Einführung der Gesundheitskarte

Spezifikation

Verzeichnisdienst

|  |  |
| --- | --- |
| Version: | 1.5.0 |
| Revision: | \main\rel\_ors1\rel\_opb1\20 |
| Stand: | 21.04.2017 |
| Status: | freigegeben |
| Klassifizierung: | öffentlich |
| Referenzierung: | gemSpec\_VZD |

Dokumentinformationen

**Änderungen zur Vorversion**

Anpassungen nach Änderungsliste

**Dokumentenhistorie**

| **Version** | **Stand** | **Kap./ Seite** | **Grund der Änderung, besondere Hinweise** | **Bearbeitung** |
| --- | --- | --- | --- | --- |
| 0.0.7 | 24.10.13 |  | initiale Version | gematik |
| 0.1.0 | 08.11.13 |  | internes Review durchgeführt | gematik |
| 1.2.0 | 17.07.15 |  | Nutzer der Schnittstelle I\_Directory\_Maintenance geändert | gematik |
| 1.3.0 | 24.08.16 |  | Anpassungen zum Online-Produktivbetrieb (Stufe 1) | gematik |
| 1.4.0 | 28.10.16 |  | Einarbeitung lt. Änderungsliste |  |
|  |  |  | Anpassung nach Änderungsliste | gematik |
| 1.5.0 | 19.04.17 |  | freigegeben | gematik |

Inhaltsverzeichnis

[1 Einordnung des Dokumentes 5](#_Toc486428185)

[1.1 Zielsetzung 5](#_Toc486428186)

[1.2 Zielgruppe 5](#_Toc486428187)

[1.3 Geltungsbereich 5](#_Toc486428188)

[1.4 Abgrenzungen 5](#_Toc486428189)

[1.5 Methodik 6](#_Toc486428190)

[2 Systemüberblick 7](#_Toc486428191)

[3 Übergreifende Festlegungen 8](#_Toc486428192)

[3.1 IT-Sicherheit und Datenschutz 8](#_Toc486428193)

[3.2 Fachliche Anforderungen 10](#_Toc486428194)

[4 Funktionsmerkmale 12](#_Toc486428195)

[4.1 Schnittstelle I\_Directory\_Query 12](#_Toc486428196)

[4.1.1 Operation search\_Directory 13](#_Toc486428197)

[4.1.1.1 Umsetzung 13](#_Toc486428198)

[4.1.1.2 Nutzung 13](#_Toc486428199)

[4.2 Schnittstelle I\_Directory\_Maintenance 14](#_Toc486428200)

[4.2.1 Operation add\_Directory\_Entry 15](#_Toc486428201)

[4.2.1.1 Umsetzung 15](#_Toc486428202)

[4.2.1.2 Nutzung 16](#_Toc486428203)

[4.2.2 Operation read\_Directory\_Entry 17](#_Toc486428204)

[4.2.2.1 Umsetzung 17](#_Toc486428205)

[4.2.2.2 Nutzung 19](#_Toc486428206)

[4.2.3 Operation modify\_Directory\_Entry 19](#_Toc486428207)

[4.2.3.1 Umsetzung 19](#_Toc486428208)

[4.2.3.2 Nutzung 21](#_Toc486428209)

[4.2.4 Operation delete\_Directory\_Entry 21](#_Toc486428210)

[4.2.4.1 Umsetzung 22](#_Toc486428211)

[4.2.4.2 Nutzung 22](#_Toc486428212)

[4.3 Schnittstelle I\_Directory\_Application\_Maintenance 23](#_Toc486428213)

[4.3.1 Operation add\_Directory\_FA-Attributes 24](#_Toc486428214)

[4.3.1.1 Umsetzung SOAP 24](#_Toc486428215)

[4.3.1.2 Nutzung SOAP 25](#_Toc486428216)

[4.3.1.3 Umsetzung LDAPv3 26](#_Toc486428217)

[4.3.1.4 Nutzung LDAPv3 26](#_Toc486428218)

[4.3.2 Operation delete\_Directory\_FA-Attributes 27](#_Toc486428219)

[4.3.2.1 Umsetzung SOAP 27](#_Toc486428220)

[4.3.2.2 Nutzung SOAP 27](#_Toc486428221)

[4.3.2.3 Umsetzung LDAPv3 28](#_Toc486428222)

[4.3.2.4 Nutzung LDAPv3 28](#_Toc486428223)

[4.3.3 Operation modify\_Directory\_FA-Attributes 29](#_Toc486428224)

[4.3.3.1 Umsetzung SOAP 29](#_Toc486428225)

[4.3.3.2 Nutzung SOAP 30](#_Toc486428226)

[4.3.3.3 Umsetzung LDAPv3 31](#_Toc486428227)

[4.3.3.4 Nutzung LDAPv3 31](#_Toc486428228)

[4.4 Prozessschnittstelle P\_Directory\_Application\_Registration (Provided) 32](#_Toc486428229)

[4.5 Prozessschnittstelle P\_Directory\_Maintenance (Provided) 32](#_Toc486428230)

[4.6 Prozessschnittstelle P\_Directory\_Administration\_Registration (Provided) 33](#_Toc486428231)

[5 Informationsmodell 34](#_Toc486428232)

[6 Anhang A - Verzeichnisse 35](#_Toc486428233)

[6.1 A1 – Abkürzungen 35](#_Toc486428234)

[6.2 A2 – Glossar 36](#_Toc486428235)

[6.3 A3 – Abbildungsverzeichnis 36](#_Toc486428236)

[6.4 A4 – Tabellenverzeichnis 36](#_Toc486428237)

[6.5 A5 - Referenzierte Dokumente 37](#_Toc486428238)

[6.5.1 A5.1 – Dokumente der gematik 37](#_Toc486428239)

[6.5.2 A5.2 – Weitere Dokumente 37](#_Toc486428240)

# Einordnung des Dokumentes

## Zielsetzung

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

Der VZD ist ein zentraler Dienst der TI-Plattform.

Das Informationsmodell des VZD ist erweiterbar.

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

## Zielgruppe

Das Dokument ist maßgeblich für Anbieter und Hersteller von Verzeichnisdiensten

## Geltungsbereich

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

**Schutzrechts-/Patentrechtshinweis**

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

## Abgrenzungen

Spezifiziert werden in dem Dokument die von dem Produkttyp bereitgestellten (angebotenen) Schnittstellen. Benutzte Schnittstellen werden hingegen in der Spezifikation desjenigen Produkttypen beschrieben, der diese Schnittstelle bereitstellt. Auf die entsprechenden Dokumente wird verwiesen (siehe auch Anhang A5).

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

Nicht Bestandteil des vorliegenden Dokumentes sind die Festlegungen zum Themenbereich

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

## Methodik

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

Sie werden im Dokument wie folgt dargestellt:

**⌦ gemxxxxxx\_AFO\_0000 <Titel der Afo>**

Text / Beschreibung

**⌫**

Dabei umfasst die Anforderung sämtliche innerhalb der Textmarken angeführten Inhalte.

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

# 

# Systemüberblick

Der VZD ist ein Produkttyp der TI gemäß [gemKPT\_Arch\_TIP].



Abbildung 1: Einordnung des VZD in die TI

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

Die Dateneinträge werden erstellt und gepflegt:

1. per Basisdatenadministration durch berechtigte Benutzer
2. durch fachanwendungsspezifische Dienste (FAD), die fachanwendungsspezifische Daten (Fachdaten) zu bereits bestehenden Basisdaten zufügen.

Der VZD kann durch LDAP Clients abgefragt werden.

# 

# Übergreifende Festlegungen

## IT-Sicherheit und Datenschutz

**⌦ TIP1-A\_5546 VZD, Integritäts- u. Authentizitätsschutz**

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

**⌫**

⌦ TIP1-A\_5547 VZD, Löschen ungültiger Zertifikate

Der VZD MUSS täglich die gespeicherten Zertifikate nach Ablaufdatum (TUC\_PKI\_002 „Gültigkeitsprüfung des Zertifikats“) und Status (TUC\_PKI\_006 "OCSP-Abfrage) prüfen. Ungültige Zertifikate werden sofort gelöscht. Ein Eintrag ohne gültige Zertifikate wird nach 4 Wochen gelöscht. Damit wird der ungewollte Erhalt von nicht mehr benutzten Einträgen vermieden.

**⌫**

**⌦ TIP1-A\_5548 VZD, Protokollierung der Änderungsoperationen**

Der VZD MUSS Änderungen der Verzeichnisdiensteinträge protokollieren und muss sie 6 Monate zur Verfügung halten.

**⌫**

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

**⌦ TIP1-A\_5549 VZD, Keine Leseprofilbildung**

Der VZD DARF Suchanfragen NICHT speichern oder protokollieren.

**⌫**

**⌦ TIP1-A\_5550 VZD, Keine Kopien von gelöschten Daten**

Der VZD DARF von gelöschten Daten KEINE Kopien speichern.

**⌫**

**⌦** **TIP1-A\_5551 VZD, Sicher gegen Datenverlust**

Der Anbieter des VZD MUSS den Dienst gegen Datenverlust absichern.

**⌫**

**⌦ TIP1-A\_5552 VZD, Begrenzung der Suchergebnisse**

Der VZD MUSS die Ergebnisliste einer Suchanfrage auf 100 Suchergebnisse begrenzen.

**⌫**

**⌦ TIP1-A\_5553 VZD, Private Schlüssel sicher speichern**

Der VZD MUSS seine privaten Schlüssel sicher speichern und ihr Auslesen verhindern um Manipulationen zu verhindern.

**⌫**

**⌦ TIP1-A\_5554 VZD, Registrierungsdaten sicher speichern**

Der VZD MUSS die Integrität und Authentizität der gespeicherten Registrierungsdaten der FAD gewährleisten.

**⌫**

**⌦ TIP1-A\_5555 VZD, SOAP-Fehlercodes**

Der VZD MUSS für seine SOAP-Schnittstelle die generischen Fehlercodes

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

aus Tabelle Tab\_Gen\_Fehler aus [gemSpec\_OM] im SOAP-Fault verwenden. Erkannte Fehler auf Transportprotokollebene müssen auf gematik SOAP Faults (Code 6 aus Tabelle Tab\_Gen\_Fehler aus [gemSpec\_OM] ) abgebildet werden.

**⌫**

**⌦ TIP1-A\_5556 VZD, Fehler Logging**

Der VZD MUSS lokal und remote erkannte Fehler in seinem lokalen Speicher protokollieren.

**⌫**

**⌦ TIP1-A\_5557 VZD, Unterstützung IPv4 und IPv6**

Der VZD MUSS IPv4 und IPv6 für alle seine IP-Schnittstellen im Dual-Stack-Mode unter­stützen.

**⌫**

**⌦ TIP1-A\_5558 VZD, Sicheres Speichern der TSL**

Der VZD MUSS die Inhalte der TSL in einem lokalen Trust Store sicher speichern und für X.509-Zertifikatsprüfungen lokal zugreifbar halten.

**⌫**

**⌦ TIP1-A\_5610 VZD, Einwilligung muss vorliegen**

Der Anbieter des VZD MUSS sicherstellen, dass die informierte Einwilligung des betroffenen Leistungserbringers vorliegt, bevor er dessen Daten auf dem Verzeichnisdienst der TI speichert.

**⌫**

**⌦ TIP1-A\_5611 VZD, Widerspruch der Einwilligung**

Der Anbieter des VZD MUSS die Daten des Leistungserbringers unverzüglich vom Verzeichnisdienst löschen, sobald ihm der Widerruf der Einwilligung durch den Leistungserbringer bekannt wird.

**⌫**

## Fachliche Anforderungen

**⌦ TIP1-A\_5560 VZD, Erweiterbarkeit für neue Fachdaten**

Der Anbieter des VZD MUSS die Erweiterbarkeit des VZD für die Aufnahme der Fachdaten neuer Fachanwendungen gewährleisten.

**⌫**

**⌦ TIP1-A\_5561 VZD, DNS-SD**

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

* + für den Zugriff auf die Schnittstelle I\_Directory\_Query:

\_ldap.\_tcp.vzd.telematik.

* + für den Zugriff auf die Schnittstelle I\_Directory\_Maintenance:

\_vzd-kon.\_tcp.vzd.telematik.

* + für den Zugriff auf die Schnittstelle I\_Directory\_Application\_Maintenance:

\_vzd-fd.\_tcp.vzd.telematik.

**⌫**

**⌦ TIP1-A\_5562 VZD, Parallele Zugriffe**

Der Betreiber des VZD MUSS sicherstellen, dass Benutzer gleichzeitig auf den VZD zugreifen können. Dies umfasst alle technischen Schnittstellen. In [gemSpec\_Perf] ist die Anzahl der parallelen Zugriffe definiert.

**⌫**

**⌦ TIP1-A\_5563 VZD, Erhöhung der Anzahl der Einträge**

Der Anbieter des VZD MUSS sicherstellen das 500 000 Einträge gespeichert werden können.

**⌫**

**⌦ TIP1-A\_5620 VZD, Nicht-Speicherung von Leading und Trailing Spaces**

Der Anbieter des VZD MUSS Leading und Trailing Spaces abschneiden.

**⌫**

# Funktionsmerkmale

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

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

**⌦ TIP1-A\_5564 VZD, Festlegung der Schnittstellen**

Der VZD MUSS die Schnittstellen gemäß Tabelle Tab\_PT\_VZD\_Schnittstellen implementieren („bereitgestellte“ Schnitt­stellen) und nutzen („benötigte“ Schnittstellen).

Tabelle 1: Tab\_PT\_VZD\_Schnittstellen

| Schnittstelle | bereitgestellt / benötigt | Bemerkung |
| --- | --- | --- |
| I\_Directory\_Query | bereitgestellt |  |
| I\_Directory\_Maintenance | bereitgestellt |  |
| I\_Directory\_Application\_Maintenance | bereitgestellt |  |
| I\_IP\_Transport | benötigt | Definition in [gemSpec\_Net] |
| I\_DNS\_Name\_Resolution | benötigt | Definition in [gemSpec\_Net] |
| I\_NTP\_Time\_Information | benötigt | Definition in [gemSpec\_Net] |
| I\_OCSP\_Status\_Information | benötigt | Definition in [gemSpec\_PKI] |
| I\_TSL\_Download | benötigt | Definition in [gemSpec\_TSL] |

**⌫**

## Schnittstelle I\_Directory\_Query

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

**⌦ TIP1-A\_5565 VZD, Schnittstelle I\_Directory\_Query**

Der VZD MUSS für LDAP Clients die Schnittstelle I\_Directory\_Query gemäß Tabelle Tab\_VZD\_Schnittstelle\_I\_Directory\_Query an­bieten.

Tabelle 2: Tab\_VZD\_Schnittstelle\_I\_Directory\_Query

|  |  |  |
| --- | --- | --- |
| Name | I\_Directory\_Query | |
| Version | wird im Produkttypsteckbrief des VZD definiert | |
| Operationen | Name | Kurzbeschreibung |
| search\_Directory | Abfragen von Daten des VZD gemäß LDAPv3 Protokoll |

**⌫**

### Operation search\_Directory

**⌦ TIP1-A\_5566 LDAP Client, LDAPS**

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

Der LDAP Client muss das Zertifikat des VZD C.ZD.TLS-S gemäß TUC\_PKI\_018 "Zertifikatsprüfung in der TI" und die Rolle (zulässig ist oid\_vzd\_ti) prüfen.

Der LDAP Client authentisiert sich nicht.

**⌫**

**⌦ TIP1-A\_5567 VZD, LDAPS bei search\_Directory**

Der VZD MUSS sicherstellen, dass die Operation search\_Directory nur über eine bestehende LDAPS -Verbindung ausgeführt werden kann.

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

**⌫**

**⌦ TIP1-A\_5568 VZD und LDAP Client, Implementierung der LDAPv3 search Operation**

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

**⌫**

#### Umsetzung

**⌦ TIP1-A\_5569 VZD, search\_Directory, Suche nach definierten Attributen**

Der VZD MUSS die enthaltenen Daten so strukturiert haben, dass mit einer einzigen LDAPv3-Suche alle einer Telematik-ID zugeordneten Attribute (Basisdaten und Fachdaten) in Form einer flachen Liste von Attributen ohne ou-Unterstruktur abgefragt werden können. Als Filter für die Suche sind alle Attribute außer der Telematik-ID möglich.

Die Telematik-ID darf nicht als Ergebnis geliefert werden.

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

**⌫**

#### Nutzung

**⌦ TIP1-A\_5570 LDAP Client, TUC\_VZD\_0001 „search\_Directory”**

Der Anbieter des VZD MUSS für die Nutzung durch LDAP Clients den technischen Use Case TUC\_VZD\_0001 „search\_Directory” gemäß Tabelle Tab\_TUC\_VZD\_0001 unterstützen.

Tabelle 3: Tab\_TUC\_VZD\_0001

|  |  |  |
| --- | --- | --- |
| 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. |
| 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. | |

**⌫**

## Schnittstelle I\_Directory\_Maintenance

Die Schnittstelle ermöglicht die Administration der Basisdaten.

**⌦ TIP1-A\_5571 VZD, Schnittstelle I\_Directory\_Maintenance**

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

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

|  |  |  |
| --- | --- | --- |
| Name | I\_Directory\_Maintenance | |
| Version | wird im Produkttypsteckbrief des VZD definiert | |
| Operationen | Name | Kurzbeschreibung |
| add\_Directory\_Entry | Erzeugung eines Basisdaten-Verzeichniseintrages oder Überschreiben eines bestehenden Verzeichniseintrages. |
| read\_Directory\_Entry | Abfrage aller Basis- und Fachdaten eines Verzeichniseintrages. |
| modify\_Directory\_Entry | Änderung eines Basisdaten-Verzeichniseintrages. |
| delete\_Directory\_Entry | Löschung eines Verzeichniseintrages (Basisdaten und Fachdaten). |

**⌫**

**⌦ TIP1-A\_5572 VZD, I\_Directory\_Maintenance, TLS-gesicherte Verbindung**

Der VZD MUSS die Schnittstelle I\_Directory\_Maintenance durch Verwendung von TLS mit beidseitiger Authentisierung sichern.

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

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

Es dürfen nur Basisdaten-Einträge geändert werden, für die der FAD eine Autorisierung hat.

**⌫**

**⌦ TIP1-A\_5574 VZD und Nutzer der Schnittstelle I\_Directory\_Maintenance, WebService**

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

**⌫**

### Operation add\_Directory\_Entry

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

#### Umsetzung

**⌦ TIP1-A\_5575 VZD, Umsetzung add\_Directory\_Entry**

Der VZD MUSS nach folgenden Vorgaben die Operation add\_Directory\_Entry implementieren:

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

Tabelle 5: VZD\_TAB\_addDirectoryEntry\_Mapping

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

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

**⌫**

#### Nutzung

**⌦ TIP1-A\_5576 Nutzer der Schnittstelle, TUC\_VZD\_0002 „add\_Directory\_Entry”**

Der Nutzer der Schnittstelle MUSS den technischen Use Case TUC\_VZD\_0002 „add\_Directory\_Entry” gemäß Tabelle Tab\_TUC\_VZD\_0002 umsetzen.

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

Tabelle 6: Tab\_TUC\_VZD\_0002

|  |  |  |
| --- | --- | --- |
| Name | TUC\_VZD\_0002 „add\_Directory\_Entry” | |
| Beschreibung | Diese Operation ermöglicht die Erzeugung von neuen Basisdaten.  Bestehende Basisdaten werden überschrieben. | |
| Vorbedingungen | keine | |
| Eingangsdaten | SOAP-Request „addDirectoryEntry“ | |
| Komponenten | Nutzer der Schnittstelle, Verzeichnisdienst | |
| Ausgangsdaten | SOAP-Response „VZD:responseMsg“ | |
| Standardablauf | Aktion | Beschreibung |
| Aufbau TLS-Verbindung | Wenn noch keine Verbindung besteht initiiert der Nutzer der Schnittstelle den Verbindungsaufbau.  Der Nutzer der Schnittstelle authentisiert sich mit dem AUT-Zertifikat C.FD.TLS-C. |
| SOAP-Request senden | Der Nutzer der Schnittstelle ruft die SOAP-Operation VZD:addDirectoryEntry auf. |
| SOAP-Response empfangen | Die SOAP-Response VZD:responseMsg mit dem VZD:status wird empfangen. |
| Varianten/Alterna­tiven | keine |  |
| Fehlerfälle | Es werden die protokollspezifischen Fehlermeldungen verwendet (TCP, HTTP, TLS).  Fehler bei der Verarbeitung des SOAP Requests werden als gematik SOAP-Fault versendet:  faultcode 4211, faultstring: Operation fehlerhaft ausgeführt, Basisdaten konnten nicht angelegt werden (Fehler im Verzeichnisdienst)  faultcode 4202, faultstring: SOAP Request enthält Fehler  faultcode 4201, faultstring: Operation enthält ungültige Daten  Erkannte Fehler auf Transportprotokollebene müssen auf gematik SOAP Faults (Code 6 aus Tabelle Tab\_Gen\_Fehler aus [gemSpec\_OM]) abgebildet werden. Zusätzlich müssen die generischen gematik SOAP-Faults  Code 2: Verbindung zurückgewiesen  Code 3: Nachrichtenschema fehlerhaft  Code 4: Version Nachrichtenschema fehlerhaft  unterstützt werden. | |

**⌫**

### Operation read\_Directory\_Entry

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

#### Umsetzung

**⌦ TIP1-A\_5577 VZD, Umsetzung read\_Directory\_Entry**

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

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

Tabelle 7: VZD\_TAB\_readDirectoryEntry\_Mapping

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

Es müssen die Fehlermeldungen gemäß Tab\_TUC\_VZD\_0003 verwendet werden.

**⌫**

#### Nutzung

**⌦ TIP1-A\_5578 Nutzer der Schnittstelle, TUC\_VZD\_0003 „read\_Directory\_Entry”**

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

Die SOAP-Response ist gemäß Tabelle VZD\_TAB\_readDirectoryEntry\_Mapping mit den zur Telematik-ID gehörenden Daten aus dem VZD ausgefüllt.

Tabelle 8: 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 4311, 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. | |

**⌫**

### Operation modify\_Directory\_Entry

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

#### Umsetzung

**⌦ TIP1-A\_5579 VZD, Umsetzung modify\_Directory\_Entry**

Der VZD MUSS nach folgenden Vorgaben die Operation modify\_Directory\_Entry implementieren:

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

Tabelle 9: VZD\_TAB\_modifyDirectoryEntry\_Mapping

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

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

**⌫**

#### Nutzung

**⌦ TIP1-A\_5580 Nutzer der Schnittstelle, TUC\_VZD\_0004 „modify\_Directory\_Entry”**

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

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

Tabelle 10: Tab\_TUC\_VZD\_0004

|  |  |  |
| --- | --- | --- |
| Name | TUC\_VZD\_0004 „modify\_Directory\_Entry” | |
| Beschreibung | Diese Operation ermöglicht die Erzeugung von neuen Basisdaten.  Bestehende Basisdaten werden überschrieben. | |
| Vorbedingungen | keine | |
| Eingangsdaten | SOAP-Request „modifyDirectoryEntry“ | |
| Komponenten | Nutzer der Schnittstelle, Verzeichnisdienst | |
| Ausgangsdaten | SOAP-Response „responseMsg“ | |
| Standardablauf | Aktion | Beschreibung |
| Aufbau TLS-Verbindung | Wenn noch keine Verbindung besteht initiiert der Nutzer der Schnittstelle den Verbindungsaufbau.  Der Nutzer der Schnittstelle authentisiert sich mit dem AUT-Zertifikat C.FD.TLS-C. |
| SOAP-Request senden | Der Nutzer der Schnittstelle ruft die SOAP-Operation VZD:modifyDirectoryEntry auf. |
| SOAP-Response empfangen | Die SOAP-Response VZD:responseMsg mit dem VZD:status wird empfangen. |
| Varianten/Alterna­tiven | keine |  |
| Fehlerfälle | Es werden die protokollspezifischen Fehlermeldungen verwendet (TCP, HTTP, TLS)  Fehler bei der Verarbeitung des SOAP Requests werden als gematik SOAP-Fault versendet:  faultcode 4231, faultstring: Operation fehlerhaft ausgeführt, Basisdaten konnten nicht modifiziert werden (Fehler im Verzeichnisdienst)  faultcode 4312, faultstring: Basisdaten konnten nicht gefunden werden  faultcode 4202, faultstring: SOAP Request enthält Fehler  Erkannte Fehler auf Transportprotokollebene müssen auf gematik SOAP Faults (Code 6 aus Tabelle Tab\_Gen\_Fehler aus [gemSpec\_OM]) abgebildet werden. Zusätzlich müssen die generischen gematik SOAP-Faults  Code 2: Verbindung zurückgewiesen  Code 3: Nachrichtenschema fehlerhaft  Code 4: Version Nachrichtenschema fehlerhaft  unterstützt werden. | |

**⌫**

### Operation delete\_Directory\_Entry

Diese Operation löscht einen bestehenden Datensatz im LDAP Verzeichnis.

#### Umsetzung

**⌦ TIP1-A\_5581 VZD, Umsetzung delete\_Directory\_Entry**

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

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

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

**⌫**

#### Nutzung

**⌦ TIP1-A\_5582 Nutzer der Schnittstelle, TUC\_VZD\_0005 „delete\_Directory\_Entry”**

Der Nutzer der Schnittstelle MUSS den technischen Use Case TUC\_VZD\_0005 „delete\_Directory\_Entry” gemäß Tabelle Tab\_TUC\_VZD\_0005 umsetzen. Der Webservice wird durch die Dokumente DirectoryMaintenance.wsdl und DirectoryMaintenance.xsd definiert.

Tabelle 11: Tab\_TUC\_VZD\_0005

|  |  |  |
| --- | --- | --- |
| Name | TUC\_VZD\_0005 „delete\_Directory\_Entry” | |
| Beschreibung | Diese Operation ermöglicht die Erzeugung von neuen Basisdaten.  Bestehende Basisdaten werden überschrieben. | |
| 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 | Es werden die protokollspezifischen Fehlermeldungen verwendet (TCP, HTTP, TLS)  Fehler bei der Verarbeitung des SOAP Requests werden als gematik SOAP-Fault versendet:  faultcode 4241, faultstring: Operation fehlerhaft ausgeführt, Basisdaten konnten nicht gelöscht werden (Fehler im Verzeichnisdienst)  faultcode 4312, faultstring: Basisdaten konnten nicht gefunden werden  faultcode 4202, faultstring: SOAP Request enthält Fehler  Erkannte Fehler auf Transportprotokollebene müssen auf gematik SOAP Faults (Code 6 aus Tabelle Tab\_Gen\_Fehler aus [gemSpec\_OM]) abgebildet werden. Zusätzlich müssen die generischen gematik SOAP-Faults  Code 2: Verbindung zurückgewiesen  Code 3: Nachrichtenschema fehlerhaft  Code 4: Version Nachrichtenschema fehlerhaft  unterstützt werden. | |

**⌫**

## Schnittstelle I\_Directory\_Application\_Maintenance

Die Schnittstelle ermöglicht die Administration der Fachdaten.

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

**⌦ TIP1-A\_5583 VZD, Schnittstelle I\_Directory\_Application\_Maintenance**

Der VZD MUSS für FADs I\_Directory\_Maintenance gemäß Tabelle Tab\_VZD\_Schnittstelle\_I\_Directory\_Application\_Maintenance an­bieten.

Tabelle 12: Tab\_VZD\_Schnittstelle\_I\_Directory\_Application\_Maintenance

|  |  |  |
| --- | --- | --- |
| Name | I\_Directory\_Application\_Maintenance | |
| Version | wird im Produkttypsteckbrief des VZD definiert | |
| Operationen | Operation | Kurzbeschreibung |
| add\_Directory\_FA-Attributes | Erzeugung eines Fachdaten-Eintrags |
| delete\_Directory\_FA-Attributes | Löschen von einzelnen oder allen zu einem FAD gehörenden Fachdaten eines Eintrags. |
| modify\_Directory\_FA-Attributes | Ändern fachspezifischer Attribute |

**⌫**

**⌦ TIP1-A\_5584 VZD, Änderung nur durch registrierte FAD**

Der Anbieter des VZD MUSS sicherstellen, dass Fachdaten eines Dienstes nur durch einen beim VZD für diesen Dienst registrierten Fachdienst erzeugt, gelöscht und geändert werden können.

**⌫**

**⌦ TIP1-A\_5585 VZD, I\_Directory\_Application\_Maintenance, TLS-gesicherte Verbindung**

Der VZD MUSS die Schnittstelle I\_Directory\_Application\_Maintenance durch Verwendung von TLS mit beidseitiger Authentisierung sichern.

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

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

**⌫**

**⌦ TIP1-A\_5586 VZD, I\_Directory\_Application\_Maintenance, Webservice und LDAPv3**

Der VZD MUSS die Schnittstelle I\_Directory\_Application\_Maintenance als Webservice (SOAP über HTTPS) und als LDPv3 über LDAPS implementieren. Der Webservice wird durch die Dokumente DirectoryApplicationMaintenance.wsdl und DirectoryApplicationMaintenance.xsd definiert. Die LDAPv3-Attribute sind in dem Informationsmodell Abb\_VZD\_logisches\_Datenmodell beschrieben.

**⌫**

**⌦ TIP1-A\_5587 VZD, Implementierung der LDAPv3 Schnittstelle**

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

**⌫**

**⌦ TIP1-A\_5588 FAD, I\_Directory\_Application\_Maintenance, Nutzung LDAP v3 oder Webservice**

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

**⌫**

**⌦ TIP1-A\_5589 FAD, Implementierung der LDAPv3 Schnittstelle**

Der FAD, der die LDAPv3-Schnittstelle I\_Directory\_Application\_Maintenance des VZD nutzt, MUSS diese Schnittstelle gemäß den LDAPv3 Standards [RFC4510], [RFC4511], [RFC4512], [RFC4513], [RFC4514], [RFC4515], [RFC4516], [RFC4517], [RFC4518], [RFC4519], [RFC4520], [RFC4522] und [RFC4523] implementieren. Die LDAPv3-Attribute sind in dem Informationsmodell Abb\_VZD\_logisches\_Datenmodell beschrieben.

**⌫**

### Operation add\_Directory\_FA-Attributes

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

Voraussetzung: Die Fachdaten müssen einem Basisdateneintrag zuordenbar sein.

#### Umsetzung SOAP

**⌦ TIP1-A\_5590 VZD, Umsetzung add\_Directory\_FA-Attributes (SOAP)**

Der VZD MUSS nach folgenden Vorgaben die Operation add\_Directory\_FA-Attributes implementieren:

1. Wenn kein zur Telematik-ID gehörender Basisdatensatz gefunden wurde, wird der Request mit einem gematik SOAP-Fault beendet:

faultcode: 4312,

faultstring: Basisdaten konnten nicht gefunden werden.

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

Tabelle 13: VZD\_TAB\_I\_Directory\_Application\_Maintenance\_Add\_Mapping

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

Es müssen die Fehlermeldungen gemäß Tab\_TUC\_VZD\_0006 verwendet werden.

**⌫**

#### Nutzung SOAP

**⌦ TIP1-A\_5591 FAD, TUC\_VZD\_0006 “add\_Directory\_FA-Attributes (SOAP)”**

Der FAD MUSS den technischen Use Case TUC\_VZD\_0006 “add\_Directory\_FA-Attributes” gemäß Tabelle Tab\_TUC\_VZD\_0006 umsetzen.

Tabelle 14: Tab\_TUC\_VZD\_0006

|  |  |  |
| --- | --- | --- |
| 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  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. | |

**⌫**

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

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

Tabelle 15: VZD\_TAB\_KOM-LE\_Attributes

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

**⌫**

#### Umsetzung LDAPv3

**⌦ TIP1-A\_5593 VZD, Umsetzung add\_Directory\_FA-Attributes (LDAPv3)**

Der VZD MUSS nach folgenden Vorgaben die Operation add\_Directory\_FA-Attributes implementieren:

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

Es müssen die Fehlermeldungen gemäß Tab\_TUC\_VZD\_0007 verwendet werden.

**⌫**

#### Nutzung LDAPv3

**⌦ TIP1-A\_5594 FAD, TUC\_VZD\_0007 “add\_Directory\_FA-Attributes (LDAPv3)”**

Der FAD MUSS den technischen Use Case TUC\_VZD\_0007 „add\_Directory\_FA-Attributes(LDAPv3)” gemäß Tabelle Tab\_TUC\_VZD\_0007 unterstützen.

Tabelle 16: Tab\_TUC\_VZD\_0007

|  |  |  |
| --- | --- | --- |
| 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. | |

**⌫**

### Operation delete\_Directory\_FA-Attributes

Diese Operation löscht einen Fachdatensatz.

#### Umsetzung SOAP

**⌦ TIP1-A\_5595 VZD, Umsetzung delete\_Directory\_FA-Attributes**

Der VZD MUSS nach folgenden Vorgaben die Operation delete\_Directory\_ FA-Attributes implementieren:

1. Wenn kein zur Telematik-ID gehörender Basisdatensatz gefunden wurde, wird der Request mit einem gematik SOAP-Fault beendet:

faultcode: 4312,

faultstring: Basisdaten konnten nicht gefunden werden.

1. Ein zur Telematik-ID gehörender Fachdatensatz wird gelöscht.
2. Ein nicht existierender Fachdatensatz zur Telematik-ID führt zu keiner Aktion.

Es müssen die Fehlermeldungen gemäß Tab\_TUC\_VZD\_0008 verwendet werden.

**⌫**

#### Nutzung SOAP

**⌦ TIP1-A\_5596 FAD, TUC\_VZD\_0008 “delete\_Directory\_FA-Attributes (SOAP)”**

Der FAD MUSS den technischen Use Case TUC\_VZD\_0008 “delete\_Directory\_FA-Attributes” gemäß Tabelle Tab\_TUC\_VZD\_0008 umsetzen.

Tabelle 17: Tab\_TUC\_VZD\_0008

|  |  |  |
| --- | --- | --- |
| 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  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. | |

**⌫**

#### Umsetzung LDAPv3

**⌦ TIP1-A\_5597 VZD, Umsetzung delete\_Directory\_FA-Attributes (LDAPv3)**

Der VZD MUSS nach folgenden Vorgaben die Operation delete\_Directory\_FA-Attributes implementieren:

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

Es müssen die Fehlermeldungen gemäß Tab\_TUC\_VZD\_0009 verwendet werden.

**⌫**

#### Nutzung LDAPv3

**⌦ TIP1-A\_5598 FAD, TUC\_VZD\_0009 “delete\_Directory\_FA-Attributes (LDAPv3)”**

Der FAD MUSS den technischen Use Case TUC\_VZD\_0009 „delete\_Directory\_FA-Attributes(LDAPv3)” gemäß Tabelle Tab\_TUC\_VZD\_0009 unterstützen.

Tabelle 18: Tab\_TUC\_VZD\_0009

|  |  |  |
| --- | --- | --- |
| 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. | |

**⌫**

### Operation modify\_Directory\_FA-Attributes

Diese Operation überschreibt einen Fachdatensatz.

#### Umsetzung SOAP

**⌦ TIP1-A\_5599 VZD, Umsetzung modify\_Directory\_FA-Attributes**

Der VZD MUSS nach folgenden Vorgaben die Operation modify\_Directory\_ FA-Attributes implementieren:

1. Wenn kein zur Telematik-ID gehörender Basisdatensatz gefunden wurde, wird der Request mit einem gematik SOAP-Fault beendet:

faultcode: 4312,

faultstring: Basisdaten konnten nicht gefunden werden.

1. Ein bereits zur Telematik-ID gehörender Fachdatensatz wird überschrieben.
2. Die Daten aus dem SOAP Request werden gemäß VZD\_TAB\_I\_Directory\_Application\_Maintenance\_Modify\_Mapping zum Basisdatensatz hinzugefügt.

Tabelle 19: VZD\_TAB\_I\_Directory\_Application\_Maintenance\_Modify\_Mapping

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

Es müssen die Fehlermeldungen gemäß Tab\_TUC\_VZD\_0010 verwendet werden.

⌫

#### Nutzung SOAP

**⌦ TIP1-A\_5600 FAD, TUC\_VZD\_0010 “modify\_Directory\_FA-Attributes (SOAP)”**

Der FAD MUSS den technischen Use Case TUC\_VZD\_0010 “modify\_Directory\_FA-Attributes” gemäß Tabelle Tab\_TUC\_VZD\_0010 umsetzen.

Tabelle 20: Tab\_TUC\_VZD\_0010

|  |  |  |
| --- | --- | --- |
| 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  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. | |

**⌫**

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

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

Tabelle 21: VZD\_TAB\_KOM-LE\_Attributes

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

**⌫**

#### Umsetzung LDAPv3

**⌦ TIP1-A\_5602 VZD, Umsetzung modify\_Directory\_FA-Attributes (LDAPv3)**

Der VZD MUSS nach folgenden Vorgaben die Operation modify\_Directory\_FA-Attributes implementieren:

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

Es müssen die Fehlermeldungen gemäß Tab\_TUC\_VZD\_0011 verwendet werden.

**⌫**

#### Nutzung LDAPv3

**⌦ TIP1-A\_5603 FAD, TUC\_VZD\_0011 “modify\_Directory\_FA-Attributes (LDAPv3)”**

Der FAD MUSS den technischen Use Case TUC\_VZD\_0011 „modify\_Directory\_FA-Attributes(LDAPv3)” gemäß Tabelle Tab\_TUC\_VZD\_0011 unterstützen.

Tabelle 22: Tab\_TUC\_VZD\_0011

|  |  |  |
| --- | --- | --- |
| 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. | |

**⌫**

## Prozessschnittstelle P\_Directory\_Application\_Registration (Provided)

**⌦ TIP1-A\_5604 VZD, Registrierung FADs**

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

* + Gültigkeit des TLS-Client-Zertifikat des FADs C.FD.TLS-C (Prüfschritte wie in TUC\_PKI\_018 und mit admission gemäß vom GBV vorgegebener OID-Liste ),
  + Name der Fachanwendung (z.B. KOM-LE),
  + Name des Fachdienstbetreibers.

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

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

**⌫**

**⌦ TIP1-A\_5605 VZD, De-Registrierung FADs**

Der Anbieter des VZD MUSS einen Deregistrierungsprozess für FAD implementieren.

Der VZD MUSS alle verbliebenen Fachdaten eines deregistrierten FAD löschen.

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

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

**⌫**

## Prozessschnittstelle P\_Directory\_Maintenance (Provided)

**⌦ TIP1-A\_5606 VZD, Mandat zur Löschung von Einträgen.**

Der Anbieter des VZD MUSS einen Prozess implementieren, der es LE ermöglicht ihren Eintrag im VZD ohne zugehörige Smartcard zu löschen.

Der Anbieter des VZD MUSS vom LE einen Nachweis fordern und prüfen, dass die zu löschenden Daten dem LE gehören. Erst nach positivem Ergebnis der Prüfung darf gelöscht werden.

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

**⌫**

## Prozessschnittstelle P\_Directory\_Administration\_Registration (Provided)

**⌦ TIP1-A\_5612 VZD, Mandatsregistrierung für FAD zur Administration von Basisdaten**

Der Anbieter des VZD MUSS einen Prozess implementieren, der es FAD ermöglicht eine Autorisierung für die Änderung eines Basisdateneintrags zu hinterlegen. Die Autorisierung muss für jeden Basisdateneintrag vorhanden sein.

Der FAD muss sich zuvor beim VZD registrieren. Der Anbieter des VZD muss bei der Registrierung des FAD dessen Client-Zertifikat überprüfen:

* Gültigkeit des TLS-Client-Zertifikats des FADs C.FD.TLS-C (Prüfschritte wie in TUC\_PKI\_018 und mit admission gemäß vom GBV vorgegebener OID-Liste).

Die Autorisierung für die Änderung eines Basisdateneintrags muss für jeden Basisdateneintrag vorhanden sein. Die Autorisierung beinhaltet folgende Schritte:

* Der VZD MUSS den Autorisierungsprozess durch beidseitige Authentisierung (FAD und VZD) sichern. Der VZD muss sich mit der Identität ID.ZD.TLS-S authentisieren. Der VZD muss das vom FAD übergebene Zertifikat C.FD.TLS-C hinsichtlich OCSP Gültigkeit und Übereinstimmung mit einem Zertifikat eines registrierten FAD prüfen.
* Der VZD fordert zur Autorisierung vom FAD an:
  + die Telematik-ID des Verzeichniseintrags, für den die Autorisierung erfolgen soll,
  + den Nachweis der Berechtigung zur Datenadminstration durch den Betroffenen (Inhaber des HBA oder der SMC-B)

Nach erfolgreicher Autorisierung können die Basisdaten im Verzeichniseintrag eines Teilnehmers über die Schnittstelle I\_Directory\_Maintenance erstellt, gepflegt und gelöscht werden.

**⌫**

**⌦ TIP1-A\_5613 VZD, Mandatsderegistrierung für FAD zur Administration von Basisdaten**

FAD KÖNNEN sich beim Verzeichnisdienst deregistrieren. Der Zugang über die Schnittstelle I\_Directory\_Maintenance ist danach für den betroffenen Verzeichniseintrag nicht mehr möglich.

**⌫**

# 

# Informationsmodell

**⌦ TIP1-A\_5607 VZD, logisches Datenmodell**

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

**⌫**



Abbildung 2: Abb\_VZD\_logisches\_Datenmodell

**⌦ TIP1-A\_5608 VZD, Ordnungskriterium Datenmodell Verzeichnisdienst**

Der VZD MUSS die Telematik-ID als Ordnungskriterium für das Datenmodell verwenden.

Die Telematik-ID ist in den zu einem Basisdatensatz gehörenden Zertifikaten (im Feld registrationNumber der Extension Admission) enthalten.

**⌫**

# 

# Anhang A - Verzeichnisse

## A1 – Abkürzungen

| **Kürzel** | **Erläuterung** |
| --- | --- |
| 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 |
| HBA | Heilberufsausweis |
| http | hypertext transport protocol |
| ID.FD.TLS-C | Client-Identität (privater und öffentlicher Schlüssel) eines fachanwendungsspezifischen Dienstes für TLS Verbindungen |
| ID.ZD.TLS-S | Server-Identität (privater und öffentlicher Schlüssel) eines zentralen Dienstes der TI-Plattform für TLS Verbindungen |
| KOM-LE | Kommunikation für Leistungserbringer (Fachanwendung) |
| LDAP | Lightweight Directory Access Protocol |
| LE | Leistungserbringer |
| OCSP | Online Certificate Status Protocol |
| PKI | Public Key Infrastructure |
| PTR Resource Record | Domain Name System Pointer Resource Record |
| SMC | Secure Module Card |
| SOAP | Simple Object Access Protocol |
| TCP | Transmission Control Protocol |
| TI | Telematikinfrastruktur |
| TIP | Telematikinfrastruktur-Plattform |
| TLS | Transport Layer Security |
| TUC | Technischer Use Case |
| URL | Uniform Resource Locator |
| VZD | Verzeichnisdienst |
| XML | Extensible Markup Language |

## A2 – Glossar

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

## A3 – Abbildungsverzeichnis

[Abbildung 1: Einordnung des VZD in die TI 7](#_Toc480445147)

[Abbildung 2: Abb\_VZD\_logisches\_Datenmodell 32](#_Toc480445148)

## A4 – Tabellenverzeichnis

[Tabelle 1: Tab\_PT\_VZD\_Schnittstellen 11](#_Toc480445150)

[Tabelle 2: Tab\_VZD\_Schnittstelle\_I\_Directory\_Query 11](#_Toc480445151)

[Tabelle 3: Tab\_TUC\_VZD\_0001 12](#_Toc480445152)

[Tabelle 4: Tab\_VZD\_Schnittstelle\_I\_Directory\_Maintenance 13](#_Toc480445153)

[Tabelle 5: VZD\_TAB\_addDirectoryEntry\_Mapping 14](#_Toc480445154)

[Tabelle 6: Tab\_TUC\_VZD\_0002 15](#_Toc480445155)

[Tabelle 7: VZD\_TAB\_readDirectoryEntry\_Mapping 16](#_Toc480445156)

[Tabelle 8: Tab\_TUC\_VZD\_0003 17](#_Toc480445157)

[Tabelle 9: VZD\_TAB\_modifyDirectoryEntry\_Mapping 18](#_Toc480445158)

[Tabelle 10: Tab\_TUC\_VZD\_0004 19](#_Toc480445159)

[Tabelle 11: Tab\_TUC\_VZD\_0005 20](#_Toc480445160)

[Tabelle 12: Tab\_VZD\_Schnittstelle\_I\_Directory\_Application\_Maintenance 21](#_Toc480445161)

[Tabelle 13: VZD\_TAB\_I\_Directory\_Application\_Maintenance\_Add\_Mapping 23](#_Toc480445162)

[Tabelle 14: Tab\_TUC\_VZD\_0006 23](#_Toc480445163)

[Tabelle 15: VZD\_TAB\_KOM-LE\_Attributes 24](#_Toc480445164)

[Tabelle 16: Tab\_TUC\_VZD\_0007 24](#_Toc480445165)

[Tabelle 17: Tab\_TUC\_VZD\_0008 25](#_Toc480445166)

[Tabelle 18: Tab\_TUC\_VZD\_0009 26](#_Toc480445167)

[Tabelle 19: VZD\_TAB\_I\_Directory\_Application\_Maintenance\_Modify\_Mapping 27](#_Toc480445168)

[Tabelle 20: Tab\_TUC\_VZD\_0010 28](#_Toc480445169)

[Tabelle 21: VZD\_TAB\_KOM-LE\_Attributes 28](#_Toc480445170)

[Tabelle 22: Tab\_TUC\_VZD\_0011 29](#_Toc480445171)

## A5 - Referenzierte Dokumente

### A5.1 – Dokumente der gematik

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

|  |  |
| --- | --- |
| **[Quelle]** | **Herausgeber: Titel** |
| [gemGlossar] | gematik: Glossar der Telematikinfrastruktur |
| [gemKPT\_Arch\_TIP] | gematik: Konzept Architektur der TI-Plattform |
| [gemKPT\_PKI\_TIP] | gematik: Konzept PKI der TI-Plattform |
| [gemKPT\_DS\_TIP] | gematik: Datenschutzkonzept TI-Plattform |
| [gemKPT\_Sich\_TIP] | gematik: Spezifisches Sicherheitskonzept TI-Plattform |
| [gemSpec\_Net] | gematik: Spezifikation Netzwerk |
| [gemSpec\_OM] | gematik: Operations und Maintenance Spezifikation |
| [gemSpec\_OID] | gematik: Spezifikation Festlegung von OIDs |
| [gemSpec\_PKI] | gematik: Spezifikation PKI |
| [gemSpec\_Perf] | gematik: Performance und Mengengerüst TI-Plattform |
| [gemSpec\_TSL] | gematik: Spezifikation TSL-Dienst |

### A5.2 – Weitere Dokumente

| **[Quelle]** | **Herausgeber (Erscheinungsdatum): Titel** |
| --- | --- |
| [BSI-AllVZD] | Bundesamt für Sicherheit in der Informationstechnik: B 5.15 Allgemeiner Verzeichnisdienst,  <https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/baust/b05/b05015.html> |
| [BSI-SiGw] | Bundesamt für Sicherheit in der Informationstechnik (o.J.): Konzeption von Sicherheitsgateways, Version 1.0 |
| [RFC2119] | RFC 2119 (March 1997): Key words for use in RFCs to Indicate Requirement Levels http://www.rfc-editor.org/rfc/rfc2119.txt |
| [RFC4510] | RFC 4510 (June 2006):  Lightweight Directory Access Protocol (LDAP): Technical Specification Road Map,  http://www.ietf.org/rfc/rfc4510.txt |
| [RFC4511] | RFC 4511 (June 2006):  Lightweight Directory Access Protocol (LDAP): The Protocol,  http://www.ietf.org/rfc/rfc4511.txt |
| [RFC4512] | RFC 4512 (June 2006): Lightweight Directory Access Protocol (LDAP): Directory Information Models http://www.rfc-editor.org/rfc/rfc4512.txt |
| [RFC4513] | RFC 4513 (June 2006): Lightweight Directory Access Protocol (LDAP): Authentication Methods and Security Mechanisms http://www.rfc-editor.org/rfc/rfc4513.txt |
| [RFC4514] | RFC 4514 (June 2006): Lightweight Directory Access Protocol (LDAP): String Representation of Distinguished Names http://www.rfc-editor.org/rfc/rfc4514.txt |
| [RFC4515] | RFC 4515 (June 2006): Lightweight Directory Access Protocol (LDAP): String Representation of Search Filters http://www.rfc-editor.org/rfc/rfc4515.txt |
| [RFC4516] | RFC 4516 (June 2006): Lightweight Directory Access Protocol (LDAP): Uniform Resource Locator http://www.rfc-editor.org/rfc/rfc4516.txt |
| [RFC4517] | RFC 4517 (June 2006): Lightweight Directory Access Protocol (LDAP): Syntaxes and Matching Rules http://www.rfc-editor.org/rfc/rfc4515.txt |
| [RFC4519] | RFC 4519 (June 2006): Lightweight Directory Access Protocol (LDAP): Schema for User Applications http://www.rfc-editor.org/rfc/rfc4519.txt |
| [RFC4522] | RFC 4522 (June 2006): Lightweight Directory Access Protocol (LDAP): The Binary Encoding Option http://www.rfc-editor.org/rfc/rfc4522.txt |
| [RFC4523] | RFC 4523 (June 2006): Lightweight Directory Access Protocol (LDAP) Schema Definitions for X.509 Certificates http://www.rfc-editor.org/rfc/rfc4523.txt |
| [RFC6763] | RFC 6763 (February 2013): DNS-Based Service Discovery http://www.rfc-editor.org/rfc/rfc6763.txt |