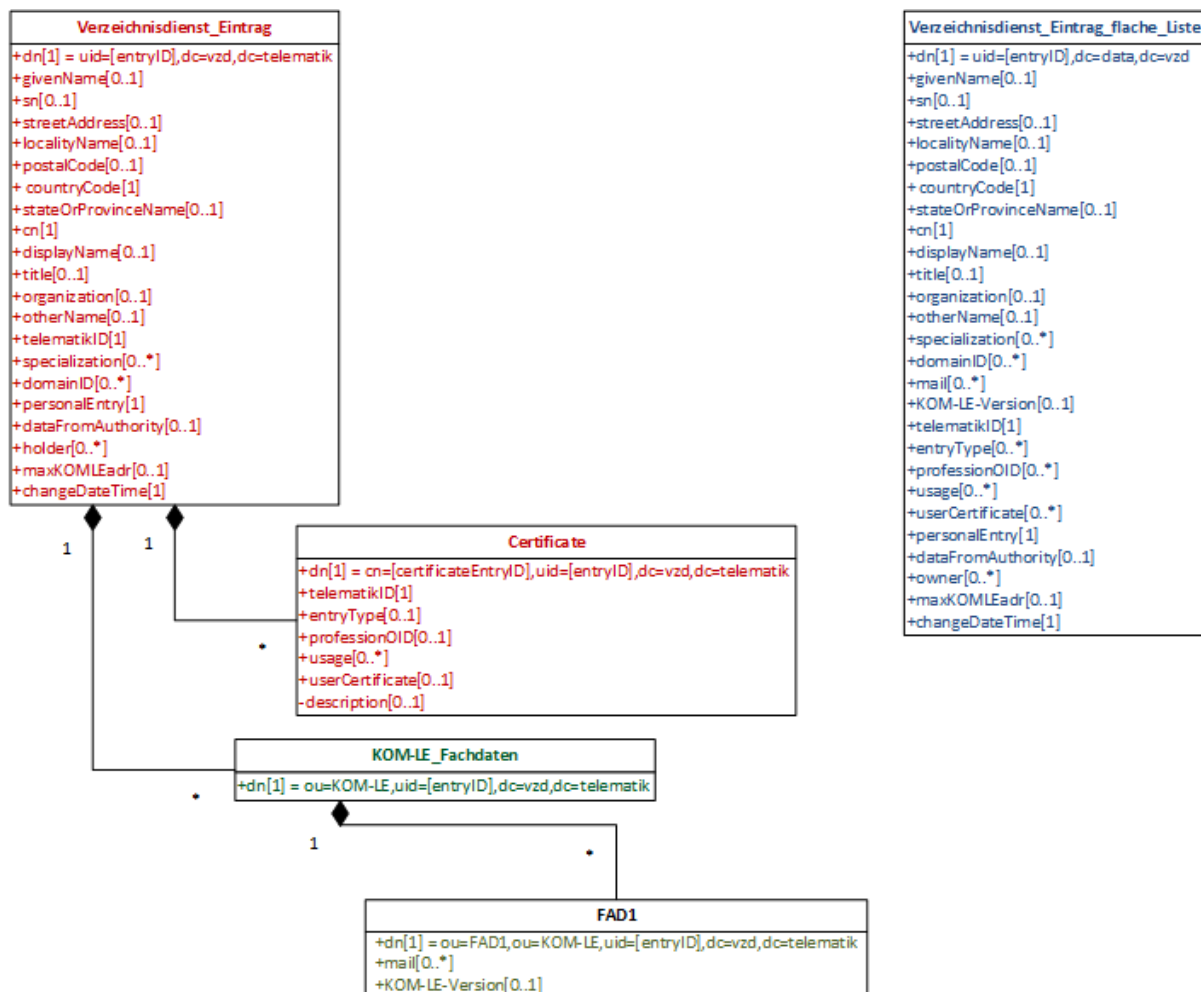
## 5 Datenmodell

---

**TIP1-A\_5607-04TIP1-A\_5607-01 - VZD, logisches Datenmodell**

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

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



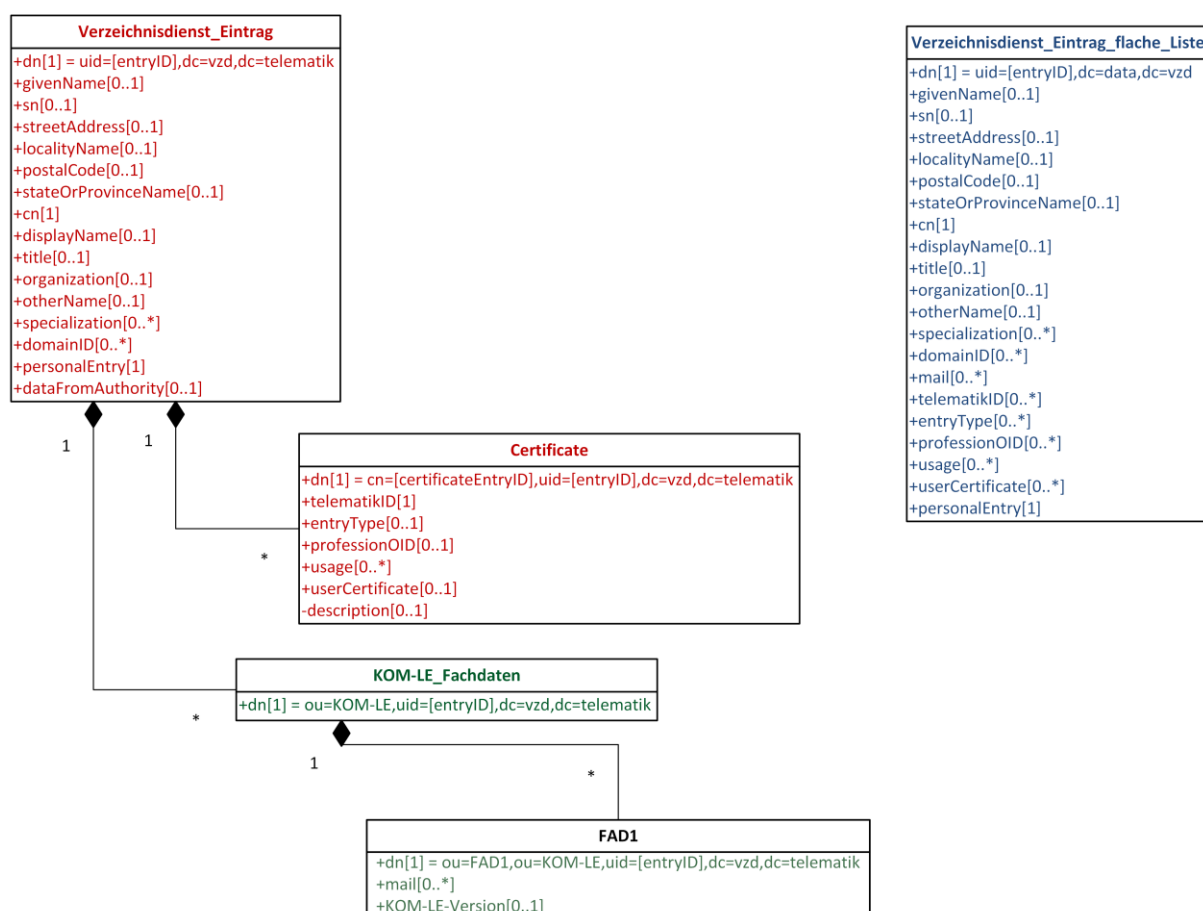


Abbildung 2: Abb\_VZD\_logisches\_Datenmodell

Tabelle 29: Tab\_VZD\_Datenbeschreibung

LDAP-Directory Attribut	Pflichtfeld?	Erläuterung
givenName	optional	HBA-Eintrag: Bezeichner: Vorname, <del>obligatorisch</del> , wird vom VZD aus dem Zertifikat übernommen. SMC-B-Eintrag: wird nicht verwendet
sn	optional	HBA-Eintrag: Bezeichner: Name, wird vom VZD aus dem Zertifikat übernommen SMC-B Eintrag: Wird vom VZD als Kopie des Attributs displayName übernommen. <del>Wird von E-Mail Clients für die Suche nach Einträgen und die Anzeige von gefundenen Einträgen verwendet.</del>
cn	obligatorisch	HBA: Eintrag: Bezeichner: <del>Vorname und</del> Nachname, Vorname SMC-B Eintrag: Bezeichner: Name Wird vom VZD <del>unabhängig vom Kartentyp</del> als Kopie des Attributs displayName übernommen. Wird von E-Mail Clients für die Suche nach Einträgen und die Anzeige von gefundenen Einträgen verwendet.

displayName	optional	Bezeichner: Anzeigename, Name nach dem der Eintrag von Nutzern gesucht wird und unter dem gefundene Einträge angezeigt werden. <a href="#">Konvention für HBA Einträge: Name, Vorname</a>
streetAddress	optional	Bezeichner: Straße und Hausnummer
postalCode	optional	Bezeichner: Postleitzahl
countryCode	obligatorisch	Kann beim Anlegen des Datensatzes und beim Ändern gesetzt werden (falls nicht gesetzt, ergänzt der VZD den Defaultwert für Deutschland).
localityName	optional	Bezeichner: Ort
stateOrProvinceName	optional	Bezeichner: Bundesland oder Region
title	optional	HBA: Bezeichner: Titel SMC-B: nicht verwendet
organization	optional	HBA: Bezeichner: Name der Organisation oder Name der Betriebsstätte SMC-B: Alternativer Name nach dem der Eintrag von Nutzern gesucht wird und unter dem gefundene Einträge angezeigt werden
otherName	optional	Bezeichner: Anderer Name <del>Wird vom VZD aus dem Zertifikatsattribut otherName übernommen.</del> Veraltet: Wird für die Suche nach Einträgen und die Anzeige von gefundenen Einträgen nicht benötigt (siehe displayName und organization)
specialization	optional	Bezeichner: Fachgebiet Kann mehrfach vorkommen (1..100).  <b>Für Einträge der Leistungserbringerorganisationen (SMC-B Eintrag)</b> Der Wertebereich entspricht den in hl7 definierten und für ePA festgelegten Werten ( <a href="https://wiki.hl7.de/index.php?title=IG:Value_Sets_f%C3%BCr_XDS#DocumentEntry.practiceSettingCode">https://wiki.hl7.de/index.php?title=IG:Value_Sets_f%C3%BCr_XDS#DocumentEntry.practiceSettingCode</a> ). urn:psc:<OID Codesystem:Code> Beispiel für Allgemeinmedizin: urn:psc:1.3.6.1.4.1.19376.3.276.1.5.4:ALLG  <b>Für Einträge der Leistungserbringer (HBA-Eintrag)</b> Der Wertebereich entspricht den in hl7 definierten Werten ( <a href="https://wiki.hl7.de/index.php?title=IG:Value_Sets_f%C3%BCr_XDS#DocumentEntry.authorSpecialty">https://wiki.hl7.de/index.php?title=IG:Value_Sets_f%C3%BCr_XDS#DocumentEntry.authorSpecialty</a> ). urn:as:<OID Codesystem:Code> Beispiel für FA Allgemeinmedizin: urn:as:1.2.276.0.76.5.114:010

domainID	optional	Bezeichner: domänenspezifisches Kennzeichen des Eintrags. kann mehrfach vorkommen (0..100)
ownerholder	obligatorisch optional	<del>Wird vom VZD eingetragen. Identifiziert den Eigentümer dieses Verzeichniseintrags, der Änderungen an ihm vornehmen darf. Der Wert wird beim Anlegen eines neuen Verzeichniseintrags von VZD aus dem ACCESS_TOKEN claim scope entnommen.</del> Legt fest, wer Änderungen an den Basisdaten des Eintrags vornehmen darf. Hat keinen Einfluss auf Fachdaten und Zertifikatsdaten.
maxKOMLEadr	optional	Maximale Anzahl von mail Adressen in den KOM-LE- Fachdaten. Falls kein Wert eingetragen wurde, können beliebig viele mail Adressen in den KOM-LE Fachdaten eingetragen werden. Falls ein Wert eingetragen wurde, können maximal so viele mail Adressen in den KOM-LE Fachdaten eingetragen werden.
personalEntry	obligatorisch	Wird vom VZD eingetragen Wert == TRUE, wenn 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. Ist in den Basisdaten und in den Zertifikatsdaten enthalten.

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)
usage	optional	Bezeichner: Nutzungskennzeichnung kann pro Zertifikat mehrfach (0..100) vergeben werden <del>vorgegebener Wertebereich [KOM-LE, ePA, eFA]</del> Hinweis: wird <del>aktuell für ePA und KOM-LE</del> 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) Wird vom KOM-LE-Fachdienst-Anbieter eingetragen.
KOM-LE-Version	optional	Bezeichner: KOM-LE-Version Enthält die KOM-LE-Version des Clientmoduls der angegebenen "mail" Adresse. Anhand dieser Version erkennt das sendende Clientmodul, welche KOM-LE-Version vom Empfänger-Clientmodul unterstützt wird und in welchem Format die Mail an diesen Empfänger versandt wird. Wenn nicht angegeben, wird KOM-LE-Version 1.0 angenommen.
changeDateT ime	obligatorisch	Der VZD setzt dieses Attribut bei jeder Schreiboperation für den Datensatz (Basisdaten) auf die aktuelle Zeit. Format entsprechend RFC 3339, section 5.6.

[&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 30: 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)
<b>6</b>	<b>Krankenkasse ePA</b>	1.2.276.0.76.4.XXX (ePA KTR-Zugriffsautorisierung)

---

## 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
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

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	Telematikinfrastuktur
TIP	Telematikinfrastuktur-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.....	9
Abbildung 2: Abb_VZD_logisches_Datenmodell.....	56
Abbildung 1: Einordnung des VZD in die TI.....	9
Abbildung 2: Abb_VZD_logisches_Datenmodell.....	56

## 6.4 Tabellenverzeichnis

Tabelle 1: Tab_PT_VZD_Schnittstellen.....	13
---	----

Tabelle 2: Tab_VZD_Schnittstelle_I_Directory_Query .....	13
Tabelle 3: Tab_TUC_VZD_0001 .....	15
Tabelle 4: Tab_VZD_Schnittstelle_I_Directory_Maintenance .....	15
Tabelle 5: Tab_VZD_Daten_Transformation .....	17
Tabelle 6: Tab_TUC_VZD_0002 .....	19
Tabelle 7: Tab_TUC_VZD_0003 .....	21
Tabelle 8: Tab_TUC_VZD_0004 .....	22
Tabelle 9: Tab_TUC_VZD_0005 .....	24
Tabelle 10: Tab_VZD_Schnittstelle_I_Directory_Application_Maintenance .....	25
Tabelle 11: VZD_TAB_I_Directory_Application_Maintenance_Add_Mapping .....	27
Tabelle 12: Tab_TUC_VZD_0006 .....	27
Tabelle 13: VZD_TAB_KOM_LE_Attributes .....	28
Tabelle 14: Tab_TUC_VZD_0007 .....	29
Tabelle 15: Tab_TUC_VZD_0008 .....	30
Tabelle 16: Tab_TUC_VZD_0009 .....	31
Tabelle 17: VZD_TAB_I_Directory_Application_Maintenance_Modify_Mapping .....	32
Tabelle 18: Tab_TUC_VZD_0010 .....	32
Tabelle 19: VZD_TAB_KOM_LE_Attributes .....	33
Tabelle 20: Tab_TUC_VZD_0011 .....	34
Tabelle 21: Tab_VZD_Schnittstelle_I_Directory_Administration .....	36
Tabelle 22: Tab_VZD „add_Directory_Entry“ .....	39
Tabelle 23: Tab_VZD „read_Directory_Entry“ .....	40
Tabelle 24: Tab_VZD „modify_Directory_Entry“ .....	42
Tabelle 25: Tab_VZD „delete_Directory_Entry“ .....	44
Tabelle 26: Tab_VZD „add_Directory_Entry_Certificate“ .....	45
Tabelle 27: Tab_VZD „read_Directory_Certificates“ .....	46
Tabelle 28: Tab_VZD_Schnittstelle_I_Directory_Search_FQDN .....	49
Tabelle 29: Tab_VZD_Schnittstelle_I_Directory_Search .....	50
Tabelle 30: Tab_VZD „search_Directory_Entry“ .....	52
Tabelle 31: Tab_VZD „get_Directory_Entry“ .....	52
Tabelle 32: Tab_VZD_Datenbeschreibung .....	56
Tabelle 33: Tab_VZD_Mapping_Eintragstyp_und_ProfessionOID .....	59
Tabelle 1: Tab_PT_VZD_Schnittstellen .....	13
Tabelle 2: Tab_VZD_Schnittstelle_I_Directory_Query .....	13
Tabelle 3: Tab_TUC_VZD_0001 .....	15
Tabelle 4: Tab_VZD_Schnittstelle_I_Directory_Maintenance .....	15

Tabelle 5: Tab_VZD_Daten-Transformation .....	17
Tabelle 6: Tab_TUC_VZD_0002 .....	19
Tabelle 7: Tab_TUC_VZD_0003 .....	21
Tabelle 8: Tab_TUC_VZD_0004 .....	22
Tabelle 9: Tab_TUC_VZD_0005 .....	24
Tabelle 10: Tab_VZD_Schnittstelle_I_Directory_Application_Maintenance .....	25
Tabelle 11: VZD_TAB_I_Directory_Application_Maintenance_Add_Mapping .....	27
Tabelle 12: Tab_TUC_VZD_0006 .....	27
Tabelle 13: VZD_TAB_KOM-LE_Attributes.....	28
Tabelle 14: Tab_TUC_VZD_0007 .....	29
Tabelle 15: Tab_TUC_VZD_0008 .....	30
Tabelle 16: Tab_TUC_VZD_0009 .....	31
Tabelle 17: VZD_TAB_I_Directory_Application_Maintenance_Modify_Mapping.....	32
Tabelle 18: Tab_TUC_VZD_0010 .....	32
Tabelle 19: VZD_TAB_KOM-LE_Attributes.....	33
Tabelle 20: Tab_TUC_VZD_0011 .....	34
Tabelle 21: Tab_VZD_Schnittstelle_I_Directory_Administration .....	36
Tabelle 22: Tab_VZD „add_Directory_Entry“ .....	39
Tabelle 23: Tab_VZD „read_Directory_Entry“ .....	40
Tabelle 24: Tab_VZD „modify_Directory_Entry“.....	42
Tabelle 25: Tab_VZD „delete_Directory_Entry“ .....	44
Tabelle 26: Tab_VZD „add_Directory_Entry_Certificate“ .....	45
Tabelle 27: Tab_VZD „read_Directory_Certificates“.....	46
Tabelle 28: Tab_VZD „read_Directory_Entry_for_Sync“ .....	47
Tabelle 29: Tab_VZD_Datenbeschreibung.....	56
Tabelle 30: Tab_VZD_Mapping_Eintragstyp_und_ProfessionOID.....	59

## 6.5 Referenzierte Dokumente

### 6.5.1 Dokumente der gematik

Die nachfolgende Tabelle enthält die Bezeichnung der in dem vorliegenden Dokument referenzierten Dokumente der gematik zur Telematikinfrastruktur. Der mit der vorliegenden Version korrelierende Entwicklungsstand dieser Konzepte und Spezifikationen wird pro Release in einer Dokumentenlandkarte definiert; Version und Stand der referenzierten Dokumente sind daher in der nachfolgenden Tabelle nicht aufgeführt. Deren zu diesem Dokument jeweils gültige Versionsnummern sind in der

aktuellen, von der gematik veröffentlichten Dokumentenlandkarte enthalten, in der die vorliegende Version aufgeführt wird.

<b>[Quelle]</b>	<b>Herausgeber: Titel</b>
[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

<b>[Quelle]</b>	<b>Herausgeber (Erscheinungsdatum): Titel</b>
[BSI APP.2.1]	Bundesamt für Sicherheit in der Informationstechnik: BSI Grundsatz-Kompendium, Baustein APP.2.1, <a href="https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/APP/APP_2_1_Allgemeiner_Verzeichnisdienst.html">https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/APP/APP_2_1_Allgemeiner_Verzeichnisdienst.html</a>
[BSI-SiGw]	Bundesamt für Sicherheit in der Informationstechnik (o.J.): Konzeption von Sicherheitsgateways, Version 1.0
[HL7FHIR]	FHIR Specification <a href="https://www.hl7.org/fhir/">https://www.hl7.org/fhir/</a>

[RFC2 119]	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>
[RFC2 696]	RFC 2696 (September 1999) LDAP Control Extension for Simple Paged Results Manipulation <a href="https://tools.ietf.org/html/rfc2696">https://tools.ietf.org/html/rfc2696</a>
[RFC4 510]	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>
[RFC4 511]	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>
[RFC4 512]	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>
[RFC4 513]	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>
[RFC4 514]	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>
[RFC4 515]	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>
[RFC4 516]	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>

[RFC4 517]	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>
[RFC4 519]	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>
[RFC4 522]	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>
[RFC4 523]	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>
[ <a href="#">RFC 6750</a> ]	The OAuth 2.0 Authorization Framework: Bearer Token Usage
[RFC6 763]	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>