

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

11 Elektronische Gesundheitskarte und Telematikinfrastruktur

20 Spezifikation

21 Verzeichnisdienst

22
23
24
25
26

Version:	1.13.1 14.0 CC
Revision:	357080 381567
Stand:	20.04 07.07.2021
Status:	<u>zur Abstimmung</u> freigegeben
Klassifizierung:	öffentlich <u>Entwurf</u>
Referenzierung:	gemSpec_VZD

27

Dokumentinformationen

Änderungen zur Vorversion

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

31

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
1.13.0	06.04.21		Anpassungen gemäß Änderungsliste KIM_Maintenance_21.1/ KIM 1.5.1	gematik

1.13.1	20.04.21		Anpassung C_10533 aus KIM_Maintenance_21.1 vervollständigt (TIP1-A_5586 entfernt)	gematik
<u>1.14.0</u> <u>CC</u>	<u>07.07.21</u>		<u>Anpassung gemäß C_10737, unter anderem:</u> <ul style="list-style-type: none"> • <u>Prüfung auf Gültigkeit der Zertifikate wird auf die korrekte PKI-Umgebung ausgeweitet</u> • <u>Enc-Zertifikate werden überprüft</u> • <u>Erhöhung möglicher KIM-Mail-Einträge von 100 auf 1.000</u> • <u>Erhöhung des Limits möglicher Zertifikate von 50 auf 100</u> • <u>Erweiterung der möglichen Basisdaten auf 1 Mio. Einträge</u> • <u>Ergänzung einer Operation für Schnittstellen I Directory Application Maintenance und I Directory Administration, welche Auskunft über die Version der Schnittstelle gibt</u> • <u>Die Attribute professionOID und entryType wurden im Datenmodell - zur besseren Suchbarkeit - in die Basisdaten gespiegelt</u> • <u>Das Limit für Attribut professionOID wurde auf 100 aktualisiert</u> • <u>Operation zum Löschen von Zertifikatseinträgen ergänzt</u> 	gematik

33

Inhaltsverzeichnis

34	<u>1 Einordnung des Dokumentes</u>	<u>6</u>
35	<u>1.1 Zielsetzung</u>	<u>6</u>
36	<u>1.2 Zielgruppe</u>	<u>6</u>
37	<u>1.3 Geltungsbereich</u>	<u>6</u>
38	<u>1.4 Abgrenzungen</u>	<u>6</u>
39	<u>1.5 Methodik</u>	<u>7</u>
40	<u>2 Systemüberblick</u>	<u>8</u>
41	<u>3 Übergreifende Festlegungen</u>	<u>9</u>
42	<u>3.1 IT-Sicherheit und Datenschutz</u>	<u>9</u>
43	<u>3.2 Fachliche Anforderungen</u>	<u>10</u>
44	<u>4 Funktionsmerkmale</u>	<u>12</u>
45	<u>4.1 Schnittstelle I Directory Query</u>	<u>12</u>
46	4.1.1 Operation search Directory	13
47	4.1.1.1 Umsetzung	13
48	4.1.1.2 Nutzung	13
49	<u>4.2 Schnittstelle I Directory Maintenance</u>	<u>14</u>
50	4.2.1 Operation add Directory Entry	15
51	4.2.1.1 Umsetzung	15
52	4.2.1.2 Nutzung	18
53	4.2.2 Operation read Directory Entry	19
54	4.2.2.1 Umsetzung	19
55	4.2.2.2 Nutzung	20
56	4.2.3 Operation modify Directory Entry	21
57	4.2.3.1 Umsetzung	21
58	4.2.3.2 Nutzung	21
59	4.2.4 Operation delete Directory Entry	22
60	4.2.4.1 Umsetzung	22
61	4.2.4.2 Nutzung	22
62	<u>4.3 Schnittstelle I Directory Application Maintenance</u>	<u>24</u>
63	4.3.1 Operation getInfo	26
64	4.3.1.1 Umsetzung REST	26
65	4.3.1.2 Nutzung REST	26
66	4.3.2 Operation add Directory FA-Attributes	27
67	4.3.2.1 Umsetzung SOAP	27
68	4.3.2.2 Nutzung SOAP	28
69	4.3.2.3 Umsetzung LDAPv3	29
70	4.3.2.4 Nutzung LDAPv3	29
71	4.3.2.5 Umsetzung REST	30
72	4.3.2.6 Nutzung REST	31
73	4.3.3 Operation delete Directory FA-Attributes	32
74	4.3.3.1 Umsetzung SOAP	32

75	<i>4.3.3.2 Nutzung SOAP</i>	<i>32</i>
76	<i>4.3.3.3 Umsetzung LDAPv3</i>	<i>33</i>
77	<i>4.3.3.4 Nutzung LDAPv3</i>	<i>33</i>
78	<i>4.3.3.5 Umsetzung REST.....</i>	<i>34</i>
79	<i>4.3.3.6 Nutzung REST.....</i>	<i>34</i>
80	<i>4.3.4 Operation modify Directory FA-Attributes</i>	<i>35</i>
81	<i>4.3.4.1 Umsetzung SOAP</i>	<i>35</i>
82	<i>4.3.4.2 Nutzung SOAP</i>	<i>36</i>
83	<i>4.3.4.3 Umsetzung LDAPv3</i>	<i>37</i>
84	<i>4.3.4.4 Nutzung LDAPv3</i>	<i>37</i>
85	<i>4.3.4.5 Umsetzung REST.....</i>	<i>38</i>
86	<i>4.3.4.6 Nutzung REST.....</i>	<i>38</i>
87	<i>4.3.5 Operation get Directory FA-Attributes</i>	<i>39</i>
88	<i>4.3.5.1 Umsetzung REST.....</i>	<i>39</i>
89	<i>4.3.5.2 Nutzung REST.....</i>	<i>39</i>
90	<u>4.4 Prozessschnittstelle P Directory Application Registration (Provided)...</u>	<u>40</u>
91	<u>4.5 Prozessschnittstelle P Directory Maintenance (Provided).....</u>	<u>40</u>
92	<u>4.6 Schnittstelle I Directory Administration</u>	<u>41</u>
93	<i>4.6.1 Operationen der Schnittstelle I Directory Administration.....</i>	<i>41</i>
94	<i>4.6.1.1 I Directory Administration - Lesen der Metadaten</i>	<i>44</i>
95	<i>4.6.1.1.1 GET</i>	<i>44</i>
96	<i>4.6.1.2 DirectoryEntry Administration</i>	<i>45</i>
97	<i>4.6.1.2.1 POST</i>	<i>45</i>
98	<i>4.6.1.2.2 GET</i>	<i>47</i>
99	<i>4.6.1.2.3 PUT</i>	<i>48</i>
100	<i>4.6.1.2.4 DELETE</i>	<i>51</i>
101	<i>4.6.1.3 Certificate Administration</i>	<i>52</i>
102	<i>4.6.1.3.1 POST</i>	<i>52</i>
103	<i>4.6.1.3.2 GET</i>	<i>53</i>
104	<i>4.6.1.3.3 DELETE</i>	<i>54</i>
105	<i>4.6.1.4 DirectoryEntry Synchronization</i>	<i>55</i>
106	<i>4.6.1.4.1 GET</i>	<i>55</i>
107	<i>4.6.2 Nutzung der Schnittstelle I Directory Administration</i>	<i>56</i>
108	<u>5 Datenmodell</u>	<u>58</u>
109	<u>6 Anhang A – Verzeichnisse</u>	<u>65</u>
110	<u>6.1 Abkürzungen</u>	<u>65</u>
111	<u>6.2 Glossar</u>	<u>66</u>
112	<u>6.3 Abbildungsverzeichnis.....</u>	<u>66</u>
113	<u>6.4 Tabellenverzeichnis</u>	<u>66</u>
114	<u>6.5 Referenzierte Dokumente</u>	<u>68</u>
115	<i>6.5.1 Dokumente der gematik.....</i>	<i>68</i>
116	<i>6.5.2 Weitere Dokumente.....</i>	<i>68</i>
117		

118

1 Einordnung des Dokumentes

1.1 Zielsetzung

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

122 Der VZD ist ein zentraler Dienst der TI-Plattform.

123 Das Informationsmodell des VZD ist erweiterbar.

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

1.2 Zielgruppe

127 Das Dokument ist maßgeblich für Anbieter und Hersteller von Verzeichnisdiensten

1.3 Geltungsbereich

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

134

1.3.1 Schutzrechts-/Patentrechtshinweis

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

1.4 Abgrenzungen

145 Spezifiziert werden in dem Dokument die von dem Produkttyp bereitgestellten
146 (angebotenen) Schnittstellen. Benutzte Schnittstellen werden hingegen in der
147 Spezifikation desjenigen Produkttypen beschrieben, der diese Schnittstelle bereitstellt.
148 Auf die entsprechenden Dokumente wird verwiesen (siehe auch 6. Anhang A.1.1
149 Verzeichnisse).

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

153 Nicht Bestandteil des vorliegenden Dokumentes sind die Festlegungen zum
154 Themenbereich

155 • Werkzeuge für Fachdienstanbieter, die die Administration von
156 fachdienstspezifischen Daten unterstützen.

157 **1.5 Methodik**

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

162 Sie werden im Dokument wie folgt dargestellt:

163 **<AFO-ID> - <Titel der Afo>**

164 Text / Beschreibung

165 [**<=**]

166

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

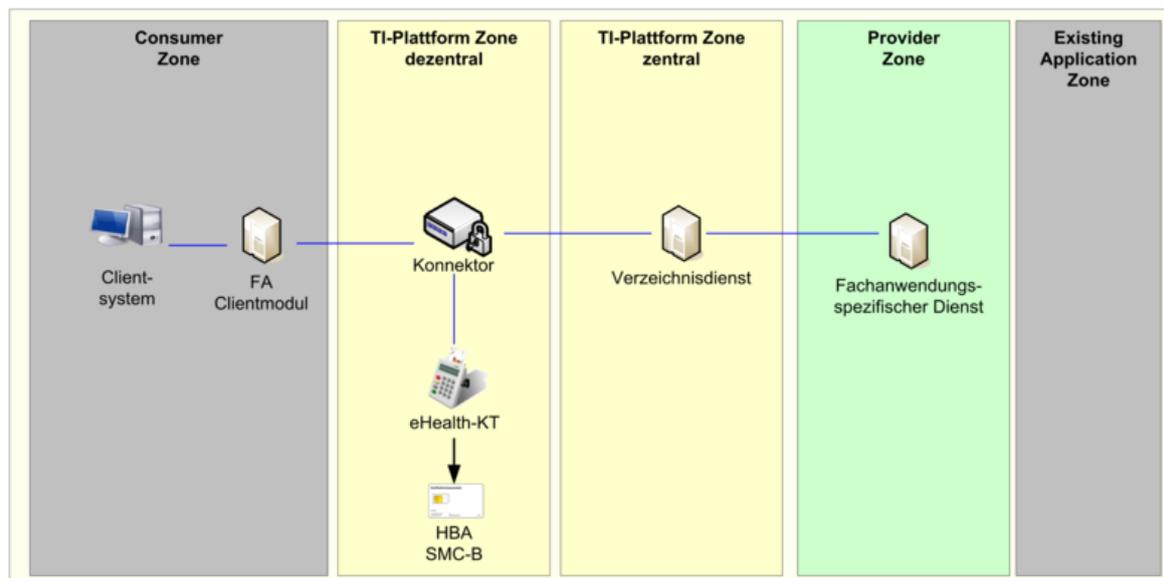
169 Für die Erzeugung der Abbildungen und Informationsmodelle wird das Tool „Enterprise
170 Architect“ verwendet.

171

2 Systemüberblick

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

173



174

175

Abbildung 1: Einordnung des VZD in die TI

176

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

178 Die Dateneinträge werden erstellt und gepflegt:

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

185 Der VZD kann durch LDAP-Clients abgefragt werden.

186

187

3 Übergreifende Festlegungen

3.1 IT-Sicherheit und Datenschutz

189 TIP1-A_5546-01 - VZD, Integritäts- u. Authentizitätsschutz
190 Der Anbieter des VZD MUSS die Integrität und Authentizität der im VZD gespeicherten
191 Daten gemäß den Richtlinien des Bundesamtes für Sicherheit in der Informationstechnik
192 für allgemeine Verzeichnisdienste, [BSI APP.2.1], implementieren. [<=]

193 TIP1-A_5547 - VZD, Löschen ungültiger Zertifikate
194 Der VZD MUSS täglich die gespeicherten Zertifikate nach Ablaufdatum (TUC_PKI_002
195 „Gültigkeitsprüfung des Zertifikats“) und Status (TUC_PKI_006 "OCSP-Abfrage) prüfen.
196 Ungültige Zertifikate werden sofort gelöscht. Ein Eintrag ohne gültige Zertifikate wird
197 nach einem Jahr gelöscht und darf nicht durch eine Anfrage über die Operation
198 search_Directory der Schnittstelle I_Directory_Query gefunden werden.
199 [<=]

200 Zum Beispiel dürfen gültige RU-/TU-Zertifikate nicht in der PU akzeptiert werden. Die
201 Prüfung über TUC PKI 018 berücksichtigt entsprechend
202 dem initialisierten Vertrauensanker (aus der jeweiligen Umgebung) die Umgebung.

203 A 21808 - VZD, Hinzufügen von professionOID und entryType in die Basisdaten
204 Der VZD MUSS beim Hinzufügen von Zertifikaten prüfen, ob der Wert der enthaltenen
205 professionOID bzw. entryType schon in den Basisdaten vorhanden ist. Falls nicht, MUSS
206 der VZD diese professionOID bzw. entryType zu den existierenden Basisdaten
207 hinzufügen. [<=]

208 A 21809 - VZD, Löschen von professionOID und entryType aus den Basisdaten
209 Der VZD MUSS gewährleisten, dass nach dem Löschen von Zertifikaten für die Attribute
210 professionOID und entryType in den Basisdaten nur Werte aus den verbleibenden
211 Zertifikaten erhalten bleiben. [<=]

212
213 TIP1-A_5548 - VZD, Protokollierung der Änderungsoperationen
214 Der VZD MUSS Änderungen der Verzeichnisdiensteinträge protokollieren und muss sie 6
215 Monate zur Verfügung halten.
216 [<=]

217 6 Monate ist die maximale Nachweistiefe ohne in den Bereich der
218 Vorratsdatenspeicherung zu kommen.

219 TIP1-A_5549 - VZD, Keine Leseprofilbildung
220 Der VZD DARF Suchanfragen NICHT speichern oder protokollieren.
221 [<=]

222 TIP1-A_5550 - VZD, Keine Kopien von gelöschten Daten
223 Der VZD DARF von gelöschten Daten KEINE Kopien speichern.
224 [<=]

225 TIP1-A_5551 - VZD, Sicher gegen Datenverlust
226 Der Anbieter des VZD MUSS den Dienst gegen Datenverlust absichern.
227 [<=]

228 TIP1-A_5552 - VZD, Begrenzung der Suchergebnisse

- 229 Der VZD MUSS die Ergebnisliste einer Suchanfrage auf 100 Suchergebnisse begrenzen.
230 [**<=**]
- 231 TIP1-A_5553 - VZD, Private Schlüssel sicher speichern
232 Der VZD MUSS seine privaten Schlüssel sicher speichern und ihr Auslesen verhindern um
233 Manipulationen zu verhindern.
234 [**<=**]
- 235 TIP1-A_5554 - VZD, Registrierungsdaten sicher speichern
236 Der VZD MUSS die Integrität und Authentizität der gespeicherten Registrierungsdaten
237 der FAD gewährleisten.
238 [**<=**]
- 239 TIP1-A_5555 - VZD, SOAP-Fehlercodes
240 Der VZD MUSS für seine SOAP-Schnittstelle die generischen Fehlercodes
- 241 • Code 2: Verbindung zurückgewiesen
242 • Code 3: Nachrichtenschema fehlerhaft
243 • Code 4: Version Nachrichtenschema fehlerhaft
244 • Code 6: Protokollfehler
- 245 aus Tabelle Tab_Gen_Fehler aus [gemSpec_OM] im SOAP-Fault verwenden. Erkannte
246 Fehler auf Transportprotokollebene müssen auf gematik SOAP Faults (Code 6 aus Tabelle
247 Tab_Gen_Fehler aus [gemSpec_OM]) abgebildet werden.
248
249 [**<=**]
- 250 TIP1-A_5556 - VZD, Fehler Logging
251 Der VZD MUSS lokal und remote erkannte Fehler in seinem lokalen Speicher
252 protokollieren.
253 [**<=**]
- 254 TIP1-A_5557 - VZD, Unterstützung IPv4 und IPv6
255 Der VZD MUSS IPv4 und IPv6 für alle seine IP-Schnittstellen im Dual-Stack-Mode
256 unterstützen.
257 [**<=**]
- 258 TIP1-A_5558 - VZD, Sicheres Speichern der TSL
259 Der VZD MUSS die Inhalte der TSL in einem lokalen Trust Store sicher speichern und für
260 X.509-Zertifikatsprüfungen lokal zugreifbar halten.
261 [**<=**]

262 **3.2 Fachliche Anforderungen**

- 263 TIP1-A_5560 - VZD, Erweiterbarkeit für neue Fachdaten
264 Der Anbieter des VZD MUSS die Erweiterbarkeit des VZD für die Aufnahme der Fachdaten
265 neuer Fachanwendungen gewährleisten.
266 [**<=**]
- 267 TIP1-A_5561 - VZD, DNS-SD
268 Der Anbieter des VZD MUSS alle erforderlichen Einträge zur Dienstlokalisierung der
269 Außenschnittstellen gemäß [RFC6763] beginnend mit folgenden PTR Resource Record-
270 Bezeichnern im Namensdienst der TI-Plattform anlegen:
- 271 • für den Zugriff auf die Schnittstelle I_Directory_Query:
272 _ldap._tcp.vzd.telematik.

- 273 • für den Zugriff auf die Schnittstelle I_Directory_Maintenance:
274 _vzd-bd._tcp.vzd.telematik.
- 275 • für den Zugriff auf die Schnittstelle I_Directory_Application_Maintenance:
276 _vzd-fd._tcp.vzd.telematik.
- 277 [**<=**]
- 278 TIP1-A_5562 - VZD, Parallele Zugriffe
279 Der Betreiber des VZD MUSS sicherstellen, dass Benutzer gleichzeitig auf den VZD
280 zugreifen können. Dies umfasst alle technischen Schnittstellen. In [gemSpec_Perf] ist die
281 Anzahl der parallelen Zugriffe definiert.
282 [**<=**]
- 283 ~~TIP1-A_5563-01~~ **TIP1-A_5563** - VZD, Erhöhung der Anzahl der Einträge
284 Der Anbieter des VZD MUSS sicherstellen ~~das 500~~, dass 1.000.000 Einträge gespeichert
285 werden können.
286 [**<=**]
- 287 TIP1-A_5620 - VZD, Nicht-Speicherung von Leading und Trailing Spaces
288 Der Anbieter des VZD MUSS Leading und Trailing Spaces abschneiden.
289 [**<=**]
- 290 A_20331 - VZD, Verhinderung LDAP Injection Attack
291 Der VZD MUSS an allen Schnittstellen - welche LDAP nutzen bzw. auf LDAP abgebildet
292 werden - LDAP Injection Attacks durch geeignete Sicherheitsprüfungen verhindern.
293 [**<=**]
- 294 A_20262 - VZD, Maximale Anzahl von KOM-LE Adressen in den Fachdaten
295 Der VZD MUSS bei dem Hinzufügen von KOM-LE Adressen in den Fachdaten folgende
296 Regeln beachten:
- 297 • Wenn maxKOMLEadr im Verzeichniseintrag keinen Wert enthält, MUSS der VZD
298 das Eintragen beliebig vieler KOM-LE Adressen in den Fachdaten erlauben.
 - 299 • Wenn maxKOMLEadr im Verzeichniseintrag einen Wert enthält, MUSS der VZD das
300 Eintragen von maximal so vielen KOM-LE Adressen in den Fachdaten erlauben.
 - 301 • Wenn der Wert von maxKOMLEadr im Verzeichniseintrag gleich oder kleiner ist als
302 die Anzahl der KOM-LE Adressen in den Fachdaten (z.B. falls der Wert
303 heruntersetzt wurde), MUSS der VZD das Eintragen von weiteren KOM-LE
304 Adressen in den Fachdaten ablehnen.
- 305 [**<=**]
- 306 A_20263 - VZD, Kein automatisches Löschen von KOM-LE Adressen in den Fachdaten
307 Der VZD DARF KOM-LE Adressen in den Fachdaten als Folge einer Änderung
308 (Verkleinerung) des Attributwerts von maxKOMLEadr NICHT automatisch löschen.
309 [**<=**]
- 310 Der betroffene KOM-LE Teilnehmer muss in diesem Fall zusammen mit dem KOM-LE-
311 Anbieter die nicht mehr benötigten KOM-LE Adressen löschen.
- 312

313

4 Funktionsmerkmale

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

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

321 TIP1-A_5564 - VZD, Festlegung der Schnittstellen
 322 Der VZD MUSS die Schnittstellen gemäß Tabelle Tab_PT_VZD_Schnittstellen
 323 implementieren („bereitgestellte“ Schnittstellen) und nutzen („benötigte“ Schnittstellen).
 324

325 **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]

326 [\leq]

327 4.1 Schnittstelle I_Directory_Query

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

330 TIP1-A_5565 - VZD, Schnittstelle I_Directory_Query
 331 Der VZD MUSS für LDAP Clients die Schnittstelle I_Directory_Query gemäß Tabelle
 332 Tab_VZD_Schnittstelle_I_Directory_Query anbieten.
 333

334 **Tabelle 2: Tab_VZD_Schnittstelle_I_Directory_Query**

Name	I_Directory_Query
------	-------------------

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

335 [**<=**]

336 4.1.1 Operation search_Directory

337 TIP1-A_5566 - LDAP Client, LDAPS

338 Der LDAP Client MUSS die Verbindung zum VZD mittels LDAPS sichern.

339 Der LDAP Client muss das Zertifikat des VZD C.ZD.TLS-S gemäß TUC_PKI_018

340 "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.

342 Der LDAP Client authentisiert sich nicht.

343 [**<=**]

344 TIP1-A_5567 - VZD, LDAPS bei search_Directory

345 Der VZD MUSS sicherstellen, dass die Operation search_Directory nur über eine bestehende LDAPS -Verbindung ausgeführt werden kann.

347 Der VZD muss die TLS-Verbindung 15 Minuten nach dem letzten Meldungsverkehr abbauen, falls sie noch besteht.

349 [**<=**]

350 TIP1-A_5568 - VZD und LDAP Client, Implementierung der LDAPv3 search Operation

351 Der VZD und die LDAP-Clients MÜSSEN die search Operation gemäß den LDAPv3

352 Standards [RFC4510], [RFC4511], [RFC4512], [RFC4513], [RFC4514], [RFC4515],

353 [RFC4516], [RFC4517], [RFC4518], [RFC4519], [RFC4520], [RFC4522] und [RFC4523]

354 implementieren.

355 [**<=**]

356 A_17794 - VZD, Testunterstützung

357 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.

360 [**<=**]

361 4.1.1.1 Umsetzung

362 TIP1-A_5569 - VZD, search_Directory, Suche nach definierten Attributen

363 Der VZD MUSS die enthaltenen Daten so strukturiert haben, dass mit einer einzigen

364 LDAPv3-Suche alle einer Telematik-ID zugeordneten Attribute (Basisdaten und

365 Fachdaten) in Form einer flachen Liste von Attributen ohne ou-Unterstruktur abgefragt werden können.

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

368 [**<=**]

369 4.1.1.2 Nutzung

370 TIP1-A_5570 - LDAP Client, TUC_VZD_0001 „search_Directory“

371 Der Anbieter des VZD MUSS für die Nutzung durch LDAP Clients den technischen Use

372 Case TUC_VZD_0001 „search_Directory“ gemäß Tabelle Tab_TUC_VZD_0001

373 unterstützen.

374

375 **Tabelle 3: Tab_TUC_VZD_0001**

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

376 [\leq]

377 4.2 Schnittstelle I_Directory_Maintenance

378 Die Schnittstelle ermöglicht die Administration der Basisdaten.

379 TIP1-A_5571 - VZD, Schnittstelle I_Directory_Maintenance

380 Der VZD MUSS die Schnittstelle I_Directory_Maintenance gemäß Tabelle

381 Tab_VZD_Schnittstelle_I_Directory_Maintenance anbieten.

382

383 **Tabelle 4: Tab_VZD_Schnittstelle_I_Directory_Maintenance**

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

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

384 [**<=**]

385 TIP1-A_5572 - VZD, I_Directory_Maintenance, TLS-gesicherte Verbindung
 386 Der VZD MUSS die Schnittstelle I_Directory_Maintenance durch Verwendung von TLS mit
 387 beidseitiger Authentisierung sichern.
 388 Der VZD muss sich mit der Identität ID.ZD.TLS-S authentisieren.
 389 Der VZD muss das vom FAD übergebene AUT-Zertifikat C.FD.TLS-C hinsichtlich OCSP-
 390 Gültigkeit und Übereinstimmung mit einem Zertifikat eines zur Nutzung dieser
 391 Schnittstelle registrierten Fachdienstes prüfen. Bei negativem Ergebnis wird der
 392 Verbindungsaufbau abgebrochen.

393 [**<=**]

394 TIP1-A_5574 - VZD und Nutzer der Schnittstelle I_Directory_Maintenance, Webservice
 395 Der VZD und Nutzer der Schnittstelle MÜSSEN die Schnittstelle I_Directory_Maintenance
 396 als SOAP-Webservice über HTTPS implementieren. Der Webservice wird durch die
 397 Dokumente DirectoryMaintenance.wsdl und DirectoryMaintenance.xsd definiert.

398 [**<=**]

399 **4.2.1 Operation add_Directory_Entry**

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

402 **4.2.1.1 Umsetzung**

403 TIP1-A_5575 - VZD, Umsetzung add_Directory_Entry
 404 Der VZD MUSS nach folgenden Vorgaben die Operation `add_Directory_Entry`
 405 implementieren:

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

411 Es müssen die Fehlermeldungen gemäß `Tab_TUC_VZD_0002` verwendet werden.

412 [**<=**]

413 In der folgenden Tabelle sind die Regeln zur Transformation
 414 von I_Directory_Maintenance Request Elementen zu LDAP-Directory Attributen und die

415 Regeln zur Transformation aus LDAP-Directory Attributen zu I_Directory_Maintenance
 416 Response Elementen beschrieben.

417

418 **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 Wird vom VZD als Kopie von otherName eingetragen.	commonName	Verwendung gemäß Tab_VZD_Datenbeschreibung
n/a	displayName Wird vom VZD als Kopie von otherName eingetragen.	displayName	
streetAddress	streetAddress	streetAddress	<u>Alias street</u> Der Alias-Wert wird in der LDAP Response verwendet.
postalCode	postalCode	postalCode	
localityName	localityName	localityName	<u>Alias l</u> Der Alias-Wert wird in der LDAP Response verwendet.
stateOrProvinceName	stateOrProvinceName	stateOrProvinceName	<u>Alias st</u> Der Alias-Wert wird in der

			LDAP Response verwendet.
title	title	title	Verwendung gemäß Tab_VZD_Datenbeschreibung
organization	organization	organization	Alias o Der Alias-Wert wird in der LDAP Response verwendet. 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	Verwendung gemäß Tab_VZD_Datenbeschreibung
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	

419 **4.2.1.2 Nutzung**

420 TIP1-A_5576 - Nutzer der Schnittstelle, TUC_VZD_0002 „add_Directory_Entry“
 421 Der Nutzer der Schnittstelle MUSS den technischen Use Case TUC_VZD_0002
 422 „add_Directory_Entry“ gemäß Tabelle Tab_TUC_VZD_0002 umsetzen.
 423 Der SOAP-Requests MUSS gemäß Tab_VZD_Datenbeschreibung mit der Bedeutung
 424 entsprechenden Daten ausgefüllt sein.
 425

426 **Tabelle 6: Tab_TUC_VZD_0002**

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

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

427 [**<=**]428 **4.2.2 Operation read_Directory_Entry**

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

430 **4.2.2.1 Umsetzung**

431 TIP1-A_5577 - VZD, Umsetzung read_Directory_Entry

432 Der VZD MUSS nach folgenden Vorgaben die Operation

433 I_Directory_Maintenance::read_Directory_Entry implementieren:

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

438 Es müssen die Fehlermeldungen gemäß Tab_TUC_VZD_0003 verwendet werden.
439 [=]

440 4.2.2.2 Nutzung

441 TIP1-A_5578 - Nutzer der Schnittstelle, TUC_VZD_0003 „read_Directory_Entry“
442 Der Nutzer der Schnittstelle MUSS den technischen Use Case TUC_VZD_0003
443 „read_Directory_Entry“ gemäß Tabelle Tab_TUC_VZD_0003 umsetzen. Der Webservice
444 wird durch die Dokumente DirectoryMaintenance.wsdl und DirectoryMaintenance.xsd
445 definiert.

446 Die SOAP-Response ist gemäß Tabelle Tab_VZD_Datenbeschreibung mit den zur
447 Telematik-ID gehörenden Daten aus dem VZD ausgefüllt.
448

449 **Tabelle 7: Tab_TUC_VZD_0003**

Name	TUC_VZD_0003 „read_Directory_Entry“	
Beschreibung	Diese Operation liest einen vollständigen Eintrag aus dem VZD aus.	
Vorbedingungen	Keine	
Eingangsdaten	SOAP-Request „readDirectoryEntry“	
Komponenten	Nutzer der Schnittstelle, Verzeichnisdienst	
Ausgangsdaten	SOAP-Response „readResponseMsg“	
Standardablauf	Aktion	Beschreibung
	Aufbau TLS-Verbindung	Wenn noch keine Verbindung besteht initiiert der Nutzer der Schnittstelle den Verbindungsaufbau. Der Nutzer der Schnittstelle authentisiert sich mit dem AUT-Zertifikat C.FD.TLS-C.
	SOAP-Request senden	Der Nutzer der Schnittstelle ruft die SOAP-Operation VZD:readDirectoryEntry auf.
	SOAP-Response empfangen	Die SOAP-Response VZD:readResponseMsg mit allen Basisdaten wird empfangen.
Varianten/Alternativen	keine	
Fehlerfälle	Es werden die protokollspezifischen Fehlermeldungen verwendet (TCP, HTTP, TLS) Fehler bei der Verarbeitung des SOAP Requests werden als gematik SOAP-Fault versendet: faultcode 4221, faultstring: Operation fehlerhaft ausgeführt, Basisdaten konnten nicht gelesen werden (Fehler im Verzeichnisdienst) faultcode 4312, faultstring: Basisdaten konnten nicht gefunden werden faultcode 4202, faultstring: SOAP Request enthält Fehler Erkannte Fehler auf Transportprotokollebene müssen auf gematik SOAP Faults (Code 6 aus Tabelle Tab_Gen_Fehler	

	aus [gemSpec_OM]) abgebildet werden. Zusätzlich müssen die generischen gematik SOAP-Faults Code 2: Verbindung zurückgewiesen Code 3: Nachrichtenschema fehlerhaft Code 4: Version Nachrichtenschema fehlerhaft unterstützt werden.
--	---

450 [<=]

451 **4.2.3 Operation modify_Directory_Entry**

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

454 **4.2.3.1 Umsetzung**

455 TIP1-A_5579 - VZD, Umsetzung modify_Directory_Entry
456 Der VZD MUSS nach folgenden Vorgaben die Operation modify_Directory_Entry
457 implementieren:

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

462 Es müssen die Fehlermeldungen gemäß Tab_TUC_VZD_0004 verwendet werden.
463 [<=]

464 **4.2.3.2 Nutzung**

465 TIP1-A_5580 - Nutzer der Schnittstelle, TUC_VZD_0004 „modify_Directory_Entry“
466 Der Nutzer der Schnittstelle MUSS den technischen Use Case TUC_VZD_0004
467 „modify_Directory_Entry“ gemäß Tabelle Tab_TUC_VZD_0004 umsetzen. Der Webservice
468 wird durch die Dokumente DirectoryMaintenance.wsdl und DirectoryMaintenance.xsd
469 definiert.
470 Der SOAP-Requests MUSS gemäß Tabelle VZD_TAB_modifyDirectoryEntry_Mapping mit
471 der Bedeutung entsprechenden Daten ausgefüllt sein.

472

473 **Tabelle 8: Tab_TUC_VZD_0004**

Name	TUC_VZD_0004 „modify_Directory_Entry“	
Beschreibung	Diese Operation ermöglicht die Änderung von Basisdaten.	
Vorbedingungen	keine	
Eingangsdaten	SOAP-Request „modifyDirectoryEntry“	
Komponenten	Nutzer der Schnittstelle, Verzeichnisdienst	
Ausgangsdaten	SOAP-Response „responseMsg“	
Standardablauf	Aktion	Beschreibung
	Aufbau TLS-Verbindung	Wenn noch keine Verbindung besteht initiiert der Nutzer der Schnittstelle den Verbindungsaufbau.

		Der Nutzer der Schnittstelle authentisiert sich mit dem AUT-Zertifikat C.FD.TLS-C.
	SOAP-Request senden	Der Nutzer der Schnittstelle ruft die SOAP-Operation VZD:modifyDirectoryEntry auf.
	SOAP-Response empfangen	Die SOAP-Response VZD:responseMsg mit dem VZD:status wird empfangen.
Varianten/Alternativen	keine	
Fehlerfälle	<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: faultcode 4231, faultstring: Operation fehlerhaft ausgeführt, Basisdaten konnten nicht modifiziert werden (Fehler im Verzeichnisdienst) faultcode 4312, faultstring: Basisdaten konnten nicht gefunden werden faultcode 4202, faultstring: SOAP Request enthält Fehler</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 Code 3: Nachrichtenschema fehlerhaft Code 4: Version Nachrichtenschema fehlerhaft unterstützt werden.</p>	

474 [\leq]475 **4.2.4 Operation delete_Directory_Entry**

476 Diese Operation löscht einen bestehenden Datensatz im LDAP Verzeichnis.

477 **4.2.4.1 Umsetzung**

478 TIP1-A_5581 - VZD, Umsetzung delete_Directory_Entry

479 Der VZD MUSS nach folgenden Vorgaben die Operation

480 I_Directory_Maintenance::delete_Directory_Entry implementieren:

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

482 Es müssen die Fehlermeldungen gemäß Tab_TUC_VZD_0005 verwendet werden.

483 [\leq]484 **4.2.4.2 Nutzung**

485 TIP1-A_5582 - Nutzer der Schnittstelle, TUC_VZD_0005 „delete_Directory_Entry“

486 Der Nutzer der Schnittstelle MUSS den technischen Use Case TUC_VZD_0005

487 „delete_Directory_Entry“ gemäß Tabelle Tab_TUC_VZD_0005 umsetzen. Der Webservice

488 wird durch die Dokumente DirectoryMaintenance.wsdl und DirectoryMaintenance.xsd

489 definiert.

490

491 **Tabelle 9: Tab_TUC_VZD_0005**

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

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

492 [**<=**]

493 **4.3 Schnittstelle I_Directory_Application_Maintenance**

494 Die Schnittstelle ermöglicht die Administration der Fachdaten.

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

498 ~~TIP1-A 5583-02~~**TIP1-A-5583-01** - VZD, Schnittstelle

499 I_Directory_Application_Maintenance

500 Der VZD MUSS ~~für FADs die Schnittstelle~~ I_Directory_Application_Maintenance gemäß
 501 Tabelle_Tab_VZD_Schnittstelle_I_Directory_Application_Maintenance anbieten.

502

503 **Tabelle 10: Tab_VZD_Schnittstelle_I_Directory_Application_Maintenance**

Name	I_Directory_Application_Maintenance	
Version	wird im Produkttypsteckbrief des VZD definiert	
Operationen	Operation	Kurzbeschreibung
	getInfo	Lesen der Metadaten dieser Schnittstelle (nur für die REST-Ausprägung verfügbar)
	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
	get_Directory_FA_Attributes	Lesen fachspezifischer Attribute

- 504
505 **[<=]**
- 506 TIP1-A_5584 - VZD, Änderung nur durch registrierte FAD
507 Der Anbieter des VZD MUSS sicherstellen, dass Fachdaten eines Dienstes nur durch einen
508 beim VZD für diesen Dienst registrierten Fachdienst erzeugt, gelöscht und geändert
509 werden können.
510 **[<=]**
- 511 Dazu wird bei der Registrierung eine FAD zugeordnet. Unter dieser FAD werden die
512 Fachdaten für den jeweiligen Dienst im VZD abgelegt. Die Zuordnung der FAD zu dem
513 Dienst wird bei Aufruf jeder Operation von Schnittstelle
514 I_Directory_Application_Maintenance durch den VZD geprüft (z.B. anhand des TLS-
515 Client-Zertifikats oder OAuth2 Tokens).
- 516 TIP1-A_5585 - VZD, I_Directory_Application_Maintenance, TLS-gesicherte Verbindung
517 Der VZD MUSS die Schnittstelle I_Directory_Application_Maintenance durch Verwendung
518 von TLS mit beidseitiger Authentisierung sichern.
519 Der VZD muss sich mit der Identität ID.ZD.TLS-S authentisieren.
520 Der VZD muss das vom FAD übergebene AUT-Zertifikat C.FD.TLS-C hinsichtlich OCSP
521 Gültigkeit und Übereinstimmung mit einem Zertifikat eines zur Nutzung dieser
522 Schnittstelle registrierten Fachdienstes prüfen. Bei negativem Ergebnis wird der
523 Verbindungsaufbau abgebrochen.
524 **[<=]**
- 525 TIP1-A_5586-01 - VZD, I_Directory_Application_Maintenance, Webservice und LDAPv3
526 Der VZD MUSS die Schnittstelle I_Directory_Application_Maintenance als Webservice
527 (SOAP und REST über HTTPS) und als LDAPv3 über LDAPS implementieren. Der
528 Webservice (SOAP) wird durch die Dokumente DirectoryApplicationMaintenance.wsdl und
529 DirectoryApplicationMaintenance.xsd definiert. Der Webservice (REST) wird durch die
530 [Directory_Application_Maintenance.yaml] Datei definiert. Die LDAPv3-Attribute sind in
531 dem Informationsmodell Abb_VZD_logisches_Datenmodell beschrieben.
532 **[<=]**
- 533 TIP1-A_5587 - VZD, Implementierung der LDAPv3 Schnittstelle
534 Der VZD MUSS die Schnittstelle I_Directory_Application_Maintenance gemäß den LDAPv3
535 Standards [RFC4510], [RFC4511], [RFC4512], [RFC4513], [RFC4514], [RFC4515],
536 [RFC4516], [RFC4517], [RFC4518], [RFC4519], [RFC4520], [RFC4522] und [RFC4523]
537 implementieren.
538 **[<=]**
- 539 TIP1-A_5588 - FAD, I_Directory_Application_Maintenance, Nutzung LDAP v3 oder
540 Webservice
541 Ein FAD, der Fachdaten im VZD verwalten will, MUSS entweder die Webservice- oder die
542 LDAPv3-Schnittstelle nutzen.
543 **[<=]**
- 544 TIP1-A_5589 - FAD, Implementierung der LDAPv3 Schnittstelle
545 Der FAD, der die LDAPv3-Schnittstelle I_Directory_Application_Maintenance des VZD
546 nutzt, MUSS diese Schnittstelle gemäß den LDAPv3 Standards [RFC4510], [RFC4511],
547 [RFC4512], [RFC4513], [RFC4514], [RFC4515], [RFC4516], [RFC4517], [RFC4518],
548 [RFC4519], [RFC4520], [RFC4522] und [RFC4523] implementieren. Die LDAPv3-Attribute
549 sind in dem Informationsmodell Abb_VZD_logisches_Datenmodell beschrieben.
550 **[<=]**
- 551 A_21466 - VZD, I_Directory_Application_Maintenance, OAuth2 Dienst
552 Der VZD MUSS einen OAuth2-Dienst bereitstellen. Dieser Dienst MUSS die Clients der
553 Schnittstelle I_Directory_Application_Maintenance anhand ihrer Client Credentials und

554 Umgebung (RU/TU/PU) authentisieren und ihnen ein AccessToken entsprechend [[RFC](#)
 555 [6750](#)] ausstellen. Das AccessToken muss im "sub" claim den Identifier des Clients
 556 enthalten.[<=]

557 A_21467 - VZD, I_Directory_Administration, Prüfung AccessToken
 558 Der VZD MUSS das vom Client übergebene AccessToken auf Gültigkeit für
 559 Schnittstelle I_Directory_Application_Maintenance und Umgebung (RU/TU/PU) prüfen.
 560 Bei negativem Ergebnis muss die Operation mit HTTP Fehler 401 Unauthorized
 561 abgebrochen werden.
 562 [<=]

563 **4.3.1 Operation getInfo**

564 Diese Operation liefert die Metadaten der Schnittstelle
 565 I_Directory_Application_Maintenance.

566 **4.3.1.1 Umsetzung REST**

567 A_21788 - VZD, Umsetzung I_Directory_Application_Maintenance getInfo (REST)
 568 Der VZD MUSS nach folgenden Vorgaben die Operation getInfo implementieren:

569
 570 In dem Rückgabewerten müssen die aktuell gültigen Metainformationen für Schnittstelle
 571 I_Directory_Application_Maintenance zurückgegeben werden. Insbesondere muss

- 572 a. Der Parameter *version* die aktuelle Version der Schnittstelle enthalten
 573 (entspricht info.version der Schnittstellendefinition
 574 DirectoryApplicationMaintenance.yaml)
- 575 b. Der Parameter *title* den Titel der Schnittstelle enthalten (entspricht info.title
 576 der Schnittstellendefinition DirectoryApplicationMaintenance.yaml)
- 577 c. Der Parameterstruktur *contact* die Kontaktinformationen für die Schnittstelle
 578 enthalten. Über die - mit contact.url adressierte - Web-Seite muss die aktuell
 579 verwendete Schnittstellendefinition DirectoryApplicationMaintenance.yaml
 580 abrufbar sein.

581 [<=]

582
 583 In dem Dokument unter dieser URL muss ein Link zum Download der aktuell genutzten
 584 YAML-Datei dieser Schnittstelle hinterlegt sein.

585 **4.3.1.2 Nutzung REST**

586 A_21787 - VZD, I_Directory_Application_Maintenance, getInfo
 587 Der VZD MUSS die Operation „getInfo“ gemäß Tabelle Tab_VZD
 588 „I_Directory_Application_Maintenance-getInfo“ umsetzen.
 589

590 **Tabelle 11: Tab_VZD „I_Directory_Application_Maintenance-getInfo“**

<u>Name</u>	<u>getInfo</u>
<u>Beschreibung</u>	<u>Liefert die Metadaten (unter anderem aus dem InfoObject) dieser</u> <u>OpenAPI-Spezifikation und ergänzt sie.</u>

Eingangsdaten	REST-Request GET / operationId: getInfo (siehe DirectoryApplicationMaintenance.yaml)	
	<u>Parameter</u>	<u>Beschreibung</u>
	keine	-
Komponenten	Nutzer der Schnittstelle	
Ausgangsdaten	REST-Response mit Metadaten (<i>InfoObject</i>).	
Ablauf	Der VZD liefert die Metadaten der Schnittstelle in der Datenstruktur InfoObject zurück.	
Fehlerfälle	Es werden die protokollspezifischen Fehlermeldungen verwendet (TCP, HTTP, TLS) und in DirectoryApplicationMaintenance.yaml mit spezifischen Fehlerbeschreibungen ergänzt.	

591 [**<=**]

592

593

594 **4.3.14.3.2 Operation add_Directory_FA-Attributes**

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

597 Voraussetzung: Die Fachdaten müssen einem Basisdateneintrag zuordenbar sein.

598 **4.3.1.14.3.2.1 Umsetzung SOAP**

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

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

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

613 **Tabelle 12: 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.
-----------------	--

614 Es müssen die Fehlermeldungen gemäß Tab_TUC_VZD_0006 verwendet werden.
615 [**<=**]

616 **4.3.1.24.3.2.2 Nutzung SOAP**

617 TIP1-A_5591 - FAD, TUC_VZD_0006 "add_Directory_FA-Attributes (SOAP)"
618 Der FAD MUSS den technischen Use Case TUC_VZD_0006 "add_Directory_FA-Attributes"
619 gemäß Tabelle Tab_TUC_VZD_0006 umsetzen.
620

621 **Tabelle 13: Tab_TUC_VZD_0006**

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

622 [**<=**]

623 TIP1-A_5592-03 - FAD, KOM-LE_FA_Add_Attributes
624 Der FAD MUSS für die FA KOM-LE die Fachdaten nach VZD_TAB_KOM-LE_Add_Attributes
625 administrieren.

626 **Tabelle 14: 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

627 [\leq]

628

629 **4.3.1.34.3.2.3 Umsetzung LDAPv3**

630 TIP1-A_5593 - VZD, Umsetzung add_Directory_FA-Attributes (LDAPv3)

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

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

638 Es müssen die Fehlermeldungen gemäß Tab_TUC_VZD_0007 verwendet werden.

639 [\leq]

640 **4.3.1.44.3.2.4 Nutzung LDAPv3**

641 TIP1-A_5594 - FAD, TUC_VZD_0007 "add_Directory_FA-Attributes (LDAPv3)"

642 Der FAD MUSS den technischen Use Case TUC_VZD_0007 „add_Directory_FA-
643 Attributes(LDAPv3)" gemäß Tabelle Tab_TUC_VZD_0007 unterstützen.

644

645 **Tabelle 15: Tab_TUC_VZD_0007**

Name	add_Directory_FA-Attributes(LDAPv3)	
Beschreibung	Mit dieser Operation werden Fachdaten zu einem bestehenden Eintrag zugefügt.	
Vorbedingungen	Der LDAPS-Verbindungsaufbau muss erfolgreich durchgeführt sein.	
Eingangsdaten	Add-Request gemäß [RFC4511]#4.7 und Informationsmodell (Abb_VZD_logisches_Datenmodell)	
Komponenten	LDAP Client des FAD, Verzeichnisdienst	
Ausgangsdaten	gemäß [RFC4511]#4.7	
Standardablauf	Aktion	Beschreibung
	Add Request senden	Der LDAP Client des FAD sendet den Add-Request gemäß [RFC4511]#4.7 an den VZD. Die RFCs [RFC4510], [RFC4511], [RFC4513], [RFC4514], [RFC4515],

		[RFC4516], [RFC4519] und [RFC4522] müssen unterstützt werden.
	Add Response empfangen	Der LDAP Client empfängt das Ergebnis der Operation gemäß [RFC4511]#4.7.
Varianten/Alternativen	keine	
Zustand nach erfolgreichem Ablauf	Das Ergebnis der Operation liegt im LDAP Client des FAD vor.	
Fehlerfälle	Zur Behandlung auftretender Fehlerfälle werden Fehlermeldungen gemäß [RFC4511]#Appendix A verwendet.	

646 [**<=**]

647 A 21834 - VZD, I Directory Application Maintenance, KOM-LE Version Prüfung LDAP
 648 Der VZD MUSS bei Änderungen an KOM-LE-Fachdaten mit den Operationen
 649 "add Directory FA-Attributes (LDAPv3)" und "modify Directory FA-Attributes (LDAPv3)"
 650 den Inhalt von Parameter KOM-LE Version des Operation Requests gegen die Liste
 651 der gültigen Werte prüfen. Im Falle von ungültigen Werten MUSS der VZD mit LDAP
 652 Result Code constraintViolation (19) antworten und darf die Operation nicht ausführen.
 653 Der VZD MUSS die Liste der gültigen Werte von Attribut KOM-LE Version konfigurierbar
 654 realisieren und der gematik Änderungsmöglichkeiten über einen Service Request
 655 bieten.[<=]

656 A 21835 - VZD, I Directory Application Maintenance, Eindeutige Zuordnung von KOM-
 657 LE Adressen zu VZD-Einträgen LDAP
 658 Der VZD MUSS sicherstellen, dass jede KOM-LE-Adresse mit den Operationen
 659 "add Directory FA-Attributes (LDAPv3)" und "modify Directory FA-Attributes (LDAPv3)"
 660 nur an maximal einen VZD-Eintrag angehängt wird. Hierzu MUSS er vor einer Eintragung
 661 einer KOM-LE Adresse prüfen, ob diese bereits im VZD hinterlegt ist. Ist sie bereits
 662 hinterlegt, MUSS der VZD mit LDAP Result Code attributeOrValueExists (20) antworten
 663 und darf die Operation nicht ausführen.
 664 [<=]

665

666 **4.3.1.54.3.2.5 Umsetzung REST**

667 A_21458 - VZD, Umsetzung add_Directory_FA-Attributes (REST)
 668 Der VZD MUSS nach folgenden Vorgaben die Operation add_Directory_FA-Attributes
 669 implementieren:
 670

- 671 1. Wenn kein zur Telematik-ID gehörender Basisdatensatz gefunden wurde, wird der
 672 Request mit einem HTTP-Statuscode beendet:
 673 HTTP-Statuscode: 404
- 674 2. Ein bereits zur Telematik-ID gehörender Fachdatensatz wird gelöscht und neu
 675 angelegt.
- 676 3. Ein noch nicht existierender Fachdatensatz zur Telematik-ID wird im LDAP
 677 Directory neu angelegt.
- 678 4. Die Daten aus dem Request werden zum dazugehörigen Fachdatensatz
 679 hinzugefügt.

680 [\leq]681 **4.3.1.64.3.2.6 Nutzung REST**

682 A_21459 - FAD, VZD, TUC_VZD_0012 "add_Directory_FA-Attributes (REST)"
 683 Der FAD MUSS den technischen Use Case TUC_VZD_0012 "add_Directory_FA-Attributes"
 684 gemäß Tabelle Tab_TUC_VZD_0012 umsetzen.

685 **Tabelle 31: Tab_TUC_VZD_0012**

Name	add_Directory_FA-Attributes	
Beschreibung	Mit dieser Operation werden Fachdaten zu einem bestehenden Basisdaten-Eintrag zugefügt.	
Vorbedingungen	Keine.	
Eingangsdaten	REST-Request „add_Directory_FA-Attributes“	
Komponenten	VZD, FAD	
Ausgangsdaten	REST-Response	
Standardablauf	Aktion	Beschreibung
	Aufbau TLS-Verbindung	Falls noch keine TLS-Verbindung besteht, wird eine aufgebaut. Der FAD authentisiert sich mit ID.FD.TLS-C.
	REST-Request senden	Der FAD ruft die REST-Operation add_Directory_FA-Attributes auf.
	REST-Response empfangen	Die REST-Response enthält den HTTP-Statuscode. Im Fehlerfall wird ein HTTP-Statuscode empfangen.
Fehlerfälle	Es werden die protokollspezifischen Fehlermeldungen verwendet (TCP, HTTP, TLS). Fehler bei der Verarbeitung des REST Requests werden als HTTP-Statuscode versendet.	

686 [\leq]

687 A_21825 - VZD, I Directory Application Maintenance, KOM-LE Version Prüfung REST
 688 Der VZD MUSS bei Änderungen an KOM-LE-Fachdaten mit den Operationen
 689 „add Directory FA-Attributes“ und "modify Directory FA-Attributes" den Inhalt von
 690 Parameter KOM-LE Version des Operation Requests gegen die Liste der gültigen Werte
 691 prüfen. Im Falle von ungültigen Werten MUSS der VZD mit HTTP-Statuscode 422
 692 (attributeName="KOM-LE Version" , attributeError="erläuternder Fehlertext") antworten
 693 und darf die Operation nicht ausführen. Der VZD MUSS die Liste der gültigen Werte von
 694 Attribut KOM-LE Version konfigurierbar realisieren und der gematik
 695 Änderungsmöglichkeiten über einen Service Request bieten.

696 [\leq]

697 A_21826 - VZD, I Directory Application Maintenance, Eindeutige Zuordnung von KOM-
 698 LE-Adressen zu VZD-Einträgen REST
 699 Der VZD MUSS sicherstellen, dass jede KOM-LE Adresse mit den Operationen
 700 „add Directory FA-Attributes“ und "modify Directory FA-Attributes" nur an maximal
 701 einen VZD-Eintrag angehängt wird. Hierzu MUSS er vor einer Eintragung einer KOM-LE
 702 Adresse prüfen, ob diese bereits im VZD hinterlegt ist. Ist sie bereits hinterlegt, MUSS
 703 der VZD mit HTTP-Statuscode 422 (attributeName="mail" , attributeError="erläuternder

704 Fehlertext") antworten und darf die Operation nicht ausführen.
 705 [<=]

706
707

708 **4.3.24.3.3 Operation delete_Directory_FA-Attributes**

709 Diese Operation löscht einen Fachdatensatz.

710 **4.3.2.14.3.3.1 Umsetzung SOAP**

711 TIP1-A_5595 - VZD, Umsetzung delete_Directory_FA-Attributes
 712 Der VZD MUSS nach folgenden Vorgaben die Operation delete_Directory_FA-Attributes
 713 implementieren:

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

720 Es müssen die Fehlermeldungen gemäß Tab_TUC_VZD_0008 verwendet werden.
 721 [<=]

722 **4.3.2.24.3.3.2 Nutzung SOAP**

723 TIP1-A_5596 - FAD, TUC_VZD_0008 "delete_Directory_FA-Attributes (SOAP)"
 724 Der FAD MUSS den technischen Use Case TUC_VZD_0008 "delete_Directory_FA-
 725 Attributes" gemäß Tabelle Tab_TUC_VZD_0008 umsetzen.
 726

727 **Tabelle 16: Tab_TUC_VZD_0008**

Name	delete_Directory_FA-Attributes	
Beschreibung	Mit dieser Operation wird ein Fachdaten-Eintrag gelöscht.	
Vorbedingungen	Keine.	
Eingangsdaten	SOAP-Request „deleteDirectoryFAAttributes“	
Komponenten	VZD, FAD	
Ausgangsdaten	SOAP-Response „responseMsg“	
Standardablauf	Aktion	Beschreibung
	Aufbau TLS-Verbindung	Falls noch keine TLS-Verbindung besteht, wird eine aufgebaut. Der FAD authentisiert sich mit ID.FD.TLS-C.
	SOAP-Request senden	Der FAD ruft die SOAP-Operation VZD:deleteDirectoryFAAttributes auf.

	SOAP-Response empfangen	Die SOAP-Response VZD:responseMsg enthält den vzd:status. Im Fehlerfall wird eine gematik SOAP-Fault Response empfangen
Fehlerfälle	Es werden die protokollspezifischen Fehlermeldungen verwendet (TCP, HTTP, TLS). Fehler bei der Verarbeitung des SOAP Requests werden als gematik SOAP-Fault versendet: faultcode 4321, faultstring: Operation fehlerhaft ausgeführt, Fachdaten konnten nicht gelöscht werden (Fehler im Verzeichnisdienst) faultcode 4312, faultstring: Basisdaten konnten nicht gefunden werden faultcode 4202, faultstring: SOAP Request enthält Fehler	

728 [**<=**]

729 **4.3.2.34.3.3 Umsetzung LDAPv3**

730 TIP1-A_5597 - VZD, Umsetzung delete_Directory_FA-Attributes (LDAPv3)
 731 Der VZD MUSS nach folgenden Vorgaben die Operation delete_Directory_FA-Attributes
 732 implementieren:

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

738 Es müssen die Fehlermeldungen gemäß Tab_TUC_VZD_0009 verwendet werden.
 739 [**<=**]

740 **4.3.2.44.3.3.4 Nutzung LDAPv3**

741 TIP1-A_5598 - FAD, TUC_VZD_0009 "delete_Directory_FA-Attributes (LDAPv3)"
 742 Der FAD MUSS den technischen Use Case TUC_VZD_0009 „delete_Directory_FA-
 743 Attributes(LDAPv3)" gemäß Tabelle Tab_TUC_VZD_0009 unterstützen.
 744

745 **Tabelle 17: Tab_TUC_VZD_0009**

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

	Delete Request senden	Der LDAP Client des FAD sendet den delete-Request gemäß [RFC4511]#4.8 an den VZD. Die RFCs [RFC4510], [RFC4511], [RFC4513], [RFC4514], [RFC4515], [RFC4516], [RFC4519] und [RFC4522] müssen unterstützt werden.
	Delete Response empfangen	Der LDAP Client empfängt das Ergebnis der Operation gemäß [RFC4511]#4.8.
Varianten/Alternativen	keine	
Zustand nach erfolgreichem Ablauf	Das Ergebnis der Operation liegt im LDAP Client des FAD vor.	
Fehlerfälle	Zur Behandlung auftretender Fehlerfälle werden Fehlermeldungen gemäß [RFC4511]#Appendix A verwendet.	

746 [<=]

747 **4.3.2.54.3.3.5 Umsetzung REST**

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

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

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

757 [<=]

758 **4.3.2.64.3.3.6 Nutzung REST**

759 A_21461 - FAD, TUC_VZD_0013 "delete_Directory_FA-Attributes (REST)"

760 Der FAD MUSS den technischen Use Case TUC_VZD_0013 "delete_Directory_FA-
761 Attributes" gemäß Tabelle Tab_TUC_VZD_0013 umsetzen.

762

763 *Tabelle 32: Tab_TUC_VZD_0013*

Name	delete_Directory_FA-Attributes	
Beschreibung	Mit dieser Operation wird ein Fachdaten-Eintrag gelöscht.	
Vorbedingungen	Keine.	
Eingangsdaten	REST-Request „delete_Directory_FA-Attributes“	
Komponenten	VZD, FAD	
Ausgangsdaten	REST-Response	
Standardablauf	Aktion	Beschreibung

	Aufbau TLS-Verbindung	Falls noch keine TLS-Verbindung besteht, wird eine aufgebaut. Der FAD authentisiert sich mit ID.FD.TLS-C.
	REST-Request senden	Der FAD ruft die REST-Operation delete_Directory_FA-Attributes auf.
	REST-Response empfangen	Die REST-Response enthält den HTTP-Statuscode. Im Fehlerfall wird ein HTTP-Statuscode empfangen.
Fehlerfälle	Es werden die protokollspezifischen Fehlermeldungen verwendet (TCP, HTTP, TLS). Fehler bei der Verarbeitung des REST Requests werden als HTTP-Statuscode versendet.	

764 [<=]

765

766

767 **4.3.34.3.4 Operation modify_Directory_FA-Attributes**

768 Diese Operation überschreibt einen Fachdatensatz.

769 **4.3.3.14.3.4.1 Umsetzung SOAP**

770 TIP1-A_5599 - VZD, Umsetzung modify_Directory_FA-Attributes

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

- 773 1. Wenn kein zur Telematik-ID gehörender Basisdatensatz gefunden wurde, wird der
774 Request mit einem gematik SOAP-Fault beendet:
775 faultcode: 4312,
776 faultstring: Basisdaten konnten nicht gefunden werden.
- 777 2. Ein bereits zur Telematik-ID gehörender Fachdatensatz wird überschrieben.
- 778 3. Die Daten aus dem SOAP Request werden gemäß
779 VZD_TAB_I_Directory_Application_Maintenance_Modify_Mapping zum
780 Basisdatensatz hinzugefügt.

781

782 **Tabelle 18: 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.

783 Es müssen die Fehlermeldungen gemäß Tab_TUC_VZD_0010 verwendet werden. [<=]

784 **4.3.3-24.3.4.2 Nutzung SOAP**

785 TIP1-A_5600 - FAD, TUC_VZD_0010 "modify_Directory_FA-Attributes (SOAP)"
 786 Der FAD MUSS den technischen Use Case TUC_VZD_0010 "modify_Directory_FA-
 787 Attributes" gemäß Tabelle Tab_TUC_VZD_0010 umsetzen.
 788

789 **Tabelle 19: Tab_TUC_VZD_0010**

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

790 [**<=**]

791

792 TIP1-A_5601-03 - FAD, KOM-LE_FA_Modify_Attributes
 793 Der FAD MUSS für die FA KOM-LE die Fachdaten nach VZD_TAB_KOM-
 794 LE_Modify_Attributes administrieren.
 795

796 **Tabelle 20: 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

797 [\leq]

798

799 **4.3.3.34.3.4.3 Umsetzung LDAPv3**

800 TIP1-A_5602 - VZD, Umsetzung modify_Directory_FA-Attributes (LDAPv3)

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

803 1. Wenn kein zur Telematik-ID gehörender Basisdatensatz gefunden wurde, wird der
804 Request beendet.

805 2. Ein bereits zur Telematik-ID gehörender Fachdatensatz wird geändert.

806 3. Der FAD darf nur die zu seinem Dienst gehörenden Fachdaten ändern.

807 Es müssen die Fehlermeldungen gemäß Tab_TUC_VZD_0011 verwendet werden.

808 [\leq]

809 **4.3.3.44.3.4.4 Nutzung LDAPv3**

810 TIP1-A_5603 - FAD, TUC_VZD_0011 "modify_Directory_FA-Attributes (LDAPv3)"

811 Der FAD MUSS den technischen Use Case TUC_VZD_0011 „modify_Directory_FA-
812 Attributes(LDAPv3)" gemäß Tabelle Tab_TUC_VZD_0011 unterstützen.

813

814 **Tabelle 21: Tab_TUC_VZD_0011**

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

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

815 [**<=**]

816 **4.3.3-54.3.4.5 Umsetzung REST**

- 817 A_21462 - VZD, Umsetzung modify_Directory_FA-Attributes (REST)
 818 Der VZD MUSS nach folgenden Vorgaben die Operation modify_Directory_FA-Attributes
 819 implementieren:
- 820 1. Wenn kein zur Telematik-ID gehörender Basisdatensatz gefunden wurde, wird der
 821 Request mit einem HTTP-Statuscode beendet:
 822 HTTP-Statuscode: 404
 - 823 2. Ein bereits zur Telematik-ID gehörender Fachdatensatz (FADx
 824 in Abb_VZD_logisches_Datenmodell) des authentifizierten Fachdienstanbieters
 825 wird überschrieben.
 - 826 3. Ein nicht existierender Fachdatensatz zur Telematik-ID führt zu keiner Aktion und
 827 HTTP-Statuscode: 404 im Response.

828 [**<=**]

829 **4.3.3-64.3.4.6 Nutzung REST**

830 A_21463 - FAD, TUC_VZD_0014 "modify_Directory_FA-Attributes (REST)"
 831 Der FAD MUSS den technischen Use Case TUC_VZD_0014 "modify_Directory_FA-
 832 Attributes" gemäß Tabelle Tab_TUC_VZD_0014 umsetzen.

833
 834 *Tabelle 33: Tab_TUC_VZD_0014*

Name	modify_Directory_FA-Attributes	
Beschreibung	Mit dieser Operation wird ein Fachdaten-Eintrag geändert.	
Vorbedingungen	Keine.	
Eingangsdaten	REST-Request „modify_Directory_FA-Attributes“	
Komponenten	VZD, FAD	
Ausgangsdaten	REST-Response	
Standardablauf	Aktion	Beschreibung
	Aufbau TLS-Verbindung	Falls noch keine TLS-Verbindung besteht, wird eine aufgebaut. Der FAD authentisiert sich mit ID.FD.TLS-C.
	REST-Request senden	Der FAD ruft die REST-Operation modify_Directory_FA-Attributes auf.

	REST-Response empfangen	Die REST-Response enthält den HTTP-Statuscode. Im Fehlerfall wird ein HTTP-Statuscode empfangen.
Fehlerfälle	Es werden die protokollspezifischen Fehlermeldungen verwendet (TCP, HTTP, TLS). Fehler bei der Verarbeitung des REST Requests werden als HTTP-Statuscode versendet.	

835 [\leq]

836 **4.3.44.3.5 Operation get_Directory_FA-Attributes**

837 Diese Operation liest einen Fachdatensatz.

838 **4.3.4.14.3.5.1 Umsetzung REST**

839 A_21464 - VZD, Umsetzung get_Directory_FA-Attributes (REST)

840 Der VZD MUSS nach folgenden Vorgaben die Operation get_Directory_FA-
841 Attributes implementieren:

- 842 1. Wenn kein zur Telematik-ID gehörender Basisdatensatz gefunden wurde, wird der
843 Request mit einem HTTP-Statuscode beendet:
844 HTTP-Statuscode: 404
- 845 2. Ein nicht existierender Fachdatensatz zur Telematik-ID führt zur Rückgabe von
846 HTTP-Statuscode: 404 im Response.

847 [\leq]

848 **4.3.4.24.3.5.2 Nutzung REST**

849 A_21465 - FAD, TUC_VZD_0015 "get_Directory_FA-Attributes (REST)"

850 Der FAD MUSS den technischen Use Case TUC_VZD_0015 "get_Directory_FA-Attributes"
851 gemäß Tabelle Tab_TUC_VZD_0015 umsetzen.

852

853 *Tabelle 34: Tab_TUC_VZD_0015*

Name	get_Directory_FA-Attributes	
Beschreibung	Mit dieser Operation wird ein Fachdaten-Eintrag gelesen.	
Vorbedingungen	Keine.	
Eingangsdaten	REST-Request „get_Directory_FA-Attributes“	
Komponenten	VZD, FAD	
Ausgangsdaten	REST-Response mit den Fachdaten	
Standardablauf	Aktion	Beschreibung
	Aufbau TLS-Verbindung	Falls noch keine TLS-Verbindung besteht, wird eine aufgebaut. Der FAD authentisiert sich mit ID.FD.TLS-C.
	REST-Request senden	Der FAD ruft die REST-Operation get_Directory_FA-Attributes auf.

	REST-Response empfangen	Die REST-Response enthält den HTTP-Statuscode und die Fachdaten. Im Fehlerfall wird ein HTTP-Statuscode empfangen.
Fehlerfälle	Es werden die protokollspezifischen Fehlermeldungen verwendet (TCP, HTTP, TLS). Fehler bei der Verarbeitung des REST Requests werden als HTTP-Statuscode versendet.	

854 [**<=**]

855

856

857

858 **4.4 Prozessschnittstelle P_Directory_Application_Registration** 859 **(Provided)**

860 TIP1-A_5604 - VZD, Registrierung FADs

861 Der Anbieter des VZD MUSS einen Registrierungsprozess für FAD implementieren. Der
862 Anbieter des VZD MUSS dazu überprüfen:

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

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

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

869 [**<=**]

870 TIP1-A_5605 - VZD, De-Registrierung FADs

871 Der Anbieter des VZD MUSS einen Deregistrierungsprozess für FAD implementieren.

872 Der VZD MUSS alle verbliebenen Fachdaten eines deregistrierten FAD löschen.

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

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

875 [**<=**]

876 **4.5 Prozessschnittstelle P_Directory_Maintenance (Provided)**

877 TIP1-A_5606 - VZD, Mandat zur Löschung von Einträgen.

878 Der Anbieter des VZD MUSS einen Prozess implementieren, der es LE ermöglicht ihren
879 Eintrag im VZD ohne zugehörige Smartcard zu löschen.880 Der Anbieter des VZD MUSS vom LE einen Nachweis fordern und prüfen, dass die zu
881 löschenden Daten dem LE gehören. Erst nach positivem Ergebnis der Prüfung darf
882 gelöscht werden.

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

884 [**<=**]

885 **4.6 Schnittstelle I_Directory_Administration**

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

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

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

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

902 **4.6.1 Operationen der Schnittstelle I_Directory_Administration**

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

906 ~~A_18371-04A_18371-02~~ - VZD, Schnittstelle I_Directory_Administration
 907 Der VZD MUSS die Schnittstelle I_Directory_Administration gemäß Tabelle
 908 Tab_VZD_Schnittstelle_I_Directory_Administration im Internet anbieten.
 909

910 **Tabelle 22: Tab_VZD_Schnittstelle_I_Directory_Administration**

Name	I_Directory_Administration	
Version	wird im Produkttypsteckbrief des VZD definiert	
Operationen	Resource: / (übergreifend für gesamte Schnittstelle)	
	Name	Kurzbeschreibung
	GET	Lesen der Metadaten dieser Schnittstelle
	Resource: DirectoryEntry	
	Name	Kurzbeschreibung
	POST	Hinzufügen eines Verzeichniseintrages inklusive dazugehörendem Zertifikat.

	GET	Abfrage aller Daten von Verzeichniseinträgen.
	PUT	Änderung eines Basisdaten-Verzeichniseintrages.
	DELETE	Löschung eines Verzeichniseintrages (kompletter Datensatz inklusive aller Zertifikate und Fachdaten).
Resource: /DirectoryEntriesSync		
	Name	Kurzbeschreibung
	GET	Abfrage aller Daten von Verzeichniseinträgen zu Synchronisationszwecken.
Resource: Certificate		
	Name	Kurzbeschreibung
	POST	Hinzufügen eines Zertifikatseintrags zu einem Verzeichniseintrag.
	GET	Abfrage von Zertifikatseinträgen.
	<u>DELETE</u>	<u>Löschen von Zertifikatseinträgen.</u>

911 **[<=]**

912

913 A_18373 - VZD, Schnittstelle I_Directory_Administration

914 Der VZD MUSS die Schnittstelle I_Directory_Administration als REST-Webservice über
915 HTTPS implementieren. Der Webservice wird durch das Dokument
916 DirectoryAdministration.yaml definiert.

917 **[<=]**

918 A_18408 - VZD, I_Directory_Administration, Registrierung

919 Der VZD-Anbieter MUSS für Clients der Schnittstelle I_Directory_Administration einen
920 Registrierungsprozess bereitstellen. Während der Registrierung muss die Berechtigung des
921 Antragstellers (Clients) zur Nutzung von Schnittstelle I_Directory_Administration durch den VZD-
922 Anbieter geprüft und durch die gematik bestätigt werden. Nach erfolgreicher Registrierung MÜSSEN
923 dem Antragsteller alle nötigen Daten - inklusive OAuth Client Credentials, CA-Zertifikat (welches zur
924 Prüfung des Serverzertifikats durch den Client benötigt wird), VZD-Serverzertifikat - zur Nutzung der
925 Schnittstelle bereitgestellt werden.

926 Der VZD-Anbieter MUSS die erfolgreich registrierten Clients immer mit aktuellen Zertifikaten
927 versorgen.

928 **[<=]**

929 A_20267 - VZD, I_Directory_Administration, Registrierung beim IdP als Relying Party

930 Der Anbieter des VZD MUSS sich über einen organisatorischen Prozess bei einem
931 vertrauenswürdigen Identity Provider (IDP) der Telematikinfrastruktur als Relying Party

- 932 registrieren und die Bereitstellung der folgenden Claims in für Nutzer ausgestellte
933 ACCESS_TOKEN mit dem IDP vereinbaren:
- 934 • name
 - 935 • sub
 - 936 • scope
 - 937 • acr
- 938 damit der VZD die Fachlogik der Autorisierung und Protokollierung auf diesen Attributen
939 umsetzen kann.
940 **[<=]**
- 941 A_20268 - VZD, Authentifizierung Nutzerrolle
942 Der VZD MUSS die fachliche Rolle eines Nutzers in jedem Operationsaufruf der
943 Schnittstelle I_Directory_Administration anhand des Attributs "scope" im übergebenen
944 ACCESS_TOKEN feststellen und für die nachfolgende Rollenprüfung je Operationsaufruf
945 verwenden. **[<=]**
- 946 A_20269 - VZD, Authentifizierung Nutzernamen
947 Der VZD MUSS den Namen eines Nutzers in jedem Operationsaufruf anhand des Attributs
948 "name" im übergebenen ACCESS_TOKEN feststellen und für die Protokollierung des
949 Zugriffs verwenden. **[<=]**
- 950 A_18470 - VZD, I_Directory_Administration, Client Secret Qualität
951 Der VZD-Anbieter MUSS bei der Erzeugung der OAuth client_secret's 128 Bit Zufall aus
952 einer Zufallsquelle gemäß GS-A_4367 [gemSpec_Krypt] verwenden.
953 **[<=]**
- 954 A_18409 - VZD, I_Directory_Administration, Sperrung OAuth Client Credentials
955 Der VZD-Anbieter MUSS – für die gematik und den Client-Betreiber selbst - einen Service
956 zur Sperrung der OAuth Client Credentials anbieten.
957 **[<=]**
- 958 A_18372 - VZD, I_Directory_Administration, TLS-gesicherte Verbindung
959 Der VZD MUSS die Schnittstelle I_Directory_Administration durch Verwendung von TLS
960 mit serverseitiger Authentisierung sichern.
961 Der VZD MUSS für diese TLS-Verbindungen öffentliche Zertifikate nutzen (keine TI-
962 Zertifikate).
963 Der VZD MUSS sich mit der Server-Identität von Schnittstelle I_Directory_Administration
964 authentisieren.
965 **[<=]**
- 966 Die Prüfung der öffentliche TLS-Server Zertifikate muss gemäß GS-A_5581
967 [gemSpec_Krypt] erfolgen. Dabei müssen in (1) von GS-A_5581 statt der
968 "Komponenten-CA-Zertifikate der TI" die CA-Zertifikate der Schnittstelle
969 I_Directory_Administration genutzt werden.
- 970 A_18374 - VZD, I_Directory_Administration, Redirect
971 Der VZD MUSS für die Schnittstelle I_Directory_Administration Anfragen der Clients –
972 welche kein AccessToken entsprechend [[RFC 6750](#)] enthalten – durch ein Redirect zu
973 dem OAuth2-Authentifizierungsdienst weiterleiten. **[<=]**
- 974 A_18375 - VZD, I_Directory_Administration, OAuth2 Dienst
975 Der VZD MUSS einen OAuth2-Dienst bereitstellen. Dieser Dienst MUSS die Clients der
976 Schnittstelle I_Directory_Administration anhand ihrer Client Credentials authentisieren
977 und ihnen ein AccessToken entsprechend [[RFC 6750](#)] ausstellen. Das AccessToken muss
978 im "sub" claim den Identifier des Clients enthalten. Die Anfrage des Clients MUSS nach
979 erfolgreicher Authentisierung durch ein Redirect wieder zur VZD

- 980 I_Directory_Administration Schnittstelle weitergeleitet werden.
- 981 [**<=**]
- 982 A_18376 - VZD, I_Directory_Administration, Prüfung AccessToken
- 983 Der VZD MUSS das vom Client übergebene AccessToken auf Gültigkeit für
- 984 Schnittstelle I_Directory_Administration prüfen. Bei negativem Ergebnis muss die
- 985 Operation mit HTTP Fehler 401 Unauthorized abgebrochen werden.
- 986 [**<=**]
- 987 A_18471-01 - VZD, I_Directory_Administration, Datenquelle
- 988 Der VZD MUSS bei den Operationen add_Directory_Entry und
- 989 modify_Directory_Entry das LDAP-Directory-Attribut dataFromAuthority auf den Wert
- 990 TRUE setzen und bei allen anderen Operationen unverändert belassen.
- 991 [**<=**]
- 992 A_18735 - VZD, Disable I_Directory_Maintenance, wenn dataFromAuthority TRUE
- 993 Der VZD DARF Änderungen an VZD-Einträgen über die Schnittstelle
- 994 I_Directory_Maintenance NICHT zulassen, wenn an dem betroffenen VZD-Eintrag das
- 995 Attribut dataFromAuthority auf TRUE gesetzt ist.
- 996 [**<=**]
- 997 A_18472-01 - VZD, I_Directory_Administration, Doubletten
- 998 Der VZD MUSS bei den Operationen add_Directory_Entry und
- 999 modify_Directory_Entry prüfen, ob die Operation eine Doublette im LDAP-Verzeichnis
- 1000 erzeugt und in diesem Fall die Operation mit HTTP-Fehlercode "400 Bad Request"
- 1001 ablehnen. Zur Prüfung auf eine potentielle Dublette MUSS der VZD alle LDAP-Directory-
- 1002 Attribute des zu erzeugenden Basisdatensatzes (Verzeichnisdienst_Eintrag ohne
- 1003 Certificate und Fachdaten) jedoch ohne den Distinguished Name heranziehen.
- 1004 [**<=**]
- 1005 A_18602 - VZD, I_Directory_Administration, keine Datenänderung über Maintenance
- 1006 Schnittstelle
- 1007 Der VZD MUSS Änderungen an Basisdatensätzen und Zertifikatseinträgen (Certificate in
- 1008 Abb_VZD_logisches_Datenmodell) über andere Schnittstellen verhindern, wenn für den
- 1009 jeweiligen Eintrag Daten über die Schnittstelle I_Directory_Administration eingetragen
- 1010 wurden (LDAP-Directory Attribut dataFromAuthority == TRUE).
- 1011 Nicht erlaubte Änderungen MUSS der VZD mit faultcode 4202 (faultstring: SOAP Request
- 1012 enthält Fehler) ablehnen. [**<=**]

1013 **4.6.1.1 I Directory Administration - Lesen der Metadaten**

1014 Über Operation getInfo können die Metadaten der Schnittstelle
 1015 I Directory Administration gelesen werden.

1016 4.6.1.1.1 GET

1017 Diese Operation liefert die Metadaten der Schnittstelle I Directory Administration.

1018 A 21786 - VZD, I Directory Administration, getInfo

1019 Der VZD MUSS Operation „getInfo“ gemäß Tabelle Tab VZD „I Directory Administration-
 1020 Info“ umsetzen.

1022 **Tabelle 23: Tab VZD „I Directory Administration-getInfo“**

Name	<u>getInfo</u>

Beschreibung	Liefert die Metadaten (unter anderem aus dem InfoObject) dieser OpenAPI Spezifikation.	
Eingangsdaten	REST-Request GET / operationId: (siehe DirectoryAdministration.yaml)	
	Parameter	Beschreibung
	keine	-
Komponenten	Nutzer der Schnittstelle	
Ausgangsdaten	REST-Response mit Metadaten (InfoObject).	
Ablauf	Der VZD liefert die Metadaten der Schnittstelle in der Datenstruktur InfoObject zurück.	
Fehlerfälle	Es werden die protokollspezifischen Fehlermeldungen verwendet (TCP, HTTP, TLS) und in DirectoryAdministration.yaml mit spezifischen Fehlerbeschreibungen ergänzt.	

1023 [**<=**]

1024 A 21789 - VZD, Umsetzung I Directory Administration (REST)
 1025 Der VZD MUSS nach folgenden Vorgaben die Operation implementieren:

1026
 1027 In den Rückgabewerten müssen die aktuell gültigen Metainformationen für Schnittstelle
 1028 I Directory Administration zurückgegeben werden. Insbesondere muss

- 1029 1. Der Parameter *version* die aktuelle Version der Schnittstelle enthalten (entspricht
 1030 info.version der Schnittstellendefinition DirectoryAdministration.yaml)
- 1031 2. Der Parameter *title* den Titel der Schnittstelle enthalten (entspricht info.title der
 1032 Schnittstellendefinition DirectoryAdministration.yaml)
- 1033 3. Der Parameterstruktur *contact* die Kontaktinformationen für die Schnittstelle
 1034 enthalten. Über die - mit contact.url adressierte - Web-Seite muss die aktuell
 1035 verwendete Schnittstellendefinition DirectoryAdministration.yaml abrufbar sein.

1036 [**<=**]

1037 **4.6.1.14.6.1.2 DirectoryEntry Administration**

1038 Die Pflege der Basiseinträge (Verzeichnisdienst_Eintrag) erfolgt mit den im Folgenden
 1039 beschriebenen Operationen.

1040 4.6.1.1.14.6.1.2.1 POST

1041 Diese Operation legt einen neuen Eintrag im LDAP-Verzeichnis an.

1042 A_18448 - VZD, I_Directory_Administration, add_Directory_Entry
 1043 Der VZD MUSS Operation „add_Directory_Entry“ gemäß Tabelle Tab_VZD
 1044 „add_Directory_Entry“ umsetzen.
 1045

1046 **Tabelle 24: Tab_VZD „add_Directory_Entry“**

Name	add_Directory_Entry
-------------	---------------------

Beschreibung	Diese Operation ermöglicht die Erzeugung eines neuen Eintrags im LDAP-Verzeichnis.	
Eingangsdaten	REST-Request POST /DirectoryEntries operationId: add_Directory_Entry (siehe DirectoryAdministration.yaml)	
	Parameter	Beschreibung
	Verzeichnisdienst_Eintrag	Siehe Abb_VZD_logisches_Datenmodell und Tab_VZD_Datenbeschreibung. Der Distinguished Name wird vom VZD belegt. Der VZD übernimmt entsprechend Tab_VZD_Datenbeschreibung eine Reihe von Attributen aus dem Zertifikat.
	Certificate	Kann optional belegt werden. Siehe Abb_VZD_logisches_Datenmodell und Tab_VZD_Datenbeschreibung. Der Distinguished Name wird vom VZD belegt. Der VZD übernimmt entsprechend Tab_VZD_Datenbeschreibung eine Reihe von Attributen aus dem Zertifikat.
Komponenten	Nutzer der Schnittstelle, Verzeichnisdienst	
Ausgangsdaten	REST-Response mit dem Distinguished Name (dn) von dem Verzeichnisdienst_Eintrag.	
Ablauf	Der VZD übernimmt entsprechend Tab_VZD_Datenbeschreibung Attribute aus dem Zertifikat und trägt die übergebenen Parameter in den Verzeichniseintrag ein. Der VZD setzt das LDAP-Directory-Attribut dataFromAuthority auf den Wert TRUE.	
Fehlerfälle	Es werden die protokollspezifischen Fehlermeldungen verwendet (TCP, HTTP, TLS) und in DirectoryAdministration.yaml mit spezifischen Fehlerbeschreibungen ergänzt.	

- 1047 [<=]
- 1048 A_20271-01 - VZD, I_Directory_Administration, add_Directory_Entry, holder setzen
- 1049 Der VZD MUSS bei Operation „add_Directory_Entry“ den Eigentümer des erzeugten
- 1050 Verzeichniseintrags im Attribut "holder" entsprechend folgenden Vorgaben setzen:
- 1051 • Ist im add_Directory_Entry Request das Attribut "holder" nicht vorhanden oder
 - 1052 enthält keine Werte:
 - 1053 • Wird vom VZD aus dem ACCESS_TOKEN claim scope der Wert entnommen
 - 1054 und als "holder" in dieses Attribut eingetragen.
 - 1055 • Ist im add_Directory_Entry Request das Attribut "holder" vorhanden und mit
 - 1056 Inhalten gefüllt
 - 1057 a. Ist ein Wert aus dem Request Attribut "holder" nicht gültig, MUSS der VZD die
 - 1058 Operation mit HTTP-Status-Code 422 abweisen und die weitere Verarbeitung
 - 1059 von diesem Request abbrechen.

1060 b. Sind alle Werte aus dem Request Attribut "holder" gültig, MUSS der VZD die
 1061 Werte aus dem Request entnehmen und sie in das "holder" Attribut des
 1062 Verzeichniseintrags übernehmen.

1063 [**<=**]

1064 A 21791 - VZD, Prüfung auf Typ der Zertifikate

1065 Der VZD MUSS beim Hinzufügen von Zertifikaten mit den Operationen
 1066 „add Directory Entry“ und "add Directory Entry Certificate" den Typ der Zertifikate
 1067 prüfen. Der VZD MUSS alle Operationen mit Zertifikaten ablehnen, die nicht vom
 1068 Zertifikatstyp C.HCI.ENC oder C.HP.ENC (siehe [gemSpec OID#Tab PKI 405-01]
 1069 sind. Im Falle von unzulässigen Zertifikaten MUSS der VZD mit HTTP-Statuscode 422
 1070 (attributeName="userCertificate", attributeError="erläuternder Fehlertext") antworten
 1071 und darf die gesamte Operation nicht ausführen. [**<=**]

1072 A 21790 - VZD, Prüfung auf Gültigkeit der Zertifikate in der korrekten PKI-Umgebung

1073 Der VZD MUSS beim Hinzufügen von Zertifikaten in der PKI-Umgebung PU mit den
 1074 Operationen „add Directory Entry“ und "add Directory Entry Certificate" die Gültigkeit
 1075 der Zertifikate für diese PKI-Umgebung (PU) prüfen (TUC PKI 018 mit erfolgreichem
 1076 Status der Prüfung). In der PKI-Umgebung PU dürfen nur die Zertifikate akzeptiert
 1077 werden, die in dieser Umgebung gültig sind. Gültige Zertifikate aus anderen Umgebungen
 1078 müssen abgelehnt werden. In den PKI-Testumgebungen (RU, TU) erfolgt keine
 1079 Prüfung. [**<=**]

1080 A 21824 - VZD, I Directory Administration, stateOrProvinceName Prüfung

1081 Der VZD MUSS vor Ausführung der Operationen „add Directory Entry“ und
 1082 "modify Directory Entry"den Inhalt von Parameter stateOrProvinceName des Operation
 1083 Requests gegen die gültigen Werte entsprechend [gemILF Pflege VZD#Tabelle
 1084 TAB VZD Wertebereiche der Attribute] prüfen, wenn es sich um eine deutsche Adresse
 1085 handelt (countryCode = DE). Im Falle von ungültigen Werten MUSS der VZD mit HTTP-
 1086 Statuscode 422 (attributeName="stateOrProvinceName", attributeError="erläuternder
 1087 Fehlertext") antworten und darf die Operation nicht ausführen. [**<=**]

1088

1089 4.6.1.1-24.6.1.2.2 GET

1090 Diese Operation liest Verzeichniseinträge aus dem LDAP-Verzeichnis.

1091 A_18449-03 - VZD, I_Directory_Administration, read_Directory_Entry

1092 Der VZD MUSS Operation „read_Directory_Entry“ gemäß Tabelle Tab_VZD
 1093 „read_Directory_Entry“ umsetzen.

1094

1095 **Tabelle 25: Tab_VZD „read_Directory_Entry“**

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

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

1096 [\leq]

1097

1098 ~~4.6.1.1~~ 34.6.1.2.3 PUT

1099 Diese Operation aktualisiert den Verzeichniseintrag (ohne Zertifikate und Fachdaten) mit
1100 den übergebenen Daten im LDAP-Verzeichnis.

1101 A_18450-03 - VZD, I_Directory_Administration, modify_Directory_Entry
1102 Der VZD MUSS Operation „modify_Directory_Entry“ gemäß Tabelle Tab_VZD
1103 „modify_Directory_Entry“ umsetzen.
1104

1105 **Tabelle 26: Tab_VZD „modify_Directory_Entry“**

Name	modify_Directory_Entry	
Beschreibung	Diese Operation ermöglicht die Aktualisierung von Verzeichniseinträgen im LDAP-Verzeichnis.	
Eingangsdaten	REST-Request PUT /DirectoryEntries/{uid}/baseDirectoryEntries operationId: modify_Directory_Entry (siehe DirectoryAdministration.yaml)	
	Parameter	Beschreibung
	uid	Die „uid“ identifiziert den Verzeichnisdienst_Eintrag (Abb_VZD_logisches_Datenmodell) welcher aktualisiert wird.

	displayName	Kann optional angegeben werden und überschreibt den Wert im selektierten Verzeichniseintrag.
	otherName	Kann optional angegeben werden und überschreibt den Wert im selektierten Verzeichniseintrag.
	streetAddress	Kann optional angegeben werden und überschreibt den Wert im selektierten Verzeichniseintrag.
	postalCode	Kann optional angegeben werden und überschreibt den Wert im selektierten Verzeichniseintrag.
	localityName	Kann optional angegeben werden und überschreibt den Wert im selektierten Verzeichniseintrag.
	stateOrProviencename	Kann optional angegeben werden und überschreibt den Wert im selektierten Verzeichniseintrag.
	title	Kann optional angegeben werden und überschreibt den Wert im selektierten Verzeichniseintrag.
	organization	Kann optional angegeben werden und überschreibt den Wert im selektierten Verzeichniseintrag.
	specialization	Kann optional angegeben werden und überschreibt den Wert im selektierten Verzeichniseintrag.
	domainID	Kann optional angegeben werden und überschreibt den Wert im selektierten Verzeichniseintrag.
	holder	Kann optional angegeben werden. Durch setzen des "holder" kann ein Verzeichniseintrag an einen anderen Eigentümer weitergegeben werden. Die Weitergabe kann nur durch den aktuellen Eigentümer/holder erfolgen.
	maxKOMLEadr	Kann optional angegeben werden. Durch setzen von "maxKOMLEadr" wird die maximale Anzahl von mail Adressen in den KOM-LE Fachdaten festgelegt.

Komponenten	Nutzer der Schnittstelle, Verzeichnisdienst
Ausgangsdaten	REST-Response mit dem Distinguished Name (dn) von dem aktualisierten Verzeichnisdienst_Eintrag.
Ablauf	Der VZD aktualisiert im LDAP-Verzeichnis den über Parameter „uid“ identifizierten Verzeichniseintrag mit den übergebenen Parametern. Der VZD setzt das LDAP-Directory-Attribut dataFromAuthority auf den Wert TRUE.
Fehlerfälle	Es werden die protokollspezifischen Fehlermeldungen verwendet (TCP, HTTP, TLS) und in DirectoryAdministration.yaml mit spezifischen Fehlerbeschreibungen ergänzt.

1106 [**<=**]

1107 A_20272-02 - VZD, I_Directory_Administration, modify_Directory_Entry, Zugriffsrechte
 1108 Der VZD MUSS bei Operation „modify_Directory_Entry“ für den - über Parameter uid
 1109 adressierten - Verzeichniseintrag das Attribut "holder" im gespeicherten
 1110 Verzeichniseintrag und die aktuellen Parameter ("holder" und ACCESS_TOKEN claim
 1111 scope) der Operation „modify_Directory_Entry“ prüfen:

- 1112 • Wurde im Request Parameters "holder" ein Wert angegeben, der keinen aktuell
 1113 gültigen Wert für Schnittstelle I_Directory_Administration entspricht, MUSS der
 1114 VZD die Operation mit HTTP-Status-Code 422 abweisen.
- 1115 • Ist im Attribut "holder" im gespeicherten Verzeichniseintrags mindestens ein Wert
 1116 vorhanden
- 1117 • MUSS der VZD die Operation auszuführen und die übergebenen Werte - nach
 1118 Prüfung ihrer Gültigkeit - in den Verzeichniseintrag übernehmen wenn der
 1119 Wert von dem ACCESS_TOKEN claim scope einem Wert des Attributs "holder"
 1120 des gespeicherten Verzeichniseintrags entspricht. Ist dies nicht der Fall, MUSS
 1121 der VZD die Operation mit HTTP-Status-Code 401 abweisen.
- 1122 • Ist im Attribut "holder" im gespeicherten Verzeichniseintrags kein Wert vorhanden
 1123 und
- 1124 • in der Operation „modify_Directory_Entry“ wurden Werte für dieses "holder"
 1125 Attribut übergeben, MUSS der VZD die Operation ausführen und diese Werte -
 1126 nach Prüfung ihrer Gültigkeit - in den Verzeichniseintrag übernehmen.
- 1127 • in der Operation „modify_Directory_Entry“ wurde kein Wert für dieses "holder"
 1128 Attribut übergeben, MUSS der VZD die Operation ausführen und den Wert von
 1129 dem ACCESS_TOKEN claim scope in das Attribut "holder" des
 1130 Verzeichniseintrags übernehmen.

1131 [**<=**]

1132 A_21823 - VZD, I_Directory_Administration, modify_Directory_Entry, Limit
 1133 maxKOMLEadr
 1134 Der VZD MUSS bei Operation „modify_Directory_Entry“ nach erfolgreicher Aktualisierung
 1135 des VZD-Datensatzes die Anzahl der hinterlegten Mail-Adressen in den KOM-LE
 1136 Fachdaten mit dem Wert von Attribut maxKOMLEadr vergleichen. Die Anzahl
 1137 der hinterlegten mail Adressen in den KOM-LE Fachdaten, die den Wert von Attribut
 1138 maxKOMLEadr übersteigen, MUSS der VZD im Responde der Operation im Header X-

1139 maxKOMLEadr-Limit zurückgeben.

1140 [**<=**]

1141 Beispiele

1142

1143 a) maxKOMLEadr (nach Ausführung des Updates) = 1

1144 hinterlegte Mail-Adressen in den KOM-LE-Fachdaten = 1

1145 Header im Response:

1146 X-maxKOMLEadr-Limit: 0

1147 b) maxKOMLEadr (nach Ausführung des Updates) = 1

1148 hinterlegte Mail-Adressen in den KOM-LE-Fachdaten = 3

1149 Header im Response:

1150 X-maxKOMLEadr-Limit: 2

1151 **4.6.1.1.44.6.1.2.4 DELETE**

1152 Diese Operation löscht den gesamten Verzeichniseintrag (inklusive Zertifikaten und
1153 Fachdaten).

1154 A_18451 - VZD, I_Directory_Administration, delete_Directory_Entry
1155 Der VZD MUSS Operation „delete_Directory_Entry“ gemäß Tabelle Tab_VZD
1156 „delete_Directory_Entry“ umsetzen.
1157

1158 **Tabelle 27: Tab_VZD „delete_Directory_Entry“**

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

1159 [**<=**]

1160 A_20273-01 - VZD, I_Directory_Administration, delete_Directory_Entry, Zugriffsrechte

1161 Der VZD MUSS bei Operation „delete_Directory_Entry“ für den - über Parameter uid
 1162 adressierten - Verzeichniseintrag das Attribut "holder" im gespeicherten
 1163 Verzeichniseintrag gegen die aktuellen Parameter der Operation „delete_Directory_Entry“
 1164 prüfen:

- 1165 • Enthalten die Werte des Attributs "holder" im gespeicherten Verzeichniseintrag
 1166 den Wert von dem ACCESS_TOKEN claim scope, MUSS der VZD die Operation
 1167 ausführen.
- 1168 • Enthält das Attributs "holder" im gespeicherten Verzeichniseintrag keine Werte,
 1169 MUSS der VZD die Operation ausführen.
- 1170 • Enthalten die Werte des Attributs "holder" im gespeicherten Verzeichniseintrag
 1171 nicht den Wert von dem ACCESS_TOKEN claim scope, MUSS der VZD die
 1172 Operation mit HTTP-Status-Code 401 abweisen.

1173 [**<=**]

1174

1175 **4.6.1.24.6.1.3 Certificate Administration**

1176 Die Pflege der Zertifikatseinträge (Certificate in Abb_VZD_logisches_Datenmodell) erfolgt
 1177 mit den im Folgenden beschriebenen Operationen.

1178 **4.6.1.2.14.6.1.3.1 POST**

1179 Diese Operation fügt einem existierenden Basisdatensatz einen Zertifikatseintrag im
 1180 LDAP-Verzeichnis an.

1181 A_18452 - VZD, I_Directory_Administration, add_Directory_Entry_Certificate
 1182 Der VZD MUSS Operation „add_Directory_Entry_Certificate“ gemäß Tabelle Tab_VZD
 1183 „add_Directory_Entry_Certificate“ umsetzen.
 1184

1185 **Tabelle 28: Tab_VZD „add_Directory_Entry_Certificate“**

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

Ausgangsdaten	REST-Response mit dem Distinguished Name (dn) von dem erzeugten Certificate-Eintrag.
Ablauf	Der VZD übernimmt entsprechend Tab_VZD_Datenbeschreibung Attribute aus dem Zertifikat und trägt die übergebenen Parameter in den Zertifikatseintrag ein. Der Distinguished Name (dn) von dem erzeugten Certificate wird vom Verzeichnisdienst gefüllt und über dn.uid mit dem übergeordneten Verzeichnisdienst_Eintrag verknüpft.
Fehlerfälle	Es werden die protokollspezifischen Fehlermeldungen verwendet (TCP, HTTP, TLS) und in DirectoryAdministration.yaml mit spezifischen Fehlerbeschreibungen ergänzt.

1186 [**<=**]

1187 ~~4.6.1.2-24.6.1.3.2~~ GET

1188 Diese Operation liest Zertifikatseinträge aus dem LDAP-Verzeichnis.

1189 A_18453-01 - VZD, I_Directory_Administration, read_Directory_Certificates

1190 Der VZD MUSS Operation „read_Directory_Certificates“ gemäß Tabelle Tab_VZD

1191 „read_Directory_Certificates“ umsetzen.

1192

1193 **Tabelle 29: Tab_VZD „read_Directory_Certificates“**

Name	read_Directory_Certificates	
Beschreibung	Diese Operation ermöglicht die Suche und das Lesen von Zertifikatseinträgen (Certificate in Abb_VZD_logisches_Datenmodell) im LDAP-Verzeichnis.	
Eingangsdaten	REST-Request GET /DirectoryEntries/Certificates operationId: read_Directory_Certificates (siehe DirectoryAdministration.yaml) Mindestens ein Filterparameter muss angegeben werden.	
	Parameter	Beschreibung
	uid	Optionalen Parameter. Die „uid“ identifiziert einen Verzeichnisdienst_Eintrag (Abb_VZD_logisches_Datenmodell). Dieser Parameter selektiert alle Zertifikatseinträge dieses Verzeichnisdiensteintrags.
certificateEntryID	Optionalen 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.
Komponenten	Nutzer der Schnittstelle, Verzeichnisdienst	
Ausgangsdaten	REST-Response mit allen zu den Filter Parametern passenden Zertifikatseinträgen.	
Ablauf	Der VZD sucht im LDAP Verzeichnis die zu den Such-Parametern passenden Zertifikatseinträge. Bei mehr als 100 gefundenen Einträgen werden nur 100 gefundenen Einträge zurückgegeben.	
Fehlerfälle	Es werden die protokollspezifischen Fehlermeldungen verwendet (TCP, HTTP, TLS) und in DirectoryAdministration.yaml mit spezifischen Fehlerbeschreibungen ergänzt.	

1194 [<=]

1195 4.6.1.3.3 DELETE

1196 Diese Operation löscht einen Zertifikatseintrag.

1197 A 18455 - VZD, I Directory Administration, delete Directory Entry Certificate

1198 Der VZD MUSS Operation „delete Directory Entry Certificate“ gemäß Tabelle Tab VZD

1199 „delete Directory Entry Certificate“ umsetzen.

1200

1201 Tabelle 30: Tab VZD „delete Directory Entry Certificate“

Name	<u>delete Directory Entry Certificate</u>	
Beschreibung	<u>Diese Operation ermöglicht die Löschung eines Zertifikatseintrags im LDAP-Verzeichnis.</u>	
Eingangsdaten	<u>REST-Request</u> <u>DELETE</u> <u>/DirectoryEntries/{uid}/Certificates/{certificateEntryID}</u> <u>operationId: delete Directory Entry Certificate (siehe DirectoryAdministration.yaml)</u>	
	<u>Parameter</u>	<u>Beschreibung</u>
	<u>uid</u>	<u>Pflichtparameter.</u> <u>Die „uid“ identifiziert den Verzeichnisdienst Eintrag (Abb VZD logisches Datenmodell) zu dem der Zertifikatseintrag gehört.</u>
	<u>certificateEntryID</u>	<u>Pflichtparameter.</u> <u>Dieser Parameter identifiziert einen Zertifikatseintrag</u>

	(Abb VZD logisches Datenmodell dn.cn von Certificate).
Komponenten	Nutzer der Schnittstelle, Verzeichnisdienst
Ausgangsdaten	REST-Response.
Ablauf	Der VZD löscht im LDAP-Verzeichnis den über die Parameter „uid“ und „certificateEntryID“ identifizierten Zertifikatseintrag.
Fehlerfälle	Es werden die protokollspezifischen Fehlermeldungen verwendet (TCP, HTTP, TLS) und in DirectoryAdministration.yaml mit spezifischen Fehlerbeschreibungen ergänzt.

1202 [<=]

1203

1204

1205 **4.6.1.34.6.1.4 DirectoryEntry Synchronization**

1206 Zur Unterstützung der Pflege der Basiseinträge (Verzeichnisdienst_Eintrag) wird die hier
 1207 beschriebene Operation zur Verfügung gestellt. Sie dient der Synchronisation mit dem
 1208 Datenbestand des Verzeichnisdienstes und erlaubt – im Gegensatz zur Operation
 1209 „read_Directory_Entry“ – das Lesen beliebig vieler eigener Verzeichniseinträge.

1210 4.6.1.3.14.6.1.4.1 GET

1211 A_21230-01 - VZD, I_Directory_Administration, read_Directory_Entry_for_Sync
 1212 Der VZD MUSS Operation „read_Directory_Entry_for_Sync“ gemäß Tabelle Tab_VZD
 1213 „read_Directory_Entry_for_Sync“ umsetzen.
 1214

1215 **Tabelle 31: Tab_VZD „read_Directory_Entry_for_Sync“**

Name	read_Directory_Entry_for_Sync	
Beschreibung	Diese Operation ermöglicht die Suche und Lesen von Verzeichniseinträgen im LDAP-Verzeichnis. Diese Operation liefert auch Einträge, die ohne gültige Zertifikate sind.	
Eingangsdaten	REST-Request GET /DirectoryEntries operationId: read_Directory_Entry (siehe DirectoryAdministration.yaml)	
	Parameter	Beschreibung
	Parameter zur Selektion der Verzeichniseinträge	Alle im Datenmodell aufgeführten Felder des Basiseintrags - insbesondere auch dataFromAuthority - können zur Suche genutzt werden. Die angegebenen Parameter werden zur Suche mit einem logischen UND verknüpft.
Komponenten	Nutzer der Schnittstelle, Verzeichnisdienst	

Ausgangsdaten	REST-Response mit allen zu den Filterparametern passenden Verzeichniseinträgen. Die Verzeichniseinträge werden optional inklusive Zertifikatseinträgen und Fachdaten geliefert.
Ablauf	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.
Fehlerfälle	Es werden die protokollspezifischen Fehlermeldungen verwendet (TCP, HTTP, TLS) und in DirectoryAdministration.yaml mit spezifischen Fehlerbeschreibungen ergänzt.

1216 [**<=**]

1217 A_20402-02 - VZD, I_Directory_Administration, read_Directory_Entry_for_Sync, Paging,
1218 Berechtigung

1219 Der VZD MUSS für den Paging Mechanismus von Operation

1220 „read_Directory_Entry_for_Sync“ sicherstellen:

- 1221 • Der "holder" Suchparameter muss den gleichen Wert enthalten wie der
1222 ACCESS_TOKEN claim scope.
- 1223 • Die pagingSize darf die Maximalgröße entsprechend TIP1-A_5552 nicht
1224 überschreiten.
- 1225 • Die Suchparameter dürfen sich während eines Pagings (mit mehreren
1226 Request/Response Sequenzen) nicht ändern (nur das "cookie" ändert sich).

1227 Bei Abweichungen von diesen Festlegungen MUSS der VZD mit einem Fehler (HTTP-
1228 Status-Code 403) antworten.

1229 [**<=**]

1230

1231 **4.6.2 Nutzung der Schnittstelle I_Directory_Administration**

1232 Der Client der Schnittstelle I_Directory_Administration muss eine TLS-Verbindung mit
1233 serverseitiger Authentisierung nutzen. Dabei muss er das Serverzertifikat des VZD
1234 prüfen. Bei negativem Ergebnis muss der Verbindungsaufbau abgebrochen werden.

1235 Mit Hilfe der Operationen der Schnittstelle muss der Client die Verzeichniseinträge
1236 eintragen und pflegen.

1237 Beispielablauf:

1238 Falls die „uid“ des Verzeichniseintrags nicht bekannt ist erfolgt die Suche nach einem
1239 vorhandenen Verzeichniseintrag mit der telematikID (operationId
1240 read_Directory_Certificates mit Parameter telematikID)

1241 a. Falls ein Eintrag gefunden wurde:

1242 1. Lesen des Basis-Verzeichniseintrags (operationId read_Directory_Entry mit Parameter
1243 „uid“ aus dem read_Directory_Certificates Response)

- 1244 2. Aktualisieren des Verzeichniseintrags und (je nach Bedarf) der dazugehörigen
1245 Zertifikatseinträge (operationId's: modify_Directory_Entry, delete_Directory_Entry,
1246 modify_Directory_Entry_Certificate, delete_Directory_Entry_Certificate)
- 1247 b. Falls kein Eintrag gefunden wurde:
- 1248 1. Erzeugen des Verzeichniseintrags und (je nach Bedarf) anhängen zusätzlicher
1249 Zertifikatseinträge (operationId's: add_Directory_Entry, add_Directory_Entry_Certificate). Der
1250 erste Zertifikatseintrag wird mit Operation add_Directory_Entry erzeugt da jeder
1251 Verzeichniseintrag mindestens einen Zertifikatseintrag enthalten muss.
1252 Zusätzliche Zertifikatseinträge können mit Operation add_Directory_Entry_Certificate
1253 hinzugefügt werden.
- 1254

ENTWURF

1255

5 Datenmodell

- 1256 ~~TIP1-A_5607-06~~**TIP1-A_5607-05** - VZD, logisches Datenmodell
- 1257 Der VZD MUSS das logische Datenmodell nach Abb_VZD_logisches_Datenmodell und
- 1258 Tab_VZD_Datenbeschreibung implementieren. Es wird keine Vorgabe an die technische
- 1259 Ausprägung des Datenmodells gemacht.
- 1260 Der VZD MUSS sicherstellen, dass ein Eintrag nur Zertifikate aus dem Vertrauensraum
- 1261 der TI mit gleicher Telematik-ID enthält.
- 1262

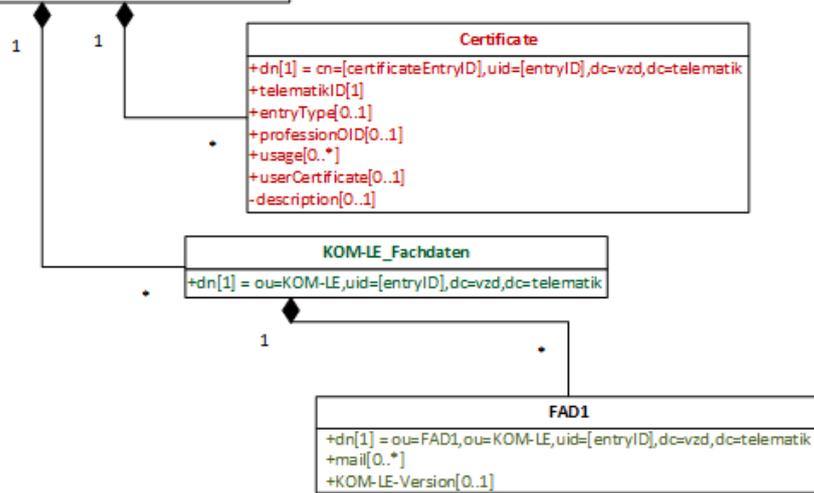
Verzeichnisdienst_Eintrag
+dn[1] = uid=[entryID],dc=vzd,dc=telematik
+givenName[0..1]
+sn[0..1]
+streetAddress[0..1]
+localityName[0..1]
+postalCode[0..1]
+countryCode[1]
+stateOrProvinceName[0..1]
+cn[1]
+displayName[0..1]
+title[0..1]
+organization[0..1]
+otherName[0..1]
+telematikID[1]
+specialization[0..*]
+domainID[0..*]
+personalEntry[1]
+dataFromAuthority[0..1]
+holder[0..*]
+maxKOMLEadr[0..1]
+changeDateTime[1]

Verzeichnisdienst_Eintrag_flache_Liste
+dn[1] = uid=[entryID],dc=data,dc=vzd
+givenName[0..1]
+sn[0..1]
+streetAddress[0..1]
+localityName[0..1]
+postalCode[0..1]
+countryCode[1]
+stateOrProvinceName[0..1]
+cn[1]
+displayName[0..1]
+title[0..1]
+organization[0..1]
+otherName[0..1]
+specialization[0..*]
+domainID[0..*]
+mail[0..*]
+KOM-LE-Version[0..1]
+telematikID[1]
+entryType[0..*]
+professionOID[0..*]
+usage[0..*]
+userCertificate[0..*]
+personalEntry[1]
+dataFromAuthority[0..1]
+owner[0..*]
+maxKOMLEadr[0..1]
+changeDateTime[1]

Certificate
+dn[1] = cn=[certificateEntryID],uid=[entryID],dc=vzd,dc=telematik
+telematikID[1]
+entryType[0..1]
+professionOID[0..1]
+usage[0..*]
+userCertificate[0..1]
-description[0..1]

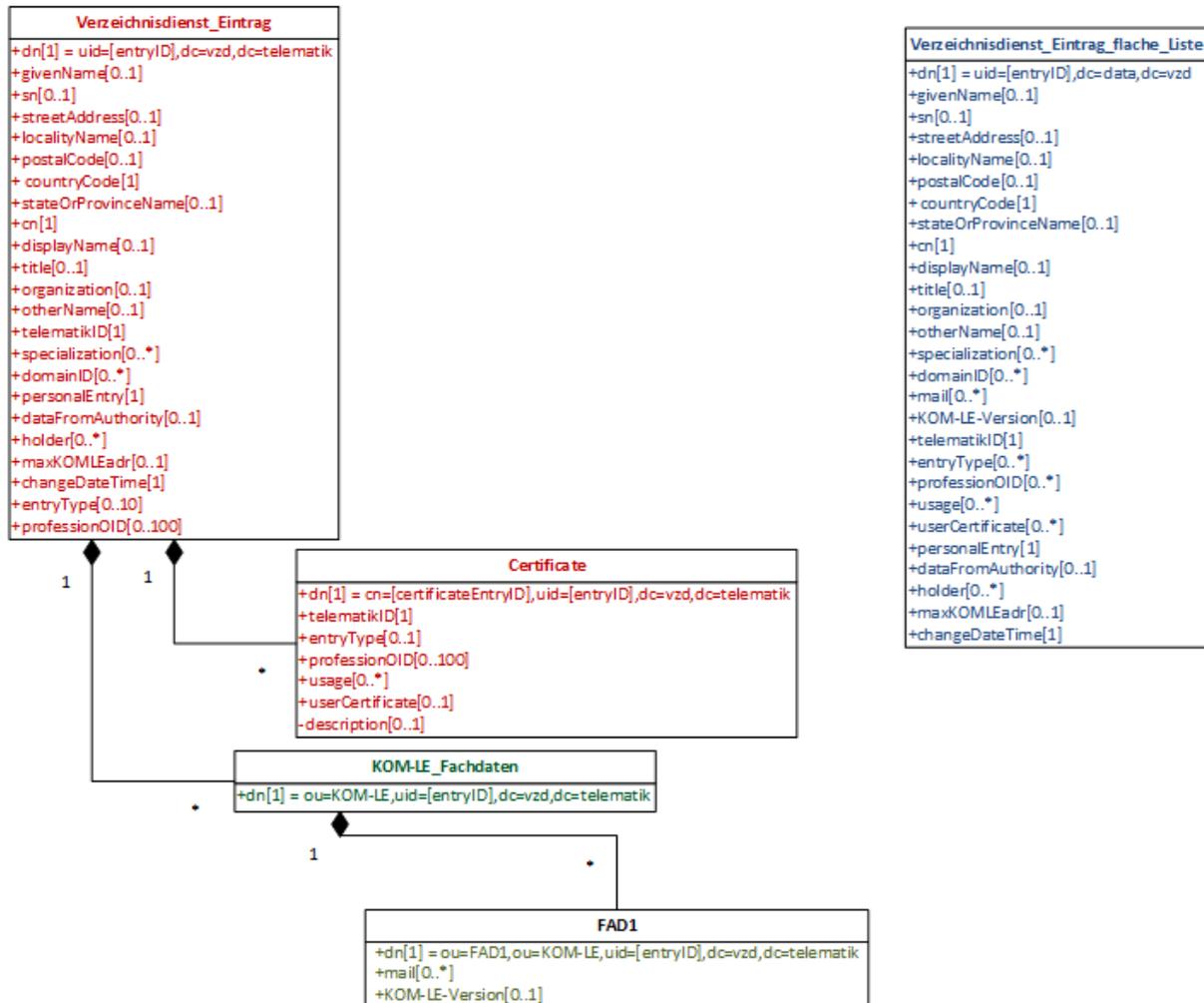
KOM-LE_Fachdaten
+dn[1] = ou=KOM-LE,uid=[entryID],dc=vzd,dc=telematik

FAD1
+dn[1] = ou=FAD1,ou=KOM-LE,uid=[entryID],dc=vzd,dc=telematik
+mail[0..*]
+KOM-LE-Version[0..1]



1263

ENTWURF



1264

1265

1266

Abbildung 2: Abb_VZD_logisches_Datenmodell

Tabelle 32: Tab_VZD_Datenbeschreibung

LDAP-Directory Attribut	Pflichtfeld ?	Erläuterung
givenName	optional	HBA-Eintrag: Bezeichner: Vorname, 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.
cn	obligatorisch	HBA: Eintrag: Bezeichner: Nachname, Vorname SMC-B Eintrag: Bezeichner: Name Wird vom VZD unabhängig vom Kartentyp 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: Anzeigenname, Name nach dem der Eintrag von Nutzern gesucht wird und unter dem gefundene Einträge angezeigt werden. Konvention für HBA Einträge: Name, Vorname
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 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). Für Einträge der Leistungserbringerorganisationen (SMC-B Eintrag) Der Wertebereich entspricht den in hl7 definierten und für ePA festgelegten Werten (https://wiki.hl7.de/index.php?title=IG:Value_Sets_f%C3%BCr_XDS#DocumentEntry.practiceSettingCode). urn:psc:<OID Codesystem:Code> Beispiel für Allgemeinmedizin: urn:psc:1.3.6.1.4.1.19376.3.276.1.5.4:ALLG Beispiel für Zahnmedizin: urn:psc:1.3.6.1.4.1.19376.3.276.1.5.4:MKZH Beispiel für Apotheke: urn:psc:1.3.6.1.4.1.19376.3.276.1.5.5:PHZ Beispiel für Krankenhaus: urn:psc:1.3.6.1.4.1.19376.3.276.1.5.4:GESU Für Einträge der Leistungserbringer (HBA-Eintrag) Der Wertebereich entspricht den in hl7 definierten Werten (https://wiki.hl7.de/index.php?title=IG:Value_Sets_f%C3%BCr_XDS#DocumentEntry.authorSpecialty).

		<p>urn:as:<OID Codesystem:Code> Psychologischer Psychotherapeut: urn:as:1.3.6.1.4.1.19376.3.276.1.5.11:82 Psychotherapeut: urn:as:1.3.6.1.4.1.19376.3.276.1.5.11:183 Fachpsychotherapeut für Kinder und Jugendliche: urn:as:1.3.6.1.4.1.19376.3.276.1.5.11:184 Fachpsychotherapeut für Erwachsene: urn:as:1.3.6.1.4.1.19376.3.276.1.5.11:185 Beispiel für FA Allgemeinmedizin: urn:as:1.2.276.0.76.5.514:011001 Beispiel für Zahnarzt: urn:as:1.2.276.0.76.5.492:1</p>
domainID	optional	Bezeichner: domänenspezifisches Kennzeichen des Eintrags. kann mehrfach vorkommen (0..100)
holder	optional	Legt fest, wer Änderungen an den Basisdaten des Eintrags vornehmen darf. Hat keinen Einfluss auf Fachdaten und Zertifikatsdaten.
maxKOMLEader	optional	Maximale Anzahl von mail Adressen in den KOM-LE-Fachdaten. Falls kein Wert eingetragen wurde, können beliebig viele mail Adressen in den KOM-LE Fachdaten eingetragen werden. Falls ein Wert eingetragen wurde, können maximal so viele mail Adressen in den KOM-LE Fachdaten eingetragen werden.
personalEntry	obligatorisch	Wird vom VZD eingetragen Wert == TRUE, wenn 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.. 50 100) 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 Hinweis: wird 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 1000) 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.
changeDateTime	obligatorisch	Der VZD setzt dieses Attribut bei jeder Schreiboperation für den Datensatz (Basisdaten) auf die aktuelle Zeit. Format entsprechend RFC 3339, section 5.6.

1267 [\leq]

1268

1269 Die Abbildung Abb_VZD_logisches_Datenmodell stellt die Datenstruktur des
1270 Verzeichnisdienstes als UML-Klassendiagramm dar. Die Basisdaten sind rot, die
1271 Fachdaten grün und die als Ergebnis der LDAP-Suche in Form einer flachen Liste
1272 gefundenen Einträge sind blau dargestellt. Zu jedem Attribut ist die Kardinalität in
1273 eckigen Klammern angegeben.

1274 Unter dem Begriff SMC-B sind alle Ausprägungen zusammengefasst (SMC-B ORG, SMC-B
1275 KTR). Wenn eine Differenzierung erforderlich ist, wird die spezifische Ausprägung der
1276 SMC-B explizit beschrieben.

1277 In der folgenden Tabelle wird der Wertebereich für das Attribut Eintragstyp (in LDAP ==
1278 entryType) sowie das Mapping auf die ProfessionOID festgelegt.

1279

1280 **Tabelle 33: Tab_VZD_Mapping_Eintragstyp_und_ProfessionOID**

Eintragstyp	Eintragstyp Bedeutung	ProfessionOID (ProfessionItem)
-------------	-----------------------	--------------------------------

1	Berufsgruppe	1.2.276.0.76.4.30 (Ärztin/Arzt) 1.2.276.0.76.4.31 (Zahnärztin/Zahnarzt) 1.2.276.0.76.4.32 (Apotheker/-in) 1.2.276.0.76.4.33 (Apothekerassistent/-in) 1.2.276.0.76.4.34 (Pharmazieingenieur/-in) 1.2.276.0.76.4.35 (pharmazeutisch-technische/-r Assistent/-in) 1.2.276.0.76.4.36 (pharmazeutisch-kaufmännische/-r Angestellte) 1.2.276.0.76.4.37 (Apothekenhelfer/-in) 1.2.276.0.76.4.38 (Apothekenassistent/-in) 1.2.276.0.76.4.39 (Pharmazeutische/-r Assistent/-in) 1.2.276.0.76.4.40 (Apothekenfacharbeiter/-in) 1.2.276.0.76.4.41 (Pharmaziepraktikant/-in) 1.2.276.0.76.4.42 (Stud.pharm. oder Famulant/-in) 1.2.276.0.76.4.43 (PTA-Praktikant/-in) 1.2.276.0.76.4.44 (PKA Auszubildende/-r) 1.2.276.0.76.4.45 (Psychotherapeut/-in) 1.2.276.0.76.4.46 (Psychologische/-r Psychotherapeut/-in) 1.2.276.0.76.4.47 (Kinder- und Jugendlichenpsychotherapeut/-in) 1.2.276.0.76.4.48 (Rettungsassistent/-in) 1.2.276.0.76.4.178 (Notfallsanitäter/-in)
2	Versicherte/-r	1.2.276.0.76.4.49 (Versicherte/-r)
3	Leistungserbringer Institution	1.2.276.0.76.4.50 (Betriebsstätte Arzt) 1.2.276.0.76.4.51 (Zahnarztpraxis) 1.2.276.0.76.4.52 (Betriebsstätte Psychotherapeut) 1.2.276.0.76.4.53 (Krankenhaus) 1.2.276.0.76.4.54 (Öffentliche Apotheke) 1.2.276.0.76.4.55 (Krankenhausapotheker) 1.2.276.0.76.4.56 (Bundeswehrapotheker) 1.2.276.0.76.4.57 (Betriebsstätte Mobile Einrichtung Rettungsdienst)
4	Organisation	1.2.276.0.76.4.187 (Betriebsstätte Leistungserbringerorganisation Vertragszahnärzte)
5	Krankenkasse	1.2.276.0.76.4.59 (Betriebsstätte Kostenträger)
6	Krankenkasse ePA	1.2.276.0.76.4.XXX (ePA KTR-Zugriffsautorisierung)

1282

6 Anhang A – Verzeichnisse

1283 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

1284

1285 **6.2 Glossar**

1286 Das Glossar wird als eigenständiges Dokument (vgl. [gemGlossar]) zur Verfügung
1287 gestellt.

1288 **6.3 Abbildungsverzeichnis**

1289 Abbildung 1: Einordnung des VZD in die TI..... 8

1290 Abbildung 2: Abb VZD logisches Datenmodell..... 60

1291

1292

1293 **6.4 Tabellenverzeichnis**

1294 Tabelle 1: Tab PT VZD Schnittstellen..... 12

1295 Tabelle 2: Tab VZD Schnittstelle I Directory Query..... 12

1296 Tabelle 3: Tab TUC VZD 0001..... 14

1297	<u>Tabelle 4: Tab VZD Schnittstelle I Directory Maintenance</u>	14
1298	<u>Tabelle 5: Tab VZD Daten-Transformation</u>	16
1299	<u>Tabelle 6: Tab TUC VZD 0002</u>	18
1300	<u>Tabelle 7: Tab TUC VZD 0003</u>	20
1301	<u>Tabelle 8: Tab TUC VZD 0004</u>	21
1302	<u>Tabelle 9: Tab TUC VZD 0005</u>	23
1303	<u>Tabelle 10: Tab VZD Schnittstelle I Directory Application Maintenance</u>	24
1304	<u>Tabelle 11: Tab VZD „I Directory Application Maintenance-getInfo“</u>	26
1305	<u>Tabelle 12: VZD TAB I Directory Application Maintenance Add Mapping</u>	27
1306	<u>Tabelle 13: Tab TUC VZD 0006</u>	28
1307	<u>Tabelle 14: VZD TAB KOM-LE Attributes.....</u>	29
1308	<u>Tabelle 15: Tab TUC VZD 0007</u>	29
1309	<u>Tabelle 16: Tab TUC VZD 0008</u>	32
1310	<u>Tabelle 17: Tab TUC VZD 0009</u>	33
1311	<u>Tabelle 18: VZD TAB I Directory Application Maintenance Modify Mapping.....</u>	35
1312	<u>Tabelle 19: Tab TUC VZD 0010</u>	36
1313	<u>Tabelle 20: VZD TAB KOM-LE Attributes.....</u>	36
1314	<u>Tabelle 21: Tab TUC VZD 0011</u>	37
1315	<u>Tabelle 22: Tab VZD Schnittstelle I Directory Administration.....</u>	41
1316	<u>Tabelle 23: Tab VZD „I Directory Administration-getInfo“</u>	44
1317	<u>Tabelle 24: Tab VZD „add Directory Entry“.....</u>	45
1318	<u>Tabelle 25: Tab VZD „read Directory Entry“</u>	47
1319	<u>Tabelle 26: Tab VZD „modify Directory Entry“.....</u>	48
1320	<u>Tabelle 27: Tab VZD „delete Directory Entry“</u>	51
1321	<u>Tabelle 28: Tab VZD „add Directory Entry Certificate“</u>	52
1322	<u>Tabelle 29: Tab VZD „read Directory Certificates“.....</u>	53
1323	<u>Tabelle 30: Tab VZD „delete Directory Entry Certificate“</u>	54
1324	<u>Tabelle 31: Tab VZD „read Directory Entry for Sync“.....</u>	55
1325	<u>Tabelle 32: Tab VZD Datenbeschreibung.....</u>	60
1326	<u>Tabelle 33: Tab VZD Mapping Eintragstyp und ProfessionOID.....</u>	63
1327		
1328		

1329 **6.5 Referenzierte Dokumente**1330 **6.5.1 Dokumente der gematik**

1331 Die nachfolgende Tabelle enthält die Bezeichnung der in dem vorliegenden Dokument
 1332 referenzierten Dokumente der gematik zur Telematikinfrastruktur. Der mit der
 1333 vorliegenden Version korrelierende Entwicklungsstand dieser Konzepte und
 1334 Spezifikationen wird pro Release in einer Dokumentenlandkarte definiert; Version und
 1335 Stand der referenzierten Dokumente sind daher in der nachfolgenden Tabelle nicht
 1336 aufgeführt. Deren zu diesem Dokument jeweils gültige Versionsnummern sind in der
 1337 aktuellen, von der gematik veröffentlichten Dokumentenlandkarte enthalten, in der die
 1338 vorliegende Version aufgeführt wird.

1339

[Quelle]	Herausgeber: Titel
[gemGlossar]	gematik: Glossar der Telematikinfrastruktur
[gemKPT_Arch_TIP]	gematik: Konzept Architektur der TI-Plattform
[gemKPT_PKI_TIP]	gematik: Konzept PKI der TI-Plattform
[gemKPT_DS_TIP]	gematik: Datenschutzkonzept TI-Plattform
[gemKPT_Sich_TIP]	gematik: Spezifisches Sicherheitskonzept TI-Plattform
[gemSpec_Net]	gematik: Spezifikation Netzwerk
[gemSpec_OM]	gematik: Operations und Maintenance Spezifikation
[gemSpec_OID]	gematik: Spezifikation Festlegung von OIDs
[gemSpec_PKI]	gematik: Spezifikation PKI
[gemSpec_Perf]	gematik: Performance und Mengengerüst TI-Plattform
[gemSpec_TSL]	gematik: Spezifikation TSL-Dienst
<u>[gemILF_Pflege_VZD]</u>	<u>gematik: Implementierungsleitfaden zur Pflege der Daten des Verzeichnisdienstes</u>

1340

1341 **6.5.2 Weitere Dokumente**

[Quelle]	Herausgeber (Erscheinungsdatum): Titel

[BSI-APP.2.1]	Bundesamt für Sicherheit in der Informationstechnik: BSI Grundsatz-Kompendium, Baustein APP.2.1, https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/APP/APP_2_1_Allgemeiner_Verzeichnisdienst.html
[BSI-SiGw]	Bundesamt für Sicherheit in der Informationstechnik (o.J.): Konzeption von Sicherheitsgateways, Version 1.0
[HL7FHIR]	FHIR Specification https://www.hl7.org/fhir/
[RFC2119]	RFC 2119 (March 1997): Key words for use in RFCs to Indicate Requirement Levels http://www.rfc-editor.org/rfc/rfc2119.txt
[RFC2696]	RFC 2696 (September 1999) LDAP Control Extension for Simple Paged Results Manipulation https://tools.ietf.org/html/rfc2696
[RFC4510]	RFC 4510 (June 2006): Lightweight Directory Access Protocol (LDAP): Technical Specification Road Map, http://www.ietf.org/rfc/rfc4510.txt
[RFC4511]	RFC 4511 (June 2006): Lightweight Directory Access Protocol (LDAP): The Protocol, http://www.ietf.org/rfc/rfc4511.txt
[RFC4512]	RFC 4512 (June 2006): Lightweight Directory Access Protocol (LDAP): Directory Information Models http://www.rfc-editor.org/rfc/rfc4512.txt
[RFC4513]	RFC 4513 (June 2006): Lightweight Directory Access Protocol (LDAP): Authentication Methods and Security Mechanisms http://www.rfc-editor.org/rfc/rfc4513.txt
[RFC4514]	RFC 4514 (June 2006): Lightweight Directory Access Protocol (LDAP): String Representation of Distinguished Names http://www.rfc-editor.org/rfc/rfc4514.txt

[RFC4 515]	RFC 4515 (June 2006): Lightweight Directory Access Protocol (LDAP): String Representation of Search Filters http://www.rfc-editor.org/rfc/rfc4515.txt
[RFC4 516]	RFC 4516 (June 2006): Lightweight Directory Access Protocol (LDAP): Uniform Resource Locator http://www.rfc-editor.org/rfc/rfc4516.txt
[RFC4 517]	RFC 4517 (June 2006): Lightweight Directory Access Protocol (LDAP): Syntaxes and Matching Rules http://www.rfc-editor.org/rfc/rfc4515.txt
[RFC4 519]	RFC 4519 (June 2006): Lightweight Directory Access Protocol (LDAP): Schema for User Applications http://www.rfc-editor.org/rfc/rfc4519.txt
[RFC4 522]	RFC 4522 (June 2006): Lightweight Directory Access Protocol (LDAP): The Binary Encoding Option http://www.rfc-editor.org/rfc/rfc4522.txt
[RFC4 523]	RFC 4523 (June 2006): Lightweight Directory Access Protocol (LDAP) Schema Definitions for X.509 Certificates http://www.rfc-editor.org/rfc/rfc4523.txt
[RFC 6750]	The OAuth 2.0 Authorization Framework: Bearer Token Usage
[RFC6 763]	RFC 6763 (February 2013): DNS-Based Service Discovery http://www.rfc-editor.org/rfc/rfc6763.txt

1342

1343