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

Änderungsbedarf:

Zum Füllen und Administrieren der Verzeichnisdaten müssen die nötigen Schnittstellen definiert werden.

Änderungen in [gemSpec_VZD]

Neu:

4 Funktionsmerkmale

Tabelle : Tab_PT_VZD_Schnittstellen

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

4.6 Schnittstelle I_Directory_Administration

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

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

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

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

4.6.1 Operationen der Schnittstelle I_ Directory_Administration

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

A_18371 - VZD, Schnittstelle I_Directory_Administration
Der VZD MUSS die Schnittstelle I_Directory_Administration gemäß Tabelle Tab_VZD_Schnittstelle_I_Directory_Administration im Internet anbieten.

Tabelle : Tab_VZD_Schnittstelle_I_Directory_Administration

Name	**I_Directory_Administration**	
Version	wird im Produkttypsteckbrief des VZD definiert	
Operationen	Resource: DirectoryEntry	
	Name	Kurzbeschreibung
	POST	Hinzufügen eines Verzeichniseintrages inklusive dazugehörendem Zertifikat.
	GET	Abfrage aller Daten von Verzeichniseinträgen.
	PUT	Änderung eines Basisdaten-Verzeichniseintrages.
	DELETE	Löschung eines Verzeichniseintrages (kompletter Datensatz inklusive aller Zertifikate und Fachdaten).
	Resource: Certificate	
	Name	Kurzbeschreibung
	POST	Hinzufügen eines Zertifikatseintrags zu einem Verzeichniseintrag.
	GET	Abfrage von Zertifikatseinträgen.
	PUT	Änderung eines Zertifikatseintrags.
	DELETE	Löschung eines Zertifikatseintrags.

A_18373 – VZD, Schnittstelle I_Directory_Administration, REST-Webservice
Der VZD MUSS die Schnittstelle I_Directory_Administration als REST-Webservice über HTTPS implementieren. Der Webservice wird durch das Dokument DirectoryAdministration.yaml definiert.

A_18408 - VZD, I_Directory_Administration, Registrierung
Der VZD Anbieter MUSS für Clients der Schnittstelle I_Directory_Administration einen Registrierungsprozess bereitstellen. Während der Registrierung muss die Berechtigung des Antragstellers (Clients) zur Nutzung von Schnittstelle I_Directory_Administration durch den VZD Anbieter geprüft und durch die gematik bestätigt werden. Nach erfolgreicher Registrierung MÜSSEN dem Antragsteller alle nötigen Daten - inklusive OAuth Client Credentials, CA Zertifikat (welches zur Prüfung des Server Zertifikats durch den Client benötigt wird), VZD Server-Zertifikat - zur Nutzung der Schnittstelle bereitgestellt werden.

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

A_18470 - VZD, I_Directory_Administration, Client Secret Qualität
Der VZD Anbieter MUSS bei der Erzeugung der OAuth client_secret‘s 128 Bit Zufall aus einer Zufallsquelle gemäß GS-A_4367 [gemSpec_Krypt] verwenden.

A_18409 - VZD, I_Directory_Administration, Sperrung OAuth Client Credentials
Der VZD Anbieter MUSS – für die gematik und den Client Betreiber selbst - einen Service zur Sperrung der OAuth Client Credentials anbieten.

A_18372 - VZD, I_Directory_Administration, TLS-gesicherte Verbindung
Der VZD MUSS die Schnittstelle I_Directory_Administration durch Verwendung von TLS mit serverseitiger Authentisierung sichern.
Der VZD muss sich mit der Server Identität von Schnittstelle I_Directory_Administration authentisieren.

A_18374 - VZD, I_Directory_Administration, Redirect
Der VZD MUSS für die Schnittstelle I_Directory_Administration Anfragen der Clients – welche kein AccessToken entsprechend [RFC 6750] enthalten – durch ein Redirect zu dem OAuth2 Authentifizierungsdienst weiterleiten.

A_18375 - VZD, I_Directory_Administration, OAuth2 Dienst
Der VZD MUSS einen OAuth2 Dienst bereitstellen. Dieser Dienst MUSS die Clients der Schnittstelle I_Directory_Administration anhand ihrer Client Credentials authentisieren und ihnen ein AccessToken entsprechend [RFC 6750] ausstellen. Das AccessToken muss im "sub" claim den Identifier des Clients enthalten. Die Anfrage des Clients MUSS nach erfolgreicher Authentisierung durch ein Redirect wieder zur VZD I_Directory_Administration Schnittstelle weitergeleitet werden.

A_18376 - VZD, I_Directory_Administration, Prüfung AccessToken
Der VZD MUSS das vom Client übergebene AccessToken auf Gültigkeit für Schnittstelle I_Directory_Administration prüfen. Bei negativem Ergebnis muss die Operation mit HTTP Fehler 401 Unauthorized abgebrochen werden.

A_18471 - VZD, I_Directory_Administration, Datenquelle
Der VZD MUSS bei den Operationen createDirectoryEntry und updateBaseDirectoryEntry das LDAP-Directory Attribut dataFromAuthority auf den Wert TRUE und bei allen anderen Operationen unverändert belassen.

A_18472 - VZD, I_Directory_Administration, Doubletten
Der VZD MUSS bei den Operationen createDirectoryEntry und updateBaseDirectoryEntry prüfen, ob die Operation eine Doublette im LDAP Verzeichnis erzeugt und in diesem Fall die Operation mit HTTP Fehlercode “400 Bad Request“ ablehnen. Zur Prüfung auf eine potentielle Dublette MUSS der VZD alle LDAP-Directory Attribute des zu erzeugenden Basisdatensatzes (Verzeichnisdienst_Eintrag ohne Certificate und Fachdaten) jedoch ohne den Distinguished Name heranziehen.

4.6.1.1 DirectoryEntry Administration

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

4.6.1.1.1 POST

Diese Operation legt einen neuen Eintrag im LDAP Verzeichnis an.

A_18448 - VZD, I_Directory_Administration, add_Directory_Entry
Der VZD MUSS Operation „add_Directory_Entry" gemäß Tabelle Tab_VZD „add_Directory_Entry" umsetzen.

Tabelle : Tab_VZD „add_Directory_Entry"

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

4.6.1.1.2 GET

Diese Operation liest Verzeichniseinträge aus dem LDAP Verzeichnis.

A_18449 - VZD, I_Directory_Administration, read_Directory_Entry
Der VZD MUSS Operation „read_Directory_Entry" gemäß Tabelle Tab_VZD „read_Directory_Entry" umsetzen.

Tabelle : Tab_VZD „read_Directory_Entry"

Name	read_Directory_Entry

Beschreibung	Diese Operation ermöglicht die Suche und Lesen von Verzeichniseinträgen im LDAP Verzeichnis.	
Eingangsdaten	REST-Request GET /DirectoryEntries operationId: read_Directory_Entry (siehe DirectoryAdministration.yaml)	
	Parameter	Beschreibung
	Parameter zur Selektion der Verzeichniseinträge	Eine Reihe von Parametern kann zur Suche in dem Verzeichnisdienst_Eintrag genutzt werden. Die angegebenen Parameter werden zur Suche mit einem logischen UND verknüpft.
Komponenten	Nutzer der Schnittstelle, Verzeichnisdienst	
Ausgangsdaten	REST-Response mit allen zu den Filter Parametern passenden Verzeichniseinträgen. Die Verzeichniseinträge werden inklusive Zertifikatseinträgen und Fachdaten geliefert.	
Ablauf	Der VZD sucht im LDAP Verzeichnis die zu den Such-Parametern passenden Verzeichniseinträge. Bei mehr als 100 gefundenen Einträgen wird der Request mit Fehler „400 Bad Request“ beantwortet.	
Fehlerfälle	Es werden die protokollspezifischen Fehlermeldungen verwendet (TCP, HTTP, TLS) und in DirectoryAdministration.yaml mit spezifischen Fehlerbeschreibungen ergänzt.	

4.6.1.1.3 PUT

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

A_18450 - VZD, I_Directory_Administration, modify_Directory_Entry
Der VZD MUSS Operation „modify_Directory_Entry” gemäß Tabelle Tab_VZD „modify_Directory_Entry” umsetzen.

Tabelle : Tab_VZD „modify_Directory_Entry”

Name	modify_Directory_Entry	
Beschreibung	Diese Operation ermöglicht die Suche und Lesen von Verzeichniseinträgen im LDAP Verzeichnis.	
Eingangsdaten	REST-Request PUT /DirectoryEntries/{uid}/baseDirectoryEntries operationId: modify_Directory_Entry (siehe DirectoryAdministration.yaml)	
	Parameter	Beschreibung
	uid	Die „uid“ identifiziert den Verzeichnisdienst_Eintrag (Abb_VZD_logisches_Datenmodell) welcher aktualisiert wird.
	displayName	Kann optional angegeben werden und überschreibt den Wert im selektierten Verzeichniseintrag.
	streetAddress	Kann optional angegeben werden und überschreibt den Wert im selektierten Verzeichniseintrag.
	postalCode	Kann optional angegeben werden und überschreibt den Wert im selektierten Verzeichniseintrag.
	localityName	Kann optional angegeben werden und

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

4.6.1.1.4 DELETE

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

A_18451 - VZD, I_Directory_Administration, delete_Directory_Entry
Der VZD MUSS Operation „delete_Directory_Entry” gemäß Tabelle Tab_VZD „delete_Directory_Entry” umsetzen.

Tabelle : Tab_VZD „delete_Directory_Entry”

Name	delete_Directory_Entry	
Beschreibung	Diese Operation ermöglicht die Löschung von kompletten Verzeichniseinträgen (inklusive Zertifikaten und Fachdaten) im LDAP Verzeichnis.	
Eingangsdaten	REST-Request DELETE /DirectoryEntries/{uid} operationId: delete_Directory_Entry (siehe DirectoryAdministration.yaml)	
	Parameter	Beschreibung
	uid	Die „uid“ identifiziert den Verzeichnisdienst_Eintrag (Abb_VZD_logisches_Datenmodell) welcher inklusive der dazu gehörenden Zertifikate und Fachdaten gelöscht wird.
Komponenten	Nutzer der Schnittstelle, Verzeichnisdienst	

Ausgangsdaten	REST-Response.
Ablauf	Der VZD löscht im LDAP Verzeichnis den über Parameter „uid“ identifizierten Verzeichniseintrag inklusive der dazu gehörenden Zertifikate und Fachdaten.
Fehlerfälle	Es werden die protokollspezifischen Fehlermeldungen verwendet (TCP, HTTP, TLS) und in DirectoryAdministration.yaml mit spezifischen Fehlerbeschreibungen ergänzt.

4.6.1.2 Certificate Administration

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

4.6.1.2.1 POST

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

A_18452 - VZD, I_Directory_Administration, add_Directory_Entry_Certificate
Der VZD MUSS Operation „add_Directory_Entry_Certificate” gemäß Tabelle Tab_VZD „add_Directory_Entry_Certificate” umsetzen.

Tabelle : Tab_VZD „add_Directory_Entry_Certificate”

Name	add_Directory_Entry_Certificate	
Beschreibung	Diese Operation fügt einem existierenden Basisdatensatz einen Zertifikatseintrag im LDAP Verzeichnis an.	
Eingangsdaten	REST-Request POST /DirectoryEntries/{uid}/Certificates operationId: add_Directory_Entry_Certificate (siehe DirectoryAdministration.yaml)	
	Parameter	Beschreibung
	uid	Die „uid“ identifiziert den Verzeichnisdienst_Eintrag (Abb_VZD_logisches_Datenmodell) an welchen der Zertifikatseintrag angehangen wird.
	userCertificate	Muss angegeben werden und enthält das Zertifikat.
	usage	Kann optional belegt werden.
	description	Kann optional belegt werden.
Komponenten	Nutzer der Schnittstelle, Verzeichnisdienst	
Ausgangsdaten	REST-Response mit dem Distinguished Name (dn) von dem erzeugten Certificate Eintrag.	
Ablauf	Der VZD übernimmt entsprechend Tab_VZD_Datenbeschreibung Attribute aus dem Zertifikat und trägt die übergebenen Parameter in den Zertifikatseintrag ein. Der Distinguished Name (dn) von dem erzeugten Certificate wird vom Verzeichnisdienst gefüllt und über dn.uid mit dem übergeordneten Verzeichnisdienst_Eintrag verknüpft.	
Fehlerfälle	Es werden die protokollspezifischen Fehlermeldungen verwendet (TCP, HTTP, TLS) und in DirectoryAdministration.yaml mit spezifischen Fehlerbeschreibungen ergänzt.	

4.6.1.2.2 GET

Diese Operation liest Zertifikatseinträge aus dem LDAP Verzeichnis.

A_18453 - VZD, I_Directory_Administration, read_Directory_Certificates
Der VZD MUSS Operation „read_Directory_Certificates" gemäß Tabelle Tab_VZD „read_Directory_Certificates" umsetzen.

Tabelle : Tab_VZD „read_Directory_Certificates"

Name	read_Directory_Certificates	
Beschreibung	Diese Operation ermöglicht die Suche und Lesen von Verzeichniseinträgen im LDAP Verzeichnis.	
Eingangsdaten	REST-Request GET /DirectoryEntries/Certificates operationId: read_Directory_Certificates (siehe DirectoryAdministration.yaml) Mindestens ein Filter Parameter muss angegeben werden.	
	Parameter	Beschreibung
	uid	Optionaler Parameter. Die „uid" identifiziert einen Verzeichnisdienst_Eintrag (Abb_VZD_logisches_Datenmodell). Dieser Parameter selektiert alle Zertifikatseinträge dieses Verzeichnisdiensteintrags.
	certificateEntryID	Optionaler Parameter. Dieser Parameter identifiziert einen Zertifikatseintrag (Abb_VZD_logisches_Datenmodell dn.cn von Certificate).
	telematikID	Optionaler Parameter. Dieser Parameter selektiert alle Zertifikatseinträge mit dieser TeleamtikID.
Komponenten	Nutzer der Schnittstelle, Verzeichnisdienst	
Ausgangsdaten	REST-Response mit allen zu den Filter Parametern passenden Zertifikatseinträgen.	
Ablauf	Der VZD sucht im LDAP Verzeichnis die zu den Such-Parametern passenden Zertifikatseinträge. Bei mehr als 100 gefundenen Einträgen wird der Request mit Fehler „400 Bad Request" beantwortet.	
Fehlerfälle	Es werden die protokollspezifischen Fehlermeldungen verwendet (TCP, HTTP, TLS) und in DirectoryAdministration.yaml mit spezifischen Fehlerbeschreibungen ergänzt.	

4.6.1.2.3 PUT

Diese Operation aktualisiert den Zertifikatseintrag mit den übergebenen Daten im LDAP Verzeichnis.

A_18454 - VZD, I_Directory_Administration, modify_Directory_Entry_Certificate
Der VZD MUSS Operation „modify_Directory_Entry_Certificate" gemäß Tabelle Tab_VZD

„modify_Directory_Entry" umsetzen.

Tabelle : Tab_VZD „modify_Directory_Entry_Certificate"

Name	modify_Directory_Entry_Certificate	
Beschreibung	Diese Operation ermöglicht die Aktualisierung von Zertifikatseinträgen (Certificate in Abb_VZD_logisches_Datenmodell) im LDAP Verzeichnis.	
Eingangsdaten	REST-Request PUT /DirectoryEntries/{uid}/Certificates/{certificateEntryID} operationId: modify_Directory_Entry_Certificate (siehe DirectoryAdministration.yaml)	
	Parameter	Beschreibung
	uid	Pflichtparameter. Die „uid" identifiziert den Verzeichnisdienst_Eintrag (Abb_VZD_logisches_Datenmodell) zu dem der Zertifikatseintrag gehört.
	certificateEntryID	Pflichtparameter. Dieser Parameter identifiziert einen Zertifikatseintrag (Abb_VZD_logisches_Datenmodell dn.cn von Certificate).
	usage	Kann optional angegeben werden und überschreibt den Wert im selektierten Verzeichniseintrag.
	description	Kann optional angegeben werden und überschreibt den Wert im selektierten Verzeichniseintrag.
	userCertificate	Pflichtparameter. Muss unverändert gegenüber dem Zertifikat im VZD sein.
Komponenten	Nutzer der Schnittstelle, Verzeichnisdienst	
Ausgangsdaten	REST-Response mit dem Distinguished Name (dn) von dem aktualisierten Zertifikatseintrag (Certificate in Abb_VZD_logisches_Datenmodell).	
Ablauf	Der VZD aktualisiert im LDAP Verzeichnis den über Parameter „certificateEntryID" identifizierten Zertifikatseintrag mit den übergebenen Parametern. Falls das übergebene userCertificate nicht mit dem Wert im LDAP Verzeichnis übereinstimmt wird mit Fehler 400 Bad Request abgebrochen.	
Fehlerfälle	Es werden die protokollspezifischen Fehlermeldungen verwendet (TCP, HTTP, TLS) und in DirectoryAdministration.yaml mit spezifischen Fehlerbeschreibungen ergänzt.	

4.6.1.2.4 DELETE

Diese Operation löscht einen Zertifiktseintrag.

A_18455 - VZD, I_Directory_Administration, delete_Directory_Entry_Certificate
Der VZD MUSS Operation „delete_Directory_Entry_Certificate" gemäß Tabelle Tab_VZD „delete_Directory_Entry_Certificate" umsetzen.

Tabelle : Tab_VZD „delete_Directory_Entry_Certificate"

Name	delete_Directory_Entry_Certificate	
Beschreibung	Diese Operation ermöglicht die Löschung eines Zertifikatsseintrags im LDAP Verzeichnis.	
Eingangsdaten	REST-Request DELETE /DirectoryEntries/{uid}/Certificates/{certificateEntryID} operationId: delete_Directory_Entry_Certificate (siehe DirectoryAdministration.yaml)	
	Parameter	Beschreibung
	uid	Pflichtparameter. Die „uid“ identifiziert den Verzeichnisdienst_Eintrag (Abb_VZD_logisches_Datenmodell) zu dem der Zertifikatseintrag gehört.
	certificateEntryID	Pflichtparameter. Dieser Parameter identifiziert einen Zertifikatseintrag (Abb_VZD_logisches_Datenmodell dn.cn von Certificate).
Komponenten	Nutzer der Schnittstelle, Verzeichnisdienst	
Ausgangsdaten	REST-Response.	
Ablauf	Der VZD löscht im LDAP Verzeichnis den über die Parameter „uid“ und „certificateEntryID“ identifizierten Zertifikatseintrag.	
Fehlerfälle	Es werden die protokollspezifischen Fehlermeldungen verwendet (TCP, HTTP, TLS) und in DirectoryAdministration.yaml mit spezifischen Fehlerbeschreibungen ergänzt.	

4.6.2 Nutzung der Schnittstelle I_Directory_Administration

Der Client der Schnittstelle I_Directory_Administration muss eine TLS Verbindung mit serverseitiger Authentisierung nutzen. Dabei muss er das Server Zertifikat des VZD prüfen. Bei negativem Ergebnis muss der Verbindungsaufbau abgebrochen werden.

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

Beispielablauf:

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

a. Falls ein Eintrag gefunden wurde:
    1. Lesen des Basis-Verzeichniseintrags (operationId read_Directory_Entry mit Parameter „uid“ aus dem read_Directory_Certificates Response)
    2. Aktualisieren des Verzeichniseintrags und (je nach Bedarf) der dazugehörigen Zertifikatseinträge (operationId‘s: modify_Directory_Entry, delete_Directory_Entry, modify_Directory_Entry_Certificate, delete_Directory_Entry_Certificate)
b. Falls kein Eintrag gefunden wurde:
    1. Erzeugen des Verzeichniseintrags und (je nach Bedarf) anhängen zusätzlicher Zertifikatseinträge (operationId‘s: add_Directory_Entry, add_Directory_Entry_Certificate). Der erste Zertifikatseintrag wird mit

Operation add_Directory_Entry erzeugt da jeder Verzeichniseintrags mindestens einen Zertifikatseintrag enthalten muss. Zusätzliche Zertifikatseinträge können mit Operation add_Directory_Entry_Certificate hinzugefügt werden.

5. Datenmodell

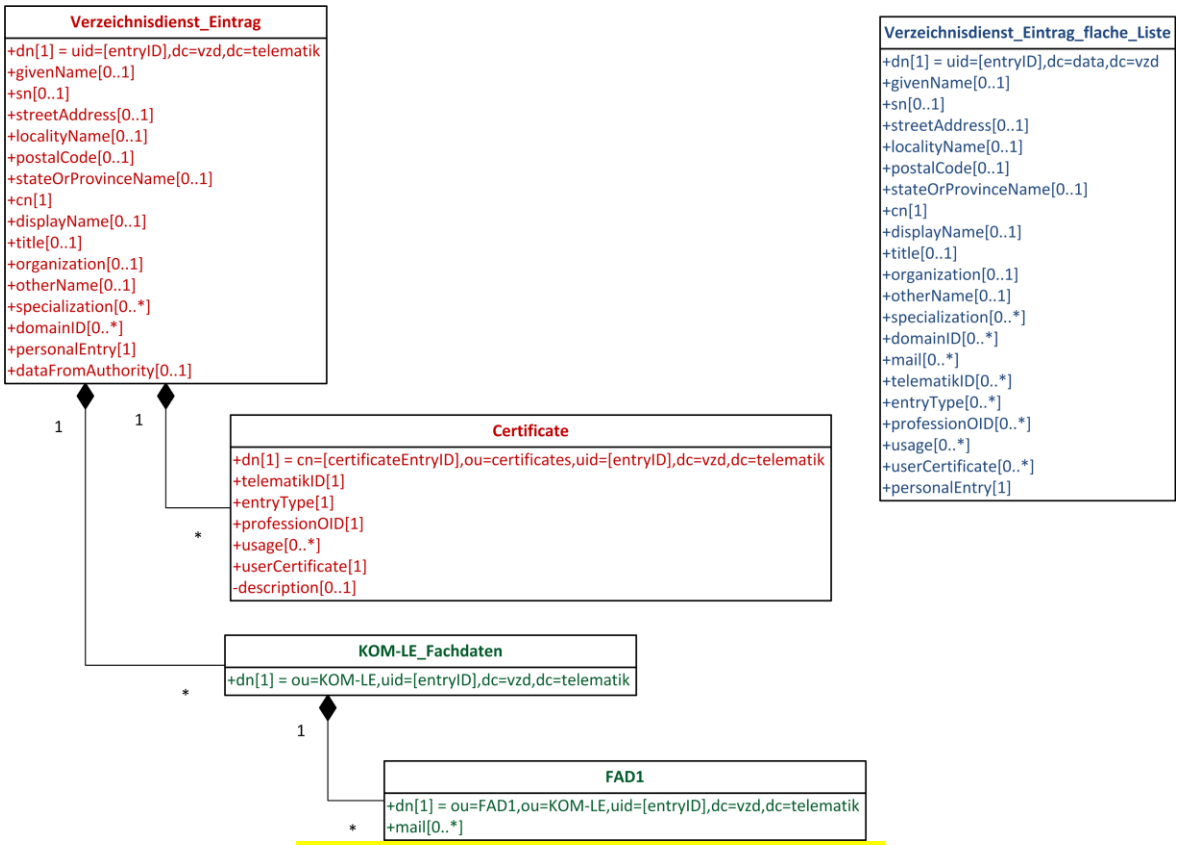

Abbildung : Abb_VZD_logisches_Datenmodell

Tabelle Tab_VZD_Datenbeschreibung

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

cn	obligatorisch	HBA: Bezeichner: Vorname und Nachname SMC-B: Bezeichner: Name Wird vom VZD aus dem Zertifikatsattribut commonName übernommen.
displayName	optional	Bezeichner: Anzeigename kann geändert werden HBA: voreingestellter Wert == givenName + sn SMC-B: voreingestellter Wert == organization SMC-B für Zahnärzte == cn (ProfessionOID 1.2.276.0.76.4.51 (Zahnarztpraxis))
streetAddress	optional	Bezeichner: Straße und Hausnummer
postalCode	optional	Bezeichner: Postleitzahl
localityName	optional	Bezeichner: Ort
stateOrProvinceName	optional	Bezeichner: Bundesland
title	optional	HBA: Bezeichner: Titel, optional SMC-B: nicht verwendet
organization	optional	Wenn vorhanden, dann wird das Zertifikatsattribut organizationName eingetragen kann geändert werden HBA: Bezeichner: Organisation, optional SMC-B: Bezeichner:Organisation, optional SMC-B KTR: Bezeichner: Betriebsnummer (BBNR)
otherName	optional	Bezeichner: Anderer Name Wird vom VZD aus dem Zertifikatsattribut otherName übernommen.
specialization	optional	HBA: Bezeichner: medizinisches Fachgebiet SMC-B: Bezeichner: Fachgebiet SMC-B KTR: nicht verwendet kann mehrfach vorkommen (0..100)
domainID	optional	kann geändert werden Ärzte: Bezeichner: Betriebsstättennummer Zahnärzte: Bezeichner: Abrechnungsnummer inkl. vorangestellter 2-stelliger KZV-Nr. KTR: Bezeichner: Institutionskennzeichen kann mehrfach vorkommen (0..100)
personalEntry	obligatorisch	Wird vom VZD eingetragen Wert == TRUE, wenn alle Zertifikate den entryType 1 haben (Berufsgruppe), Wert == FALSE sonst

dataFromAuthority	optional	Wird vom VZD eingetragen Wert == TRUE, wenn der Verzeichnisdienst_Eintrag von dem Kartenherausgeber geschrieben wurde, Wert == FALSE sonst
userCertificate	optional	Bezeichner: Zertifikat kann mehrfach vorkommen (0..50) Neue Einträge können nur mit Zertifikat angelegt werden. Das Zertifikat wird jedoch gelöscht, wenn es ungültig geworden ist. Wenn kein Zertifikat vorliegt, dann kann der Eintrag nicht mittels LDAP-Abfrage gefunden werden. Über die Schnittstelle I_Directory_Maintenance können Zertifikate hinzugefügt werden. Format: DER, Base64 kodiert
entryType	optional	Bezeichner: Eintragstyp Wird vom VZD anhand der in den Zertifikaten enthaltenen OIDs (Extension Admission, Attribut ProfessionOID) und der Spalte Eintragstyp in Tab_VZD_Mapping_Eintragstyp_und_ProfessionOID automatisch eingetragen. Siehe auch [gemSpecOID]# Tab_PKI_402 und Tab_PKI_403.
telematikID	obligatorisch	Bezeichner: TelematikID Wird vom VZD anhand der im jeweiligen Zertifikat enthaltenen Telematik-ID (Feld registrationNumber der Extension Admission) übernommen.
professionOID	optional	Bezeichner: Profession OID Wird vom VZD anhand der in den Zertifikaten enthaltenen OIDs (Extension Admission, Attribut ProfessionOID) und dem Mapping in ab_VZD_Mapping_Eintragstyp_und_ProfessionOID automatisch eingetragen. Siehe [gemSpecOID]# Tab_PKI_402 und Tab_PKI_403. kann mehrfach vorkommen (0..100)
usage	optional	Bezeichner: Nutzungskennzeichnung kann pro Zertifikat mehrfach (0..100) vergeben werden vorgegebener Wertebereich [KOM-LE, ePA, eFA]
description	optional	Bezeichner: Beschreibung Dieses Attribut ermöglicht das Zertifikat zu beschreiben, um die Administration des VZD Eintrags zu vereinfachen.
mail	optional	Bezeichner: E-Mail-Adresse kann mehrfach vorkommen (0..100)

<=

[RFC 6750] The OAuth 2.0 Authorization Framework: Bearer Token Usage

Änderungen in gemProdT_VZD_PTV

Anmerkung: Die Anforderungen der folgenden Tabelle stellen einen Auszug dar und verteilen sich innerhalb der Tabelle des Originaldokuments [gemProdT_VZD_PTV]. Alle Anforderungen der Tabelle des Originaldokuments, die in der folgenden Tabelle nicht ausgewiesen sind, bleiben unverändert bestehenden.

Tabelle Anforderungen zur funktionalen Eignung "Produkttest/Produktübergreifender Test"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
A_18371	VZD, Schnittstelle I_Directory_Administration	gemSpec_VZD
A_18373	VZD, Schnittstelle I_Directory_Administration, REST-Webservice	gemSpec_VZD
A_18408	VZD, I_Directory_Administration, Registrierung	gemSpec_VZD
A_18409	VZD, I_Directory_Administration, Sperrung OAuth Client Credentials	gemSpec_VZD
A_18372	VZD, I_Directory_Administration, TLS-gesicherte Verbindung	gemSpec_VZD
A_18374	VZD, I_Directory_Administration, Redirect	gemSpec_VZD
A_18375	VZD, I_Directory_Administration, OAuth2 Dienst	gemSpec_VZD
A_18376	VZD, I_Directory_Administration, Prüfung AccessToken	gemSpec_VZD
A_18448	VZD, I_Directory_Administration, TUC_VZD_0012 „createDirectoryEntry”	gemSpec_VZD
A_18449	VZD, I_Directory_Administration, TUC_VZD_0013 „getDirectoryEntries”	gemSpec_VZD
A_18450	VZD, I_Directory_Administration, TUC_VZD_0014 „updateBaseDirectoryEntry”	gemSpec_VZD
A_18451	VZD, I_Directory_Administration, TUC_VZD_0015 „deleteDirectoryEntry”	gemSpec_VZD
A_18452	VZD, I_Directory_Administration, TUC_VZD_0012 „addCertificate”	gemSpec_VZD
A_18453	VZD, I_Directory_Administration, TUC_VZD_0016 „getCertificates”	gemSpec_VZD
A_18454	VZD, I_Directory_Administration, TUC_VZD_0017 „updateCertificate”	gemSpec_VZD
A_18455	VZD, I_Directory_Administration, TUC_VZD_0018 „ deleteCertificate”	gemSpec_VZD

Änderungen in [gemKPT_Arch_TIP]

Geändert:

5.4.4 Produkttyp Verzeichnisdienst

TIP1-A_5774 - Produkttyp Verzeichnisdienst, Schnittstellen und Prozesse
Der Produkttyp Verzeichnisdienst MUSS alle Festlegungen gemäß Tabelle "Produkttyp Verzeichnisdienst" erfüllen.

Tabelle 26: Schnittstellen und Prozesse des Produkttyps Verzeichnisdienst

Verzeichnisdienst		
Beschreibung	Der Verzeichnisdienst beinhaltet alle serverseitigen Anteile des Basisdienstes Verzeichnis_Identitäten. Dazu zählen im Besonderen die Speicherung aller Einträge von Leistungserbringern und Organisationen/Institutionen mit allen definierten Attributen, die in das Verzeichnis aufgenommen werden sollen. Anhand einer Suchanfrage können ~~Konnektor und fachanwendungsspezifische Dienste~~ diese Daten ~~abfragen (z. B. X.509 Zertifikate)~~abgefragt werden. Ferner können Einträge des Verzeichnisses durch Kartenherausgeber (Basisdaten) oder berechtigte fachanwendungsspezifische Dienste (Fachanwendungsdaten) geändert, hinzugefügt und gelöscht werden.	
Bereitgestellte Schnittstellen	**Nutzer**	**Bedingungen**
I_Directory_Query	TIP, FA_spez_Dienst, aAdG, aAdG-NetG-TI, SÜV	
I_Directory_Maintenance	FA_spez_Dienst	Die Schnittstelle wird über TLS mit beidseitiger Authentifizierung bereitgestellt. Hinweis: Diese Schnittstelle wird zukünftig abgekündigt und durch I_Directory_Administration ersetzt werden. Aus Kompatibilitätsgründen bleibt sie vorerst erhalten, sollte aber nicht mehr verwendet werden.
I_Directory_Application_Maintenance	FA_spez_Dienst	Die Schnittstelle wird über TLS mit beidseitiger Authentifizierung bereitgestellt
I_Directory_Administration	Kartenherausgeber	
Benötigte Schnittstellen		
I_NTP_Time_Information, I_DNS_Name_Resolution, I_IP Transport, I_OCSP_Status_Information		
Fachliche Prozesse	**Nutzer**	**Bedingungen**
P_Directory_Maintenance	Inhaber des Eintrages	
P_Directory_Application_Registration	FA_spez_Dienst	

<=

3.10 Außensicht der TI-Plattform im Ganzen

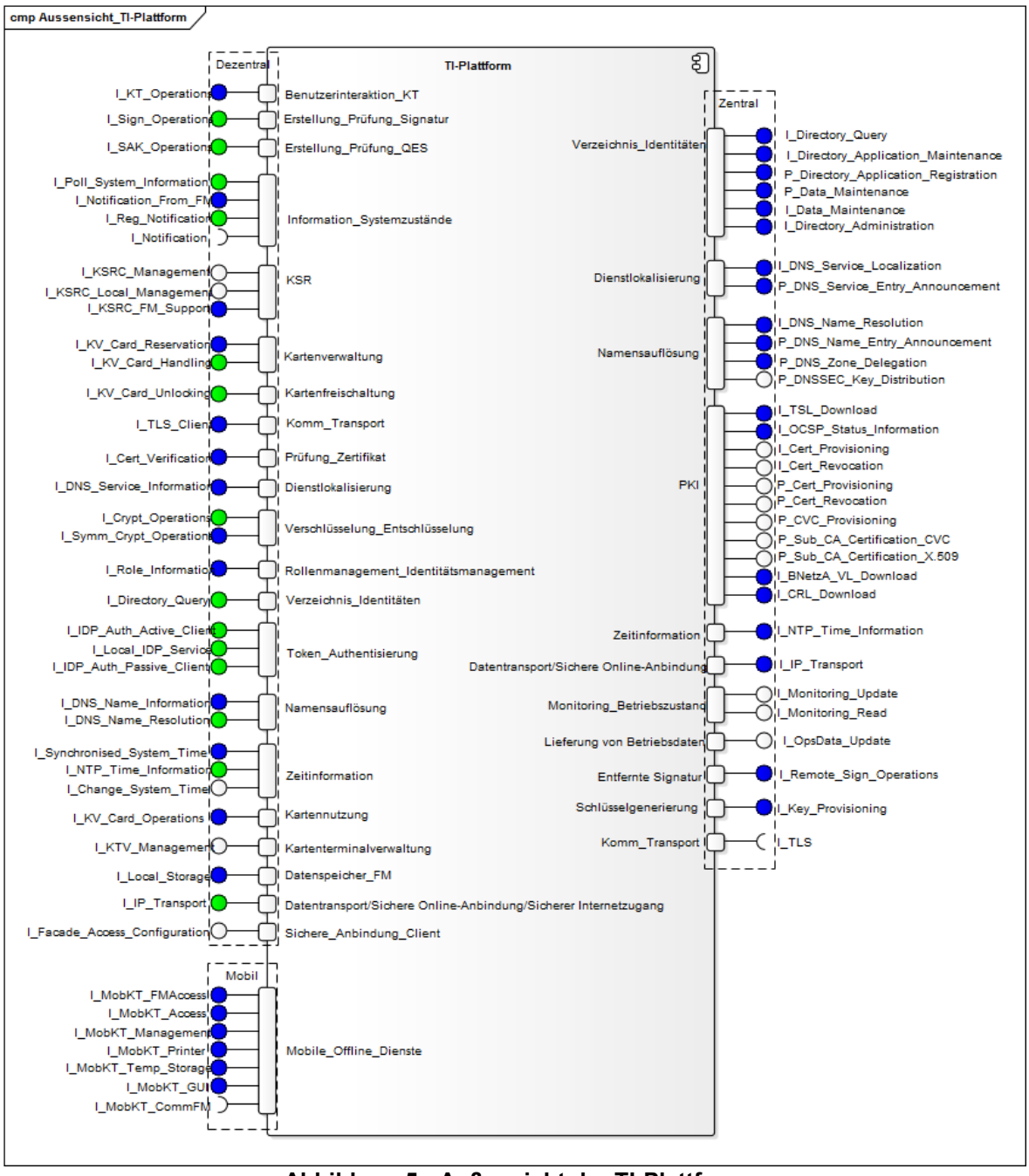

Abbildung 5 : Außensicht der TI-Plattform

Neu:

5.6.1.4.2 I_Directory_Administration (Provided)

A_18490 - Die Schnittstelle I_Directory_Administration
Die Schnittstelle I_Directory_Administration MUSS alle zugehörigen logischen Operationen implementieren. <=

A_18491 - Die Schnittstelle I_Directory_Administration::add_Directory_Entry

Die Schnittstelle I_Directory_Administration MUSS die logische Operation add_Directory_Entry implementieren.

Tabelle : Operation I_Directory_Administration::add_Directory_Entry

I_Directory_Administration					Berechtigung: Kartenherausgeber
add_Directory_Entry	Parameter				Vertr./Integr./Auth.
	In	Entry	DirectoryEntry	IM116	M/H/H
Mit dieser Operation wird ein neuerVerzeichniseintrag *Entry* inklusive Basisdaten (z.B. Attribute, ENC-Zertifikat, Telematik_ID) erzeugt.					
Verfügbarkeit: H, Nichtabstreitbarkeit: H					

<=

A_18492 - Die Schnittstelle I_Directory_Administration::read_Directory_Entry

Die Schnittstelle I_Directory_Administration MUSS die logische Operation read_Directory_Entry implementieren.

Tabelle : Operation I_Directory_Administration::read_Directory_Entry

I_Directory_Administration					Berechtigung: Kartenherausgeber
read_Directory_Entry	Parameter				Vertr./Integr./Auth.
	In	TelematikID	Telematik_ID	IM425	M/H/H
	Out	Entry	DirectoryEntry	IM116	M/H/H
Mit dieser Operation kann der vollständige Verzeichniseintrag *Entry* bestehend aus Basisdaten und FA-Daten mit der Telematik-ID *TelematikID* gelesen werden.					
Verfügbarkeit: M, Nichtabstreitbarkeit: N					

<=

A_18943 - Die Schnittstelle I_Directory_Administration::modify_Directory_Entry

Die Schnittstelle I_Directory_Administration MUSS die logische Operation modify_Directory_Entry implementieren.

Tabelle : Operation I_Directory_Administration::modify_Directory_Entry

I_Directory_Administration					Berechtigung: Kartenherausgeber
modify_Directory_Entry	Parameter				Vertr./Integr./Auth.
	In	Entry	DirectoryEntry	IM116	M/H/H
	Out	Entry	DirectoryEntry	IM116	M/H/H
Mit dieser Operation können die Attribute *Attributes* bzw. ENC-Zertifikat *EncCertificate* der Basisdaten des Verzeichniseintrags *Entry* modifiziert werden.					
Verfügbarkeit: H, Nichtabstreitbarkeit: H					

<=

A_18494 - Die Schnittstelle I_Directory_Administration::delete_Directory_Entry

Die Schnittstelle I_Directory_Administration MUSS die logische Operation delete_Directory_Entry implementieren.

Tabelle : Operation I_Directory_Administration::delete_Directory_Entry

I_Directory_Administration	Berechtigung:

					Kartenherausgeber
delete_Directory_Entry	Parameter				Vertr./Integr./Auth.
	In	TelematikID	Telematik_ID	IM425	M/H/H
Mit dieser Operation kann der vollständige Verzeichniseintrag *Entry* inklusive Basisdaten und FA-Daten gelöscht werden.					
Verfügbarkeit: H, Nichtabstreitbarkeit: H					

<=