gematik
Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

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

1.1 Zielsetzung

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

Der VZD ist ein zentraler Dienst der TI-Plattform.

Das Informationsmodell des VZD ist erweiterbar.

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

1.2 Zielgruppe

Das Dokument ist maßgeblich für Anbieter und Hersteller von Verzeichnisdiensten

1.3 Geltungsbereich

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

Schutzrechts-/Patentrechtshinweis

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

1.4 Abgrenzungen

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

1.5 Methodik

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

Sie werden im Dokument wie folgt dargestellt:

⌦ **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.

2 Systemüberblick

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

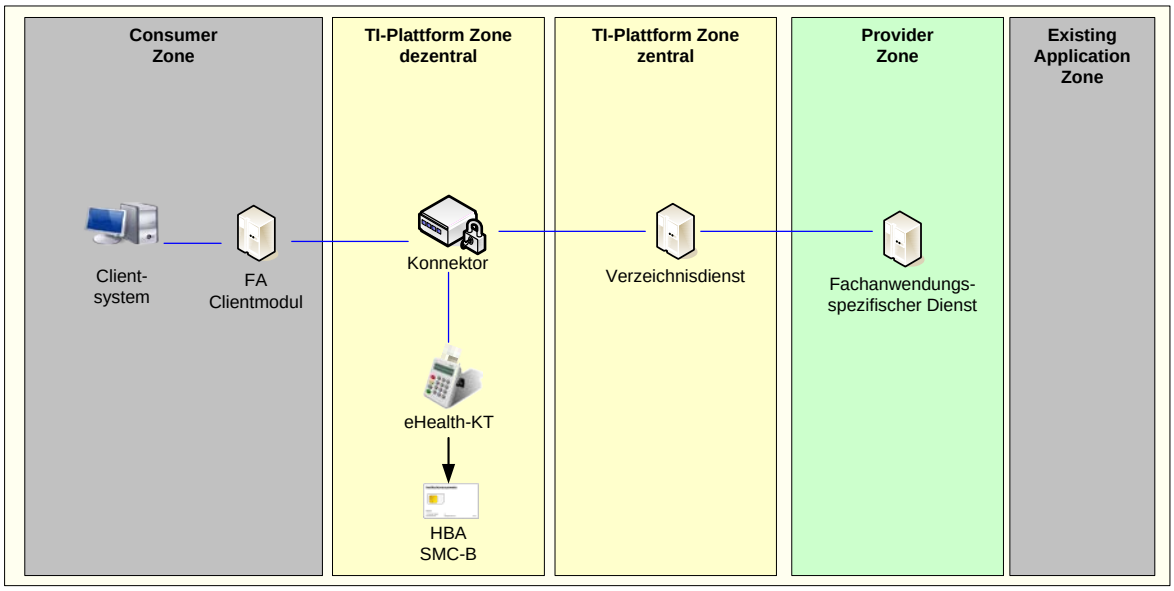

Abbildung 1: Einordnung des VZD in die TI

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

Die Dateneinträge werden erstellt und gepflegt:

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

Der VZD kann durch LDAP Clients abgefragt werden.

3 Übergreifende Festlegungen

3.1 IT-Sicherheit und Datenschutz

TIP1-A_5546 VZD, Integritäts- u. Authentizitätsschutz

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

TIP1-A_5547 VZD, Löschen ungültiger Zertifikate

Der VZD MUSS täglich die gespeicherten Zertifikate nach Ablaufdatum (TUC_PKI_002 „Gültigkeitsprüfung des Zertifikats“) und Status (TUC_PKI_006 "OCSP-Abfrage) prüfen. Ungültige Zertifikate werden sofort gelöscht. Ein Eintrag ohne gültige Zertifikate wird nach 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.⌫

3.2 Fachliche Anforderungen

⌦ **TIP1-A_5560 VZD, Erweiterbarkeit für neue Fachdaten**

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

⌦ **TIP1-A_5561 VZD, DNS-SD**

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

- für den Zugriff auf die Schnittstelle I_Directory_Query:

  _ldap._tcp.vzd.telematik.

- für den Zugriff auf die Schnittstelle I_Directory_Maintenance:

  _vzd-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. ⌫

4 Funktionsmerkmale

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

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

⌦ **TIP1-A_5564 VZD, Festlegung der Schnittstellen**

Der VZD MUSS die Schnittstellen gemäß Tabelle Tab_PT_VZD_Schnittstellen implementieren („bereitgestellte“ Schnittstellen) und nutzen („benötigte“ Schnittstellen).

Tabelle 1: Tab_PT_VZD_Schnittstellen

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

⌫

4.1 Schnittstelle I_Directory_Query

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

⌦ **TIP1-A_5565 VZD, Schnittstelle I_Directory_Query**

Der VZD MUSS für LDAP Clients die Schnittstelle I_Directory_Query gemäß Tabelle Tab_VZD_Schnittstelle_I_Directory_Query anbieten.

Tabelle 2: Tab_VZD_Schnittstelle_I_Directory_Query

Name	I_Directory_Query	
Version	wird im Produkttypsteckbrief des VZD definiert	
Operationen	Name	Kurzbeschreibung
	search_Directory	Abfragen von Daten des VZD gemäß LDAPv3 Protokoll

⌫

4.1.1 Operation search_Directory

TIP1-A_5566 LDAP Client, LDAPS

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

Der LDAP Client muss das Zertifikat des VZD C.ZD.TLS-S gemäß TUC_PKI_018 "Zertifikatsprüfung in der TI" und die Rolle (zulässig ist oid_vzd_ti) prüfen.

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.

4.1.1.1 Umsetzung

TIP1-A_5569 VZD, search_Directory, Suche nach definierten Attributen

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

Die Telematik-ID darf nicht als Ergebnis geliefert werden.

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

4.1.1.2 Nutzung

TIP1-A_5570 LDAP Client, TUC_VZD_0001 „search_Directory”

Der Anbieter des VZD MUSS für die Nutzung durch LDAP Clients den technischen Use Case TUC_VZD_0001 „search_Directory” gemäß Tabelle Tab_TUC_VZD_0001 unterstützen.

Tabelle 3: Tab_TUC_VZD_0001

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/Alterna-tiven	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.	

⌫

4.2 Schnittstelle I_Directory_Maintenance

Die Schnittstelle ermöglicht die Administration der Basisdaten.

⌦ **TIP1-A_5571 VZD, Schnittstelle I_Directory_Maintenance**

Der VZD MUSS die Schnittstelle I_Directory_Maintenance gemäß Tabelle Tab_VZD_Schnittstelle_I_Directory_Maintenance anbieten.

Tabelle 4: Tab_VZD_Schnittstelle_I_Directory_Maintenance

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.⌫

4.2.1 Operation add_Directory_Entry

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

4.2.1.1 Umsetzung

⌦ **TIP1-A_5575 VZD, Umsetzung add_Directory_Entry**

Der VZD MUSS nach folgenden Vorgaben die Operation add_Directory_Entry implementieren:

1) Ein bereits zur Telematik-ID gehörender Basisdatensatz wird gelöscht und neu angelegt.
2) Existiert noch kein Basisdatensatz zur Telematik-ID wird ein neuer angelegt.
3) Die Daten aus dem SOAP Request bilden gemäß VZD_TAB_addDirectoryEntry_Mapping 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
	aus ENC-Zertifikat: Subject/givenName		givenName	
aus ENC-Zertifikat: Subject/organisationName	aus ENC-Zertifikat: Subject/surname		sn	

SMC-B-Daten	HBA-Daten	SOAP-Request Element	LDAP-Directory Basisdatensatz Attribut	Beschreibung
aus ENC-Zertifikat: Subject/organisationName	aus ENC-Zertifikat: Subject/surname, Subject/givenName		displayName	eingetragen.
		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.⌫

4.2.1.2 Nutzung

⌦ **TIP1-A_5576 Nutzer der Schnittstelle, TUC_VZD_0002 „add_Directory_Entry"**

Der Nutzer der Schnittstelle MUSS den technischen Use Case TUC_VZD_0002 „add_Directory_Entry" gemäß Tabelle Tab_TUC_VZD_0002 umsetzen.

Der SOAP-Requests MUSS gemäß Tabelle VZD_TAB_addDirectoryEntry_Mapping mit der Bedeutung entsprechenden Daten ausgefüllt sein.

Tabelle 6: Tab_TUC_VZD_0002

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.

⌫

4.2.2 Operation read_Directory_Entry

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

4.2.2.1 Umsetzung

⌦ **TIP1-A_5577 VZD, Umsetzung read_Directory_Entry**

Der VZD MUSS nach folgenden Vorgaben die Operation I_Directory_Maintenance::read_Directory_Entry implementieren:

1) Der zur Telematik-ID gehörende Eintrag wird im LDAP Directory ermittelt.

2) Es wird eine SOAP Response VZD:readResponseMsg aus dem kompletten Eintrag (Basisdaten + Fachdaten) gemäß 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/common Name	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>,	

LDAP-Directory Basisdatensatz Attribut	SOAP-Response Element	Beschreibung	Kardinalität
		<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.⌫

4.2.2.2 Nutzung

⌦ **TIP1-A_5578 Nutzer der Schnittstelle, TUC_VZD_0003 „read_Directory_Entry”**

Der Nutzer der Schnittstelle MUSS den technischen Use Case TUC_VZD_0003 „read_Directory_Entry” gemäß Tabelle Tab_TUC_VZD_0003 umsetzen. Der Webservice wird durch die Dokumente DirectoryMaintenance.wsdl und DirectoryMaintenance.xsd definiert.

Die SOAP-Response ist gemäß Tabelle VZD_TAB_readDirectoryEntry_Mapping 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-	Wenn noch keine Verbindung besteht initiiert der Nutzer der

	Verbindung	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/Alterna-tiven	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.	

⌫

4.2.3 Operation modify_Directory_Entry

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

4.2.3.1 Umsetzung

⌦ **TIP1-A_5579 VZD, Umsetzung modify_Directory_Entry**

Der VZD MUSS nach folgenden Vorgaben die Operation modify_Directory_Entry implementieren:

1) Der zur Telematik-ID gehörende Basisdatensatz wird im LDAP Directory ermittelt.

2) Die Daten im Basisdatensatz werden durch die Daten aus dem SOAP Request gemäß 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/common	aus ENC-Zertifikat: Subject/commonN		cn	Diese Werte werden dem in VZD:x509CertificateEnc enthaltenen Zertifikat

SMC-B-Zertifikats-Eintrag	HBA-Zertifikats-Eintrag	SOAP-Request Element	LDAP-Directory Basisdatensatz Attribut	Beschreibung
Name	ame			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.⌫

4.2.3.2 Nutzung

⌦ **TIP1-A_5580 Nutzer der Schnittstelle, TUC_VZD_0004 „modify_Directory_Entry”**

Der Nutzer der Schnittstelle MUSS den technischen Use Case TUC_VZD_0004 „modify_Directory_Entry” gemäß Tabelle Tab_TUC_VZD_0004 umsetzen. Der Webservice wird durch die Dokumente DirectoryMaintenance.wsdl und DirectoryMaintenance.xsd definiert.

Der SOAP-Requests MUSS gemäß Tabelle VZD_TAB_modifyDirectoryEntry_Mapping mit der Bedeutung entsprechenden Daten ausgefüllt sein.

Tabelle 10: Tab_TUC_VZD_0004

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/Alterna-tiven	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.	

⌫

4.2.4 Operation delete_Directory_Entry

Diese Operation löscht einen bestehenden Datensatz im LDAP Verzeichnis.

4.2.4.1 Umsetzung

⌦ **TIP1-A_5581 VZD, Umsetzung delete_Directory_Entry**

Der VZD MUSS nach folgenden Vorgaben die Operation I_Directory_Maintenance::delete_Directory_Entry implementieren:

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

Es müssen die Fehlermeldungen gemäß Tab_TUC_VZD_0005 verwendet werden.⌫

4.2.4.2 Nutzung

⌦ **TIP1-A_5582 Nutzer der Schnittstelle, TUC_VZD_0005 „delete_Directory_Entry”**

Der Nutzer der Schnittstelle MUSS den technischen Use Case TUC_VZD_0005 „delete_Directory_Entry” gemäß Tabelle Tab_TUC_VZD_0005 umsetzen. Der Webservice wird durch die Dokumente DirectoryMaintenance.wsdl und DirectoryMaintenance.xsd definiert.

Tabelle 11: Tab_TUC_VZD_0005

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.	

⌫

4.3 Schnittstelle I_Directory_Application_Maintenance

Die Schnittstelle ermöglicht die Administration der Fachdaten.

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

⌦ **TIP1-A_5583 VZD, Schnittstelle I_Directory_Application_Maintenance**

Der VZD MUSS für FADs I_Directory_Maintenance gemäß Tabelle Tab_VZD_Schnittstelle_I_Directory_Application_Maintenance anbieten.

Tabelle 12: Tab_VZD_Schnittstelle_I_Directory_Application_Maintenance

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.

4.3.1 Operation add_Directory_FA-Attributes

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

Voraussetzung: Die Fachdaten müssen einem Basisdateneintrag zuordenbar sein.

4.3.1.1 Umsetzung SOAP

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

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

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

   faultcode: 4312,

   faultstring: Basisdaten konnten nicht gefunden werden.

2) Ein bereits zur Telematik-ID gehörender Fachdatensatz wird gelöscht und neu angelegt.

3) Ein noch nicht existierender Fachdatensatz zur Telematik-ID wird im LDAP Directory neu angelegt.

4) Die Daten aus dem SOAP Request werden gemäß VZD_TAB_I_Directory_Application_Maintenance_Add_Mapping zum Basisdatensatz hinzugefügt.

Tabelle 13: VZD_TAB_I_Directory_Application_Maintenance_Add_Mapping

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

Es müssen die Fehlermeldungen gemäß Tab_TUC_VZD_0006 verwendet werden.⌫

4.3.1.2 Nutzung SOAP

⌦ TIP1-A_5591 FAD, TUC_VZD_0006 “add_Directory_FA-Attributes (SOAP)”

Der FAD MUSS den technischen Use Case TUC_VZD_0006 “add_Directory_FA-Attributes” gemäß Tabelle Tab_TUC_VZD_0006 umsetzen.

Tabelle 14: Tab_TUC_VZD_0006

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	Die SOAP-Response VZD:responseMsg enthält den vzd:status.

	empfangen	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

⌫

4.3.1.3 Umsetzung LDAPv3

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

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

1) Wenn kein zur Telematik-ID gehörender Basisdatensatz gefunden wurde, wird der Request mit einer Fehlermeldung beendet.

2) Ein noch nicht existierender Fachdatensatz zur Telematik-ID wird im VZD neu angelegt.

3) Der FAD darf nur die zu seinem Dienst gehörenden Fachdaten schreiben.

Es müssen die Fehlermeldungen gemäß Tab_TUC_VZD_0007 verwendet werden.⌫

4.3.1.4 Nutzung LDAPv3

⌦ TIP1-A_5594 FAD, TUC_VZD_0007 “add_Directory_FA-Attributes (LDAPv3)”

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

Tabelle 16: Tab_TUC_VZD_0007

Name	add_Directory_FA-Attributes(LDAPv3)

Beschreibung	Mit dieser Operation werden Fachdaten zu einem bestehenden Eintrag zugefügt.	
Vorbedingungen	Der LDAPS-Verbindungsaufbau muss erfolgreich durchgeführt sein.	
Eingangsdaten	Add-Request gemäß [RFC4511]#4.7 und Informationsmodell (Abb_VZD_logisches_Datenmodell)	
Komponenten	LDAP Client des FAD, Verzeichnisdienst	
Ausgangsdaten	gemäß [RFC4511]#4.7	
Standardablauf	Aktion	Beschreibung
	Add Request senden	Der LDAP Client des FAD sendet den Add-Request gemäß [RFC4511]#4.7 an den VZD. Die RFCs [RFC4510], [RFC4511], [RFC4513], [RFC4514], [RFC4515], [RFC4516], [RFC4519] und [RFC4522] müssen unterstützt werden.
	Add Response empfangen	Der LDAP Client empfängt das Ergebnis der Operation gemäß [RFC4511]#4.7.
Varianten/Alternativen	keine	
Zustand nach erfolgreichem Ablauf	Das Ergebnis der Operation liegt im LDAP Client des FAD vor.	
Fehlerfälle	Zur Behandlung auftretender Fehlerfälle werden Fehlermeldungen gemäß [RFC4511]#Appendix A verwendet.	

⌫

4.3.2 Operation delete_Directory_FA-Attributes

Diese Operation löscht einen Fachdatensatz.

4.3.2.1 Umsetzung SOAP

⌦ TIP1-A_5595 VZD, Umsetzung delete_Directory_FA-Attributes

Der VZD MUSS nach folgenden Vorgaben die Operation delete_Directory_ FA-Attributes implementieren:

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

   faultcode: 4312,

   faultstring: Basisdaten konnten nicht gefunden werden.

2) Ein zur Telematik-ID gehörender Fachdatensatz wird gelöscht.

3) Ein nicht existierender Fachdatensatz zur Telematik-ID führt zu keiner Aktion.

Es müssen die Fehlermeldungen gemäß Tab_TUC_VZD_0008 verwendet werden.⌫

4.3.2.2 Nutzung SOAP

⌦ TIP1-A_5596 FAD, TUC_VZD_0008 “delete_Directory_FA-Attributes (SOAP)”

Der FAD MUSS den technischen Use Case TUC_VZD_0008 “delete_Directory_FA-Attributes” gemäß Tabelle Tab_TUC_VZD_0008 umsetzen.

Tabelle 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.	

⌫

4.3.2.3 Umsetzung LDAPv3

⌦ **TIP1-A_5597 VZD, Umsetzung delete_Directory_FA-Attributes (LDAPv3)**

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

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

Es müssen die Fehlermeldungen gemäß Tab_TUC_VZD_0009 verwendet werden.⌫

4.3.2.4 Nutzung LDAPv3

⌦ **TIP1-A_5598 FAD, TUC_VZD_0009 “delete_Directory_FA-Attributes (LDAPv3)”**

Der FAD MUSS den technischen Use Case TUC_VZD_0009 „delete_Directory_FA-Attributes(LDAPv3)” gemäß Tabelle Tab_TUC_VZD_0009 unterstützen.

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

⌫

4.3.3 Operation modify_Directory_FA-Attributes

Diese Operation überschreibt einen Fachdatensatz.

4.3.3.1 Umsetzung SOAP

⌦ **TIP1-A_5599 VZD, Umsetzung modify_Directory_FA-Attributes**

Der VZD MUSS nach folgenden Vorgaben die Operation modify_Directory_ FA-Attributes implementieren:

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

   faultcode: 4312,

   faultstring: Basisdaten konnten nicht gefunden werden.

2) Ein bereits zur Telematik-ID gehörender Fachdatensatz wird überschrieben.

3) Die Daten aus dem SOAP Request werden gemäß VZD_TAB_I_Directory_Application_Maintenance_Modify_Mapping zum Basisdatensatz hinzugefügt.

Tabelle 19: VZD_TAB_I_Directory_Application_Maintenance_Modify_Mapping

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

Es müssen die Fehlermeldungen gemäß Tab_TUC_VZD_0010 verwendet werden.⌫

4.3.3.2 Nutzung SOAP

⌦ **TIP1-A_5600 FAD, TUC_VZD_0010 “modify_Directory_FA-Attributes (SOAP)”**

Der FAD MUSS den technischen Use Case TUC_VZD_0010 “modify_Directory_FA-Attributes” gemäß Tabelle Tab_TUC_VZD_0010 umsetzen.

Tabelle 20: Tab_TUC_VZD_0010

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

⌫

4.3.3.3 Umsetzung LDAPv3

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

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

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

Es müssen die Fehlermeldungen gemäß Tab_TUC_VZD_0011 verwendet werden.⌫

4.3.3.4 Nutzung LDAPv3

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

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

Tabelle 22: Tab_TUC_VZD_0011

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

⌫

4.4 Prozessschnittstelle P_Directory_Application_Registration (Provided)

⌦ **TIP1-A_5604 VZD, Registrierung FADs**

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

- Gültigkeit des TLS-Client-Zertifikat des FADs C.FD.TLS-C (Prüfschritte wie in TUC_PKI_018 und mit admission gemäß vom 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.⌫

4.5 Prozessschnittstelle P_Directory_Maintenance (Provided)

⌦ **TIP1-A_5606 VZD, Mandat zur Löschung von Einträgen.**

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

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

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

4.6 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.⌫

5 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.

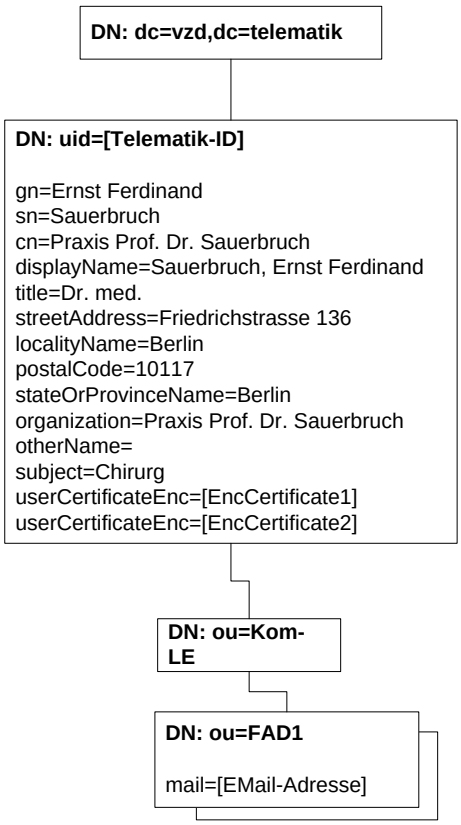

Abbildung 2: Abb_VZD_logisches_Datenmodell

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

Kürzel	Erläuterung
XML	Extensible Markup Language

A2 – Glossar

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

A3 – Abbildungsverzeichnis

A4 – Tabellenverzeichnis

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):

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
	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