Telematikinfrastruktur 2.0

Spezifikation

Versichertenstammdaten-management 2.0 (VSDM 2.0)

Version:	1.0.0_CC
Revision:	1045110
Stand:	15.11.2024
Status:	Freigegeben für interne QS
Klassifizierung:	
Referenzierung:	gemSpec_VSDM_2

Dokumentinformationen

Änderungen zur Vorversion

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

Dies ist die erste Version des Dokuments.

Dokumentenhistorie

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
1.0.0_CC	15.11.2024		Version zur Kommentierung	gematik

<<Genereller Hinweis:

Hidden Text wird blau dargestellt

In doppelten spitzen Klammen gefasste Mustertexte der Vorlage sind Hidden Text und sind für die Druckaufbereitung normalerweise ausgeblendet.

In einfachen spitzen Klammern gesetzte Begriffe sind Platzhalter und sinngemäß auszutauschen bzw. zu entfernen.>>

Inhaltsverzeichnis

1 Einordnung des Dokuments

1.1 Zielsetzung

Beim vorliegenden Dokument handelt es sich um die Festlegungen der zweiten Ausbaustufe von VSDM (VSDM 2.0). Diese ist definiert durch den Abruf der Versichertenstammdaten (VSD) durch das Primärsystem des Leistungserbringers direkt vom Fachdienst der Krankenkasse. Die VSD werden im Gegensatz zu VSDM 1.0 nicht mehr auf der eGK aktualisiert und von dort gelesen.

Die vorliegende Spezifikation definiert Anforderungen zu Herstellung, Test und Betrieb der Produkttypen und beschreibt, wie die fachlichen Abläufe umzusetzen sind.

Zu den Produkttypen gehören

1. Fachdienst VSDM
2. Primärsystem des Leistungserbringers.

1.2 Zielgruppe

Das Dokument richtet sich an

1. den Hersteller des Fachdienstes VSDM
2. den Hersteller und Anbieter von weiteren Produkttypen der Fachanwendung VSDM

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 GmbH in gesonderten Dokumenten (z. B. gemPTV_ATV_Festlegungen, Produkttypsteckbrief, Leistungsbeschreibung) festgelegt und bekannt gegeben.

Wichtiger 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 GmbH 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.

Die vollständige Anforderungslage für den Produkttyp ergibt sich aus weiteren Spezifikationsdokumenten, diese sind in dem Produkttypsteckbrief des Produkttyps Fachdienst VSDM (VSDM 2.0) verzeichnet.

Nicht Bestandteil des vorliegenden Dokumentes sind die informativen und normativen Ergänzungen zur Nutzung der Schnittstellen des Fachdienstes VSDM in der separaten API-Dokumentation, sowie zur Profilierung der verwendeten FHIR Ressourcen.

1.5 Methodik

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

Da in dem Beispielsatz „Eine leere Liste DARF NICHT ein Element besitzen.“ die Phrase „DARF NICHT“ semantisch irreführend wäre (wenn nicht ein, dann vielleicht zwei?), wird in diesem Dokument stattdessen „Eine leere Liste DARF KEIN Element besitzen.“ verwendet. Die Schlüsselworte werden außerdem um Pronomen in Großbuchstaben ergänzt, wenn dies den Sprachfluss verbessert oder die Semantik verdeutlicht.

Anwendungsfälle und Anforderungen werden im Dokument wie folgt dargestellt:
<AF-ID> - <Titel des Anwendungsfalles>
Text / Beschreibung
[<=]

bzw.

<AFO-ID> - <Titel der Anforderung>
Text / Beschreibung
[<=]

Dabei umfasst der Anwendungsfall bzw. die Anforderung sämtliche zwischen ID und Textmarke [<=] angeführten Inhalte.

1.5.1 Hinweis auf offene Punkte

Themen, die noch intern geklärt werden müssen oder eine Entscheidung, sind wie folgt im Dokument gekennzeichnet:

Beispiel für einen offenen Punkt.

2 Systemkontext

Die Fachdienste VSDM (Synonyme: Versichertenstammdatendienste, VSDD) stellen eine Schnittstelle für den Abruf der VSD und des Prüfungsnachweises für die Primärsysteme einer Leistungserbringerinstitution (LEI) bereit. Ein Abruf erfolgt jedoch nur bei einem vorliegenden Versorgungskontext, der durch den Proof-of-Patient-Presence Dienst (PoPP-Service) in Form eines PoPP-Token nachgewiesen werden muss.

Der VSDD ist für Primärsysteme direkt über das Internet erreichbar und ist aufgrund dessen durch Mechanismen und Komponenten gemäß den Zero-Trust Prinzipien abgesichert.

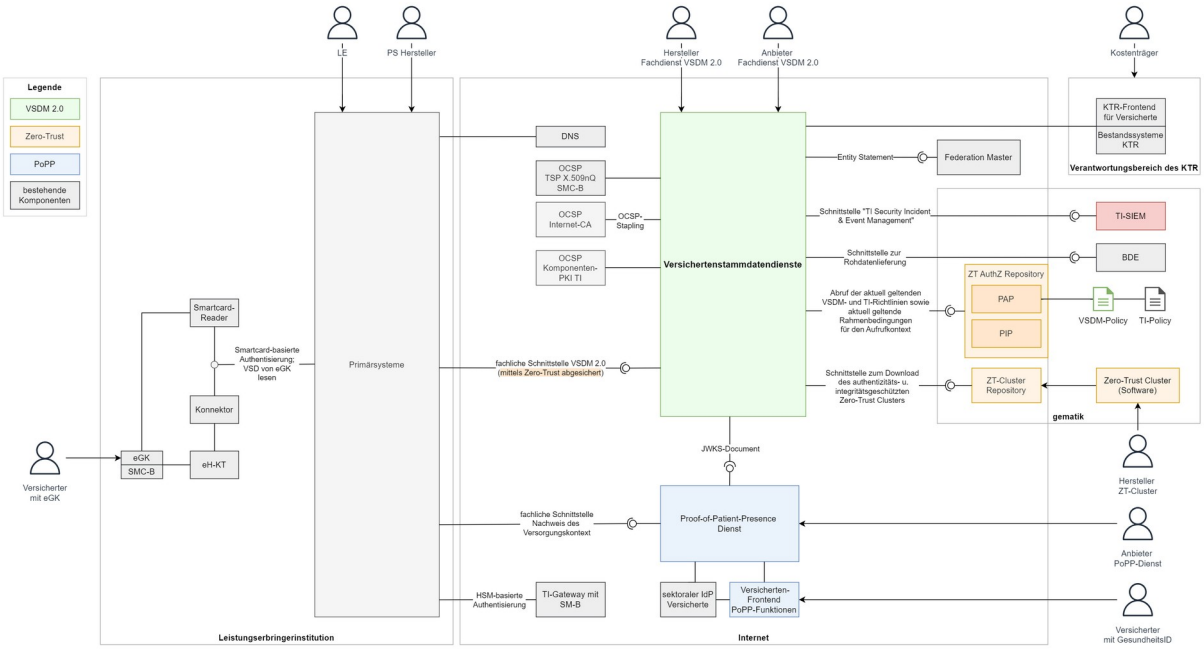

Abbildung 1 : Kontextdiagramm VSDM

2.1 Akteure und Rollen

Im Kontext der Anwendung VSDM werden verschiedene Akteure und Rollen definiert:

2.1.1 Hersteller Zero-Trust Cluster

Der Hersteller des Zero-Trust Cluster implementiert und entwickelt die Komponenten des Cluster gemäß den Vorgaben der gematik [gemSpec_Zero_Trust].

2.1.2 Hersteller Fachdienst VSDM

Der Hersteller eines Fachdienstes VSDM implementiert und entwickelt den Fachdienst gemäß den Vorgaben der gematik.
Der Hersteller muss eine Produktzulassung für den Fachdienst erreichen. Dazu muss er

den Fachdienst nach den Vorgaben der gematik testen und der gematik für Zulassungstests zur Verfügung stellen.

2.1.3 Anbieter Fachdienst VSDM

Der Anbieter eines Fachdienstes VSDM betreibt den zugelassenen Fachdienst im Internet gemäß den Vorgaben der gematik. Dabei muss er den von der gematik beigestellten Zero-Trust Cluster verwenden.
Neben dem Betrieb einer Instanz für den Produktivbetrieb müssen weitere Instanzen für die Test-, Entwicklungs- und Referenzumgebungen betrieben werden.

2.1.4 Kostenträger

Kostenträger bzw. Krankenversicherer stellen über einen Fachdienst VSDM die Versichertenstammdaten ihrer Versicherten zur Verfügung.

Kostenträger bzw. Krankenversicherer ermöglichen ihren Versicherten den Zugriff auf die versichertenindividuellen Zugriffsprotokolle eines Fachdienst VSDM.

2.1.5 gematik

Die gematik spezifiziert den Fachdienst VSDM und legt die Zulassungsbedingungen sowie -verfahren fest. Die gematik lässt den jeweiligen Fachdienst VSDM und den Anbieter eines Fachdienstes, inklusive den anbieterrelevanten Vorgaben zum Betrieb des Zero-Trust Cluster, zu.

Die gematik stellt dem Anbieter eines Fachdienstes VSDM das qualitätsgesicherte Zero-Trust Cluster zur Integration und den Betrieb zur Verfügung.

Die gematik stellt dem Anbieter eines Fachdienstes VSDM Möglichkeiten zur Konfiguration des Zero-Trust Clusters mittels Konfigurationsdateien (Manifest-Dateien) in Form von Templates zur Verfügung und stellt dem Anbieter diese Konfigurationsdateien qualitätsgesichert zur Verfügung.

Die gematik stellt dem Anbieter eines Fachdienstes VSDM Richtlinien in Form von TI-weit sowie anwendungsspezifisch geltende Policies qualitätsgesichert zur Verfügung.

Die gematik führt ihre Governance-Rolle für die Fachdienste VSDM und deren Anbieter aus.

2.1.6 Primärsystemhersteller

Primärsystem-Hersteller nutzen den vom Anbieter eines Fachdienstes VSDM bereitgestellten Fachdienst in der Referenzumgebung, um ihre jeweiligen Primärsysteme mit den VSDM und Trust-Client Funktionen zu entwickeln und zu testen.

2.1.7 Leistungserbringer, LE-Institution oder Medizinische Fachangestellte

Die Leistungserbringerinstitutionen bzw. deren Leistungserbringer oder medizinische Fachangestellte benutzen mittels eines Primärsystems mit VSDM und Trust-Client Funktionen den Fachdienst VSDM, um aktuelle Versichertenstammdaten sowie einen Prüfungsnachweis für Abrechnungszwecke zu erhalten.

Die Leistungserbringerinstitutionen bzw. deren Leistungserbringer oder medizinische Fachangestellte lesen mittels eines Primärsystems und der Nutzung eines Konnektors sowie eH-KT oder eines handelsüblichen Smartcard-Readers die Versichertenstammdaten von der elektronischen Gesundheitskarte (eGK).

2.1.8 Anbieter PoPP-Service

Der Anbieter des PoPP-Service stellt Leistungserbringerinstitutionen einen über das Internet erreichbaren Dienst zur Verfügung, um einen Nachweis für einen zustande gekommenen Versorgungskontext zwischen einer dedizierten Leistungserbringerinstitution und einem dedizierten Versicherten bzw. Patienten in Form eines PoPP-Tokens zu erhalten. Dieser Nachweis ist Voraussetzung zur Durchführung eines Online-Abrufes der Versichertenstammdaten und des Prüfungsnachweises.

2.1.9 Versicherter

Versicherte bestätigen durch das Stecken der eGK oder unter Nutzung der GesundheitsID das Zustandekommen eines Versorgungskontextes mit einer dedizierten Leistungserbringerinstitution.

Versicherte stellen durch das Stecken ihrer eGK der Leistungserbringerinstitution die Versichertenstammdaten bereit (Offline-Fall).

2.2 Nachbarsysteme

2.2.1 Systeme in der Leistungserbringerinstitution

Die Schnittstellen der Fachdienste VSDM werden durch die Primärsysteme (Praxisverwaltungs-, Krankenhausinformations- und Apothekenverwaltungssysteme) der Leistungserbringer im Versorgungsprozess genutzt.

Ein Primärsystem kann die Versichertenstammdaten und den Prüfungsnachweis zu einem Versicherten von einem Fachdienst VSDM nur dann abrufen, wenn dieses ein Testat über einen aktuell bestehenden Versorgungskontext zwischen einer Leistungserbringerinstitution und einem Versicherten übermittelt. Der aktuelle Versorgungskontext wird für die Leistungserbringerinstitution auf Basis der SMC-B und für den Versicherten auf Basis der eGK oder der GesundheitsID-Versicherte gegenüber dem PoPP-Service nachgewiesen. Der PoPP-Service attestiert diesen Versorgungskontext zwischen einer dedizierten LEI und einem dedizierten Versicherten zu einem dedizierten Zeitpunkt in Form eines PoPP-Tokens (Testat).
Eine Authentisierung der Leistungserbringerinstitution mittels Konnektor, eH-KT und SMC-B oder mittels TI-Gateway und SM-B gegenüber den Fachdiensten VSDM ist einmal am Tag erforderlich.

Können die Versichertenstammdaten nicht online von dem jeweiligen Fachdienst VSDM abgerufen werden, liest das Primärsystem die (zukünftig reduzierten) Versichertenstammdaten unter Nutzung von Konnektor oder TI-Gateway und eH-KT von der eGK. Zukünftig wird die Nutzung handelsüblicher Smartcard-Reader für die eGK ohne Notwendigkeit eines Konnektors oder TI-Gateways angestrebt.

2.2.2 TI-Gateway

Für Leistungserbringerinstitutionen, die anstatt des Konnektors ein TI-Gateway nutzen, erfolgt die LEI-Authentisierung gegenüber dem PoPP-Service und einem Fachdienst VSDM auf Basis der vom Betreiber des TI-Gateway (zukünftig) gehosteten SM-B.

2.2.3 PoPP-Service

Der PoPP-Service attestiert einen aktuellen Versorgungskontext zwischen einer auf Basis der SMC-B oder SM-B am PoPP-Service authentifizierten Leistungserbringerinstitution und einem Versicherten durch die Bereitstellung eines technischen Nachweises in Form eines sogenannten PoPP-Tokens, der unter anderem die Telematik-ID, das Institutionskennzeichen, die Krankenversichertennummer sowie einen Zeitstempel enthält. Die Authentizität des Versicherten kann dem PoPP-Service mittels eGK und unter Nutzung von Konnektor oder TI-Gateway oder zukünftig unter Nutzung eines handelsüblichen Smartcard-Readers nachgewiesen werden. Zudem besteht für den Versicherten die Möglichkeit, sich durch Nutzung eines Frontend für Versicherte mit enthaltenen PoPP-Funktionalitäten mittels seiner GesundheitsID respektive des jeweiligen sektoralen IDP gegenüber dem PoPP-Service zu authentisieren.

Zur Prüfung der Authentizität des PoPP-Tokens stellt der PoPP-Service einem Fachdienst VSDM einen Endpunkt zum Abruf des JSON Web Key Set Dokumentes (JWKS-Document) mit dem dort enthaltenen und aktuell gültigen öffentlichen Schlüssel zur Prüfung der PoPP-Token Signatur zur Verfügung.

2.2.4 Federation Master

Der Federation Master stellt dem Fachdienst VSDM die Adresse des `./well-known` Endpunktes des PoPP-Service zur Verfügung. Über diesen `./well-known` Endpunkt erhält der Fachdienst VSDM alle aktuellen Endpunkte des PoPP-Service und insbesondere des Endpunktes für das JWKS-Document.

2.2.5 DNS

Das Domain Name System ermöglicht einem Primärsystem die Dienstlokalisierung anhand der Institutionskennung des Kostenträgers sowie der Auflösung des Fachdienst VSDM spezifischen Hostname in die entsprechende IP-Adresse und stellt somit die grundsätzliche Kommunikation zwischen Primärsystem und Fachdienst VSDM über das Internet sicher.

2.2.6 OCSP TSP X.509nQ SMC-B

Dieser im Internet verfügbare OCSP-Responder ermöglicht die Abfrage des Sperrstatus zum jeweiligen C.HCI.AUT-Zertifikat der Leistungserbringerinstitution im Rahmen der LEI-Authentifizierung am Fachdienst VSDM. Hiermit wird sichergestellt, dass ausschließlich Leistungserbringerinstitutionen mit einer gültigen Leistungserbringeridentität Versichertenstammdaten von einem Fachdienst VSDM abrufen können.

2.2.7 OCSP Internet-CA

Dieser OCSP-Responder eines TSP gemäß [CAB-Forum] ermöglicht den Primärsystemen die Überprüfung des Sperrstatus des jeweiligen Server-Zertifikates im Rahmen der

Etablierung eines TLS-Kanals zum Fachdienst VSDM. Die OCSP-Response wird dem Primärsystem im Rahmen des Verbindungsaufbaus übermittelt (OCSP Stapling). Hiermit wird sichergestellt, dass ausschließlich VSDM Fachdienste mit einer gültigen Identität von den Primärsystemen genutzt werden können.

2.2.8 OCSP Komponenten-CA TI

Dieser im Internet verfügbare OCSP-Responder einer Komponenten-CA der TI ermöglicht den Primärsystemen die Überprüfung des Sperrstatus des jeweiligen Server-Zertifikates im Rahmen der Etablierung eines VAU-Kanals zum Fachdienst VSDM. Die OCSP-Response wird dem Primärsystem im Rahmen des Verbindungsaufbaus übermittelt (OCSP Stapling). Hiermit wird sichergestellt, dass ausschließlich VSDM Fachdienste mit einer gültigen VAU-Identität von den Primärsystemen genutzt werden können.

2.2.9 ZT-Authorization Repository

Das Zero-Trust Authorization Repository stellt dem Fachdienst VSDM die für einen Autorisierungsvorgang aktuell gültigen und anzuwendenden Sicherheitsrichtlinien im Kontext der Anwendung VSDM (VSDM-Policy) sowie der TI (TI-Policy) über den Policy Administration Point (PAP) zur Verfügung. Darüber hinaus werden über den Policy Information Point (PIP) zusätzliche und von der Sicherheitsrichtlinie geforderte Informationen wie bspw. erlaubte (Positivliste) oder verbotene (Negativliste) Endsystemkonfigurationen zur Verfügung gestellt, die ein Fachdienst VSDM im Rahmen der Evaluierung der Autorisierungsanfrage durch das Primärsystem gegen die Sicherheitsrichtlinie einbezieht.

2.2.10 ZT-Cluster Repository

Das Zero-Trust Cluster Repository stellt dem Anbieter/Betreiber eines Fachdienstes VSDM die für den Zugriffsschutz gemäß der TI 2.0 Zero-Trust Architektur zu verwendenden bzw. betreibenden Software-Komponenten in Form eines Kubernetes-Cluster bereit. Die aus dem Cluster zwingend zu verwendenden Komponenten und deren Konfigurationen werden durch die jeweiligen Fachdienstspezifikationen der gematik vorgegeben. Festlegungen für einen Fachdienst VSDM erfolgen im Kapitel 4.2- Zero-Trust Cluster.

Das Softwareprodukt "Zero-Trust Cluster" wird durch einen von der gematik beauftragten Hersteller entwickelt und von der gematik freigegeben sowie authentizitäts- und integritätsgeschützt bereitgestellt.

2.2.11 Betriebsdatenerfassung (BDE)

Ziel der Betriebsdatenerfassung ist es, die betriebliche Steuerung und das differenzierte Aufrufverhalten für einen Fachdienst auf Basis der übermittelten Betriebsdaten qualitativ einzuordnen. Hierbei stehen das zeitnahe Monitoring und die monatliche Service Level Bewertung durch die gematik im Vordergrund.

2.2.12 Security Information and Event Management (SIEM)

Wie jeder Fachdienst der TI (ePA, E-Rezept, KIM etc.) müssen im Fachdienst VSDM sicherheitskritische Ergebnisse erkannt werden. Erkannte Alarme, Betriebsdaten und Reports werden an das TI-SIEM übermittelt und dienen dazu, dass die gematik anbieterübergreifend Anomalien und Angriffsversuche umgehend erkennen, Schwell- und

Messwerte kontinuierlich verbessern, potenzielle Sicherheitsvorfälle auch auf Seiten der gematik analysieren und sicherheitsrelevante Trends (z. B. Anzahl abgelehnter Zugriffe über einen bestimmten Zeitraum) erkennen und bewerten kann.

2.2.13 Systeme der Kostenträger

Die Systeme der Kostenträger können der Bereitstellung der originären Versichertenstammdaten für den Fachdienst VSDM in einem nicht näher festgelegtem Datenformat und über eine nicht näher festgelegte Schnittstelle dienen. Zudem können über diese Systeme den Versicherten die Zugriffsprotokolle des jeweiligen Fachdienstes VSDM verfügbar gemacht werden.

2.3 User Stories

Die folgenden User Stories sollen die Bedarfe von Leistungserbringern beispielhaft verdeutlichen.

Die in diesem Kapitel aufgeführten User Stories schildern die Absichten des Nutzers in Verbindung mit dem Primärsy und dienen als Lesehilfe zu den fachlichen Anwendungsfällen. Die User Stories erheben keinen Anspruch auf Vollständigkeit.

2.3.1 VSD vom Fachdienst abrufen

- Als Leistungserbringer muss ich vor der eigentlichen Behandlung des anwesenden Patienten dessen Versicherungsverhältnis prüfen, um meine erbrachten Leistungen gegenüber der zuständigen Krankenkasse abrechnen zu können. Dafür muss ich die Versichertenstammdaten des Versicherten von seiner Krankenkasse abrufen und zusätzlich den Prüfungsnachweis über die getätigte Abfrage in meinem Primärsystem speichern. Um diesen Prozess zu starten, muss vorher der Versorgungskontext mittels eGK oder GesundheitsID des Versicherten nachgewiesen werden.
- Als Leistungserbringer muss ich zur Abrechnung meiner Leistungen den Prüfungsnachweis über die abgefragten VSD im Primärsystem speichern.
- Als Leistungserbringer möchte ich die VSD bei jedem Besuch des Patienten innerhalb eines Quartals abrufen, um immer die jeweils aktuellen VSD im Primärsystem speichern zu können.

2.3.2 VSD von eGK lesen

- Als Leistungserbringer muss ich in der Lage sein, meine Leistungen am Patienten auch dann abrechnen zu können, wenn die Herstellung des Versorgungskontextes fehlschlägt und die VSD des Versicherten nicht von der zuständigen Krankenkasse abgerufen werden können. In diesem Fall nutze ich die auf der eGK gespeicherten Daten, um ein zur Abrechnung geeignetes Ersatzverfahren anwenden zu können.

2.3.3 Zugriffsprotokoll einsehen

- Als Versicherter möchte ich mich informieren, wer wann auf die mich betreffenden Versichertenstammdaten zugegriffen hat und somit meine Datenschutzrechte wahrnehmen können. Protokolleinträge werden im Fachdienst ein Jahr aufbewahrt und anschließend sicher gelöscht.

3 Systemüberblick

Ein Fachdienst VSDM stellt die Versichertenstammdaten (VSD) der Versicherten einer Krankenkasse des jeweiligen Fachdienstes als ein zentraler Resource Server auf Basis des FHIR-Standards über eine im Internet erreichbare REST-API zum Abruf durch das Primärsystem des Leistungserbringers bereit. Zusätzlich protokolliert der Fachdienst alle Zugriffe auf die VSD durch den Leistungserbringer für den Versicherten.

In der folgenden Abbildung sind alle beteiligten Komponenten (das Primärsystem verallgemeinernd als Clientsystem) der VSDM-Architektur dargestellt:

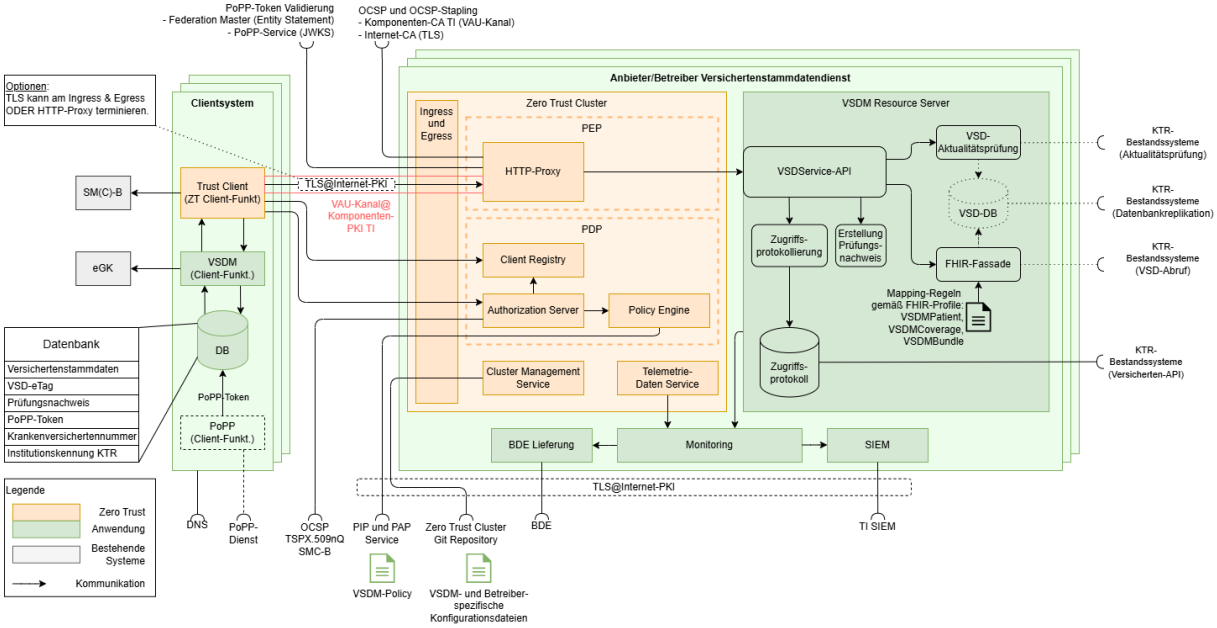

Abbildung 2 : Systemdiagramm VSDM

4 Zerlegung des Produkttyps

4.1 Clientsystem

Die folgenden Anforderungen an ein Clientsystem haben rein informativen Charakter und beschränken sich auf die zwingend zu schaffende Voraussetzungen zur Nutzung eines Fachdienstes VSDM. Darüber hinaus dienen diese für ein besseres Verständnis über die Funktionsweise der Anwendung VSDM. Weiterführende und detaillierte Informationen sind im Implementierungsleitfaden [gemILF_PS] dokumentiert.

4.1.1 Datenbank

Die logische Komponente "Datenbank" dient lediglich als Strukturierungselement für diese Spezifikation und soll verdeutlichen, dass im Rahmen von VSDM bestimmte Informationen für einen dedizierten Zeitraum persistiert werden müssen. Diese Persistierung könnte bspw. als Teil des jeweiligen Patientenstammes realisiert werden.

A_26700 - Clientsystem VSDM - Persistierung Versorgungskontextnachweis
Ein Clientsystems VSDM MUSS nach Erhalt eines Nachweises zu einem Versorgungskontext in Form eines PoPP-Tokens folgende Informationen gemäß [gemSpec_PoPP_Service] aus dem PoPP-Token extrahieren und persistieren:

1. PoPP-Token (exakt so, wie vom PoPP-Service erhalten)
2. `<patient.identifier.value>` (Krankenversichertennummer; KVNR)
3. `<patient.insurer.identifier.value>` (Institutionskennung des Krankenversicherers; IK),

damit ein Versichertenstammdatenabruf bei einem Folgebesuch eines Patienten innerhalb des selben Quartals ohne erneutes Stecken der eGK oder Nutzung der GesundheitsID-Versicherte vollautomatisch durchgeführt oder bei einer Nicht-Verfügbarkeit eines VSDM Fachdienstes auch später (innerhalb desselben Quartals) ein Prüfungsnachweis erhalten werden kann.**[**<=, CS_VSDM_2, funkt. Eignung: Konformitätsbestätigung**]**

A_26701 - Clientsystem VSDM - Persistierung VSD
Ein Clientsystems VSDM MUSS nach Erhalt der Versichertenstammdaten folgende Informationen persistieren:

1. VSD (Versichertenstammdaten)
2. VSD-Änderungsindikator (Wert des HTTP ETag Headers),

damit u. a. nur bei veralteten Versichertenstammdaten neue Versichertenstammdaten übertragen werden müssen. Insbesondere der ETag-Wert DARF NICHT verändert werden. **[**<=, CS_VSDM_2, funkt. Eignung: Konformitätsbestätigung**]**

A_26702 - Clientsystem VSDM - Prüfungsnachweis Persistierung
Ein Clientsystems VSDM MUSS nach Erhalt eines Prüfungsnachweises diesen persistieren, damit ein Leistungserbringer diesen zu Abrechnungszwecken verwenden kann.**[**<=, CS_VSDM_2, funkt. Eignung: Konformitätsbestätigung**]**

4.1.2 VSDM-Client Funktionen

Die logische Komponente "VSDM-Client" dient lediglich als Strukturierungselement für diese Spezifikation und soll die VSDM-spezifischen Funktionen eines Clientsystems verdeutlichen.

4.1.2.1 Online-Abruf Versichertenstammdaten und Prüfungsnachweis

A_26703 - Clientsystem VSDM - Aktualisierung Versorgungskontextnachweis
Ein Clientsystem VSDM MUSS beim erstmaligen Besuch eines Patienten innerhalb eines Quartals den Nachweis zu einem Versorgungskontext in Form eines PoPP-Tokens gemäß [gemSpec_PoPP_Service] durchführen bzw. abrufen, und die Informationen gemäß A_26700 aktualisieren, damit ein Versichertenstammdatenabruf durchgeführt werden kann.**[**<=, CS_VSDM_2, funkt. Eignung: Konformitätsbestätigung**]**

A_26704 - Clientsystem VSDM - Fachdienstlokalisierung
Ein Clientsystem VSDM MUSS für die Lokalisierung desjenigen Fachdienst VSDM, der die VSD des Patienten verwaltet, ein Fachdienstlokalisierung gemäß A_26800 auf Basis der Institutionskennung (IK) der Krankenkasse, bei dem der Patient versichert ist, durchführen.**[**<=, CS_VSDM_2, funkt. Eignung: Konformitätsbestätigung**]**

A_26967 - Clientsystem VSDM - ausschließlich TLS
Ein Clientsystem VSDM MUSS sicherstellen, dass es mit dem Fachdienst VSDM ausschließlich über TLS kommuniziert. **[**<=, CS_VSDM_2, funkt. Eignung: Konformitätsbestätigung**]**

Hinweis: Es gelten die Vorgaben aus [gemSpec_Krypt] für TLS.

A_26706 - Clientsystem VSDM - unzulässige TLS-Verbindungen
Ein Clientsystem VSDM MUSS bei jedem Verbindungsaufbau den Fachdienst VSDM anhand seines TLS-Zertifikats authentifizieren, und MUSS die Verbindungen ablehnen, falls die Authentifizierung fehlschlägt. **[**<=, CS_VSDM_2, funkt. Eignung: Konformitätsbestätigung**]**

A_26707 - Clientsystem VSDM - Prüfung der TLS-Zertifikate
Das Clientsystem VSDM MUSS für die Prüfung eines Zertifikats für den TLS-Verbindungsaufbau zum Fachdienst VSDM Zertifikate auf ein CA-Zertifikat einer CA, die [CAB-Forum] erfüllt, kryptographisch (Signaturprüfung) zurückführen können. Ansonsten MUSS es das Zertifikat als "ungültig" bewerten. Das Clientsystem MUSS die zeitliche Gültigkeit des Zertifikats prüfen. Falls diese Prüfung negativ ausfällt, MUSS es das Zertifikat als "ungültig" bewerten.**[**<=, CS_VSDM_2, funkt. Eignung: Konformitätsbestätigung**]**

Hinweis: Der erste Teil ist gleichbedeutend damit, dass das CA-Zertifikat im Zertifikats-Truststore eines aktuellen Webbrowsers ist.

A_26708 - Clientsystem VSDM - Endpunktlokalisierung Fachdienst VSDM
Ein Clientsystem VSDM MUSS für die Lokalisierung der dedizierten Endpunkte des jeweiligen Fachdienstes VSDM die Vorgaben von [gemSpec_Zero_Trust] umsetzen. **[**<=, CS_VSDM_2, funkt. Eignung: Konformitätsbestätigung**]**

A_26709 - Clientsystem VSDM - Fachdienst-Endpunkte
Ein Clientsystem VSDM MUSS für Anfragen an den Fachdienst VSDM den Vorgaben dieser Spezifikation und [gemSpec_Zero_Trust] nachkommen und MUSS sicherstellen, dass es nur erlaubte Anfragen und Endpunkte verwenden.**[**<=, CS_VSDM_2, funkt. Eignung: Konformitätsbestätigung**]**

A_26710 - Clientsystem VSDM - VSDService-API
Ein Clientsystem VSDM MUSS für Anfragen an die Fachdienst VSDM API `/vsdservice` den Vorgaben dieser Spezifikation und [OpenAPI_VSDM_2] nachkommen und MUSS

sicherstellen, dass es nur erlaubte Anfragen und Endpunkte verwenden.
[<=, CS_VSDM_2, funkt. Eignung: Konformitätsbestätigung**]**

A_26711 - Clientsystem VSDM - Übertragung des Versorgungskontextnachweises
Ein Clientsystem VSDM MUSS für jede Anfrage an die Fachdienst VSDM API `/vsdservice` einen gültigen Versorgungskontextnachweis in Form eines PoPP-Tokens im Header `PoPP` als Bearer-Token übertragen. **[**<=, CS_VSDM_2, funkt. Eignung: Konformitätsbestätigung**]**

A_26712 - Clientsystem VSDM - Übertragung des VSD-Änderungsindikator
Ein Clientsystem VSDM MUSS für jede Anfrage an die Fachdienst VSDM API `/vsdservice` den vom Fachdienst VSDM übermittelten VSD-Änderungsindikator als starken `etag_value` des HTTP-Headers `If-None-Match` gemäß [RFC7232] übertragen. Liegt dem Clientsystem (noch) kein VSD-Änderungsindikator vor, MUSS der `etag_value` auf `0` gesetzt werden und als hexadezimal kodierten 256-Bit Binärwert übertragen. **[**<=, CS_VSDM_2, funkt. Eignung: Konformitätsbestätigung**]**

A_26713 - Clientsystem VSDM - Aktualisierung VSD bei erstmaligem Patientenkontakt im Quartal
Ein Clientsystem VSDM MUSS beim erstmaligen Besuch eines Patienten innerhalb eines Quartals einen Versichertenstammdatenabruf durchführen und die Informationen gemäß A_26700 aktualisieren. **[**<=, CS_VSDM_2, funkt. Eignung: Konformitätsbestätigung**]**

A_26957 - Clientsystem VSDM - Aktualisierung VSD bei wiederholtem Patientenkontakt im Quartal
Ein Clientsystem VSDM SOLL bei Folgebesuchen eines Patienten innerhalb eines Quartals einen Versichertenstammdatenabruf durchführen und die Informationen gemäß A_26700 aktualisieren.**[**<=, CS_VSDM_2, funkt. Eignung: Konformitätsbestätigung**]**

A_26958 - Clientsystem VSDM - vollautomatische Aktualisierung VSD bei wiederholtem Patientenkontakt im Quartal
Der VSD-Abruf für Folgebesuche eines Patienten im selben Quartal MUSS von einem Clientsystem vollautomatisch durchgeführt werden.**[**<=, CS_VSDM_2, funkt. Eignung: Konformitätsbestätigung**]**

Hinweis: Ein für das Quartal gültiger Nachweis über einen Versorgungskontext zwischen einer LEI und einem Patienten in Form eines PoPP-Tokens muss beim ersten Besuche des Patienten innerhalb des aktuellen Quartals vom PoPP-Service bezogen werden. Für alle weiteren Besuche dieses Patienten in dieser LEI innerhalb des gleichen Quartals wird der vom Clientsystem gespeicherte PoPP-Token verwendet - somit muss für Folgebesuche keine eGK oder GesundheitsID verwendet werden und das Clientsystem kann die VSD vollautomatisch (bspw. auf Basis des Öffnens des Patientenstammes durch einen Mitarbeiter der Leistungserbringerinstitution) durchgeführt werden.

A_26714 - Clientsystem VSDM - Angabe FHIR-MimeType
Ein Clientsystem VSDM SOLL das bevorzugte Dateiformat für die FHIR Ressourcen mittels HTTP-Header `accept` in der Form `application/fhir+json` oder `application/fhir+xml` angeben.**[**<=, CS_VSDM_2, funkt. Eignung: Konformitätsbestätigung**]**

A_26715 - Clientsystem VSDM - FHIR-Resource VSDMBundle
Ein Clientsystem VSDM MUSS die FHIR Ressourcen `VSDMPatient` und `VSDMCoverage` aus der FHIR-Resource `VSDMBundle` zur Weiterverarbeitung gemäß [FHIR-Resource Bundle] extrahieren sowie `VSDMPatient` gemäß [FHIR-Resource Patient] und `VSDMCoverage` gemäß [FHIR-Resource Coverage] weiterverarbeiten.**[**<=, CS_VSDM_2, funkt. Eignung: Konformitätsbestätigung**]**

A_26716 - Clientsystem VSDM - FHIR-Resource VSDMOperationOutcome
Ein Clientsystem VSDM MUSS Fehlermeldungen in Form der FHIR-Resource VSDMOperationOutcome gemäß [FHIR-Resource OperationOutcome] weiterverarbeiten und dem Nutzer anzeigen.**[**<=, CS_VSDM_2, funkt. Eignung: Konformitätsbestätigung**]**

A_26717 - Clientsystem VSDM - Prüfungsnachweis
Ein Clientsystem VSDM MUSS den Prüfungsnachweis aus dem HTTP-Header `VSDM-Pn` extrahieren, BASE64URL dekodieren sowie mittels gzip dekomprimieren und gemäß [gemILF_PS] verarbeiten. **[**<=, CS_VSDM_2, funkt. Eignung: Konformitätsbestätigung**]**

A_26718 - Clientsystem VSDM - Prüfungsnachweis Speicherung
Ein Clientsystem KANN den Prüfungsnachweis gemäß HTTP-Header `VSDM-Pn-Disposition` als Datei `filename="pruefungsnachweis.xml"` (zwischen)speichern. **[**<=, CS_VSDM_2, funkt. Eignung: Konformitätsbestätigung**]**

A_26953 - Clientsystem VSDM - Prüfungsnachweis Übertragung
Ein Clientsystem VSDM MUSS den Prüfungsnachweis als Bearer-Token des HTTP-Headers `PoPP` übertragen.**[**<=, CS_VSDM_2, funkt. Eignung: Konformitätsbestätigung**]**

A_26719 - Clientsystem VSDM - Anzeige geänderter VSD
Ein Clientsystem VSDM SOLL Änderungen der VSD benutzerfreundlich im Clientsystem anzeigen. **[**<=, CS_VSDM_2, funkt. Eignung: Konformitätsbestätigung**]**

A_26720 - Clientsystem VSDM - Fehlerbehandlung
Ein Clientsystem VSDM MUSS die in A_27014 beschriebene Fehlerbehandlung umsetzen. **[**<=, CS_VSDM_2, funkt. Eignung: Konformitätsbestätigung**]**

Beispiel für den HTTP-Request des Clientsystems

```
GET /vsdservice/v1/vsdmbundle HTTP/1.1
HOST: 101575519.vsdm2.ti-dienste.de
Authorization: DPoP <access_token>
DPoP: <dpop_proof_jwt>

{
      GET /vsdservice/v1/vsdmbundle HTTP/1.1
      HOST: 101575519.vsdm2.ti-dienste.de
      If-None-Match:
      "e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855"
      Accept: {application/fhir+json, application/fhir+xml}
      PoPP: Bearer <popp_token>

      {


      }
}
```

Beispiel für die HTTP-Response für den Status HTTP 304 Not Modified:

```
HTTP/1.1 304 Not Modified
...
{
      HTTP/1.1 304 Not Modified
      ETag:
      "e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855"
```

```
      VSDM-Pn: <Base64URL kodierter Prüfungsnachweis>
      VSDM-Pn-Type: application/xml
      VSDM-Pn-Encoding: gzip
      VSDM-Pn-Lenght: 256
      VSDM-Pn-Disposition: attachment; filename="pruefungsnachweis.xml"
      {
      }
}
```

Beispiel für die HTTP-Response für den Status HTTP 200 OK:

```
HTTP/1.1 200 OK
...
{
      HTTP/1.1 200 OK
      ETag:
      "e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855"
      Content-Type:
      {application/fhir+json, application/fhir+xml};charset=utf-8
      Content-Encoding: gzip
      ...
      VSDM-Pn: <Base64URL kodierter Prüfungsnachweis>
      VSDM-Pn-Type: application/xml
      VSDM-Pn-Encoding: gzip
      VSDM-Pn-Length: 256
      VSDM-Pn-Disposition: attachment; filename="pruefungsnachweis.xml"
      {
            "resourceType": "VSDMBundle",
            ...
      }
}
```

Beispiel für eine HTTP-Response mit Fehlermeldung mittels FHIR-Ressource

```
HTTP/1.1 404 Not Found
...
{
      HTTP/1.1 404 Not Found
      Content-Type:
      {application/fhir+json, application/fhir+xml};charset=utf-8
      Content-Encoding
      ...
      {
            "resourceType": "VSDMOperationOutcome",
            ...
      }
}
```

4.1.2.2 Offline-Fall: Versichertenstammdaten von eGK lesen

A_26721 - Clientsystem VSDM - eH-KT - VSD von eGK lesen

Ein Clientsystem VSDM MUSS im Offline-Fall (Fachdienst VSDM ist nicht erreichbar) in der Lage sein, die Versichertenstammdaten aus dem ungeschützten Bereich der eGK (Container PD und VD) gemäß [gemILF_PS] unter Nutzung eines eH-KT von der eGK zu lesen.**[**<=, CS_VSDM_2, funkt. Eignung: Konformitätsbestätigung**]**

A_26722 - Clientsystem VSDM - Smartcard-Reader - VSD von eGK lesen
Ein Clientsystems VSDM MUSS im Offline-Fall (Fachdienst VSDM ist nicht erreichbar) in der Lage sein, die Versichertenstammdaten aus dem ungeschützten Bereich der eGK (Container PD und VD) gemäß [gemILF_PS] unter Nutzung eines handelsüblichen Smartcard-Readers von der eGK zu lesen.**[**<=, CS_VSDM_2, funkt. Eignung: Konformitätsbestätigung**]**

Hinweis: Der Verweis auf den Implementierungsleitfaden für Primärsysteme bezieht sich ausschließlich auf die Verarbeitung der Versichertenstammdaten der eGK (Dekomprimierung, Dekodierung, VSD-Container von der eGK lesen, Interpretation der Stammdaten etc.

Ausblick:

Ab einem noch festzulegenden Datum wird nur noch der verkürzte Versichertenstammdatensatz auf elektronische Gesundheitskarten hinterlegt. Ein Clientsystem muss somit zukünftig für vor diesem Datum herausgegebene eGKs die kompletten als auch für ab diesem Zeitpunkt herausgegebene eGKs den reduzierten Versichertenstammdatensatz aus dem ungeschützten Bereich der eGK (Container PD und VD) lesen, verarbeiten und anzeigen können.

4.1.3 Trust-Client Funktionen

Die logische Komponente "Trust-Client" dient lediglich als Strukturierungselement für diese Spezifikation und soll die VSDM-spezifischen Clientsystem-Anforderungen an die Trust-Client Funktionen gemäß [gemSpec_Zero_Trust] verdeutlichen.

A_26724 - Clientsystem VSDM - Trust-Client
Ein Clientsystems VSDM MUSS die Trust-Client Funktionen gemäß [gemSpec_Zero_Trust] umsetzen.**[**<=, CS_VSDM_2, funkt. Eignung: Konformitätsbestätigung**]**

A_26984 - Clientsystem VSDM - Authentisierung
Ein Clientsystem MUSS die Authentisierung mittels SM(C)-B gemäß [gemSpec_Zero_Trust] verwenden.
[<=, CS_VSDM_2, funkt. Eignung: Konformitätsbestätigung**]**

A_26726 - Clientsystem VSDM - VAU-Protokoll
Ein Clientsystems VSDM MUSS für jede Anfrage an die Fachdienste VSDM API `/vsdservice` die Trust-Client Funktion mit aktiven ZT/ASL (VAU-Protokoll) gemäß [gemSpec_Zero_Trust] und [gemSpect_Krypt] verwenden. **[**<=, CS_VSDM_2, funkt. Eignung: Konformitätsbestätigung**]**

Hinweis: VAU-Protokoll und VAU-Kanal sind im Kontext VSDM Synonyme.

4.1.4 Fehlerbehandlung

A_27014 - Clientsystem VSDM - Fehlerbehandlung
Ein Clientsystem SOLL bei den durch die FHIR-Resource `VSDMOperationOutcome` übermittelten Fehler die folgende Fehlerbehandlung durchführen:

Tabelle 1 : TAB_FACHDIENST_VSDM_FEHLERMELDUNGEN_FÜR_CLIENTSYSTEM

VSDMErrorcodeCS Code	Fehlerbehandlung
VSDSERVICE_POPPTOKEN_EXPIRED	Nachweis zum Versorgungskontext mittels eGK oder GesundheitsID am PoPP-Service erneuern.
VSDSERVICE_INVALID_IK	Nachweis zum Versorgungskontext mittels eGK oder GesundheitsID am PoPP-Service 1 x erneuern. Bei erneutem Fehler: Abbruch, da wahrscheinlich ein Implementierungsfehler vorliegt (Clientsystem oder PoPP-Service) oder die KTR gar nicht bei diesem FD-Anbieter ist (fehlerhafter DNS-Eintrag).
VSDSERVICE_INVALID_KVNR	Nachweis zum Versorgungskontext mittels eGK oder GesundheitsID am PoPP-Service 1 x erneuern. Bei erneutem Fehler: Abbruch, da wahrscheinlich ein Implementierungsfehler vorliegt (Clientsystem oder PoPP-Service).
VSDSERVICE_PATIENT_RECORD_NOT_FOUND	Nachweis zum Versorgungskontext mittels eGK oder GesundheitsID am PoPP-Service 1 x erneuern. Bei erneutem Fehler: Abbruch, da wahrscheinlich ein Implementierungsfehler vorliegt (Clientsystem, PoPP-Service oder Schnittstelle zu KTR-Bestandssystemen).
VSDSERVICE_MISSING_OR_INVALID_HEADER	Im Falle des Headers PoPP: Nachweis zum Versorgungskontext mittels eGK oder GesundheitsID am PoPP-Service 1 x erneuern. Bei erneutem Fehler: Abbruch, da wahrscheinlich ein Implementierungsfehler vorliegt (Clientsystem).
VSDSERVICE_UNSUPPORTED_MEDIATYPE	- (Implementierungsfehler)

VSDSERVICE_UNSUPPORTED_ENCODING	- (Implementierungsfehler)
VSDSERVICE_INVALID_PATIENT_RECORD_VERSION	- (Implementierungsfehler)
VSDSERVICE_INVALID_HTTP_OPERATION	- (Implementierungsfehler)
VSDSERVICE_INVALID_ENDPOINT	- (Implementierungsfehler)
VSD_SERVICE_INTERNAL_SERVER_ERROR	Wiederholungsversuch im 'Exponential Backoff'-Verfahren. Abbruch nach maximal 5 Versuchen. Danach 15 Minuten warten.
VSDSERVICE_VSDDB_NOTREACHABLE	Wiederholungsversuch im 'Exponential Backoff'-Verfahren. Abbruch nach maximal 5 Versuchen. Danach 15 Minuten warten.
VSDSERVICE_VSDDB_TIMEOUT	Wiederholungsversuch im 'Exponential Backoff'-Verfahren. Abbruch nach maximal 5 Versuchen. Danach 15 Minuten warten.

[<=, CS_VSDM_2, funkt. Eignung: Konformitätsbestätigung**]**

4.2 Zero-Trust Cluster

Dieses Kapitel beschränkt sich folgend nur auf die Zero-Trust Cluster Komponenten mit VSDM-spezifischen Konfigurationsanforderungen. Vorgaben zur operativen Umsetzung der folgenden Konfigurationsanforderungen sind [gemSpec_Zero_Trust] zu entnehmen.

Die folgenden Anforderungen an die Komponenten des Zero-Trust Cluster (als Teil eines Fachdienstes VSDM) werden durch Einträge in die VSDM-spezifische Konfigurationsdaten (Manifest-Dateien) gemäß [gemSpec_Zero_Trust] umgesetzt (siehe auch 7.6- VSDM-spezifische Konfigurationsdaten Zero-Trust Cluster). Da zum Veröffentlichungszeitpunkt dieser Spezifikation die konkrete Ausgestaltung der Manifest-Dateien noch nicht feststeht, werden die Konfigurationsvorgaben in Form von Anforderungen und als Teil dieser Spezifikation festgelegt, und dem Produkttypsteckbrief zugeordnet. Steht die konkrete Ausgestaltung der Manifest-Dateien fest, werden zukünftige Spezifikationen nur noch auf die Manifest-Dateien in Form einer Anforderung verweisen.

Tabelle 2 : TAB_VSDM_KONFIGURATIONSÜBERSICHT_ZERO-TRUST_CLUSTER

Zero-Trust Komponente	VSDM-spezifische Konfigurationsanforderungen auf Anwendungsebene

Ingress und Egress	nein
HTTP-Proxy	ja
Client Registry	nein
Authorization Server	ja
Datenbank	nein
Policy Engine	nein
Cluster Management Service	nein
Telemetrie-Daten Service	nein

A_26727 - Anbieter Fachdienst VSDM - Nutzung des Zero-Trust Clusters
Der Anbieter eines Fachdienstes VSDM MUSS folgende Komponenten des Zero-Trust Clusters gemäß den Anforderungen von [gemSpec_Zero_Trust] verwenden.
[<=, Anb_VSDM_2_FD, Sich.techn. Eignung: Anbietererklärung**]**

A_26728 - Anbieter Fachdienst VSDM - Bezug des Zero-Trust Clusters
Der Anbieter eines Fachdienst VSDM MUSS sicherstellen, das er das Zero-Trust Cluster ausschließlich von einem Downloadpunkt gemäß [gemSpec_Zero_Trust] bezieht.
[<=, Anb_VSDM_2_FD, Sich.techn. Eignung: Anbietererklärung**]**

4.2.1 HTTP-Proxy Konfiguration

Der HTTP-Proxy nimmt die Anfragen eines Clientsystems entgegen und prüft die Anfrage vor dem Aufbau eines VAU-Kanals mittels VAU-Protokoll auf erlaubte Endpunkte sowie auf eine vorhandene sowie gültige Berechtigung auf Basis von DPoP- und Access-Token. Anschließend wird auf das Vorhandensein des Headers `PoPP` innerhalb des VAU-Kanals geprüft und - wenn vorhanden - der PoPP-Token sicherheitstechnisch verifiziert. Anschließend stellt der HTTP-Proxy eine HTTP-basierte Anfrage (ohne VAU-Protokoll, aber mit allen Informationen der Anfrage des Clientsystems) an den Ressource-Server und fügt dieser die Zero-Trust Cluster spezifischen Header `ZTA-User-Info`, `ZTA-PoPP-Token-Content` und bei entsprechender HTTP-Proxy Konfiguration `ZTA-Client-Data` hinzu.

Antworten des Ressource-Servers nimmt der HTTP-Proxy entgegen und setzt diese Richtung Clientsystem auf das VAU-Protokoll um.

4.2.1.1 Schnittstelle zum Clientsystem

A_26731 - Fachdienst VSDM - HTTP-Proxy - ZT/ASL (VAU-Protokoll)
Der Anbieter VSDM MUSS den HTTP-Proxy derart konfigurieren, sodass ein Verbindungsaufbau mit einem Clientsystem nur mittels ZT/ASL (VAU-Protokoll) gemäß [gemSpec_Zero_Trust] erlaubt wird.**[**<=, VSDM_2_FD, funkt. Eignung: Test Produkt/FA**]**

A_26732 - Fachdienst VSDM - HTTP-Proxy - ZT/ASL (VAU-Protokoll) für FHIR Ressourcen

Der HTTP-Proxy VSDM MUSS die Versichertenstammdaten in Form der FHIR-Resource `VSDMBundle` sowie die FHIR Ressource `VSDMOperationOutcome` durch das ZT/ASL (VAU-Protokoll) gemäß [gemSpect_Zero_Trust] gesichert an das Clientsystem übertragen. **[**<=, VSDM_2_FD, funkt. Eignung: Test Produkt/FA**]**

Hinweis: Diese Anforderung dient zur Überprüfung der Eignung des Fachdienstes VSDM in seiner Endkonfiguration. Der Anbieter eines Fachdienst VSDM muss diese korrekte Funktionalität nur überprüfen.

A_26733 - Fachdienst VSDM - HTTP-Proxy - unzulässige HTTP-Methoden
Der Anbieter VSDM MUSS den HTTP-Proxy derart konfigurieren, sodass alle von einem Clientsystem eingehenden Anfragen, die nicht die HTTP-Methode GET verwenden, unterbunden werden. Er DARF solche Anfragen NICHT an den VSDM Resource Server weiterleiten, damit keine unzulässigen Operationen auf Versichertenstammdaten ausgeführt werden können.**[**<=, VSDM_2_FD, funkt. Eignung: Test Produkt/FA**]**

A_26734 - Fachdienst VSDM - HTTP-Proxy - unzulässige URI
Der Anbieter VSDM MUSS den HTTP-Proxy derart konfigurieren, sodass alle von einem Clientsystem eingehenden Anfragen mit einer URI, die nicht konform zu [OpenAPI_VSDM_2] ist, unterbunden werden. Er DARF solche Anfragen NICHT an den VSDM Resource Server weiterleiten, damit keine unzulässigen Operationen auf Versichertenstammdaten ausgeführt werden können.**[**<=, VSDM_2_FD, funkt. Eignung: Test Produkt/FA**]**

A_26735 - Fachdienst VSDM - HTTP-Proxy - unzulässige Endpunkte
Der Anbieter VSDM MUSS den HTTP-Proxy derart konfigurieren, sodass alle von einem Clientsystem eingehenden Anfragen, die nicht mit den in [OpenAPI_VSDM_2] spezifizierten Endpunkte übereinstimmen, unterbinden. Er DARF solche Anfragen NICHT an den VSDM Resource Server weiterleiten, damit keine unzulässigen Operationen auf Versichertenstammdaten ausgeführt werden können.**[**<=, VSDM_2_FD, funkt. Eignung: Test Produkt/FA**]**

4.2.1.2 Schnittstelle zum VSDM Resource Server

A_26742 - Fachdienst VSDM - HTTP-Proxy - Übermittlung von Client-Daten
Der Anbieter VSDM MUSS den HTTP-Proxy derart konfigurieren, sodass bei jeder Anfrage an die Fachdienst VSDM API `/vsdservice` Client-Daten mittels HTTP-Header `ZTA-Client-Data` gemäß [gemSpec_Zero_Trust] an den Resource Server übermittelt werden, um fehlerhafte Aufrufe einem dedizierten Client zuordnen zu können.**[**<=, VSDM_2_FD, funkt. Eignung: Test Produkt/FA**]**

Hinweis: Diese Anforderung dient zur Überprüfung der Eignung des Fachdienstes VSDM in seiner Endkonfiguration. Der Anbieter eines Fachdienst VSDM muss diese korrekte Funktionalität nur überprüfen.

4.2.2 Authorization-Server Konfiguration

A_26638 - Fachdienst VSDM - AuthZ-Server - Authentifizierung mit SM(C)-B
Der Anbieter VSDM MUSS den Authorization-Server derart konfigurieren, sodass die Authentifizierung einer Leistungserbringerinstitution nur auf Basis einer SM(C)-B durchgeführt wird.**[**<=, VSDM_2_FD, funkt. Eignung: Test Produkt/FA**]**

A_26985 - Fachdienst VSDM - AuthZ-Server - Authentifizierung mit SM(C)-B einmal am Tag

Der Anbieter VSDM MUSS den Authorization-Server derart konfigurieren, sodass einmal täglich die Authentifizierung der Leistungserbringerinstitution und unabhängig von einem möglicherweise noch gültigem Refresh-Token durchgeführt wird.**[**<=, VSDM_2_FD, funkt. Eignung: Test Produkt/FA**]**

Hinweis: Die tägliche Authentifizierung ist ein Standardwert, der bspw. aufgrund von Sicherheitsereignissen oder auf Basis der Sicherheitsbewertung des Clientsystems (Client-Attestation) im Betrieb mittels ZT-Policy geändert werden kann. Zukünftig und bei Verfügbarkeit der VSDM-Policy wird dieser Standardwert über die VSDM-Policy festgelegt und nicht mehr innerhalb dieser Spezifikation.

A_26743 - Fachdienst VSDM - AuthZ-Server - RBAC auf Basis der ProfessionOID
Der Anbieter VSDM MUSS den Authorization-Server derart konfigurieren, sodass er ausschließlich für die folgend positiv gelisteten ProfessionOIDs einen Access- und Refresh-Token ausstellt.

Tabelle 3 : TAB_FACHDIENST_VSDM_ERLAUBTE_PROFESSION_OID

OID-Referenz in anderen Dokumenten	Profession Item (Beschreibung der Institution)	Zugriff VSDM
oid_praxis_arzt (Hinweis: Die Praxis bzw. Betriebsstätte eines/-r ärztlichen Psychotherapeuten/-in wird mit dem ProfessionOID {oid_praxis_arzt} bezeichnet bzw. mit dem ProfessionItem „Betriebsstätte Arzt“ beschrieben.)	Betriebsstätte Arzt (Hinweis: Die Praxis bzw. Betriebsstätte eines/-r ärztlichen Psychotherapeuten/-in wird mit dem ProfessionOID {oid_praxis_arzt} bezeichnet bzw. mit dem ProfessionItem „Betriebsstätte Arzt“ beschrieben.)	ja
oid_zahnarztpraxis	Zahnarztpraxis	ja
oid_praxis_psychotherapeut (Hinweis: Die Praxis bzw. Betriebsstätte eines/-r ärztlichen Psychotherapeuten/-in wird mit dem ProfessionOID {oid_praxis_arzt} bezeichnet bzw. mit dem ProfessionItem „Betriebsstätte Arzt“ beschrieben.)	Betriebsstätte Psychotherapeut (Hinweis: Die Praxis bzw. Betriebsstätte eines/-r ärztlichen Psychotherapeuten/-in wird mit dem ProfessionOID {oid_praxis_arzt} bezeichnet bzw. mit dem ProfessionItem „Betriebsstätte Arzt“ beschrieben.)	ja
oid_krankenhaus	Krankenhaus	ja
oid_oeffentliche_apotheke	Öffentliche Apotheke	ja
oid_krankenhausapotheke	Krankenhausapotheke	ja
oid_bundeswehrapotheke	Bundeswehrapotheke	ja
oid_mobile_einrichtung_rettungsdienst	Betriebsstätte Mobile Einrichtung Rettungsdienst	ja
oid_bs_gematik	Betriebsstätte gematik	nein
oid_kostentraeger	Betriebsstätte Kostenträger	nein

oid_leo_zahnaerzte	Betriebsstätte Leistungserbringerorganisation Vertragszahnärzte	nein
oid_adv_ktr	AdV-Umgebung bei Kostenträger	ja
oid_leo_kassenaerztliche_vereinigung	Betriebsstätte Leistungserbringerorganisation Kassenärztliche Vereinigung	nein
oid_bs_gkv_spitzenverband	Betriebsstätte GKV-Spitzenverband	nein
oid_leo_krankenhausverband	Betriebsstätte Mitgliedsverband der Krankenhäuser	nein
oid_leo_dktig	Betriebsstätte der Deutsche Krankenhaus TrustCenter und Informationsverarbeitung GmbH	nein
oid_leo_dkg	Betriebsstätte der Deutschen Krankenhausgesellschaft	nein
oid_leo_apothekerverband	Betriebsstätte Apothekerverband	nein
oid_leo_dav	Betriebsstätte Deutscher Apothekerverband	nein
oid_leo_baek	Betriebsstätte der Bundesärztekammer	nein
oid_leo_aerztekammer	Betriebsstätte einer Ärztekammer	nein
oid_leo_zahnaerztekammer	Betriebsstätte einer Zahnärztekammer	nein
oid_leo-kbv	Betriebsstätte der Kassenärztlichen Bundesvereinigung	nein
oid_leo-bzaek	Betriebsstätte der Bundeszahnärztekammer	nein
oid_leo-kzbv	Betriebsstätte der Kassenzahnärztlichen Bundesvereinigung	nein
oid_institution-pflege	Betriebsstätte Gesundheits-, Kranken- und Altenpflege	ja
oid_institution-geburtshilfe	Betriebsstätte Geburtshilfe	ja
oid_praxis-physiotherapeut	Betriebsstätte Physiotherapie	ja

oid_institution-augenoptiker	Betriebsstätte Augenoptiker	ja
oid_institution-hoerakustiker	Betriebsstätte Hörakustiker	ja
oid_institution-orthopaedieschuhmacher	Betriebsstätte Orthopädieschuhmacher	ja
oid_institution-orthopaedietechniker	Betriebsstätte Orthopädietechniker	ja
oid_institution-zahntechniker	Betriebsstätte Zahntechniker	ja
oid_institution-rettungsleitstellen	Rettungsleitstelle	ja
oid_sanitaetsdienst-bundeswehr	Betriebsstätte Sanitätsdienst Bundeswehr	ja
oid_institution-oegd	Betriebsstätte Öffentlicher Gesundheitsdienst	nein
oid_institution-arbeitsmedizin	Betriebsstätte Arbeitsmedizin	nein
oid_institution-vorsorge-reha	Betriebsstätte Vorsorge- und Rehabilitation	ja
oid_epa_ktr	ePA KTR-Zugriffsautorisierung	nein
oid_pflegeberatung	Betriebsstätte Pflegeberatung nach § 7a SGB XI	nein
oid_leo_psychotherapeuten	Betriebsstätte Psychotherapeutenkammer	nein
oid_leo_bptk	Betriebsstätte Bundespsychotherapeutenkammer	nein
oid_leo_lak	Betriebsstätte Landesapothekerkammer	nein
oid_leo_bak	Betriebsstätte Bundesapothekerkammer	nein
oid_leo_egbr	Betriebsstätte elektronisches Gesundheitsberuferegister	nein
oid_leo_handwerkskammer	Betriebsstätte Handwerkskammer	nein
oid_gesundheitsdatenregister	Betriebsstätte Register für	nein

	Gesundheitsdaten	
oid_abrechnungsdienstleister	Betriebsstätte Abrechnungsdienstleister	nein
oid_pkv_verband	Betriebsstätte PKV-Verband	nein
oid_praxis-ergotherapeut	Ergotherapiepraxis	ja
oid_praxis-logopaede	Logopaedische Praxis	ja
oid_praxis-podologe	Podologiepraxis	ja
oid_praxis-ernaehrungstherapeut	Ernährungstherapeutische Praxis	ja
oid_bs-weitere-kostentraeger	Betriebsstätte Weitere Kostenträger im Gesundheitswesen	ja
oid_org-gesundheitsversorgung	Weitere Organisationen der Gesundheitsversorgung	nein
oid_kim-anbieter	KIM-Hersteller und -Anbieter	nein
oid_diga	DiGA-Hersteller und -Anbieter	nein
oid_tim-anbieter	TIM-Hersteller und -Anbieter	nein
oid_ncpeh	NCPeH Fachdienst	nein
oid_ombudsstelle	Ombudsstelle eines Kostenträgers	ja
oid_bs-opto-audio	Betriebsstätte Augenoptiker und Hörakustiker	ja
oid_bs-orthopaed-hw	Betriebsstätte Orthopädieschuhmacher und Orthopädietechniker	ja
oid_bs-himi	Betriebsstätte Hilfsmittelerbringer (Hinweis: Betriebsstätten der Hilfsmittelerbringer, welche nicht den Gesundheitshandwerken zugeordnet sind)	ja

[<=, VSDM_2_FD, funkt. Eignung: Test Produkt/FA**]**

Hinweis: Zukünftig und bei Verfügbarkeit der VSDM-Policy werden die erlaubten OIDs über die VSDM-Policy festgelegt und nicht mehr innerhalb dieser Spezifikation.

A_26744 - Fachdienst VSDM - AuthZ-Server - Scopes
Der Anbieter VSDM MUSS den Authorization-Server derart konfigurieren, sodass ausschließlich für zugriffsberechtigte ProfessionOIDs ein Access- und Refresh-Token mit

dem `scope : vsdservice` ausgestellt wird.**[**<=, VSDM_2_FD, funkt. Eignung: Test Produkt/FA**]**

Hinweis: Der Authorization-Server autorisiert auf Ebene eines API-Zugriffes bzw. für den Zugriff auf die VSDService-API des Resource Server eines Fachdienstes VSDM.

A_26745 - Fachdienst VSDM - AuthZ-Server - Gültigkeitsdauer Refresh-Token
Der Anbieter VSDM MUSS den Authorization-Server derart konfigurieren, sodass Refresh-Token standardmäßig mit einer Gültigkeitsdauer von 24 Stunden versehen werden.
[<=, VSDM_2_FD, funkt. Eignung: Test Produkt/FA**]**

Hinweis: Die Gültigkeitsdauer von 24 Stunden ist ein Standardwert, der bspw. aufgrund von Sicherheitsereignissen oder auf Basis der Sicherheitsbewertung des Clientsystems (Client-Attestation) im Betrieb mittels ZT-Policy geändert werden kann. Zukünftig und bei Verfügbarkeit der VSDM-Policy wird dieser Standardwert über die VSDM-Policy festgelegt und nicht mehr innerhalb dieser Spezifikation.

A_26746 - Fachdienst VSDM - AuthZ-Server - Gültigkeitsdauer Access-Token
Der Anbieter VSDM MUSS den Authorization-Server derart konfigurieren, sodass Access-Token standardmäßig mit einer Gültigkeitsdauer von 5 Minuten versehen werden.
[<=, VSDM_2_FD, funkt. Eignung: Test Produkt/FA**]**

Hinweis: Die Gültigkeitsdauer von 5 Minuten ist ein Standardwert, der bspw. aufgrund von Sicherheitsereignissen oder auf Basis der Sicherheitsbewertung des Clientsystems (Client-Attestation) im Betrieb mittels ZT-Policy geändert werden kann. Zukünftig und bei Verfügbarkeit der VSDM-Policy wird dieser Standardwert über die VSDM-Policy festgelegt und nicht mehr innerhalb dieser Spezifikation.

4.3 VSDM Resource Server

4.3.1 VSDService-API

Die VSDService-API stellt Clientsystemen unter dem Endpunkt `/vsdservice/v1/vsdmbundle` folgende Ressourcen bereit:

Tabelle 4 : TAB_FACHDIENST_VSDM_RESSOURCEN

Resource	Zugriffs-methode	Standard, Format	Übertragung	Bereitstellungsbedingung
VSDMBundle (VSDMPatient + VSDMCoverage)	HTTP GET	fhir+xml fhir+json	HTTP-Body innerhalb des VAU-Protokolls	gültiger Access-Token gültiger PoPP-Token zeitliche Gültigkeit des Versorgungskontext Clientsystem besitzt veraltete VSD kein Fehlerfall
Prüfungsnachweis	intern	xml	HTTP Custom-Header innerhalb	gültiger Access-Token gültiger PoPP-Token VSD-Aktualitätsprüfung wurde durchgeführt

			des VAU-Protokolls	kein Fehlerfall
VSDMOperationOutcome	intern	fhir+xml fhir+json	HTTP-Body innerhalb des VAU-Protokolls	nur im Fehlerfall

A_26749 - Fachdienst VSDM - Resource Server - VSDService-API MimeType fhir+xml
Der Resource Server VSDM MUSS in seinen Schnittstellen für die Zugriffe durch Leistungserbringer und Leistungserbringerinstitutionen standardmäßig den MimeType `application/fhir+xml` für alle FHIR Ressourcen verwenden.**[**<=, VSDM_2_FD, funkt. Eignung: Test Produkt/FA**]**

A_26750 - Fachdienst VSDM - Resource Server - VSDService-API MimeType Aufrufparameter
Der Resource Server VSDM MUSS in seinen Schnittstellen einen von der Standardfestlegung abweichenden MimeType für alle FHIR Ressourcen verwenden, wenn der jeweilige Client eine entsprechende Anforderung mittels des Accept-Attributs im HTTP-Anfrage-Header als `application/fhir+xml` bzw. `application/fhir+json` anfordert, damit Clientsysteme ein für sie leichter verarbeitbares Format in der Antwort mit einer FHIR Ressource erhalten können.**[**<=, VSDM_2_FD, funkt. Eignung: Test Produkt/FA**]**

A_26751 - Fachdienst VSDM - Resource Server - RESTful API charset utf-8
Der Resource Server VSDM MUSS in seinen Schnittstellen für die Zugriffe durch Leistungserbringer und Leistungserbringerinstitutionen standardmäßig das character set utf-8 in Antworten mit einer FHIR Ressource verwenden.**[**<=, VSDM_2_FD, funkt. Eignung: Test Produkt/FA**]**

A_26752 - Fachdienst VSDM - Resource Server - HTTP-Version
Der Resource Server VSDM MUSS mindestens HTTP Version 1.1 unterstützen. Die Unterstützung höherer HTTP-Versionen ist erlaubt.**[**<=, VSDM_2_FD, funkt. Eignung: Test Produkt/FA**]**

A_26753 - Fachdienst VSDM - Resource Server - unzulässige HTTP-Methoden
Der Resource Server VSDM MUSS alle eingehenden Anfragen, die nicht die HTTP-Methode GET verwenden, ablehnen, damit keine unzulässigen Operationen auf Versichertenstammdaten ausgeführt werden können.**[**<=, VSDM_2_FD, funkt. Eignung: Test Produkt/FA**]**

A_26754 - Fachdienst VSDM - Resource Server - ZTA Header
Der Resource Server VSDM MUSS alle eingehenden Anfragen, die nicht den HTTP-Header `ZTA-PoPP-Token-Content`, `ZTA-User-Info`, `ZTA-Client-Data` übertragen, ablehnen und den HTTP Status Code 400 Bad Request in der Antwort verwenden.
[<=, VSDM_2_FD, funkt. Eignung: Test Produkt/FA**]**

A_26755 - Fachdienst VSDM - Resource Server - If-None-Match Header

Der Resource Server VSDM MUSS alle eingehenden Anfragen, die nicht den HTTP-Header `If-None-Match` übertragen, ablehnen. Die Antwort des Ressource Server VSDM MUSS den HTTP Status Code 400 Bad Request sowie eine Fehlerbeschreibung gemäß A_2670 beinhalten.**[**<=, VSDM_2_FD, funkt. Eignung: Test Produkt/FA**]**

A_26977 - Eingabe Validierung
Der Resource Server VSDM MUSS sicherstellen, dass alle anwendungsspezifischen Header sowie URLs, die über die API `/vsdservice` kommuniziert werden, sicherheitstechnisch validiert werden.**[**<=, VSDM_2_FD, Sich.techn. Eignung: Gutachten**]**

A_26756 - Fachdienst VSDM - Resource Server - Gültigkeit Versorgungskontext prüfen
Der Resource Server VSDM MUSS beim Aufruf der HTTP-GET-Operation an die Fachdienst VSDM API `/vsdservice` zuerst auf einen zeitlich gültigen Versorgungskontext gegen die Systemzeit prüfen. Der Wert `patient.proofTime` MUSS zum Zeitpunkt der HTTP-GET-Operation innerhalb des aktuellen Quartals des aktuellen Jahres liegen. Liegt der Wert `patient.proofTime` nicht innerhalb des aktuellen Quartals des aktuellen Jahres, MUSS die Antwort den HTTP Status Code 403 Forbidden sowie eine Fehlerbeschreibung gemäß A_2670 beinhalten.**[**<=, VSDM_2_FD, funkt. Eignung: Test Produkt/FA**]**

A_26757 - Fachdienst VSDM - Resource Server - Übermittlung VSD-Änderungsindikator als ETag
Der Resource Server VSDM MUSS für jede Antwort, die keinen Fehlerfall darstellt, den aktuellen VSD-Änderungsindikator in Form eines starken ETag und als String im HTTP-Header `ETag` gemäß [RFC7232] an das Clientsystem übermitteln. **[**<=, VSDM_2_FD, funkt. Eignung: Test Produkt/FA**]**

A_26758 - Fachdienst VSDM - Resource Server - FHIR-Resource Komprimierung
Der Resource Server VSDM SOLL alle FHIR Ressourcen nach dem Kompressionsschema `gzip` gemäß [RFC1952] komprimiert übertragen.**[**<=, VSDM_2_FD, funkt. Eignung: Test Produkt/FA**]**

Hinweis: Bei hoher Auslastung des VSDM Resource Servers größer 80% darf auf eine Komprimierung verzichtet werden.

4.3.1.1 Versichertenstammdaten

Auf eine Zugriffsprüfung auf Ressourcen-Ebene wird verzichtet, da die VSDService-API aktuell nur eine einzige und für alle zugriffsberechtigten Leistungserbringerinstitutionen gleiche Ressource (VSDMBundle) bereitstellt. Die Zugriffsprüfung entspricht damit exakt der Zugriffsautorisierung und Zugriffsprüfung durch das Zero-Trust Cluster. Sollte zukünftig die Notwendigkeit einer rollenspezifischen Versichertenstammdatenbereitstellung (VSDMBundle) entstehen, wird eine Zugriffsprüfung auf Ressourcen-Ebene und auf Basis von ProfessionOID eingeführt.

A_26759 - Fachdienst VSDM - Resource Server - VSD-Identifier
Der Resource Server VSDM MUSS beim Aufruf der HTTP-GET-Operation an die Fachdienst VSDM API `/vsdservice` die KVNR des Elements `patient.identifier.value` des HTTP-Headers `ZTA-PoPP-Token-Content` zur Lokalisierung der VSD-Änderungskennung und der Versichertenstammdaten verwenden.**[**<=, VSDM_2_FD, funkt. Eignung: Test Produkt/FA**]**

A_26760 - Fachdienst VSDM - Resource Server - VSD-Aktualitätsprüfung

Der Resource Server VSDM MUSS beim Aufruf der HTTP-GET-Operation an die Fachdienst VSDM API `/vsdservice` vor dem Abruf der VSD von dem KTR-Bestandssystem eine VSD-Aktualitätsprüfung durchführen.**[**<=, VSDM_2_FD, funkt. Eignung: Test Produkt/FA**]**

A_26761 - Fachdienst VSDM - Resource Server - Rückgabe nur bei VSD-Änderungen
Der Resource Server VSDM MUSS sicherstellen, dass er ausschließlich bei dem Ergebnis "Nicht-Übereinstimmung" der VSD-Aktualitätsprüfung die Versichertenstammdaten abruft, verarbeitet und an das Clientsystem übermittelt. **[**<=, VSDM_2_FD, funkt. Eignung: Test Produkt/FA**]**

A_26963 - Fachdienst VSDM - Resource Server - VSD-Übermittlung im Fehlerfall der Aktualitätsprüfung
Der Resource Server VSDM MUSS sicherstellen, dass das Ergebnis der VSD-Aktualitätsprüfung bei einem Client-Request, der keinen `If-None-Match` Header oder einen fehlerhaften oder ungültigen Wert des Headers enthält, immer "Nicht-Übereinstimmung" ist. Dieses Ergebnis MUSS auch bei internen Fehlern, die bei der Aktualitätsprüfung auftreten, gesetzt werden.**[**<=, VSDM_2_FD, funkt. Eignung: Test Produkt/FA**]**

A_26762 - Fachdienst VSDM - Resource Server - Rückgabe VSD als FHIR-Bundle
Der Resource Server VSDM MUSS die Versichertenstammdaten als FHIR-Bundle `VSDMBundle` an das Clientsystem übermitteln.**[**<=, VSDM_2_FD, funkt. Eignung: Test Produkt/FA**]**

Hinweis: Die FHIR-Resource `VSDMBundle` beinhaltet die beiden FHIR Ressourcen `VSDMPatient` und `VSDMCoverage`.

A_26763 - Fachdienst VSDM - Resource Server - keine Rückgabe von Resource Collections
Der Resource Server VSDM MUSS sicherstellen, dass bei einem Aufruf der HTTP-GET-Operation an den Endpunkt `/vsdservice/v1/vsdmbundle` ausschließlich die Versichertenstammdaten respektive das `VSDMBundle` für die KVNR des Elements `patient.identifier.value` an das Clientsystem übermitteln werden. Er DARF KEINE KVNR-übergreifende Versichertenstammdaten `VSDMBundles` an das Clientsystem übermitteln.**[**<=, VSDM_2_FD, funkt. Eignung: Test Produkt/FA**]**

4.3.1.2 Prüfungsnachweis

A_26764 - Fachdienst VSDM - Resource Server - Prüfungsnachweis in jeder Response
Der Resource Server VSDM MUSS für jeden Aufruf der HTTP-GET-Operation an die Fachdienst VSDM API `/vsdservice`, bei dem die VSD-Aktualitätsprüfung zu einem fehlerfreien Ergebnis (Übereinstimmung, Nicht-Übereinstimmung) gekommen ist, den Prüfungsnachweis gemäß A_26966 an das Clientsystem übermitteln, insofern die Anfrage mit dem HTTP-Status 200 OK oder 304 Not Modified beantwortet werden kann.
[<=, VSDM_2_FD, funkt. Eignung: Test Produkt/FA**]**

Hinweis: Gemeint ist, dass der Prüfungsnachweis immer an das Clientsystem und unabhängig davon, ob die Versichertenstammdaten in Form der FHIR-Resource VSDMBundle übermittelt werden oder nicht, übermittelt werden. Bedingung ist die

korrekt durchgeführte Aktualitätsprüfung. In einem anderweitig auftretenden Fehlerfall, wird die Fehlermeldung ohne Prüfungsnachweis übermittelt.

A_26765 - Fachdienst VSDM - Resource Server - Prüfungsnachweis Komprimierung
Der Resource Server VSDM MUSS den Prüfungsnachweis in Form der XML-Datei nach dem Kompressionsschema "gzip" gemäß [RFC1952] komprimiert übertragen.
[<=, VSDM_2_FD, funkt. Eignung: Test Produkt/FA**]**

A_26766 - Fachdienst VSDM - Resource Server - Prüfungsnachweis Kodierung
Der Resource Server VSDM MUSS den komprimierten Prüfungsnachweis Base64URL gemäß [RFC4648] kodiert übertragen.**[**<=, VSDM_2_FD, funkt. Eignung: Test Produkt/FA**]**

A_26767 - Fachdienst VSDM - Resource Server - Prüfungsnachweis im HTTP-Header
Der Resource Server VSDM MUSS den Prüfungsnachweis im Custom-Header `VSDM-Pn` übertragen und über den Custom-Header `VSDM-Pn-Type` als `application/xml` deklarieren, damit der Prüfungsnachweis auch bei einer HTTP Status `304 Not Modified` Antwort übermittelt werden kann.**[**<=, VSDM_2_FD, funkt. Eignung: Test Produkt/FA**]**

4.3.1.3 Beispiele für die HTTP-Response des Resource Servers

Beispiel für die Übertragung des Prüfungsnachweises für den Fall HTTP 304 Not Modified:

HTTP-Header

```
HTTP/1.1 304 Not Modified
ETag: "e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855"
VSDM-Pn: <Base64URL kodierter Prüfungsnachweis>
VSDM-Pn-Type: application/xml
VSDM-Pn-Encoding: gzip
VSDM-Pn-Lenght: 256
VSDM-Pn-Disposition: attachment; filename="pruefungsnachweis.xml"
```

Beispiel für die Übertragung des Prüfungsnachweises für den Fall HTTP 200 OK:

```
HTTP/1.1 200 OK
Content-Type: {application/fhir+json, application/fhir+xml};charset=utf-8
...
ETag: "e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855"
VSDM-Pn: <Base64URL kodierter Prüfungsnachweis>
VSDM-Pn-Type: application/xml
VSDM-Pn-Encoding: gzip
VSDM-Pn-Length: 256
VSDM-Pn-Disposition: attachment; filename="pruefungsnachweis.xml"
{
      "resourceType": "VSDMBundle",
      ...
}
```

4.3.1.4 Fehlermeldungen

Werte des Feldes `BDE-Code` dienen zur Kennzeichnung eines dedizierten Fehlers im Rahmen der Betriebsdatenlieferung und -erfassung. Der Wertebereich dieser Codes ist mit 79xxx festgelegt, um nicht mit anderen Nomenklaturen zu kollidieren.

A_26768 - Fachdienst VSDM - Resource Server - HTTP Status Codes
Der Resource Server VSDM MUSS für die Fehlermeldungen die HTTP Status Codes gemäß `TAB_FACHDIENST_VSDM_HTTP_STATUS_CODES` verwenden. **[**<=, VSDM_2_FD, funkt. Eignung: Test Produkt/FA**]**

A_26770 - Fachdienst VSDM - Resource Server - FHIR-Resource OperationOutcome
Der Resource Server VSDM MUSS im Fehlerfall und für Fehlermeldungen mit dem Clientsystem als Empfänger Hinweise zur Fehlerursache als FHIR-Resource `OperationOutcome` gemäß [FHIR-Profil VSDMOperationOutcome] an das Clientsystem übermitteln.**[**<=, VSDM_2_FD, funkt. Eignung: Test Produkt/FA**]**

A_26998 - Fachdienst VSDM - Resource Server - keine Implementierungsdetails in Fehlermeldungen
Der Resource Server VSDM DARF KEINE Implementierungsdetails (z. B. kein Stacktrace) in Fehlermeldungen an das Clientsystem preisgeben.**[**<=, VSDM_2_FD, funkt. Eignung: Test Produkt/FA**]**

A_26993 - Fachdienst VSDM - Resource Server - Fehlersignalisierung für HTTP-Proxy Fehler
Der Resource Server VSDM MUSS für Fehler mit dem HTTP-Proxy als Empfänger der Fehlermeldung den Custom-Header `ZTA-Cause: Proxy` setzen, damit der HTTP-Proxy erkennen kann, dass er der Fehleradressat und nicht das Clientsystem ist.
[<=, VSDM_2_FD, funkt. Eignung: Test Produkt/FA**]**

A_26955 - Fachdienst VSDM - Resource Server - keine VSDMOperationOutcome Ressource bei HTTP-Proxy Fehlern
Der Resource Server VSDM DARF KEINE FHIR-Ressource VSDMOperationOutcome für Fehler mit dem HTTP-Proxy als Empfänger der Fehlermeldung verwenden.
[<=, VSDM_2_FD, funkt. Eignung: Test Produkt/FA**]**

A_26956 - Fachdienst VSDM - Resource Server - PoPP-Info Fehler
Der Resource Server VSDM MUSS bei einem fehlenden oder ungültigen `ZTA-PoPP-Content` auf Vorhandensein des HTTP-Headers `PoPP` prüfen, um die Fehlerquelle "Clientsystem" oder "HTTP-Proxy" zu identifizieren und mit der entsprechenden Fehlermeldung antworten zu können.Bei vorhandenem `PoPP` Header ist der HTTP-Proxy und bei fehlendem `PoPP` Header das Clientsystem als Fehlerursache anzunehmen. **[**<=, VSDM_2_FD, funkt. Eignung: Test Produkt/FA**]**

Beispiel für die Übertragung einer Fehlernachricht mit FHIR-Resource:

```
HTTP/1.1 404 Not Found
Content-Type: {application/fhir+json, application/fhir+xml};charset=utf-8
...
{
      "resourceType": "VSDMOperationOutcome",
      ...
```

}

4.3.2 VSD-Aktualitätsprüfung

Da VSD-Abfragen häufig stattfinden, aber VSD-Änderungen im Vergleich dazu relativ selten sind, soll der VSDM Resource Server in Zusammenarbeit mit dem KTR-Bestandssystem einen eindeutigen Identifier als HTTP-ETag zur Verfügung stellen (https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/ETag). Damit kann ein Clientsystem diesen ETag (256-Bit-Wert) lokal speichern und bei einer VSD-Abfrage prüfen, ob überhaupt eine Aktualisierung notwendig ist bzw. ob die lokal im Clientsystem gespeicherten VSD noch aktuell sind.

A_26774 - Fachdienst VSDM - Ressource Server - HTTP-ETag als VSD-Änderungsindikator
Der Resource Server VSDM MUSS einen HTTP-ETag als hexadezimal kodierten (kleingeschrieben 0-9a-f) 256-Bit Binärwert übermitteln. Der Resource Server VSDM MUSS hierfür einen VSD-Änderungsindikator, der sich bei jeder Änderung der VSD ebenfalls ändert, verwenden. Der VSD-Änderungsindikator DARF NICHT `0` sein.
[<=, VSDM_2_FD, funkt. Eignung: Test Produkt/FA**]**

Hinweis: Als Ausgangswert für der ETag kann die Gesamtheit eines dedizierten Versichertenstammdatensatzes, eine Versions-ID, ein Zeitstempel oder eine Zufallszahl dienen. Der finale ETag ist dann wie folgt zu bilden:

- *SHA-256 Hash-Wert über die Gesamtheit des dedizierten Versichertenstammdatensatzes*
- *HMAC(SHA256)-Wert über die Versions-ID oder den Zeitstempel*
- *Zufallszahl mit hoher Güte (mit hoher Wahrscheinlichkeit nicht erratbar oder nachvollziehbar/nachrechenbar)*

EIn SHA-256 Hash-Wert kann nicht ohne weitere Maßnahmen für die Erzeugung des ETags auf Basis einer reinen Versions-ID oder eines Zeistempels dienen, da man so als Abfragender erfährt (im Sinne von "nachrechnen") wie oft oder zu welcher Zeit sich diese VSD eines Versicherten sich geändert haben. Aufgrund dessen ist in diesen Fällen die Funktion HMAC-SHA-256(geheimer-Schlüssel, KVNR + VSD-Version oder Zeitstempel) als Pseudorandom-Funktion zu verwenden.

A_26775 - Fachdienst VSDM - Resource Server - VSD-Änderungsindikator Abruf
Der Resource Server VSDM MUSS für jeden (im Sinne von "jedes mal") Aufruf der HTTP-GET-Operation an die Fachdienst VSDM API `/vsdservice` stets den aktuellen Hash-Wert der zu der KVNR des Elements `patient.identifier.value` des HTTP-Headers `ZTA-PoPP-Token-Content` zugehörigen Versichertenstammdaten verwenden.
[<=, VSDM_2_FD, funkt. Eignung: Test Produkt/FA**]**

A_26776 - Fachdienst VSDM - Resource Server - VSD-Änderungsindikator Vergleich
Der Resource Server VSDM MUSS für jeden (im Sinne von "jedes mal") Aufruf der HTTP-GET Operation an die Fachdienst VSDM API `/vsdservice` den Wert aus dem HTTP-Header `ETag` des Aufrufes mit dem VSD-Änderungsindikator vergleichen. Der Vergleich MUSS als `strong comparison` gemäß [RFC7232] durchgeführt werden und zu einem eindeutigen Ergebnis bezüglich Übereinstimmung oder Nicht-Übereinstimmung gelangen. Im

Fehlerfall MUSS das Ergebnis auf eine Nicht-Übereinstimmung gesetzt werden. **[**<=, VSDM_2_FD, funkt. Eignung: Test Produkt/FA**]**

Hinweis: Die korrekte Umsetzung des Vergleiches von ETag und Änderungsindikator ist notwendig, um das Ziel der Übertragung von VSD nur bei einer Änderung dieser zu erreichen. Damit die Funktion der Änderungserkennung sich nicht negativ auf die Nutzer auswirkt, ist bei einem System-internen Fehlerfall dieser Funktion immer so zu verfahren, dass im Endeffekt das Clientsystem die Versichertenstammdaten und den Prüfungsnachweis erhält.

A_26777 - Fachdienst VSDM - Resource Server - ETag Löschung
Der Resource Server VSDM MUSS nach Übermittlung des VSD-Änderungsindikators an das Clientsystem in Form eines eTAGs sowohl den ETAG aus dem Clientsystem-Request löschen.**[**<=, VSDM_2_FD, funkt. Eignung: Test Produkt/FA**]**

4.3.3 FHIR-Fassade

A_26778 - Fachdienst VSDM - Resource Server - VSD-Abruf
Falls der Resource Server VSDM Versichertenstammdatensätze von einem weiteren System abruft, MUSS er sicherstellen, dass dieses System ausschließlich zu einem Kostenträger gemäß §4 Absatz 2 SGB V verantwortet wird.**[**<=, VSDM_2_FD, funkt. Eignung: Herstellererklärung**]**

A_26779 - Fachdienst VSDM - Resource Server - VSD-Lokalisierung
Der Resource Server VSDM MUSS zur Lokalisierung der VSD die KVNR des Elements `patient.identifier.value` des HTTP-Headers `ZTA-PoPP-Token-Content` verwenden. Falls der Resource Server VSDM Versichertenstammdatensätze von einem weiteren System abruft, MUSS er sicherstellen, dass das genau das System abgefragt wird, welches auch den zur KVNR zugehörigen Versichertenstammdatensatz verantwortet.**[**<=, VSDM_2_FD, funkt. Eignung: Test Produkt/FA**]**

A_26780 - Fachdienst VSDM - Resource Server - Versichertenindividuelle VSD-Abrufe
Der Resource Server VSDM MUSS sicherstellen, dass ausschließlich der Versichertenstammdatensatz desjenigen Versicherten, den ein Clientsystem mittels der KVNR des Elements `patient.identifier.value` des HTTP-Headers `ZTA-PoPP-Token-Content` zugehörigen Versichertenstammdaten anfragt, an das Clientsystem übermittelt werden.**[**<=, VSDM_2_FD, funkt. Eignung: Test Produkt/FA**]**

A_26781 - Fachdienst VSDM - Resource Server - FHIR-Resource VSDMPatient
Der Resource Server VSDM MUSS sicherstellen, dass die originären VSD in die FHIR-Resource VSDMPatient gemäß [FHIR-Profil VSDMPatient] korrekt überführt wird.
[<=, VSDM_2_FD, funkt. Eignung: Test Produkt/FA**]**

A_26783 - Fachdienst VSDM - Resource Server - FHIR-Resource VSDMCoverage
Der Resource Server VSDM MUSS sicherstellen, dass die originären VSD in die FHIR-Resource VSDMPatient gemäß FHIR-Profil [FHIR-Profile VSDMCoverage] korrekt überführt wird.**[**<=, VSDM_2_FD, funkt. Eignung: Test Produkt/FA**]**

A_26785 - Fachdienst VSDM - Resource Server - FHIR-Resource VSDMBundle
Der Resource Server VSDM MUSS die FHIR-Resource `VSDMPatient` und `VSDMCoverage` in der FHIR-Resource `VSDMBundle` gemäß [FHIR-Profil VSDMBundle] bündeln.
[<=, VSDM_2_FD, funkt. Eignung: Test Produkt/FA**]**

4.3.4 Erstellung Prüfungsnachweis

Der Prüfungsnachweis dient als Nachweis über die Durchführung der Prüfung des Versicherungsstatus und der Prüfung der Aktualität der Versichertenstammdaten. Er dient als Nachweis für die Abrechnungsdaten nach § 295 SGB V.

A_26788 - Fachdienst VSDM - Resource Server - Prüfungsnachweis bei jedem Aufruf
Der Resource Server VSDM MUSS für jeden (im Sinne von "jedes mal") Aufruf der HTTP-GET Operation an die Fachdienst VSDM API`/vsdservice` einen Prüfungsnachweis gemäß A_26965 für die KVNR des Elements `patient.identifier.value` des HTTP-Headers `ZTA-PoPP-Token-Content` erzeugen und an das Clientsystem übermitteln.
[<=, VSDM_2_FD, funkt. Eignung: Test Produkt/FA**]**

A_26789 - Fachdienst VSDM - Resource Server - Prüfungsnachweis XML-Format
Der Resource Server VSDM MUSS den Prüfungsnachweis nach dem XML-Schema gemäß [Prüfungsnachweis.xsd] erstellen.**[**<=, VSDM_2_FD, funkt. Eignung: Test Produkt/FA**]**

Beispiel: Prüfungsnachweis mit Base64 kodierter Prüfziffer (PZ).

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<PN xmlns="http://ws.gematik.de/fa/vsdm/pnw/v1.0" CDM_VERSION="1.0.0">
    <TS>20240919092007</TS>
    <E>1</E>
    <PZ>VDAyMzU5MDA1MDE3MjY3Mzc2MDFVVDLYyBOm+EDF0oe1aW/ndQe2p36MGAzvyBk=</
PZ>
</PN>
```

A_26790 - Fachdienst VSDM - Resource Server - Prüfziffer HMAC
Der Resource Server VSDM MUSS für die Erzeugung der Prüfziffer des Prüfungsnachweises die Anforderungen aus [gemSpec_Krypt] A_23460 und A_23461 beachten.**[**<=, VSDM_2_FD, funkt. Eignung: Test Produkt/FA**]**

A_26791 - Fachdienst VSDM - Resource Server - Prüfziffer Kodierung
Der Resource Server VSDM MUSS die Prüfziffer Base64 kodiert in den Prüfungsnachweis einbetten.**[**<=, VSDM_2_FD, funkt. Eignung: Test Produkt/FA**]**

A_26792 - Fachdienst VSDM - Resource Server - Prüfungsnachweis Zeitstempel
Der Resource Server VSDM MUSS für den Zeitstempel die aktuelle Systemzeit im UNIX-Zeitstempel Format verwenden.**[**<=, VSDM_2_FD, funkt. Eignung: Test Produkt/FA**]**

A_26793 - Fachdienst VSDM - Resource Server - Prüfungsnachweis Löschung
Der Resource Server VSDM MUSS den Prüfungsnachweis nach Übermittlung an das Clientsystem löschen. Der Prüfungsnachweis DARF NICHT zwischengespeichert (im Sinne einer Cache-Funktion) oder persistiert werden.**[**<=, VSDM_2_FD, funkt. Eignung: Test Produkt/FA**]**

4.3.5 Zugriffsprotokollierung

Der Fachdienst VSDM führt Zugriffsprotokolle für die Versicherten, in denen alle Zugriffe auf die personenbezogenen und medizinischen Daten eines Versicherten für den Versicherten einsehbar sind. Die Protokolleinträge werden gemäß der Löschfrist im VSDM Resource Server gespeichert und nach Ablauf dieser Frist automatisch gelöscht. Diese Zugriffsprotokolle sind unabhängig von technischen Protokollen und stehen ausschließlich dem Versicherten zur Wahrnehmung seiner Betroffenenrechte zur Einsicht zur Verfügung. Den Zugriff auf die Protokolle durch den Versicherten verantwortet der jeweilige Kostenträger und stellt seinen Versicherten geeignete Mittel und Wege zur Verfügung.

Anforderungen zum Inhalt des Nutzerprotokolls sind im Abschnitt 7.4- Zugriffsprotokoll für Versicherte formuliert.

A_26794 - Fachdienst VSDM - Resource Server - Zugriffsprotokoll Rollenprüfung
Der VSDM Resource Server MUSS bei jedem Zugriff auf die Zugriffsprotokolle sicherstellen, dass ausschließlich Versicherte Protokolleinträge einsehen können (Entitäten, die nicht Versicherte sind, haben also grundsätzlich keinen Zugriff auf diese Funktionalität).**[**<=, VSDM_2_FD, Sich.techn. Eignung: Gutachten**]**

A_26795 - Fachdienst VSDM - Resource Server - Zugriffsprotokoll Identitätsprüfung
Der VSDM Resource Server MUSS bei jedem Zugriff auf das Protokoll eines dedizierten Versicherten sicherstellen, dass ausschließlich dieser Versicherte das Zugriffsprotokoll einsehen kann.**[**<=, VSDM_2_FD, Sich.techn. Eignung: Gutachten**]**

A_26813 - Fachdienst VSDM - Resource Server - Zugriffsprotokoll Schutz der Vertraulichkeit
Der VSDM Resource Server MUSS die Zugriffsprotokoll mit den gleichen oder sicherheitstechnisch mindestens äquivalenten Sicherheitsmaßnahmen wie die VSD selbst schützen. **[**<=, VSDM_2_FD, Sich.techn. Eignung: Gutachten**]**

A_26796 - Fachdienst VSDM - Resource Server - Zugriffsprotokoll Rückgabe im Bundle
Der VSDM Resource Server MUSS bei einem Abruf eines Zugriffsprotokolls durch einen Versicherten die Ergebnisliste des Zugriffsprotokolls bei mehr als einem Eintrag als Ergebnis-Bundle an den Aufrufer zurückgeben, damit der Versicherte eine vollständige Einsicht in das Zugriffsprotokoll erhält. **[**<=, VSDM_2_FD, funkt. Eignung: Test Produkt/FA**]**

A_26797 - Fachdienst VSDM - Resource Server - Zugriffsprotokoll Löschfrist veraltete Protokolleinträge
Der VSDM Resource Server MUSS Zugriffsprotokolleinträge nach einem Jahr ab dem Erzeugungsdatum innerhalb von einem Monat löschen, damit veraltete Einträge nach

Ende der regulären Aufbewahrungsfrist entfernt werden. **[**<=, VSDM_2_FD, Sich.techn. Eignung: Herstellererklärung**]**

*Hinweis: Es darf, wenn es die Implementierung vereinfacht, angenommen werden, dass ein Jahr 60*60*24*365 Sekunden hat.*

4.3.6 VSD-DB

A_27004 - Fachdienst VSDM - Resource Server - Datenreplizierungszyklus
Falls der VSDM Resource Server Versichertenstammdaten repliziert (beispielsweise mittels Cache oder Datenbankreplikation) MUSS er einmal täglich diese Versichertenstammdaten aktualisieren.**[**<=, VSDM_2_FD, funkt. Eignung: Test Produkt/FA**]**

A_27005 - Fachdienst VSDM - Resource Server - Vertraulichkeit der VSD
Falls der VSDM Resource Server Versichertenstammdaten speichert (beispielsweise mittels Cache oder Datenbank) MUSS er die Versichertenstammdaten mit für deren Schutzbedarf geeigneten Sicherheitsmaßnahmen schützen.**[**<=, VSDM_2_FD, Sich.techn. Eignung: Gutachten**]**

4.4 BDE-Lieferung

A_27012 - Fachdienst VSDM - Resource Server - Fehlercodes für BDE-Lieferung
Der Fachdienst VSDM MUSS folgende Fehler als BDE-Code im Rahmen der Betriebsdatenlieferung verwenden:

Tabelle 5 : TAB_FACHDIENST_VSDM_BDE-Codes

BDE-Code	VSDMErrorcodeCS Referenz	Beschreibung	Fehler-adressat
79000	VSDSERVICE_POPPTOKEN_EXPIRED	The proof of patient presence token is expired.	Clientsystem
79010	VSDSERVICE_INVALID_IK	Invalid health insurer mark <ik>.	Clientsystem
79011	VSDSERVICE_INVALID_KVNR	Invalid health insured person number <kvnr>.	Clientsystem
79020	VSDSERVICE_PATIENT_RECORD_NOT_FOUND	The patient record for <kvnr> could not found at health insurer with id <ik>.	Clientsystem
79030	VSDSERVICE_MISSING_OR_INVALID_HEADER	The required header	Clientsyste

		<header> is missing or invalid.	m
79031	VSDSERVICE_UNSUPPORTED_MEDIATYPE	The clientsystem asked for an unsupported media type <media type>.	Clientsystem
79032	VSDSERVICE_UNSUPPORTED_ENCODING	The clientsystem asked for an unsupported encoding scheme <encoding scheme>.	Clientsystem
79033	VSDSERVICE_INVALID_PATIENT_RECORD_VERSION	The etag_value does not exists or could not processed.	Clientsystem
79040	VSDSERVICE_INVALID_HTTP_OPERATION	ERROR	Clientsystem
79041	VSDSERVICE_INVALID_ENDPOINT	ERROR	Clientsystem
79100	VSD_SERVICE_INTERNAL_SERVER_ERROR	Unexpected internal server error.	Clientsystem
79110	VSDSERVICE_VSDDB_NOTREACHABLE	Health insurer system with id <ik> is offline.	Clientsystem
79111	VSDSERVICE_VSDDB_TIMEOUT	Health insurer system with id <ik> timed out.	Clientsystem
79205	-	Header ZTA-Client-Data fehlt.	HTTP-Proxy
79206	-	Header ZTA-User-Info fehlt.	HTTP-Proxy
79207	-	Header ZTA-PoPP-Content fehlt.	HTTP-Proxy

79400	-	Client-Data Daten können nicht verarbeitet werden.	HTTP-Proxy
79401	-	User-Info Daten können nicht verarbeitet werden.	HTTP-Proxy
79402	-	PoPP-Info Daten können nicht verarbeitet werden.	HTTP-Proxy

<kvnr>: Krankenversichertennummer (Feld:`patient.identifier.value` des PoPP-Tokens)
<ik>: Institutionskennzeichen des jeweiligen Krankenversicherers (Feld:`patient.insurer.identifier.type` des PoPP-Tokens)**[**<=, VSDM_2_FD, funkt. Eignung: Test Produkt/FA**]**

4.5 SIEM

Ein VSDM2-FD muss sicherheitskritische Ereignisse im Fachdienst erfassen und je nach Schweregrad an das SIEM der TI übermitteln. Die Anforderungen dafür werden wie bei allen anderen Fachdiensten über die Zuweisung von Anforderungen aus [gemSpec_DS_Anbieter] dem Anbieter-Produkttypsteckbrief für VSDM-Anbieter zugeordnet.

5 Systemablauf

5.1 Online-Abruf Versichertenstammdaten und Prüfungsnachweis

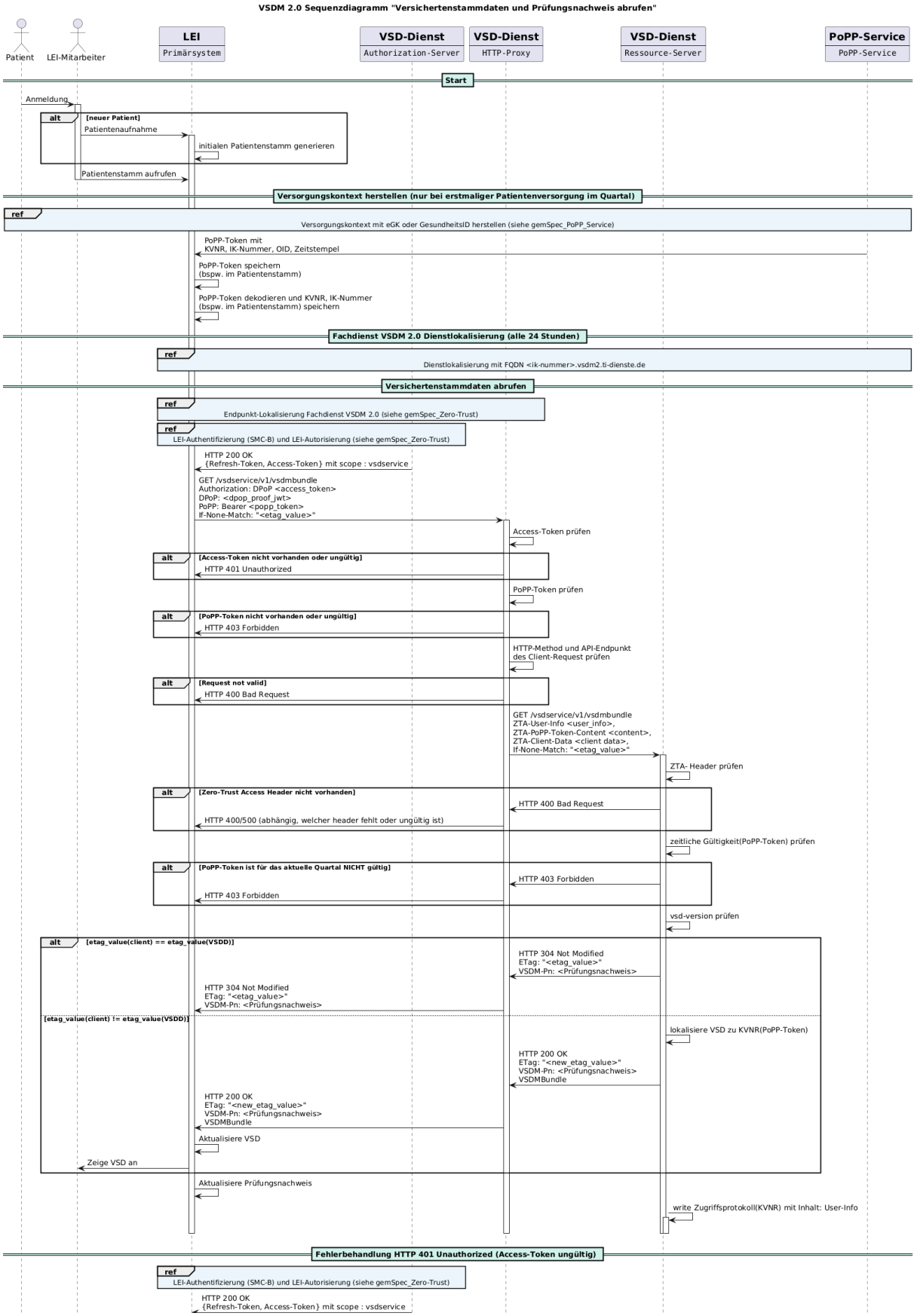
VSDM 2.0 Sequenzdiagramm "Versichertenstammdaten und Prüfungsnachweis abrufen"
Patient
LEI-Mitarbeiter
LEI
Primärsystem
VSD-Dienst
Authorization-Server
VSD-Dienst
HTTP-Proxy
VSD-Dienst
Ressource-Server
PoPP-Service
PoPP-Service
Start
Anmeldung
alt
[neuer Patient]
Patientenaufnahme
initialen Patientenstamm generieren
Patientenstamm aufrufen
Versorgungskontext herstellen (nur bei erstmaliger Patientenversorgung im Quartal)
ref
Versorgungskontext mit eGK oder GesundheitsID herstellen (siehe gemSpec_PoPP_Service)
PoPP-Token mit KVNR, IK-Nummer, OID, Zeitstempel
PoPP-Token speichern (bspw. im Patientenstamm)
PoPP-Token dekodieren und KVNR, IK-Nummer (bspw. im Patientenstamm) speichern
Fachdienst VSDM 2.0 Dienstlokalisierung (alle 24 Stunden)
ref
Dienstlokalisierung mit FQDN <ik-nummer>.vsdm2.ti-dienste.de
Versichertenstammdaten abrufen
ref
Endpunkt-Lokalisierung Fachdienst VSDM 2.0 (siehe gemSpec_Zero-Trust)
ref
LEI-Authentifizierung (SMC-B) und LEI-Autorisierung (siehe gemSpec_Zero-Trust)
HTTP 200 OK {Refresh-Token, Access-Token} mit scope : vsdservice
GET /vsdservice/v1/vsdmbundle
Authorization: DPoP <access_token>
DPoP: <dpop_proof_jwt>
PoPP: Bearer <popp_token>
If-None-Match: "<etag_value>"
Access-Token prüfen
alt
[Access-Token nicht vorhanden oder ungültig]
HTTP 401 Unauthorized
PoPP-Token prüfen
alt
[PoPP-Token nicht vorhanden oder ungültig]
HTTP 403 Forbidden
HTTP-Method und API-Endpunkt des Client-Request prüfen
alt
[Request not valid]
HTTP 400 Bad Request
GET /vsdservice/v1/vsdmbundle
ZTA-User-Info <user_info>,
ZTA-PoPP-Token-Content <content>,
ZTA-Client-Data <client data>,
If-None-Match: "<etag_value>"
ZTA- Header prüfen
alt
[Zero-Trust Access Header nicht vorhanden]
HTTP 400 Bad Request
HTTP 400/500 (abhängig, welcher header fehlt oder ungültig ist)
zeitliche Gültigkeit(PoPP-Token) prüfen
alt
[PoPP-Token ist für das aktuelle Quartal NICHT gültig]
HTTP 403 Forbidden
HTTP 403 Forbidden
vsd-version prüfen
alt
[etag_value(client) == etag_value(VSDD)]
HTTP 304 Not Modified
ETag: "<etag_value>"
VSDM-Pn: <Prüfungsnachweis>
HTTP 304 Not Modified
ETag: "<etag_value>"
VSDM-Pn: <Prüfungsnachweis>
[etag_value(client) != etag_value(VSDD)]
lokalisiere VSD zu KVNR(PoPP-Token)
HTTP 200 OK
ETag: "<new_etag_value>"
VSDM-Pn: <Prüfungsnachweis>
VSDMBundle
HTTP 200 OK
ETag: "<new_etag_value>"
VSDM-Pn: <Prüfungsnachweis>
VSDMBundle
Aktualisiere VSD
Zeige VSD an
Aktualisiere Prüfungsnachweis
write Zugriffsprotokoll(KVNR) mit Inhalt: User-Info
Fehlerbehandlung HTTP 401 Unauthorized (Access-Token ungültig)
ref
LEI-Authentifizierung (SMC-B) und LEI-Autorisierung (siehe gemSpec_Zero-Trust)
HTTP 200 OK
{Refresh-Token, Access-Token} mit scope : vsdservice

Abbildung 3: Sequenzdiagramm VSDM

6 Übergreifende Festlegungen

Der folgende Abschnitt beschreibt übergreifende Anforderungen an den Fachdienst VSDM zur Unterstützung der Fachlogik.

6.1 Systemzeit

A_26799 - Anbieter VSDM - Aktualisierung und Überwachung Systemzeit
Der Anbieter VSDM 2 Fachdienst MUSS die Systemzeit der betriebenen Komponenten (ZT-Komponenten, VSDM Resource Server etc.) des Fachdienstes kontinuierlich überwachen und bei Abweichungen über 15 Sekunden synchronisieren.
[<=, Anb_VSDM_2_FD, organ./betriebl. Eignung: Prozessprüfung**]**

Hinweis: Üblicherweise wird ein VSDM-Betreiber auf den relevanten Serversystemen das NTP-Protokoll zur Zeitsynchronisation gegenüber einer vertrauenswürdigen RZ-lokalen Zeitquelle verwenden. Für die Authentisierung von Abfragenden (LEI und Versicherten) und die Korrektheit der erzeugten Zugriffsprotokolle ist eine korrekte Systemzeit in den Komponenten notwendig, Dabei ist hierbei keine Genauigkeit im Nanosekundenbereich notwendig -- in A_26799 wurde +/-15 Sekunden als fachlich vertretbare Abweichung innerhalb der Komponenten bewertet.

6.2 Fachdienstlokalisierung

Unter Verwendung von DNS-Abfragen im Internet durch den VSDM-Client erfolgt die Lokalisierung der VSDM Schnittstellen. Dafür muss der Anbieter Fachdienst VSDM pro Institutionskennung einen Alias in der übergreifenden Domäne vsdm2.ti-dienste.de bereitstellen. Für die verschiedenen Umgebungen der TI werden third-level Domänen eingerichtet: .ref (RU1), .dev (RU2) und .test (TU).

Jeder VSDM-Client kann unter Verwendung der ermittelten Institutionskennung aus dem PoPP-Token und der Lokalisierung die benötigte Schnittstelle des Fachdienstes VSDM ermitteln.

A_26800 - Anbieter VSDM - CNAME Resource Records für die Lokalisierung
Der Anbieter Fachdienst VSDM MUSS im Internet CNAME Resource Records gemäß folgender Tabelle verwalten.

Tabelle 6 : TAB_FACHDIENST_VSDM_LOKALISIERUNG

Resource Record Bezeichner	Resource Record Type	Beschreibung
<IK-NR>.vsdm2.ti-dienste.de	CNAME	CNAME Resource Record für die Produktivumgebung pro Institutionskennungen mit dem "canonical name"
<IK-NR-XX>.<ref/dev/test>.vsdm2.ti-dienste.de	CNAME	CNAME Resource Record für die Referenz- (ref), Entwicklungs- (dev) und Testumgebung (test) pro Institutionskennungen mit dem "canonical name"

[<=, Anb_VSDM_2_FD, funkt. Eignung: Anbietererklärung**]**

Die Idee, die mit dieser Festlegung verfolgt wird, ist folgende:

Die CNAME Resource Records in den Subdomänen unterhalb von vsdm2.ti-dienste.de werden zentral verwaltet und auf Basis der zugelieferten Informationen bereitgestellt. Der Canonical Name im Resource Record zeigt auf einen FQDN der Betreiber. Dadurch werden die Betreiber ertüchtigt, alle weiteren DNS-Einträge in ihren Nameservern eigenständig zu administrieren.

A_26801 - Anbieter Fachdienst VSDM - FQDN Resource Records für VSDM2
Der Anbieter Fachdienst VSDM MUSS in seinen Nameservern im Internet mindestens einen FQDN, der dem CNAME in der übergreifenden Domäne entspricht, bereitstellen und für die VSDM-Clients auflösen.**[**<=, Anb_VSDM_2_FD, funkt. Eignung: Anbietererklärung**]**

Beispiel zur Lokalisierung der dev - Umgebung für die Institutionskennung *123456789* und Betreiber *betreiber-1*:

```
123456789.dev.vsdm2.ti-dienste.de 86400 IN CNAME
host.dev.vsdm2.betreiber-1.de

host.dev.vsdm2.betreiber-1.de IN A 198.51.100.1
```

A_26802 - Anbieter VSDM - Time To Live Werte für die Resource Records
Der Anbieter Fachdienst VSDM MUSS alle Resource-Records mit einer Time To Live (TTL) von 86400 im Nameserver eintragen. **[**<=, Anb_VSDM_2_FD, funkt. Eignung: Test Produkt/FA (Anwendung), funkt. Eignung: Anbietererklärung**]**

Hinweis: Die TTL-Werte können im Rahmen des Change-Managements verändert werden.

Ist ein Dienstleister für das Management der Domäne und Resource-Records beauftragt worden, muss dieser die Eintragungen in Übereinstimmungen mit den Festlegungen vornehmen.

Die in TAB_VSDM_Lokalisierung genannte `IK-NR-XX` für die Referenz-, Test- und Entwicklungsumgebung des jeweiligen Anbieters eines Fachdienstes VSDM ist zum aktuellen Zeitpunkt noch nicht festgelegt, wird sich aber vermutlich nach den entsprechenden Nummern der eGK-Testkarten richten.

6.3 Systemprotokolle

Der Fachdienst VSDM muss Protokolldateien schreiben, die eine Analyse technischer Vorgänge erlauben. Diese Protokolldateien sind dafür vorgesehen, aufgetretene Fehler zu identifizieren und die Performance zu analysieren. Für diese Zwecke führt der Fachdienst VSDM ein Systemprotokoll, mit dem der Anbieter des Dienstes jederzeit den Betriebszustand des Systems kontrollieren kann.

A_26803 - Fachdienst VSDM - Systemprotokoll für Betriebszustand
Der Fachdienst VSDM MUSS ein Systemprotokoll über durchgeführte Operationen und deren Erfolg/Misserfolg führen, um dem Anbieter des Dienstes jederzeit eine Übersicht über den aktuellen Betriebszustand zu ermöglichen.**[**<=, VSDM_2_FD, funkt. Eignung: Herstellererklärung**]**

A_26804 - Fachdienst VSDM - Systemprotokoll für Fehlerbehebung
Der Fachdienst VSDM MUSS insbesondere Operationen mit dem Ergebnis eines Misserfolges derart protokollieren, dass die Fehlerursache nachvollzogen und der Fehler durch den Anbieter des Fachdienstes VSDM behoben werden kann.
[<=, VSDM_2_FD, funkt. Eignung: Herstellererklärung**]**

A_26805 - Fachdienst VSDM - Systemprotokoll ohne personenbezogene und ohne medizinische Daten
Der Fachdienst VSDM MUSS in jedem zu tätigenden Systemprotokolleintrag alle personenbezogenen, personenbeziehbaren und medizinischen Informationen vor der Speicherung entfernen, damit vom administrativen Personal keine personenbezogenen Daten der Versicherten oder Leistungserbringer eingesehen werden können.
[<=, VSDM_2_FD, Sich.techn. Eignung: Gutachten**]**

A_26806 - Anbieter VSDM - Systemprotokoll Verfügbarkeit interner Logdaten
Der Anbieter eines Fachdienstes VSDM MUSS im Rahmen von Testmaßnahmen dem Testbetriebsverantwortlichen auf Anforderung die Log-Dateien des Systemprotokolls übermitteln.**[**<=, Anb_VSDM_2_FD, funkt. Eignung: Anbietererklärung**]**

A_26807 - Anbieter VSDM - Systemprotokoll Aufbewahrungsfristen
Der Anbieter eines Fachdienstes VSDM MUSS die Systemprotokolle mindestens sechs Monate verfügbar halten.**[**<=, Anb_VSDM_2_FD, funkt. Eignung: Anbietererklärung**]**

Hinweis: Die Systemprotokolle können nach Ablauf der Aufbewahrungsfrist gelöscht werden.

6.4 Berechtigungen

Grundsätzlich ist jede Leistungserbringerinstitution mit einer gültigen SM(C)-B für das Lesen der Versichertenstammdaten von der eGK und zusätzlich mit einem vorhandenen sowie gültigen Versorgungskontext (PoPP-Token) für den Online-Abruf der Versichertenstammdaten berechtigt.

A_26808 - Anbieter Fachdienst VSDM - Erlaubte Akteure

Der Anbieter eines Fachdienstes VSDM MUSS sicherstellen, dass für UC_1 und UC_3 die entsprechend gelisteten Berechtigungsregeln durchgesetzt werden:

Tabelle 7 : TAB_FACHDIENST_VSDM_BERECHTIGUNGSREGELN

Akteur	**UC_1 VSD von VSDD abrufen**	**UC_2 VSD von eGK lesen**	**UC_3 Zugriffsprotokoll einsehen**
Leistungserbringerinstitution	X	X	nicht erlaubt
Mitarbeiter Institution des Kostenträgers	nicht anwendbar	nicht vorgesehen	nicht erlaubt
Versicherter	nicht vorgesehen	nicht vorgesehen	X
Admin einer Organisation oder Institution des Gesundheitswesens	nicht erlaubt	nicht erlaubt	nicht erlaubt
Mitarbeiter des VSDD-Betreibers	nicht erlaubt	nicht erlaubt	nicht erlaubt
nicht registrierter Client	nicht erlaubt	nicht anwendbar	nicht anwendbar
nicht identifizierbarer oder nicht gesetzlich mandatierter Akteur	nicht erlaubt	nicht anwendbar	nicht erlaubt

[<=, Anb_VSDM_2_FD, funkt. Eignung: Anbietererklärung**]**

Erläuterung: X = der fachliche Akteur ist berechtigt

Hinweis: Die Regeln im Kontext UC_1 für Zugriffe auf die Fachdienst VSDM API `/vsdservice` werden technisch durch das Zero-Trust Cluster durchgesetzt.

6.5 Authentifizierung und Autorisierung von Nutzern

Die Authentifizierung von Nutzern bzw. Leistungserbringerinstitutionen (LEI) erfolgt durch die Zero-Trust Komponente "Authorization Server" und auf Basis der SMC-B (zukünftig auch SM-B). Eine erfolgreiche LEI-Authentifizierung ist Voraussetzung für die Durchführung der Autorisierung, die im Erfolgsfall mit der Ausgabe eines Refresh- und Access-Token für die LEI endet. Die Autorisierung erfolgt auf Basis der in der VSDM-Policy hinterlegten Regeln. Die Authentisierungsabläufe mit SMC-B in der LEI-Umgebung werden durch die logische Zero-Trust Komponente "Trust-Client" realisiert und durch den VSDM Authorization-Server (SW-Komponente des Zero-Trust Clusters) durchgesetzt.

VSDM-spezifische Anforderungen sind im Kapitel 4.2.2- Authorization-Server Konfiguration beschrieben. Das konkrete Regelwerk in Form einer VSDM-Policy ist unter [VSDM-Policy] hinterlegt.

Allgemeingültige Anforderungen im Rahmen der Authentifizierung und Autorisierung einer Leistungserbringerinstitution sind der Spezifikation [gemSpec_Zero_Trust] und dem Produkttypsteckbrief [gemProdT_VSDM_2_FD] zu entnehmen.

6.6 HTTP Status Codes

Der Fachdienst VSDM stellt eine http-Schnittstelle für den Aufruf durch Clientsysteme bereit. Das Ergebnis der Operation wird in der Verwendung von Http-Status-Codes gemäß [RFC2616] mitgeteilt. Die folgende Tabelle listet die vom Fachdienst VSDM genutzten Http-Status-Codes auf.

Tabelle 8 : TAB_FACHDIENST_VSDM_HTTP_STATUS_CODES

Client Registry	
siehe [gemSpec_Zero_Trust]	
Authorization-Server	
siehe [gemSpec_Zero_Trust]	
HTTP-Proxy	
siehe [gemSpec_Zero_Trust]	
Resource-Server GET /vsdservice/v1/vsdmbundle	
HTTP-Status-Code	**Statusmeldung für Clientsysteme inkl. Fehlermeldungen gemäß 4.3.1.4- Fehlermeldungen**
200	Anfrage konnte erfolgreich bearbeitet werden. Versichertenstammdaten (VSDMBundle) und Prüfungsnachweis sind in der Antwort enthalten.
304	Anfrage konnte erfolgreich bearbeitet werden. Das Clientsystem besitzt schon die aktuellsten Versichertenstammdaten und es erfolgt keine Aktualisierung. Der Prüfungsnachweis ist in der Antwort enthalten.
400	79010 79011 79030 79031 79032 79205 79206 79207 79400 79401 79402

403	79000 79041
404	79020
405	79040
412	79032
428	79033
500	79100
502	79110
504	79111

6.7 Zero-Trust Cluster

A_26809 - Anbieter VSDM - Zero-Trust Cluster Informationspflicht via Betriebshandbuch
Der Anbieter eines Fachdienst VSDM MUSS alle Informationen und Regelungen zu Bereitstellung, Konfiguration und Verwendung des Zero Trust Clusters dem Betriebshandbuch des Zero Trust Cluster Herstellers entnehmen und anwenden. **[**<=, Anb_VSDM_2_FD, Sich.techn. Eignung: Gutachten (Anbieter)**]**

A_26810 - Anbieter VSDM - Zero-Trust Cluster VSDM Policy erstellen
Der Anbieter eines Fachdienst VSDM MUSS bei der Erstellung der Policy für den PoPP Service mit der gematik zusammenarbeiten. Diese Policy wird über den PAP deployed und durch die Policy-Engine verarbeitet. **[**<=, Anb_VSDM_2_FD, funkt. Eignung: Anbietererklärung**]**

Hinweis: Die PoPP-Service Policy wird in GIT erstellt (CID-Prozess).

A_26811 - Anbieter VSDM - Zero-Trust Cluster Konfigurationsdateien erstellen
Der Anbieter eines Fachdienst VSDM MUSS die Konfigurationen (Manifest-Dateien) des Zero Trust Clusters für alle Umgebungen (Produktiv-, Referenz-, Test-, Entwicklungsumgebung) im GIT erstellen, diese werden durch die gematik geprüft und freigegeben.**[**<=, Anb_VSDM_2_FD, funkt. Eignung: Anbietererklärung**]**

Hinweis: Die Erstellung und das Deployment werden durch einen CID-Prozess gesteuert.

6.8 Sicherheit und Datenschutz

Ein VSDM2-FD bewahrt Zugriffsprotokolle für Versicherte ein Jahr auf (vgl. Abschnitt 4.3.5) und macht diese den Versicherten nach sicherer Authentisierung lesbar.

Anforderungen an den Anbieter bzw. Betreiber ergeben sich, wie für alle andere Fachdienste der TI, aus [gemSpec_DS_Anbieter] und sind dem Anbietertypsteckbrief zugewiesen.

A_26969 - Anbieter VSDM - Verbot Profilbildung
Der Anbieter (im Sinne eines Betreibers) eines Fachdienst VSDM DARF Profile - außer zum Zweck des Logging oder Monitorings - NICHT bilden.**[**<=, Anb_VSDM_2_FD, Sich.techn. Eignung: Gutachten (Anbieter)**]**

A_26970 - Anbieter VSDM - Verarbeitung von Profildaten
Der Anbieter (im Sinne eines Betreibers) eines Fachdienst VSDM MUSS Daten zum Zwecke des Loggings oder Monitorings, die für eine Profilbildung genutzt werden können, ausschließlich zum Zweck der Fehlererkennung und Fehlerbehandlung verarbeiten und nutzen.**[**<=, Anb_VSDM_2_FD, Sich.techn. Eignung: Gutachten (Anbieter)**]**

A_26971 - Anbieter VSDM - Verbot der Datenweitergabe
Der Anbieter (im Sinne eines Betreibers) eines Fachdienst VSDM DARF NICHT Daten an Dritte weitergegeben. Dies betrifft insbesondere personenbeziehbare (medizinische) Daten oder Daten, die für eine Profilbildung genutzt werden können. Anforderungen des Anbietertypsteckbriefes VSDM sind hiervon nicht betroffen.
[<=, Anb_VSDM_2_FD, Sich.techn. Eignung: Gutachten (Anbieter)**]**

Hinweis zur Profilbildung: Dies betrifft in besonderem Maße Daten, aus denen Rückschlüsse über ein dediziertes Arzt-Patienten-Verhältnis gezogen werden können.

6.9 Betrieb

In diesem Kapitel werden übergreifende, betriebliche Anforderungen getroffen oder auf Kapitel mit speziellen Ausprägungen für den Fachdienst VSDM in normativen Querschnittsdokumenten verwiesen.

Folgende, produktspezifische Vorgaben werden getroffen:

6.9.1 Schnittstellen und Anwendungsfälle

Die vom Fachdienst VSDM zur Verfügung gestellten Schnittstellen und Anwendungsfälle werden im entsprechenden Kapitel von [gemKPT_Betr] dargestellt.

6.9.2 Leistungsanforderungen und Performance

Die vom Fachdienst VSDM zu leistenden Performancevorgaben werden im entsprechenden Kapitel von [gemSpec_Perf] dargestellt. Dazu gehören insbesondere Vorgaben zur Verfügbarkeit, eingesetzten Redundanz und der Leistungsfähigkeit der Schnittstellenabrufe. Darüber hinaus werden Vorgaben zur Verarbeitung der eingesetzten Datenliefermodelle gemacht, die sich sowohl auf den Fachdienst, als auch organisatorisch auf den entsprechenden Anbieter beziehen, welcher diese Datenlieferungen gewährleisten muss.

6.9.3 Migration

Es ist vereinbart, dass ein definierter Zeitraum für die Migration von VSDM 1 zu VSDM 2 vorgesehen wird. Dabei kommt es zum Parallelbetrieb von VSDM 1 und VSDM 2. Dabei wird es notwendig sein, dass die angestrebte Transition mittels qualifizierter Unterstützungsleistungen von gematik und den Anbietern intensiv betreut wird.

6.9.3.1 Verfahren zum Umgang mit der strukturierten Prüfziffer

Das Verfahren der strukturierten Prüfziffer als Zugriffselement auf andere TI-Dienste aus dem Vorgängersystem VSDM 1 wird nicht weitergeführt. Stattdessen wird der originäre Sinn der Prüfziffer genutzt, um die Prüfung auf einen kryptografisch sichergestellten Abruf der Versichertenstammdaten - und damit die Abrechnungsgrundlage - zu ermöglichen. Um die Migration von TI 1.0 auf die TI 2.0 im Übergang flexibel zu gestalten, wird zukünftig übergangsweise der PoPP-Service eine strukturierte Prüfziffer ausschließlich zur Benutzung als Zugriffselement auf andere TI-Dienste anbieten. Perspektivisch soll durch die Akzeptanz von PoPP-Token anderer TI-Dienste (TI 2.0 Readiness) diese Notwendigkeit ersatzlos entfallen. In Zukunft ist es vorgesehen, dass der PoPP-Token (ohne die strukturierte Prüfziffer) als Nachweismerkmal des Behandlungskontextes den Zugriff auf andere TI 2.0 Dienste mit ermöglicht.

6.10 Test

Die Teststrategie der gematik für die TI 2.0 Anwendungen befindet sich aktuell in der Abstimmung mit den Gesellschaftern. Das daraus abzuleitende konkrete Testkonzept für VSDM und die daraus resultierenden Anforderungen an die VSDM Umsetzung sind dadurch noch nicht für eine Vorveröffentlichung verbindlich festgelegt.

Sobald die Teststrategie der gematik abgestimmt ist, wird dieses Kapitel entsprechend angepasst.

6.11 Zulassung Fachdienste

Die Zulassung/Bestätigung für die VSDM 2 Fachdienste, bezüglich deren funktionalen, betrieblichen und weiteren Anforderungen an das Produkt selbst und an den Betrieb der Lösung gliedert sich in die nachfolgenden Zulassungen/Bestätigungen auf.

Produktzulassung:
Der Fachdienst VSDM erhält eine Produktzulassung.

Anbieterzulassung:
Die Anbieterzulassung muss durch die Organisation bzw. das Unternehmen beantragt werden, die bzw. das die Einhaltung der im Anbietertypsteckbrief adressierten Anforderungen vollumfänglich selbst oder im Rahmen seiner bestehenden Vertrags- und Rechtsverhältnisse um- bzw. durchsetzen kann. Aus der Anbieterrolle kann sich eine datenschutzrechtliche Verantwortlichkeit aus § 307 SGB V ergeben. - Hier ist somit der Antragsteller die Krankenkasse.

Betreiberbestätigung:
Wenn der Anbieter des Fachdienstes VSDM einen Betreiber des Fachdienstes VSDM

beauftragt hat, kann der Nachweis der betrieblichen Eignung durch den Betreiber in einem gesonderten Bestätigungsverfahren erbracht werden, welches ein Vorverfahren zur Zulassung Anbieter Fachdienstes VSDM ist.

Ausblick:

Die gematik strebt an, das Konstrukt der Anbieterzulassungen der einzelnen konkreten Kasse für die verschiedenen Produkte (VSDM und weitere) zu optimieren.

6.12 Verfahren für Primärsysteme

Es ist vorgesehen für Primärsysteme ein Bestätigungsverfahren zum Nachweis der spezifikationskonformen Umsetzung der Anforderungen, die die Interoperabilität zwischen den Primärsystemen und der TI bzw. den für VSDM 2 benötigten Diensten sicherstellen, durchzuführen.

7 Informationsmodell

Die Informationsmodelle des systemspezifischen Konzepts VSDM leiten sich aus dem fachlichen Informationsmodell des Konzeptes VSDM ab.

7.1 Informationsmodell VSDM online

Die Spezifikation des fachlichen Informationsmodells erfolgt in Form von FHIR-Profilen im simplifier-Projekt https://simplifier.net/vsdm2, die als FHIR-Package in einer semantischen Versionierung veröffentlicht und gemanaged werden.

7.2 Informationsmodell verkürzte VSD auf eGK

Entsprechend den Vorgaben des SGB V werden die VSD auf der eGK nur noch in einem reduzierten Umfang abgelegt, der auch nicht mehr online aktualisiert wird. Diese Daten sind ab dieser VSDM Version nicht mehr relevant. Der Leistungserbringer kann jedoch zur Anwendung von Ersatzverfahren weiterhin auf diese Daten zugreifen. Diese Ersatzverfahren sind nicht Gegenstand der Anwendung VSDM.

Zukünftig werden nur noch folgende Daten auf neu ausgegebene elektronische Gesundheitskarten abgelegt:

Tabelle 9 : Übersicht der auf der eGK bereitgestellten Daten

Container	Feld	Beschreibung
Allgemeine Versichertendaten	Name	Name des Kostenträgers
	Kostenträgerkennung	Gibt den Kostenträger des Versicherten an. Es handelt sich um das bundesweit gültige Institutionskennzeichen (IK) des jeweiligen Kostenträgers.
Persönliche Versicherungsdaten	Versicherten_ID	Die Versicherten-ID ist der 10-stellige unveränderliche Teil der 30-stelligen Krankenversichertennummer.
	Vorname	Gibt den Vornamen der Person an.
	Nachname	Gibt den Nachnamender Person an.
	Geburtsdatum	Gibt das Geburtsdatum des Versicherten an.

7.3 Prüfungsnachweis

Der Prüfungsnachweis dient als Nachweis über die Durchführung eines Versichertenstammdatenabrufes für das laufende Quartal und wird bei jedem Abruf an das Clientsystem übermittelt. Für die Erstellung der Abrechnungsunterlagen kann nur der vom Fachdienst VSDM übermittelte Prüfungsnachweis verwendet werden. Der durch den PoPP-Service im Rahmen der Herstellung des Behandlungskontextes übermittelte Prüfungsnachweis darf nicht verwendet werden.

A_26965 - Fachdienst VSDM - Resource Server - Erzeugung Prüfungsnachweis
Der Resource Server VSDM MUSS den Prüfungsnachweis entsprechend dem nachfolgend aufgeführten `Informationsmodell Prüfungsnachweis` erzeugen

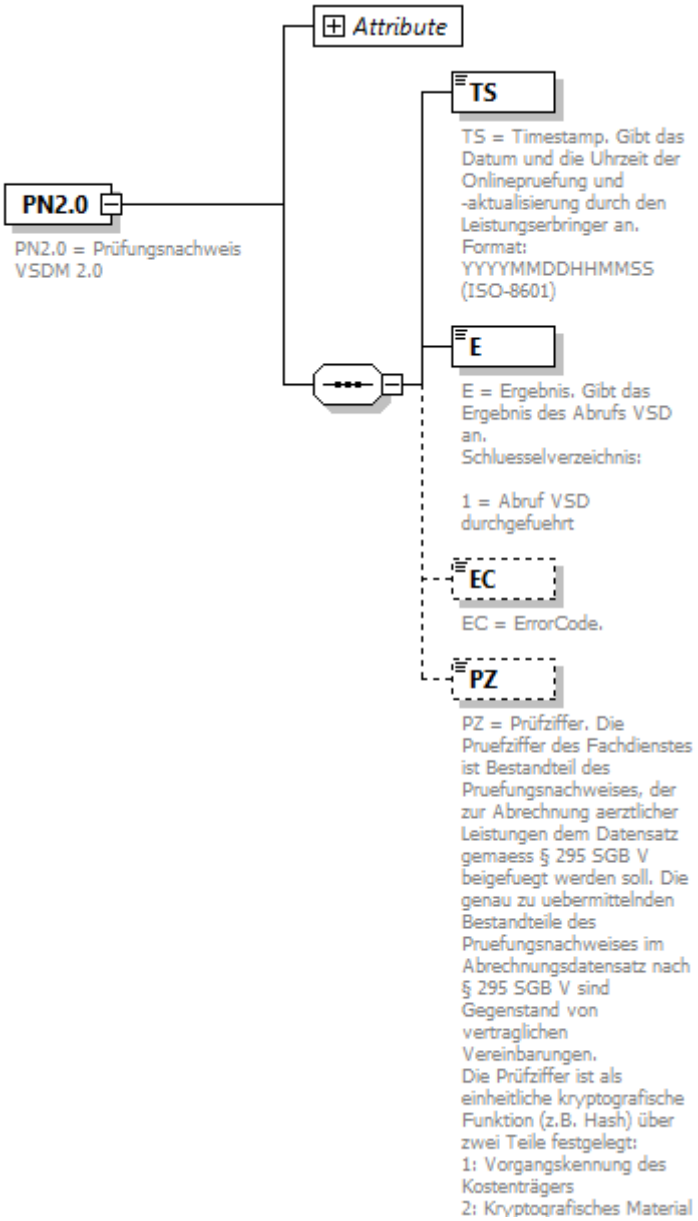

Abbildung 4 : Informationsmodell Prüfungsnachweis

und mit folgenden Feldern befüllen:

Tabelle 10 : TAB_FACHDIENST_VSDM_STRUKTUR_PRÜFUNGSNACHWEIS

CDM:Version	Enthält die logische Version 1.0.0 für fachliche Datenstrukturen („Corresponding Data Modell“, Versionskennung mit Bezug zum jeweiligen Architektur-Modell).
Timestamp	Aktueller Zeitstempel UTC
Ergebnis	Ergebnis der Abrufs VSD 1= Abruf VSD durchgeführt
ErrorCode	./.
Prüfziffer	Vom Fachdienst VSDM gesendete Prüfziffer

[<=, VSDM_2_FD, funkt. Eignung: Test Produkt/FA**]**

A_26900 - Clientsystem VSDM - Verwendung Prüfungsnachweis für Abrechnungsunterlagen
Das Clientsystem VSDM MUSS zur Erstellung der Abrechnungsunterlagen die Werte aus dem vom Fachdienst VSDM gelieferten Prüfungsnachweis verwenden.
[<=, CS_VSDM_2, funkt. Eignung: Konformitätsbestätigung**]**

A_26901 - Clientsystem VSDM - Nichtverwendung Prüfungsnachweis PoPP-Service für Abrechnungsunterlagen
Das Das Clientsystem VSDM DARF NICHT Werte aus dem vom PoPP-Service übermittelten Prüfungsnachweis zur Erstellung der Abrechnungsunterlagen verwenden.
[<=, CS_VSDM_2, funkt. Eignung: Konformitätsbestätigung**]**

7.3.1 Aufbau der Prüfziffer

A_26966 - VSDM Resource Server -Erzeugung der Prüfziffer
Der Resource Server VSDM MUSS für die Erzeugung der Prüfziffer folgende Struktur erstellen:

Tabelle 11 : Struktur der Prüfziffer

Nr	Feld	Format	Länge
1	10-stelliger unveränderlicher Teil der KVNR	alphanummerisch	10
2	aktuelle Unix-Zeit (bspw. "1673551622")	alphanummerisch	10
3	Ausstellender Dienst 2 - VSDM	alphanummerisch	1
4	Kennung des Betreibers Fachdienste VSDM gemäß Liste der gematik	alphanummerisch	1

5	Für den Betreiber des Fachdienstes spezifische Version des HMAC-Schlüssels	alphanummerisch	1
6	Es wird ein HMAC nach A_23461-* über die konkatenierten Felder 1-5 mittels des betreiberspezifischen Schlüssel berechnet. Dieser berechnete HMAC-Wert (256-Bit) wird auf 192 Bit (also 24 Byte) gekürzt (die ersten 24 Byte des HMAC-Wertes werden verwendet, die restlichen 8 Byte werden verworfen). Dieser gekürzte HMAC-Wert ist das 6-te Datenfeld.	binär	24

[<=, VSDM_2_FD, funkt. Eignung: Test Produkt/FA**]**

Hinweise:

Die Liste der Kennungen der Betreiber wird von der gematik bereitgestellt.

Die Ausgabelänge der HMAC(SHA-256)-Hashfunktion ist 32 Byte lang. Für die Prüfziffer werden die ersten 24 Byte verwendet. Die restlichen 8 Bytes werden verworfen.

Die gemäß A_26766 kodierte Datenstruktur ist die Prüfziffer.

7.4 Zugriffsprotokoll für Versicherte

A_26812 - VSDM Resource Server - Zugriffsprotokoll Versicherte - Protokolleintrag
Der VSDM Resource Server MUSS bei jedem Aufruf der HTTP-GET Operation auf den Endpunkt `/vsdservice/v1/vsdmbundle` und damit auf die dedizierten Versichertenstammdaten folgende Informationen protokollieren:

Tabelle 12 : Informatiosmodell_Zugrifssprotokoll

Information	Protokollelement	Protokollwert
Wann ist der Zugriff erfolgt?	Zugriffszeitpunkt	Zeitangabe kodiert im Format nach ISO-8601 Beispiel: "2024-11-22T10:00:00.123456"
Wer hat zugegriffen?	LEI	<CommonName> (aus dem HTTP-Header`ZTA-User-Info`)
	Organisations-bezeichnung	<organizationName> (aus dem HTTP-Header`ZTA-User-Info`)
	LEI-ID	<Telematik-ID> (aus dem HTTP-Header`ZTA-User-Info`)
Worauf wurde zugegriffen?	Daten	"Versichertenstammdaten"

Welcher Art war der Zugriff?	Aktion	"lesen"
War der Zugriff erfolgreich?	Ergebnis	"Versichertenstammdaten übermittelt." ODER "Versichertenstammdaten angefragt - Versichertenstammdatenübermittlung nicht notwendig." ODER "Zugriff verweigert."

[<=, VSDM_2_FD, funkt. Eignung: Test Produkt/FA**]**

Hilfestellung zu ISO-8601:

Code-Beispiel in python

datetime datetime.datetime.now().isoformat() >>> '2024-10-16T14:38:32.489558'

7.5 VSDM-Policy

Die VSDM-Policy wird von der gematik erstellt und gemäß [gemSpec_Zero_Trust] über den Policy Administration Point (PAP) dem Anbieter eines Fachdienstes VSDM bereitgestellt.

7.6 VSDM-spezifische Konfigurationsdaten Zero-Trust Cluster

Die VSDM-spezifische Konfigurationen für die Komponenten des Zero-Trust Cluster müssen von dem Anbieter eines VSDM Fachdienstes nach dem Verfahren gemäß [gemSpec_Zero_Trust] erstellt werden. Die zugehörigen Konfigurationsdateien (Manifest-Dateien) werden dem Anbieter eines Fachdienstes VSDM über das Zero-Trust Cluster Repository bereitgestellt. Wesentliche Konfigurationsdaten sind bspw. zu setzende Routen, Firewall-Regeln, Entity-Statements etc.

Die Manifest-Dateien werden dem Anbieter eines Fachdienstes VSDM als Templates zur Verfügung gestellt. Diese Templates beinhalten auch von der gematik festgelegte Konfigurationsdaten.

8 Anhang A – Verzeichnisse

8.1 Abkürzungen

Kürzel	Erläuterung
AuthZ-Server	Authorization-Server
DNS	Domain Name System
eH-KT	eHealth-Kartenterminal
eGK	elektronische Gesundheitskarte
JWKS	JSON Web Key Set
LE	Leistungserbringer
LEI	Leistungserbringerinstitution
OCSP	Online Certificate Status Protocol
OCSP-Responder	Online Certificate Status Protocol Responder
PAP	Policy Administration Point
PoPP	Proof-of-Patient-Presence
PoPP-Service	Proof-of-Patient-Presence Dienst
SMC-B	Secure Module Card Type B
SM-B	Secure Module Type B
VSD	Versichertenstammdaten
VSDD	Versichertenstammdatendienste
VSDM	Versichertenstammdatenmanagement
VSDM 2.0	Versichertenstammdatenmanagement V2.0
ZT	Zero-Trust

8.2 Glossar

Begriff	Erläuterung
Authorization-Server	Ist im Kontext VSDM eine Komponente des ZT-Cluster zur Authentifizierung und Autorisierung von Leistungserbringerinstitutionen für die Anwendung VSDM.
Clientsystem	Bezeichnung für dezentrale Systeme, die als Clients mit dem Fachdienst VSDM interagieren, jedoch ohne Bestandteil der TI zu sein (z.B. PVS-, AVS-, KIS-Systeme). Sie bestehen aus Hard- und Software-Bestandteilen.
Domain Name System	Löst die Fachdienst-spezifischen Fully Qualified Domain Names (FQDN) in IP-Adressen des Internets auf.
Fachdienst VSDM	Zentraler Teil der Fachanwendung VSDM.
Federation Master	Der Federation Master basiert auf den Standards OpenID Connect (OIDC), Open Authorization 2.0 (OAuth 2) und JSON Web Token (JWT). Der Federation Master ist einerseits der Trust Anchor des Vertrauensbereichs der Föderation. Andererseits stellt der Federation Master Schnittstellen bereit, welche Auskunft über die in der Föderation registrierten sektoralen IDP gibt.
FHIR Ressourcen	Der Standard „FHIR“® (Fast Healthcare Interoperability Resources wurde von Health Level Seven International (HL7) ins Leben gerufen. Der Standard unterstützt den Datenaustausch zwischen Softwaresystemen im Gesundheitswesen.
Funktionsmerkmal	Der Begriff beschreibt eine Funktion oder auch einzelne, eine logische Einheit bildende Teilfunktionen der TI im Rahmen der funktionalen Zerlegung des Systems.
GesundheitsID	Elektronische Identität eines Akteurs im Gesundheitswesen.
GesundheitsID-Versicherte	Elektronische Identität eines Versicherten.
JSON Web Key Set Dokument	Ein JSON Web Key Set (JWKS) Dokument enthält ein Set von öffentlichen Schlüsseln eines asymmetrischen kryptografischen Verfahrens. Diese Schlüssel werden zur Prüfung von JSON Web Token (JWT) verwendet.
Leistungserbringer	Ein Leistungserbringer gehört zu einem zugriffsberechtigten Personenkreis nach § 352SGB V und erbringt Leistungen des Gesundheitswesens für Versicherte. Nach § 339 SGB V darf er auf Versichertendaten in Anwendungen der Telematikinfrastruktur zugreifen.

Leistungserbringerinstitution	Die in organisatorischen Einheiten oder juristischen Perso-nen zusammengefassten Leistungserbringer (z.B. Arztpra-xen, Krankenhäuser).
LEI-Authentifizierung	Identitätsprüfung einer Leistungserbringerinstitution auf Basis der SM(C)-B.
OCSP-Responder	Der OCSP-Responder ermöglicht die Statusprüfungen von X.509 Zertifikaten.
Policy Administration Point	Ein Policy Administration Point ist eine wichtige Komponente in der TI 2.0 für die Zugriffskontrolle. Er ist für die Erstellung, Verwaltung und Aktualisierung von Sicherheitsrichtlinien verantwortlich, die die Zugriffskontrollen von Anwendungen und Diensten der TI 2.0 regeln.
Primärsystem	Ein IT-System, das bei einem Leistungserbringer eingesetzt wird – z.B. eine Praxisverwaltungssoftware (PVS), ein Zahnarztpraxisverwaltungssystem (ZVS), ein Kranken-hausinformationssystem (KIS) oder eine Apothekensoft-ware (AVS) – und sich unter dessen administrativer Hoheit befindet. Das Primärsystem ist kein Bestandteil der TI.
Proof-of-Patient-Presence	Bezeichnet das Leistungsmerkmal der technischen Prüfung über einen aktuell bestehenden Versorgungskontext zwischen einer dedizierten Leistungserbringerinstitution und einem Versicherten. Dieser Versorgungskontext kann über den technischen Nachweis in Form eines PoPP-Tokens von Anwendungen und Diensten geprüft werden.
TI-Gateway	Dienst der Telematikinfrastruktur, der die Funktion eines Zugangsdienst und Teilfunktionen des Konnektors zusammenfasst.
VSDM	Fachanwendung Versichertenstammdatenmanagement
Zero-Trust	Ist ein Sicherheitskonzept im Bereich der Informationstechnologie (IT), das davon ausgeht, dass kein Benutzer, Gerät oder Netzwerk von Natur aus vertrauenswürdig ist.

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

8.3 Abbildungsverzeichnis

8.4 Tabellenverzeichnis

8.5 Referenzierte Dokumente

8.5.1 Dokumente der gematik

Die nachfolgende Tabelle enthält die Bezeichnung der in dem vorliegenden Dokument referenzierten Dokumente der gematik zur Telematikinfrastruktur.

[Quelle]	Herausgeber: Titel
[gemGlossar]	gematik: Einführung der Gesundheitskarte – Glossar
[gemILF_PS]	gematik: Implementierungsleitfaden Primärsysteme – Telematikinfrastruktur (TI)
[gemKPT_Betr]	gematik: Betriebskonzept Online-Produktivbetrieb
[gemSpec_DS_Anbieter]	gematik: Spezifikation Datenschutz- und Sicherheitsanforderungen der TI an Anbieter
[gemSpec_Krypt]	gematik: Übergreifende Spezifikation "Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur"
[gemSpec_Perf]	gematik: Übergreifende Spezifikation "Performance und Mengengerüst TI-Plattform"
[gemSpec_PoPP_Service]	gematik: Spezifikation Proof of Patient Presence Service (PoPP-Service)
[gemSpec_Zero_Trust]	gematik: Spezifikation Zero-Trust
[gemAnbT_VSDM_2_FD]	gematik: Anbietertypsteckbrief Anbieter VSDM 2 Fachdienst

[gemProdT_VSDM_2_FD]	gematik: Produkttypsteckbrief VSDM 2 Fachdienst
[VSDMErrorcodeVS]	gematik: FHIR ValueSet für die Anwendung VSDM https://simplifier.net/vsdm2/vsdm-errorcode-vs
[VSDM-Konfigurationsdatei]	gematik: Konfigurationsdatei(en) für das Zero-Trust Cluster eines Fachdienst VSDM [Referenz steht noch nicht fest.]
[VSDM-Policy]	gematik: von der Policy Enginge zu verarbeitende Berechtigungsregeln für den Zugriff auf einen Fachdienst VSDM [Referenz steht noch nicht fest.]
[OpenAPI_VSDM_2]	gematik: OpenAPI Spezifikation VSDM https://github.com/gematik/spec-VSDM2/blob/main/src/openapi/vsdm2.yaml
[Prüfungsnachweis.xsd]	gematik: XML-Schemadatei zur Erstellung eines Prüfungsnachweises https://github.com/gematik/spec-VSDM2/blob/main/src/vsds/vsdmpruefungsnachweis2.xsd
[FHIR-Profil VSDMPatient]	gematik: FHIR-Profil für die FHIR-Resource VSDMPatient https://simplifier.net/vsdm2/vsdmpatient
[FHIR-Profil VSDMCoverage]	gematik: FHIR-Profil für die FHIR-Resource VSDMCoverage https://simplifier.net/vsdm2/vsdmcoverage
[FHIR-Profil VSDMBundle]	gematik: FHIR-Profil für die FHIR-Resource VSDMBundle https://simplifier.net/vsdm2/vsdmbundle
[FHIR-Profil VSDMOperationOutcome]	gematik: FHIR-Profil für die FHIR-Resource VSDMOperationOutcome https://simplifier.net/vsdm2/vsdmoperationoutcome

8.5.2 Weitere Dokumente

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[FHIR-Resource Bundle]	HL7: https://build.fhir.org/bundle.html
[FHIR-Resource Patient]	HL7: https://build.fhir.org/patient.html
[FHIR-Resource Coverage]	HL7: https://build.fhir.org/coverage.html
[FHIR-Resource OperationOutcome]	HL7: https://build.fhir.org/operationoutcome.html

[CAB-Forum]	CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates https://cabforum.org/baseline-requirements-documents/
[RFC1952]	Network Working Group: GZIP file format specification version 4.3 https://www.rfc-editor.org/rfc/rfc1952.html
[RFC2119]	Network Working Group: Key words for use in RFCs to Indicate Requirement Levels https://www.rfc-editor.org/rfc/rfc2119
[RFC2616]	Network Working Group: Hypertext Transfer Protocol -- HTTP/1.1 https://www.rfc-editor.org/rfc/rfc2616.html
[RFC4648]	Network Working Group: The Base16, Base32, and Base64 Data Encodings https://www.rfc-editor.org/rfc/rfc4648.html
[RFC7232]	Internet Engineering Task Force: Hypertext Transfer Protocol (HTTP/1.1): Conditional Requests https://www.rfc-editor.org/rfc/rfc7232.html
[RFC9457]	Internet Engineering Task Force: Problem Details for HTTP APIs https://www.rfc-editor.org/rfc/rfc9457.html

8.6 Klärungsbedarf <<optional>>

Kapitel	Offener Punkt	Zuständig

8.7 Allgemeine Erläuterungen <<optional>>

<<hier können die Interfaces und Operationen mit Verweis auf die jeweilige Seite gelistet werden. Lesehilfe zur Auflösung von Querbezügen>>