

Telematikinfrastruktur 2.0

Spezifikation Versichertenstammdaten- management 2.0 (VSDM 2.0)

Version:	1.1.0-0_CC
Revision:	12740341280558
Stand:	04-0330.06.2025
Status:	zur Abstimmung freigegeben
Klassifizierung:	öffentlich_Entwurf
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	04.03.2025		Initiale Version	gematik
1.0.1	01.04.2025	Kap. 4.3.1 Kap. 4.3.2 Kap. 6.2	A_26754: ZETA-Client-Data Header gestrichen A_26755: Rückgabewert von 400 zu 428 geändert A_26774: ETag-Value für JSON/XML konkretisiert A_26800: FQDN für Produktionsumgebung korrigiert	gematik
1.1.0_CC	30.06.2025	Kap. 3 Kap. 4.1.2 Kap. 5 Kap. 6.2 Kap. 6.4 Kap. 7.3	Bild: Zugriffsprotokoll auf Fachdienst-Ebene gehoben A_26710, A_26711, A_26712: /vsdservice entfernt (API umfasst aus Client-Sicht auch den HTTP-Proxy und nicht nur den Endpunkt des Ressource-Server); Beispiele: "prod" als fourth level domain eingefügt Bild: ZETA-Client-Data Header entfernt A_26800: <prod> geändert zu prod Kapitel verschoben: Zugriffsprotokoll muss nicht mehr im Ressource-Server, sondern kann allg. im FD VSDM umgesetzt werden. Anforderungen wurden dem Anbieter zugeordnet. A_26812-01: Rolle "Versicherter" aufgenommen und div. Konkretisierungen eingefügt	

Inhaltsverzeichnis

1 Einordnung des Dokuments	9
1.1 Zielsetzung	9
1.2 Zielgruppe	9
1.3 Geltungsbereich	9
1.4 Abgrenzungen	10
1.5 Methodik	10
1.5.1 Hinweis auf offene Punkte	11
2 Systemkontext	12
2.1 Akteure und Rollen	13
2.1.1 Hersteller ZETA Guard	13
2.1.2 Hersteller Resource Server VSDM	13
2.1.3 Anbieter Fachdienst VSDM	13
2.1.4 Kostenträger	13
2.1.5 gematik	13
2.1.6 Primärsystemhersteller	14
2.1.7 Leistungserbringer, LE Institution oder Medizinische Fachangestellte	14
2.1.8 Anbieter PoPP Service	14
2.1.9 Versicherter	14
2.2 Nachbarsysteme	14
2.2.1 Systeme in der Leistungserbringerinstitution	14
2.2.2 TI Gateway	15
2.2.3 PoPP Service	15
2.2.4 Federation Master	15
2.2.5 DNS	16
2.2.6 OCSP TSP X.509nQ SMC-B	16
2.2.7 OCSP Internet CA	16
2.2.8 OCSP Komponenten CA TI	16
2.2.9 ZETA PIP und PAP Service	16
2.2.10 ZETA Git Repository	17
2.2.11 Betriebsdatenerfassung (BDE)	17
2.2.12 Security Information and Event Management (SIEM)	17
2.2.13 Systeme der Kostenträger	17
2.3 User Stories	17
2.3.1 Versichertenstammdaten vom Fachdienst abrufen	18
2.3.2 Versichertenstammdaten von eGK lesen	18
2.3.3 Zugriffsprotokoll einsehen	18
3 Systemüberblick	19
4 Zerlegung des Produkttyps	21
4.1 Clientsystem	21
4.1.1 Datenbank	21
4.1.2 VSDM-Client Funktionen	22

4.1.2.1 Online-Abruf Versichertenstammdaten und Prüfziffer	22
4.1.2.2 Offline-Fall: Versichertenstammdaten von eGK lesen	25
4.1.3 ZETA Client Funktionen	26
4.1.4 Fehlerbehandlung	26
4.2 ZETA Guard	28
4.2.1 HTTP-Proxy Konfiguration	29
4.2.1.1 Schnittstelle zum Clientsystem	30
4.2.1.2 Schnittstelle zum VSDM Resource Server	31
4.2.2 Authorization-Server Konfiguration	31
4.3 VSDM Resource Server	33
4.3.1 VSDService-API	33
4.3.1.1 Versichertenstammdaten	35
4.3.1.2 Prüfziffer	36
4.3.1.3 Beispiele für die HTTP-Response des Resource Servers	37
4.3.1.4 Fehlermeldungen	37
4.3.2 VSD-Aktualitätsprüfung	38
4.3.3 FHIR-Fassade	39
4.3.4 Erstellung Prüfziffer	40
4.3.5 Zugriffsprotokollierung	41
4.3.6 VSD-DB	42
4.4 Fehlercodes	42
4.5 Monitoring und SIEM	44
5 Systemablauf	45
5.1 Online-Abruf Versichertenstammdaten und Prüfziffer	46
6 Übergreifende Festlegungen	50
6.1 Systemzeit	50
6.2 Fachdienstlokalisierung	50
6.3 Systemprotokolle	52
6.4 Berechtigungen	54
6.5 Authentifizierung und Autorisierung von Nutzern	55
6.6 HTTP-Status-Codes	56
6.7 ZETA-Guard	57
6.8 Sicherheit und Datenschutz	57
6.9 Betrieb	58
6.9.1 Schnittstellen und Anwendungsfälle	58
6.9.2 Leistungsanforderungen und Performance	58
6.9.3 Migration	59
6.9.3.1 Verfahren zum Umgang mit der strukturierten Prüfziffer	60
6.10 Test	60
6.11 Zulassung Fachdienste	60
6.12 Verfahren für Primärsysteme	60
7 Informationsmodell	61

7.1 Informationsmodell VSDM online	61
7.2 Informationsmodell verkürzte VSD auf eGK	61
7.3 Zugriffsprotokoll für Versicherte	62
7.4 VSDM Policy	65
7.5 VSDM spezifische Konfigurationsdaten ZETA Guard	65
8 Anhang A Verzeichnisse	66
8.1 Abkürzungen	66
8.2 Glossar	67
8.3 Abbildungsverzeichnis	69
8.4 Tabellenverzeichnis	69
8.5 Referenzierte Dokumente	70
8.5.1 Dokumente der gematik	70
8.5.2 Weitere Dokumente	71
1 Einordnung des Dokuments	9
1.1 Zielsetzung	9
1.2 Zielgruppe	9
1.3 Geltungsbereich	9
1.4 Abgrenzungen	10
1.5 Methodik	10
1.5.1 Hinweis auf offene Punkte	11
2 Systemkontext	12
2.1 Akteure und Rollen	13
2.1.1 Hersteller ZETA Guard	13
2.1.2 Hersteller Resource Server VSDM	13
2.1.3 Anbieter Fachdienst VSDM	13
2.1.4 Kostenträger	13
2.1.5 gematik	13
2.1.6 Primärsystemhersteller	14
2.1.7 Leistungserbringer, LE-Institution oder Medizinische Fachangestellte	14
2.1.8 Anbieter PoPP-Service	14
2.1.9 Versicherter	14
2.2 Nachbarsysteme	14
2.2.1 Systeme in der Leistungserbringerinstitution	14
2.2.2 TI-Gateway	15
2.2.3 PoPP-Service	15
2.2.4 Federation Master	15
2.2.5 DNS	16
2.2.6 OCSP TSP X.509nQ SMC-B	16
2.2.7 OCSP Internet-CA	16
2.2.8 OCSP Komponenten-CA TI	16
2.2.9 ZETA PIP und PAP Service	16
2.2.10 ZETA Git-Repository	17

2.2.11 Betriebsdatenerfassung (BDE)	17
2.2.12 Security Information and Event Management (SIEM)	17
2.2.13 Systeme der Kostenträger	17
2.3 User Stories	17
2.3.1 Versichertenstammdaten vom Fachdienst abrufen	18
2.3.2 Versichertenstammdaten von eGK lesen	18
2.3.3 Zugriffsprotokoll einsehen	18
3 Systemüberblick	19
4 Zerlegung des Produkttyps	21
4.1 Clientsystem	21
4.1.1 Datenbank	21
4.1.2 VSDM-Client Funktionen	22
4.1.2.1 Online-Abruf Versichertenstammdaten und Prüzfiffer	22
4.1.2.2 Offline-Fall: Versichertenstammdaten von eGK lesen	25
4.1.3 ZETA Client Funktionen	26
4.1.4 Fehlerbehandlung	26
4.2 ZETA Guard	28
4.2.1 HTTP-Proxy Konfiguration	29
4.2.1.1 Schnittstelle zum Clientsystem	30
4.2.1.2 Schnittstelle zum VSDM Resource Server	31
4.2.2 Authorization-Server Konfiguration	31
4.3 VSDM Resource Server	33
4.3.1 VSDService-API	33
4.3.1.1 Versichertenstammdaten	35
4.3.1.2 Prüzfiffer	36
4.3.1.3 Beispiele für die HTTP-Response des Resource-Servers	37
4.3.1.4 Fehlermeldungen	37
4.3.2 VSD-Aktualitätsprüfung	38
4.3.3 FHIR-Fassade	39
4.3.4 Erstellung Prüzfiffer	40
4.3.5 VSD-DB	41
4.4 Fehlercodes	42
4.5 Monitoring und SIEM	44
5 Systemablauf	45
5.1 Online-Abruf Versichertenstammdaten und Prüzfiffer	46
6 Übergreifende Festlegungen	50
6.1 Systemzeit	50
6.2 Fachdienstlokalisierung	50
6.3 Systemprotokolle	52
6.4 Zugriffsprotokollierung	53
6.5 Berechtigungen	54
6.6 Authentifizierung und Autorisierung von Nutzern	55

6.7 HTTP Status Codes	56
6.8 ZETA Guard.....	57
6.9 Sicherheit und Datenschutz.....	57
6.10 Betrieb.....	58
6.10.1 Schnittstellen und Anwendungsfälle	58
6.10.2 Leistungsanforderungen und Performance	58
6.10.3 Migration.....	59
6.10.3.1 Verfahren zum Umgang mit der strukturierten Prüfziffer.....	60
6.11 Test	60
6.12 Zulassung Fachdienste	60
6.13 Verfahren für Primärsysteme	60
7 Informationsmodell	61
7.1 Informationsmodell VSDM online	61
7.2 Informationsmodell verkürzte VSD auf eGK	61
7.3 Zugriffsprotokoll für Versicherte	62
7.4 VSDM-Policy	65
7.5 VSDM-spezifische Konfigurationsdaten ZETA Guard	65
8 Anhang A – Verzeichnisse	66
8.1 Abkürzungen	66
8.2 Glossar	67
8.3 Abbildungsverzeichnis.....	69
8.4 Tabellenverzeichnis	69
8.5 Referenzierte Dokumente	70
8.5.1 Dokumente der gematik.....	70
8.5.2 Weitere Dokumente.....	71

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) fest-gelegt 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 Schlüsselwörter 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 Schlüsselwörter 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 der Prüzfiffer 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.

Der Zugriff auf einen Fachdienst VSDM ist nur mit einer erfolgreichen Authentifizierung auf Basis einer SMC-B oder SMB möglich. Hieraus ergeben sich folgende Infrastrukturoptionen für die Authentisierung einer Leistungserbringerinstitution:

- mittels SMC-B, eHealth-Kartenterminal und Konnektor oder
- mittels SMC-B, eHealth-Kartenterminal und TI-Gateway oder
- mittels SM-B und TI-Gateway.

Im Rahmen der Nachweiserstellung über einen bestehenden Versorgungskontext ergeben sich folgende Infrastrukturoptionen für die Authentisierung eines Versicherten:

- mittels eGK, eHealth-Kartenterminal und Konnektor oder
- mittels eGK, eHealth-Kartenterminal und TI-Gateway oder
- mittels einer zukünftig angestrebten Nutzung der eGK mit einem handelsüblichen Smartcard-Reader oder
- mittels GesundheitsID-Versicherte

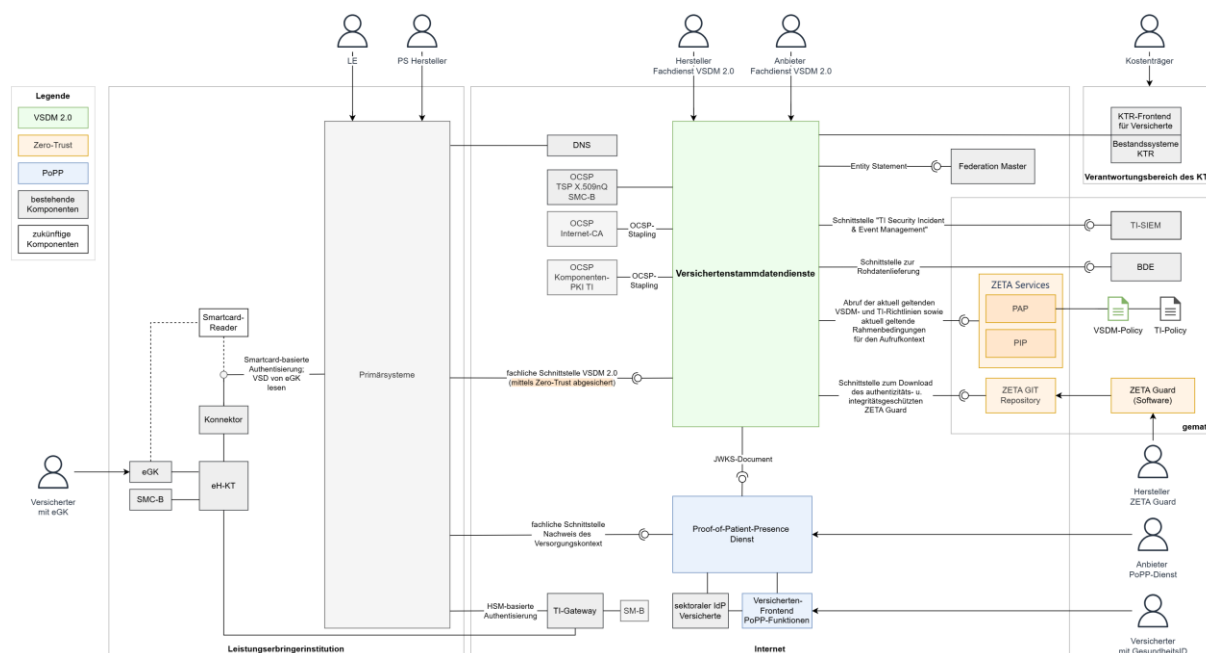


Abbildung 1-: Kontextdiagramm VSDM

2.1 Akteure und Rollen

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

2.1.1 Hersteller ZETA Guard

Der Hersteller des ZETA Guard implementiert und entwickelt den ZETA Guard und dessen Komponenten gemäß den Vorgaben der gematik [gemSpec_ZETA].

2.1.2 Hersteller Resource Server VSDM

Der Hersteller eines Resource Server VSDM implementiert und entwickelt den Resource Server gemäß den Vorgaben der gematik und den Krankenversicherungen. Der Hersteller eines Resource Servers kann zusätzlich eine Monitoring-Komponente für den Resource Server einbinden.

2.1.3 Anbieter Fachdienst VSDM

Der Anbieter eines Fachdienstes VSDM integriert den ZETA Guard und Resource Server VSDM zu einem Fachdienst VSDM und betreibt den zugelassenen Fachdienst im Internet gemäß den Vorgaben der gematik. Zudem verantwortet der Anbieter das Monitoring und Security Information and Event Management (SIEM) des Fachdienstes.

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 ZETA Guard, zu.

Die gematik stellt den qualitätsgesicherten ZETA Guard zur Integration und den Betrieb zur Verfügung.

Die gematik stellt dem Anbieter eines Fachdienstes VSDM Möglichkeiten zur Konfiguration des ZETA Guard 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 ZETA 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 ZETA Client Funktionen den Fachdienst VSDM, um aktuelle Versichertenstammdaten sowie eine Prüfziffer für Abrechnungszwecke zu erhalten.

Die Leistungserbringerinstitutionen bzw. deren Leistungserbringer oder medizinische Fachangestellte lesen mittels eines Primärsystems und der Nutzung eines handelsüblichen Smartcard-Readers oder eines eH-KT über den Konnektor oder TI-Gateway die Versichertenstammdaten aus dem Bereich der allgemeinen Versicherungsdaten (EF.VD) der elektronischen Gesundheitskarte (eGK). Das Auslesen des Bereiches der geschützten Versichertendaten (EF.GVD) entfällt.

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 dem Erhalt einer Prüfziffer.

2.1.9 Versicherter

Versicherte bestätigen durch das Stecken der eGK oder unter Nutzung der GesundheitsID das Zustandekommen eines Versorgungskontextes mit einer dedizierten Leistungserbringerinstitution als Voraussetzung für den Abruf der VSD.

Ist der Abruf der VSD vom Fachdienst VSDM nicht möglich oder der PoPP-Service nicht erreichbar (offline-Fall) stellen Versicherte durch das Stecken ihrer eGK der Leistungserbringerinstitution die Versichertenstammdaten, welche sich auf der eGK befinden, bereit.

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 die Prüfziffer 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).

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. Darüber hinaus eröffnet die Umsetzung dieses Konzeptes die Nutzung eines handelsüblichen Smartcard-Readers zum Auslesen der (zukünftig reduzierten) Versichertenstammdaten von der eGK ohne Notwendigkeit eines Konnektors oder TI-Gateways.

2.2.2 TI-Gateway

Für Leistungserbringerinstitutionen, die anstatt des Konnektors ein TI-Gateway nutzen, erfolgt die Authentisierung einer Leistungserbringerinstitution gegenüber dem PoPP-Service und einem Fachdienst VSDM auf Basis der über ein eHealth-Kartenterminal an das TI-Gateway angebotenen SMC-B oder der vom Betreiber des TI-Gateway 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 Krankenversicherungsnummer sowie einen Zeitstempel enthält. Die Authentizität des Versicherten kann dem PoPP-Service mittels eGK und unter Nutzung vom eHealth-Kartenterminal und Konnektor oder TI-Gateway nachgewiesen werden. Zudem eröffnet die Umsetzung des Konzeptes zum Nachweis des Versorgungskontextes die Möglichkeit zur Nutzung "handelsüblicher Smartcard-Readers". 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-Dokument) 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 den authentischen FQDN zur Bildung der Adresse des `./well-known` Endpunktes des PoPP-Service zur Verfügung. Über diesen `./well-known` Endpunkt erhält der Fachdienst [VSDMalleVSDM](#) alle aktuellen Endpunkte des PoPP-Service und insbesondere den Endpunkt zum Abruf [des](#)

JWKSdesJWKS-Documents, welches den aktuell gültigen Schlüssel zur Verifizierung der PoPP-Token Signatur enthält..

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 ZETA/ASL-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 ZETA/ASL-Identität von den Primärsystemen genutzt werden können.

2.2.9 ZETA PIP und PAP Service

Der ZETA Service Policy Administration Point (PAP) 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) zur Verfügung. Darüber hinaus werden über den ZETA Service 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 ZETA Git-Repository

Das ZETA Git-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 (ZETA Guard) 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. ZETA Guard.

Das Softwareprodukt "ZETA Guard" 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)

Zur Erkennung von sicherheitskritischen Ergebnissen ist für einen Fachdienst VSDM ein SIEM erforderlich. 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 Primärsystem und dienen als Lesehilfe zu den fachlichen Anwendungsfällen. Die User Stories erheben keinen Anspruch auf Vollständigkeit.

2.3.1 Versichertenstammdaten vom Fachdienst abrufen

AF_10412 -Versichertenstammdaten vom Fachdienst abrufen

- Als Leistungserbringer möchte ich mindestens einmal im Quartal die aktuellen Versichertenstammdaten erhalten und in mein Primärsystem übernehmen können.
- Als Leistungserbringer möchte ich auswählen können, dass die Versichertenstammdaten auch bei Folgebesuchen des Patienten innerhalb eines Quartals automatisch und ohne erneutem Stecken der eGK oder erneuten Nutzung der GesundheitsID durch den Versicherten abgerufen werden, um immer die jeweils aktuellen Versichertenstammdaten im Primärsystem speichern zu können.
- 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 die Prüfziffer 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 die Prüfziffer über die abgefragten VSD im Primärsystem speichern.

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

2.3.2 Versichertenstammdaten von eGK lesen

AF_10413 -Versichertenstammdaten von eGK lesen

- Als Leistungserbringer möchte ich mindestens einmal im Quartal auch dann die Versichertenstammdaten erhalten und in mein Primärsystem übernehmen können, wenn die Herstellung des Versorgungskontextes fehlschlägt und/oder die Versichertenstammdaten des Versicherten nicht von der zuständigen Krankenkasse abgerufen werden können. In diesem Fall nutze ich die auf der eGK gespeicherten Daten.
- Als Leistungserbringer muss ich in der Lage sein, das Versicherungsverhältnis des anwesenden Patienten prüfen sowie meine Leistungen am Patienten abrechnen zu können, wenn die Herstellung des Versorgungskontextes fehlschlägt und/oder die Versichertenstammdaten des Versicherten nicht von der zuständigen Krankenkasse abgerufen werden können. In diesem Fall nutze ich die auf der eGK gespeicherten Daten.

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

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 3 Jahre 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:

Spezifikation Versichertenstammdatenmanagement 2.0 (VSDM 2.0)

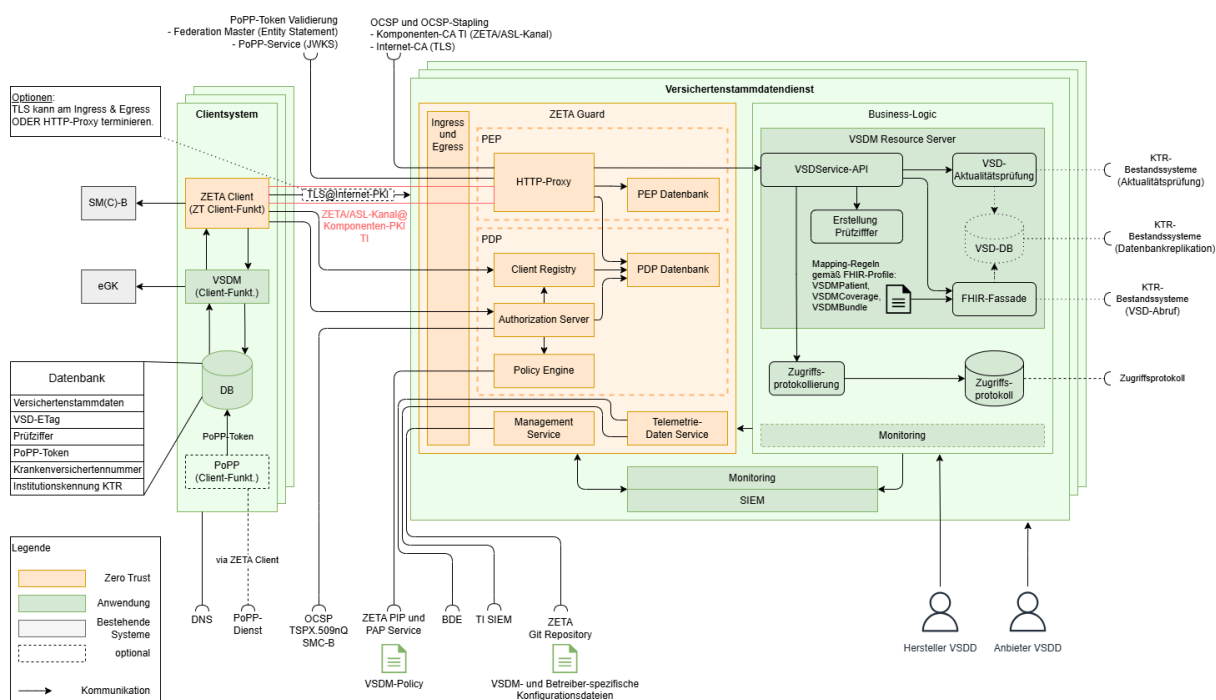
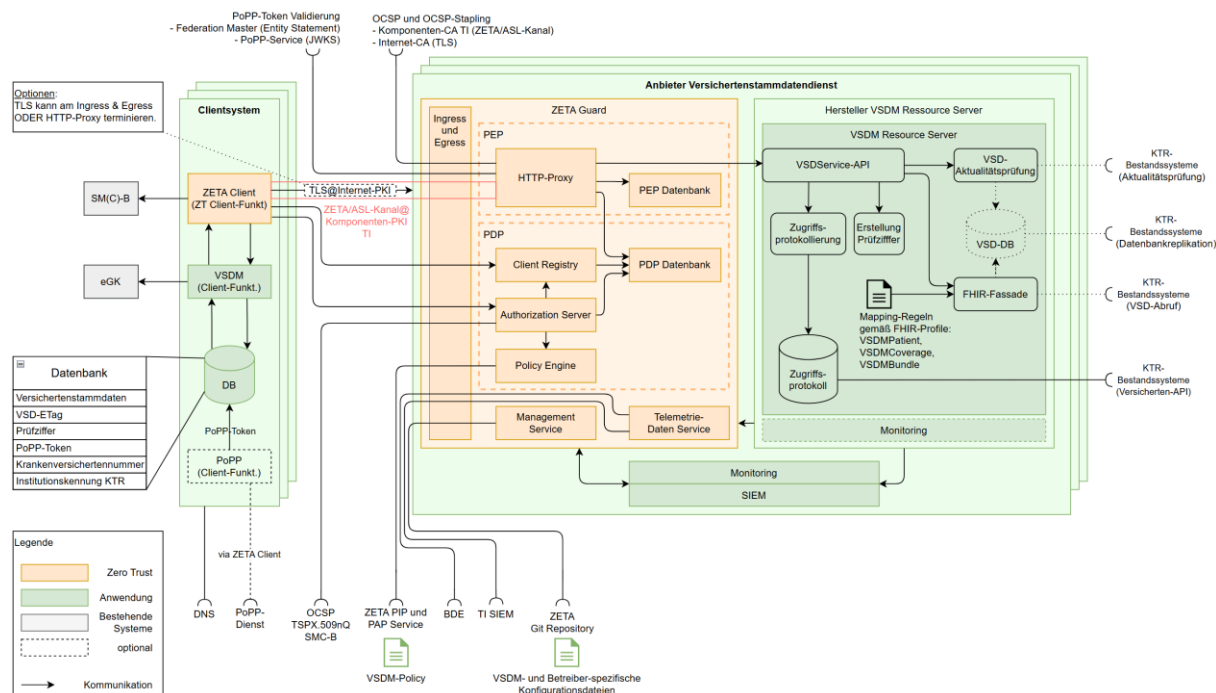


Abbildung 2- Systemdiagramm VSDM

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. <patientID> (Krankenversichertennummer; KVNR)
3. <insurerId> (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) eine Prüfziffer erhalten werden kann. [~~CS_VSDM_2, funkt. Eignung: Herstellererklärung~~]

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: Herstellererklärung~~]

A_26702 -Clientsystem VSDM - Prüfziffer Persistierung

Ein Clientsystems VSDM MUSS nach Erhalt einer Prüfziffer diese persistieren, damit ein Leistungserbringer diese zu Abrechnungszwecken verwenden kann. [~~CS_VSDM_2, funkt. Eignung: Herstellererklärung~~]

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 Prüfziffer

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: Herstellererklärung<=]

A_26704 -Clientsystem VSDM - Fachdienstlokalisierung

Ein Clientsystem VSDM MUSS für die Lokalisierung desjenigen Fachdienst VSDM, der die VSD des Patienten verwaltet, eine Fachdienstlokalisierung gemäß A_26800 und A_26802 sowie auf Basis der Institutionskennung (IK) der Krankenkasse, bei dem der Patient versichert ist, durchführen. Für die IK MUSS das Feld `insurerID` des PoPP-Tokens verwendet werden. [~~=~~, CS_VSDM_2, funkt. Eignung: Herstellererklärung<=]

A_26709 -Clientsystem VSDM - Fachdienst-Endpunkte

Ein Clientsystem VSDM MUSS für Anfragen an den Fachdienst VSDM sicherstellen, dass es nur erlaubte Anfragen und Endpunkte verwenden. [~~=~~, CS_VSDM_2, funkt. Eignung: Herstellererklärung<=]

A_26710-01A_26710 -Clientsystem VSDM - VSDService-API

Ein Clientsystem VSDM MUSS für Anfragen an die Fachdienst VSDM API ~~/vdservice~~ 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: Herstellererklärung]

A_26711-01A_26711 -Clientsystem VSDM - Übertragung des Versorgungskontextnachweises

Ein Clientsystem VSDM MUSS für jede Anfrage an die Fachdienst VSDM API ~~/vdservice~~ einen gültigen Versorgungskontextnachweis in Form eines PoPP-Tokens im Header `PoPP` als Bearer-Token übertragen. [~~=~~ [~~=~~, CS_VSDM_2, funkt. Eignung: Herstellererklärung]

A_26712-01A_26712 -Clientsystem VSDM - Übertragung des VSD-Änderungsindikator

Ein Clientsystem VSDM MUSS für jede Anfrage an die Fachdienst VSDM API ~~/vdservice~~ den vom Fachdienst VSDM übermittelten VSD-Änderungsindikator als `starkenetag_value` des HTTP-Headers `If-None-Match` gemäß [RFC7232] übertragen. Liegt dem Clientsystem (noch) kein VSD-Änderungsindikator vor, MUSS `deretag_value` auf 0 gesetzt werden und als hexadezimal kodierten 256-Bit Binärwert übertragen. [~~=~~ [~~=~~, CS_VSDM_2, funkt. Eignung: Herstellererklärung]

A_26713 -Clientsystem VSDM - VSD-Aktualisierung bei erstmaligem Patientenkontakt

Ein Clientsystem VSDM MUSS beim erstmaligen Besuch eines Patienten innerhalb eines Quartals den Versorgungskontext am PoPP-Service erneuern und einen Versichertenstammdatenabruf durchführen sowie die Informationen gemäß A_26700 aktualisieren. [~~=~~ [~~=~~, CS_VSDM_2, funkt. Eignung: Herstellererklärung]

A_26957 -Clientsystem VSDM - VSD-Aktualisierung bei wiederholtem Patientenkontakt

Ein Clientsystem VSDM MUSS technisch in der Lage sein, bei Folgebesuchen eines Patienten innerhalb eines Quartals einen Versichertenstammdatenabruf mit vorhandenem PoPP-Token (das heißt: ohne Verwendung der eGK oder GesundheitsID) durchzuführen und die Informationen gemäß A_26700 aktualisieren. [~~←=, CS_VSDM_2, funkt. Eignung: Herstellererklärung<=~~]

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 unter Verwendung der eGK oder GESundheitsID 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. Das Clientsystem kann diesen VSD-Abruf bspw. als Hintergrunddienst bei einer dedizierten Nutzerinteraktion wie dem Aufruf des Patientenstamm oder dem Anklicken eines Aktualisierungsschalters zum Patientenstamm durchgeführt werden.

Das Feature der Versichertenstammdatenaktualisierung bei Folgebesuchen eines Patienten hat keinerlei rechtliche Verpflichtungen für die Leistungserbringerinstitution.

A_26958 -Clientsystem VSDM - Konfigurierbarkeit der VSD-Aktualisierung

Ein Clientsystem VSDM MUSS standardmäßig den Versichertenstammdatenabruf einmal im Quartal gemäß A_26713 ausführen. Es MUSS jedoch dem Nutzer den Abruf von Versichertenstammdaten bei Folgebesuchen eines Patienten innerhalb desselben Quartals gemäß A_26957 aktiv anbieten. [~~←=, CS_VSDM_2, funkt. Eignung: Herstellererklärung<=~~]

A_27371 -Clientsystem VSDM - Hinweis-Text bei Abwahl der wiederholten VSD-Aktualisierung

Ein Clientsystem VSDM MUSS beim Angebot des automatischen Versichertenstammdatenabruf bei Folgebesuchen eines Patienten innerhalb eines Quartals den Nutzer darauf hinweisen, dass es keinerlei rechtliche Verpflichtungen hierfür gibt und es sich lediglich um ein Feature handelt, um auch bei Folgebesuchen eines Patienten ohne erneutes Stecken der eGK oder erneuerter Nutzung der GesundheitsID Versichertenstammdaten aktualisieren zu können. [~~←=, CS_VSDM_2, funkt. Eignung: Herstellererklärung<=~~]

A_26714 -Clientsystem VSDM - Angabe FHIR MediaType

Ein Clientsystem VSDM MUSS 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: Herstellererklärung<=~~]

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: Herstellererklärung<=~~]

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: Herstellererklärung<=~~]

A_26900 -Clientsystem VSDM - Verwendung Prüfziffer für Abrechnungsunterlagen

Das Clientsystem VSDM MUSS zur Erstellung der Abrechnungsunterlagen den Wert aus dem HTTP-Header `VSDM-Pz` als Prüfziffer verwenden. [~~←, CS_VSDM_2, funkt. Eignung: Herstellererklärung~~]

Hinweis: Im Gegensatz zu vorherigen VSDM-Versionen erstellt ein Fachdienst VSDM keinen Prüfungsnachweis mehr, sondern nur noch eine Prüfziffer.

A_26719 -Clientsystem VSDM - Anzeige geänderter VSD

Ein Clientsystem VSDM SOLL Änderungen der VSD benutzerfreundlich im Clientsystem anzeigen. [~~←, CS_VSDM_2, funkt. Eignung: Herstellererklärung~~]

Beispiel für den HTTP-Request des Clientsystems VSDM an den ZETA Client

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

{
}
```

Beispiel für den HTTP-Request des ZETA Client mit ZETA/ASL-Kanal

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

{
    <HTTP-Request des Clientsystems VSDM>
}
```

Beispiel für die HTTP-Response für den Status HTTP304 Not Modified:

```
HTTP/1.1 304 Not Modified
ETag: "e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855"
VSDM-Pz:<Base64URL kodierte Prüfziffer>

{
}
```

Hinweis: Diese Response wurde schon vom ZETA Client aus dem ZETA/ASL-Kanal extrahiert.

Beispiel für die HTTP-Response für den Status HTTP200 OK:

```
HTTP/1.1 200 OK
ETag: "e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855"
Content-Type: application/fhir+json; charset=utf-8
...
VSDM-Pz:<Base64URL kodierte Prüfziffer>
```

```
{
  "resourceType": "VSDMBundle",
  ...
}
```

Hinweis: Dieser Response wurde schon vom ZETA Client aus dem ZETA/ASL-Kanal extrahiert.

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

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

Hinweis: Dieser Request wurde schon vom ZETA Client aus dem ZETA/ASL-Kanal extrahiert.

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 von der eGK (Container PD und VD) gemäß [gemILF_PS] unter Nutzung eines eH-KT von der eGK zu lesen. [~~←=, CS_VSDM_2, funkt. Eignung: Herstellererklärung<=]~~]

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: Herstellererklärung<=]~~]

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 ZETA Client Funktionen

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

A_26724 -Clientsystem VSDM - ZETA Client

Ein ClientsystemsVSDM MUSS die ZETA Client Funktionen gemäß [gemSST_PS_ZETA] umsetzen. [~~≤, CS_VSDM_2, Sich.techn. Eignung: Herstellererklärung~~≤]

A_27357 -Clientsystem - ZETA Client Fachdienstkommunikation

Ein ClientsystemsVSDM MUSS sicherstellen, dass jegliche Kommunikation mit dem Fachdienst VSDM über den ZETA Client erfolgt. [~~≤, CS_VSDM_2, Sich.techn. Eignung: Herstellererklärung~~≤]

Hinweis: Der Zeta-Client beinhaltet zwingend zu nutzende Kommunikationsfunktionen wie TLS, ZETA/ASL-Kanal und weitere (siehe [gemSpec_ZETA])

A_26984 -Clientsystem VSDM - ZETA Client Authentisierung

Ein Clientsystem MUSS zur Authentisierung der Leistungserbringerinstitution das Verfahren mittels SM(C)-B signiertem Client Assertion JWT und DPoP gemäß [RFC7523] und [RFC9449] verwenden.

[~~≤, CS_VSDM_2, Sich.techn. Eignung: Herstellererklärung~~≤]

A_26726 -Clientsystem VSDM - ZETA Client ZETA/ASL-Kanal

Ein Clientsystem VSDM MUSS für jede Anfrage an die Fachdienste VSDM API /vsdservice die ZETA Client Funktion mit aktivem ZETA/ASL-Kanalverwenden. [~~≤, CS_VSDM_2, Sich.techn. Eignung: Herstellererklärung~~≤]

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_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 beim Clientsystem - der Hersteller des Clientsystems ist zu kontaktieren.

VSDMErrorcodeCS Code	Fehlerbehandlung
VSDSERVICE_UNSUPPORTED_ENCODING	Implementierungsfehler beim Clientsystem - der Hersteller des Clientsystems ist zu kontaktieren.
VSDSERVICE_INVALID_PATIENT_RECORD_VERSION	Implementierungsfehler beim Clientsystem - der Hersteller des Clientsystems ist zu kontaktieren.
VSDSERVICE_INVALID_HTTP_OPERATION	Implementierungsfehler beim Clientsystem - der Hersteller des Clientsystems ist zu kontaktieren.
VSDSERVICE_INVALID_ENDPOINT	Implementierungsfehler beim Clientsystem - der Hersteller des Clientsystems ist zu kontaktieren.
VSD_SERVICE_INTERNAL_SERVER_ERROR	Wiederholungsversuch im 'Exponential Backoff'-Verfahren gemäß A_25339 [gemSpec_ZETA].
VSDSERVICE_VSDD_NOTREACHABLE	Wiederholungsversuch im 'Exponential Backoff'-Verfahren gemäß A_25339 [gemSpec_ZETA].
VSDSERVICE_VSDD_TIMEOUT	Wiederholungsversuch im 'Exponential Backoff'-Verfahren gemäß A_25339 [gemSpec_ZETA].

[<=, CS_VSDM_2, funkt. Eignung: Herstellererklärung][<=]

4.2 ZETA Guard

Dieses Kapitel beschränkt sich folgend nur auf die ZETA Guard Komponenten mit VSDM-spezifischen Konfigurationsanforderungen. Vorgaben zur operativen Umsetzung der folgenden Konfigurationsanforderungen sind [gemSpec_ZETA] zu entnehmen.

Die folgenden Anforderungen an die Komponenten des ZETA Guard (als Teil eines Fachdienstes VSDM) werden durch Einträge in die VSDM-spezifische Konfigurationsdaten (Manifest-Dateien) gemäß [gemSpec_ZETA] umgesetzt (siehe auch 7.5.: VSDM-spezifische Konfigurationsdaten ZETA Guard). Da zum Veröffentlichungszeitpunkt dieser Spezifikation die konkrete Ausgestaltung der Manifest-Dateien noch nicht feststeht,

werden die Manifest-Dateien zu einem späteren Zeitpunkt normativ referenziert und in den Anforderungshaushalt von VSDM 2.0 eingebunden.

Tabelle 2 : TAB_VSDM_KONFIGURATIONSÜBERSICHT_ZETA_GUARD

ZETA Guard Komponente	VSDM-spezifische Konfigurationsanforderungen auf Anwendungsebene
Ingress und Egress	nein
HTTP-Proxy	ja
PEP Datenbank	nein
Client Registry	nein
Authorization Server	ja
PDP Datenbank	nein
Policy Engine	nein
Management Service	nein
Telemetrie-Daten Service	nein
Notification Service	nein (Service für VSDM nicht relevant)

A_27359 -Fachdienst VSDM - Ausschließlich TLS-gesicherte Verbindungen mit Clientsystem

Der Anbieter VSDM MUSS den ZETA-Guard derart konfigurieren, dass ausschließlich durch TLS gesicherte Verbindungen mit einem Clientsystem aufgebaut werden. [[=> VSDM_2_FD, Sich.techn. Eignung: Gutachten<=](#)]

Hinweis:

Für Zugriffe auf den Resource-Server obliegt es dem Anbieter zu wählen, ob die Ingress & Egress Komponente oder die HTTP-Proxy Komponente des ZETA-Guard diese Anforderung durchsetzt.

4.2.1 HTTP-Proxy Konfiguration

Der HTTP-Proxy nimmt die Anfragen eines Clientsystems entgegen und prüft die Anfrage vor dem Aufbau eines ZETA/ASL-Kanals 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 ZETA/ASL-Kanals geprüft und - wenn vorhanden - der PoPP-Token sicherheitstechnisch verifiziert. Anschließend stellt der HTTP-Proxy eine HTTP-basierte Anfrage (ohne ZETA/ASL-Kanal, aber mit allen Informationen der Anfrage des Clientsystems) an den Resource-Server und fügt dieser die ZETA Guard spezifischen Header `ZETA-User-Info`, `ZETA-PoPP-Token-Content` und bei entsprechender HTTP-Proxy Konfiguration `ZETA-Client-Data` hinzu.

Antworten des Resource-Servers nimmt der HTTP-Proxy entgegen und setzt diese Richtung Clientsystem auf den ZETA/ASL-Kanal um.

4.2.1.1 Schnittstelle zum Clientsystem

A_26731 -Fachdienst VSDM - HTTP-Proxy - ZETA/ASL

Der Anbieter VSDM MUSS den HTTP-Proxy derart konfigurieren, sodass ein Verbindungsaufbau mit einem Clientsystem nur mittels ZETA/ASL erlaubt wird. [~~≤~~, VSDM_2_FD, funkt. Eignung: Test Produkt/FA<=]

A_26732 -Fachdienst VSDM - HTTP-Proxy - ZETA/ASL für FHIR Ressourcen

Der HTTP-Proxy VSDM MUSS die Versichertenstammdaten in Form der FHIR-Resource VSDMBundle sowie die FHIR Ressource VSDMOperationOutcome durch ZETA/ASL gesichert an das Clientsystem übertragen. [~~≤~~, VSDM_2_FD, funkt. Eignung: Test Produkt/FA<=]

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<=]

A_27329 -Fachdienst VSDM - HTTP-Proxy - PoPP-Token Prüfung

Der Anbieter VSDM MUSS den HTTP-Proxy derart konfigurieren, sodass beim Aufruf der HTTP-GET-Operation an die Fachdienst VSDM API /vsdservice stets auf Vorhandensein des HTTP-Headers PoPP sowie der kryptografischen und zeitlichen Gültigkeit des dort enthaltenen PoPP-Tokens geprüft wird und der Aufruf bei fehlendem HTTP-Header PoPP oder ungültigem PoPP-Token abgelehnt wird. [~~≤~~, VSDM_2_FD, funkt. Eignung: Test Produkt/FA<=]

A_27330 -Fachdienst VSDM - HTTP-Proxy - zeitliche Gültigkeit des PoPP-Tokens

Der Anbieter VSDM MUSS den HTTP-Proxy derart konfigurieren, sodass nur PoPP-Token als zeitlich gültig akzeptiert werden, deren Ausstellungszeitpunkt iat innerhalb des aktuellen Quartals des aktuellen Jahres bezogen auf die Systemzeit liegt. Bei einem Quartalswechsel MUSS eine grace-period von 5 Minuten akzeptiert werden. [~~≤~~, VSDM_2_FD, funkt. Eignung: Test Produkt/FA<=]

4.2.1.2 Schnittstelle zum VSDM Resource Server

A_26742 -Fachdienst VSDM - HTTP-Proxy - Keine Übermittlung von Client-Daten

Der Anbieter VSDM MUSS den HTTP-Proxy derart konfigurieren, sodass der HTTP-Header ZETA-Client-Data nicht an den Resource Server VSDM übermittelt wird. [~~←=, VSDM_2_FD, funkt. Eignung: Test Produkt/FA<=~~]

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-Referenz in anderen Dokumenten	Profession Item (Beschreibung der Institution)	Zugriff VSDM
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_krankenhausapotheker	Krankenhausapotheker	ja
oid_bundeswehrapotheke	Bundeswehrapotheke	ja
oid_mobile_einrichtung_rettungsdienst	Betriebsstätte Mobile Einrichtung Rettungsdienst	ja
oid_kostentraeger	Betriebsstätte Kostenträger	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.

Die Angabe der konkreten ProfessionOIDs (OIDs der Berufsgruppe) befindet sich im Dokument "gemSpec_OID).

A_26744 -Fachdienst VSDM - AuthZ-Server - Scopes

Der Anbieter VSDM MUSS den Authorization-Server derart konfigurieren, sodass ein Access-Token mit dem claim "scope": "vdservice" 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. Zukünftig und bei Verfügbarkeit der VSDM-Policy wird dieser Wert über die VSDM-Policy festgelegt und nicht mehr innerhalb dieser Spezifikation.

A_27400 -Fachdienst VSDM - AuthZ-Server - Audience

Der Anbieter VSDM MUSS den Authorization-Server derart konfigurieren, sodass ein Access-Token mit dem claim "aud": "https://<IK-NR>.vsdm2.ti-dienste.de" ausgestellt wird.[<=, VSDM_2_FD, funkt. Eignung: Test Produkt/FA<=]

Hinweis: Zukünftig und bei Verfügbarkeit der VSDM-Policy wird dieser Wert über die VSDM-Policy festgelegt und nicht mehr innerhalb dieser Spezifikation.

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 `/vdservice/v1/vsdbundle` 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 ZETA/ASL- Kanals	gültiger Access-Token gültiger PoPP-Token zeitliche Gültigkeit des Versorgungskontext Clientsystem besitzt veraltete VSD kein Fehlerfall
Prüfziffer	intern	string	HTTP Custom- Header innerhalb des ZETA/ASL- Kanals	gültiger Access-Token gültiger PoPP-Token VSD-Aktualitätsprüfung wurde durchgeführt kein Fehlerfall

Resource	Zugriffs- method e	Standard , Format	Übertragung	Bereitstellungsbeding ung
VSDMOperationOutcome	intern	fhir+xml fhir+json	HTTP-Body innerhalb des ZETA/ASL- Kanals	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 - ZETA Header

Der Resource Server VSDM MUSS alle eingehenden Anfragen, die nicht den HTTP-Header ZETA-PoPP-Token-Content, ZETA-User-Info, ~~ZETA-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 Resource Server VSDM MUSS den HTTP Status Code ~~400-Bad-Request~~428 Precondition Required sowie eine Fehlermeldung gemäß A_26770 mit dem Fehler

VSDSERVICE_MISSING_OR_INVALID_HEADERPATIENT_RECORD_VERSION
beinhalten. [~~≤~~, ~~≤~~, VSDM_2_FD, funkt. Eignung: Test-Produkt/FA]

A_26977 -Fachdienst VSDM - 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_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]

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 den ZETA Guard. 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-Identifizierung

Der Resource Server VSDM MUSS beim Aufruf der HTTP-GET-Operation an die Fachdienst VSDM API/vsdservice die KVN der ElementspatientId des HTTP-Headers ZETA-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 der Verarbeitung von Versichertenstammdaten eine VSD-Aktualitätsprüfung gemäß Kapitel 4.3.2- 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 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 bei internen Fehlern, die bei der Aktualitätsprüfung auftreten, das Ergebnis der VSD-Aktualitätsprüfung immer "Nicht-Übereinstimmung" ist und somit die Übertragung der Versichertenstammdaten sowie der Prüfziffer durch einen solchen internen Fehler nicht beeinträchtigt wird. [~~=, 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 `/vdservice/v1/vsdbundle` ausschließlich die Versichertenstammdaten respektive das `VSDMBundle` für die KVNR desElements`patientId` an das Clientsystem übermitteln werden. Er DARF KEINE KVNR-übergreifende oder KVNR-abweichenden Versichertenstammdaten `VSDMBundle` an das Clientsystem übermitteln. [~~=, VSDM_2_FD, funkt. Eignung: Test Produkt/FA~~]

4.3.1.2 Prüfziffer

A_26764 -Fachdienst VSDM - Resource Server - Prüfziffer in jeder fehlerfreien Response

Der Resource Server VSDM MUSS für jeden Aufruf der HTTP-GET-Operation an die Fachdienst VSDM API `/vdservice` die Prüfziffer in dem HTTP-Header `VSDM-Pz` 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 die Prüfziffer 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 Prüfziffer übermittelt.

4.3.1.3 Beispiele für die HTTP-Response des Resource-Servers

Beispiel für die Übertragung der Prüfziffer für den Fall HTTP304 Not Modified:

HTTP-Header

```
HTTP/1.1 304 Not Modified
ETag: "e3b0c44298fc1c149afb4c8996fb92427ae41e4649b934ca495991b7852b855"
VSDM-Pz:<Base64URL kodierte Prüfziffer>
```

Beispiel für die Übertragung der Prüfziffer für den Fall HTTP200 OK:

```
HTTP/1.1 200 OK
Content-Type: application/fhir+json; charset=utf-8
...
ETag: "e3b0c44298fc1c149afb4c8996fb92427ae41e4649b934ca495991b7852b855"
VSDM-Pz:<Base64URL kodierte Prüfziffer>
```

```
{
  "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 VSDMOperationOutcome

Der Resource Server VSDM MUSS im Fehlerfall und für Fehlermeldungen mit dem Clientsystem als Empfänger Hinweise zur Fehlerursache als FHIR-Resource `VSDMOperationOutcome` 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 Stack-Trace) 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 gemäß A_27012 mit dem HTTP-Proxy als Empfänger der Fehlermeldung den Custom-Header `zeta-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-Resource VSDMOperationOutcome für Fehler mit dem HTTP-Proxy als Empfänger der Fehlermeldung verwenden. [~~=, VSDM_2_FD, funkt. Eignung: Test Produkt/FA~~]

Beispiel für die Übertragung einer Fehlermeldung mit FHIR-Resource:

```
HTTP/1.1 404 Not Found
Content-Type: application/fhir+json; 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 dem Fachdienst VSDM übermitteln. Nun kann ein Fachdienst VSDM prüfen, ob überhaupt eine Aktualisierung bzw. eine Übertragung der Versichertenstammdaten notwendig ist oder ob die lokal im Clientsystem gespeicherten VSD noch aktuell sind (für diesen Fall wird nur die Prüfziffer übertragen).

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 MUSS unabhängig vom Datenformat (xml oder json) sein und den gleichen Wert besitzen.~~ 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 Zeitstempels 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 `patientId` des HTTP-Headers `ZETA-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 `If-None-Match` 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 die Prüfziffer erhält.

4.3.3 FHIR-Fassade

A_26778 -Anbieter Fachdienst VSDM - Resource Server - VSD-Abruf

Falls der Resource Server VSDM Versichertenstammdatensätze von weiteren Systemen abrufen, MUSS er sicherstellen, dass diese Systeme ausschließlich von einem Kostenträger gemäß §4 Absatz 2 SGB V verantwortet werden. [~~←=, Anb_VSDM_2_FD, funkt. Eignung: Anbietererklärung~~←=]

A_26779 -Fachdienst VSDM - Resource Server - VSD-Lokalisierung

Der Resource Server VSDM MUSS zur Lokalisierung der VSD die KVNR des Elements `patientId` des HTTP-Headers `ZETA-PoPP-Token-Content` verwenden. Falls der Resource Server VSDM Versichertenstammdatensätze von weiteren Systemen abrufen, MUSS er sicherstellen, dass 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 KVN-R des Elements `patientId` des HTTP-Headers `ZETA-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 VSDMCoverage gemäß FHIR-Profil [FHIR-Profil 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 Prüfziffer

Die Prüfziffer dient als Nachweis über die durchgeführte Prüfung des Versicherungsstatus sowie der Aktualität der Versichertenstammdaten. Er dient als Nachweis für die Abrechnungsdaten nach § 295 SGB V.

A_26766 -Fachdienst VSDM - Resource Server - Prüfziffer Kodierung

Der Resource Server VSDM MUSS die Prüfziffer als BASE64URL kodierten Wert übertragen. [~~←=, VSDM_2_FD, funkt. Eignung: Test Produkt/FA<=~~]

A_26790 -Fachdienst VSDM - Resource Server - Prüfziffer Länge

Der Resource Server VSDM MUSS sicherstellen, dass die kodierte Prüfziffer eine Länge von 64 Byte hat. [~~←=, VSDM_2_FD, funkt. Eignung: Test Produkt/FA<=~~]

Hinweis: Der Inhalt der Prüfziffer ist nicht weiter festgelegt und obliegt den Krankenversicherern.

~~4.41.1 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 7.3 Zugriffsprotokoll für Versicherte formuliert.~~

~~A_26794 Fachdienst VSDM Resource Server Zugriffsprotokoll Zugriffsberechtigung prüfen~~

~~Der VSDM Resource Server MUSS sicherstellen, dass ausschließlich Versicherte, Mitarbeiter eines Kostenträgers oder einer Ombudsstelle Zugriff auf das Zugriffsprotokoll eines Versicherten erhalten. [\leq , VSDM_2_FD, Sich.techn. Eignung: Gutachten]~~

~~*Hinweis: Der Zugriff durch Kostenträger oder Ombudsstellen darf ausschließlich auf Verlangen des Versicherten und zum Zweck der Beauskunftung gegenüber diesem erfolgen.*~~

~~A_26795 Fachdienst VSDM Resource Server Zugriffsprotokoll Zugriffsprotokollierung~~

~~Der VSDM Resource Server MUSS jeden Zugriff auf das Zugriffsprotokoll eines Versicherten gemäß A_26812 im Zugriffsprotokoll protokollieren. [\leq , VSDM_2_FD, Sich.techn. Eignung: Gutachten]~~

~~A_26813 Fachdienst VSDM Resource Server Zugriffsprotokoll Schutz der Vertraulichkeit~~

~~4.4.1 Der VSDM Resource Server MUSS das Zugriffsprotokoll mit den gleichen oder sicherheitstechnisch mindestens äquivalenten Sicherheitsmaßnahmen wie die VSD selbst schützen. [\leq , 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 die Ergebnisliste des Zugriffsprotokolls bei mehr als einem Eintrag als Ergebnis-Bundle (Ergebnis-Liste) an den Aufrufer zurückgeben, damit der Versicherte eine vollständige Einsicht in oder Auskunft über das Zugriffsprotokoll erhält. [\leq , 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 3 Jahren ab dem Erzeugungsdatum und innerhalb von einem Monat löschen, damit veraltete Einträge nach Ende der regulären Aufbewahrungsfrist entfernt werden. [\leq , VSDM_2_FD, Sich.techn. Eignung: Herstellererklärung]~~

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

4.4.24.3.5 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. [\leq , VSDM_2_FD, funkt. Eignung: Test Produkt/FA \leq]

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. [\leq , VSDM_2_FD, Sich.techn. Eignung: Gutachten \leq]

4.54.4 Fehlercodes

~~A_27012-01A_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_FEHLER-REFERENZEN_UND_BDE-CODES

BDE - Code	VSDMErrorcodeCS Referenz	Beschreibung	Fehler-adressat
79010	VSDSERVICE_INVALID_IK	Ungültige oder nicht bekannte Institutionskennung <ik>.	Clientsystem
79011	VSDSERVICE_INVALID_KVNR	Ungültige oder nicht bekannte Krankenversichertennummer <kvnr>.	Clientsystem

BDE - Cod e	VSDMErrorcodeCS Referenz	Beschreibung	Fehler- adressa t
790 20	VSDSERVICE_PATIENT_RECORD_NOT_FOUND	Die Versichertenstammdaten zur Versichertennummer <kvnr> konnten für die Institutionskennung <ik> nicht ermittelt werden.	Clientsys tem
790 30	VSDSERVICE_MISSING_OR_INVALID_HEADER	Der erforderliche HTTP-Header <header> fehlt oder ist ungültig.	Clientsys tem
790 31	VSDSERVICE_UNSUPPORTED_MEDIATYPE	Der vom Clientsystem angefragte Medientyp <media type> wird nicht unterstützt.	Clientsys tem
790 32	VSDSERVICE_UNSUPPORTED_ENCODING	Das vom Clientsystem angefragte Komprimierungsverfahren <encoding scheme> wird nicht unterstützt.	Clientsys tem
790 33	VSDSERVICE_INVALID_PATIENT_RECORD_VERSION	Der Änderungsindikator <etag_value> kann nicht verarbeitet werden.	Clientsys tem
790 40	VSDSERVICE_INVALID_HTTP_OPERATION	Die HTTP-Operation <http-operation> wird nicht unterstützt.	Clientsys tem
790 41	VSDSERVICE_INVALID_ENDPOINT	Der angefragte Endpunkt <endpoint> wird nicht unterstützt.	Clientsys tem
791 00	VSD_SERVICE VSDSERVICE_INTERNAL_SERVER_ERROR	Unerwarteter interner Fehler des Fachdienstes VSDM.	Clientsys tem
791 10	VSDSERVICE_VSDD_NOTREACHABLE	Fachdienst VSDM ist für den Kostenträger <ik> nicht erreichbar.	Clientsys tem

BDE - Cod e	VSDMErrorcodeCS Referenz	Beschreibung	Fehler- adressa t
791 11	VSDSERVICE_VSDD_TIMEOUT	Fachdienst VSDM für den Kostenträger <ik> hat das Zeitlimit für eine Antwort überschritten.	Clientsys tem
792 05	-	Header ZETA-Client-Data fehlt.	HTTP- Proxy
792 06	-	Header ZETA-User-Info fehlt.	HTTP- Proxy
792 07	-	Header ZETA-PoPP-Token-Content fehlt.	HTTP- Proxy
794 00	-	Client-Data-Daten können nicht verarbeitet werden.	HTTP- Proxy
794 01	-	User-Info Daten können nicht verarbeitet werden.	HTTP- Proxy
794 02	-	PoPP-Info Daten können nicht verarbeitet werden.	HTTP- Proxy

<kvnr>: Krankenversichertennummer

(Feld: patientId des HTTP-Headers ZETA-PoPP-Token-Content)

<ik>: Institutionskennzeichen des jeweiligen Krankenversicherers

(Feld: insurerId des HTTP-Headers ZETA-PoPP-Token-Content) [~~≤, VSDM_2_FD,~~
~~funkt. Eignung: Test-Produkt/FA ≤~~]

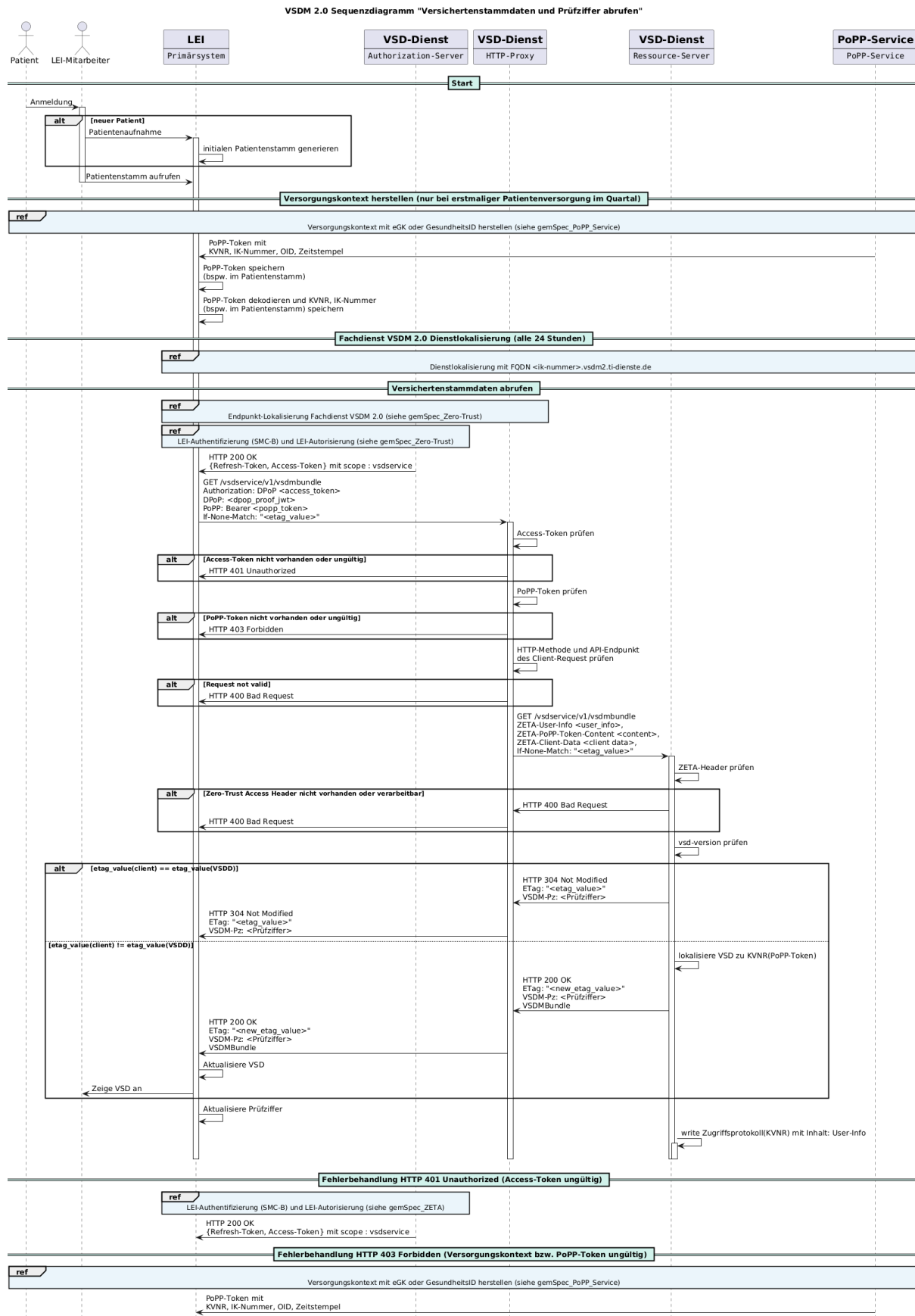
4.64.5 Monitoring und SIEM

Ein Fachdienst VSDM muss betriebliche und sicherheitskritische Ereignisse erfassen und je nach Schweregrad und Vorgaben der gematik an die Betriebsdatenerfassung und das SIEM der TI übermitteln. Die entsprechenden Anforderungen werden wie bei allen anderen Fachdiensten über den Anbietertypsteckbrief dem Anbieter VSDM zugeordnet.

Weitere Details zur Einbindung des ZETA Guard und Resource Server in das Monitorings und SIEM des Fachdienstes werden in [gemSpec_ZETA] erläutert.

5 Systemablauf

5.1 Online-Abruf Versichertenstammdaten und Prüfziffer



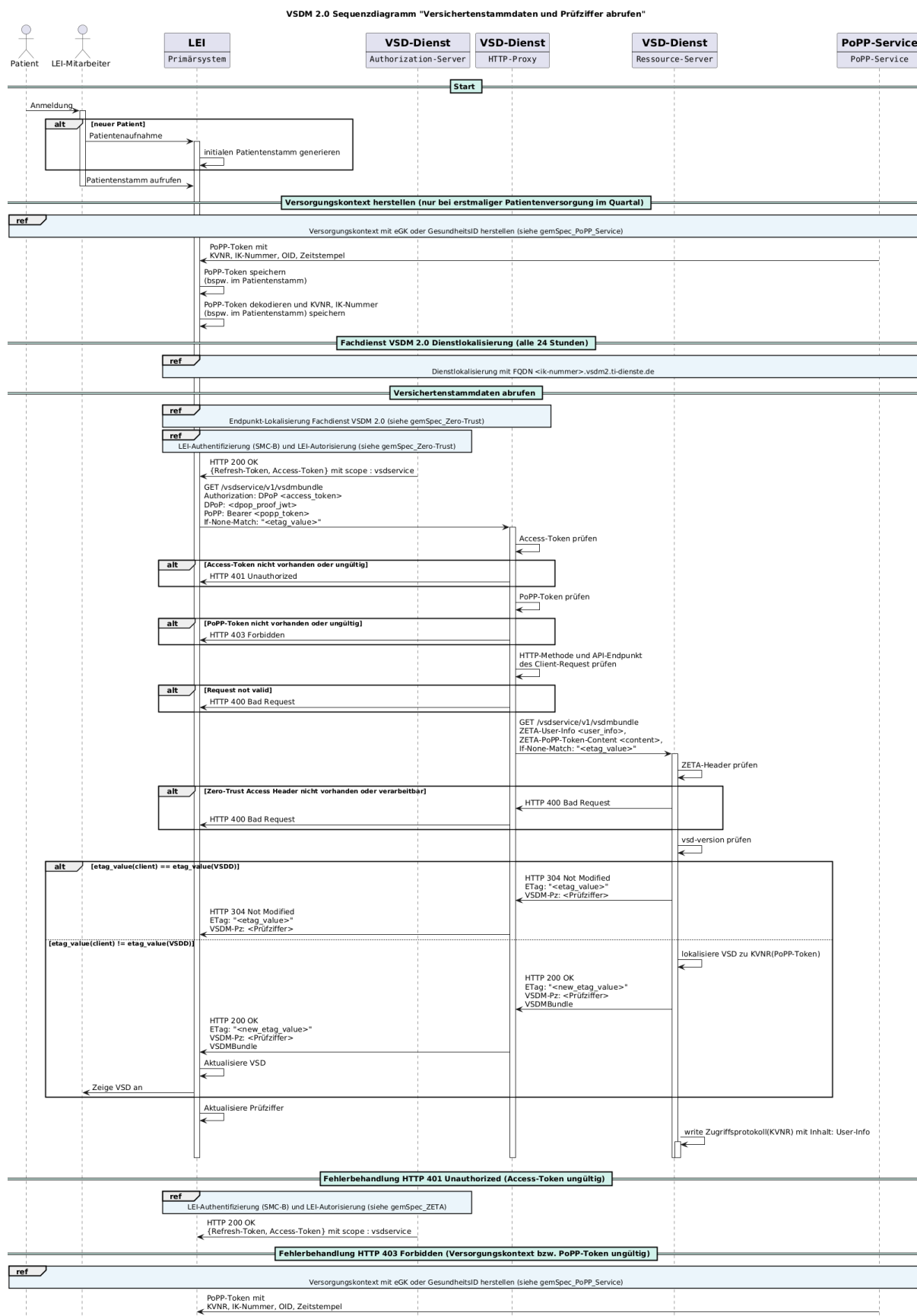


Abbildung 3: Sequenzdiagramm VSDM

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 Fachdienst MUSS die Systemzeit der betriebenen Komponenten (ZETA 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 Umgebungen Referenzumgebung ~~1~~RU1, Referenzumgebung ~~2~~~~und~~RU2, Testumgebung TU und Produktionsumgebung PU der TI werden fourth-level Domänen eingerichtet: .ref (RU1), .dev (RU2~~und~~), .test (TU) und .prod (PU).

~~Die endgültige Festlegung der fourth-level Domänen erfolgt mit der Finalisierung und Freigabe des neuen Testkonzeptes für die TI 2.0.~~

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

A_26800-01A_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>.prod.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 Übereinstimmung 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 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 Zugriffsprotokolleinträge 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 7.3- Zugriffsprotokoll für Versicherte formuliert.

A_26794-01 -Anbieter VSDM - Zugriffsprotokoll Zugriffsberechtigung prüfen

Der Anbieter des Fachdienstes VSDM MUSS sicherstellen, dass ausschließlich Versicherte, Mitarbeiter eines Kostenträgers oder einer Ombudsstelle Zugriff auf das Zugriffsprotokoll eines Versicherten erhalten. [\leq]

Hinweis:

(1) Der Zugriff durch Kostenträger oder Ombudsstellen darf ausschließlich auf Verlangen des Versicherten und zum Zweck der Beauskunftung gegenüber diesem erfolgen.

(2) A_26794-01 beschreibt die Sicht des Fachdienstes in Bezug auf die Nutzer des Fachdienstes. "Innere" Prozesse beim Betrieb des Fachdienstes, bspw. wenn Administratoren wie üblich (automatisierte) Datensicherungen durchführen, sind davon nicht betroffen.

A_26795-01 -Anbieter VSDM - Zugriffsprotokoll Zugriffsprotokollierung

Der Anbieter des Fachdienstes VSDM MUSS jeden Zugriff auf das Zugriffsprotokoll eines Versicherten gemäß A_26812-* (vgl. dort definierte "Informationsmodell Zugriffsprotokoll") im Zugriffsprotokoll protokollieren. [\leq]

A_26813-01 -Anbieter VSDM - Zugriffsprotokoll Schutz der Protokolldaten

Der Anbieter des Fachdienstes VSDM MUSS das Zugriffsprotokoll mit den gleichen oder sicherheitstechnisch mindestens äquivalenten Sicherheitsmaßnahmen in Bezug auf Vertraulichkeit, Integrität und Authentizität wie die VSD selbst schützen. [\leq]

Hinweis:

Der Zugriff auf die Zugriffsprotokolldaten erfolgt durch die schon etablierten Prozesse (Kassen-Apps oder Ombusstellen der Kassen). Über diese Prozesse können die VSD schon heute eingesehen und ggf. verändert werden. Die dabei umgesetzten Sicherheitsmechanismen in Bezug auf Vertraulichkeit, Integrität und Authentizität für die VSD oder mindestens gleichwertige Sicherheitsmechanismen sollen auch für den Schutz der Zugriffsprotokolldaten gemäß A_26813-* verwendet werden.

A_26796-01 -Anbieter VSDM - Zugriffsprotokoll Rückgabe im Bundle

Der Anbieter des Fachdienstes VSDM MUSS bei einem Abruf eines Zugriffsprotokolls die Ergebnisliste des Zugriffsprotokolls bei mehr als einem Eintrag als Ergebnis-Bundle (Ergebnis-Liste) an den Aufrufer zurückgeben, damit der Versicherte eine vollständige Einsicht in oder Auskunft über das Zugriffsprotokoll erhält. [\leq]

A_26797-01 -Anbieter VSDM - Zugriffsprotokoll Löschfrist veraltete Protokolleinträge

Der Anbieter des Fachdienstes VSDM Server MUSS Zugriffsprotokolleinträge nach 3 Jahren ab dem Erzeugungsdatum und innerhalb von einem Monat löschen, damit veraltete Einträge nach Ende der regulären Aufbewahrungsfrist entfernt werden. [\leq]

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

6.46.5 Berechtigungen

Grundsätzlich ist jede Leistungserbringerinstitution mit einer ProfessionOID gemäß A_26743 und 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 überFachdienst VSDM API/vsdservice abrufen	UC_2 VSD von eGK lesen	UC_3 Zugriffsprotokoll einsehen
Leistungserbringerinstitution	X	X	nicht erlaubt
Mitarbeiter Institution des Kostenträgers	X	nicht vorgesehen	eingeschränkt erlaubt
Mitarbeiter einer Ombudsstelle	nicht erlaubt	nicht vorgesehen	eingeschränkt erlaubt
Versicherter	nicht vorgesehen	nicht vorgesehen	X
Administrator einer Organisation oder Institution des Gesundheitswesens	nicht erlaubt	nicht erlaubt	nicht erlaubt
Mitarbeiter des VSDD-Betreibers	nicht erlaubt	nicht erlaubt	nicht erlaubt

Akteur	UC_1 VSD über Fachdienst VSDM API/vsdservice abrufen	UC_2 VSD von eGK lesen	UC_3 Zugriffsprotokoll einsehen
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

nicht anwendbar: Kein Regelungsbestandteil durch die gematik und im Rahmen dieser Spezifikation.

nicht vorgesehen: Rechtlich nicht verboten, aber nicht als Use Case vorgesehen.

eingeschränkt erlaubt: Die Verarbeitung der Daten ist ausschließlich auf Verlangen des Versicherten und nur zum Zwecke der Auskunft gegenüber dem Versicherten innerhalb des gesetzlichen Rahmens zulässig.

nicht erlaubt: Ist zu unterbinden.

Hinweis:

Die Regeln im Kontext UC_1 für Zugriffe auf die Fachdienst VSDM API/vsdservice werden technisch durch den ZETA Guard durchgesetzt.

6-56.6 Authentifizierung und Autorisierung von Nutzern

Die Authentifizierung von Nutzern bzw. Leistungserbringerinstitutionen (LEI) erfolgt durch die Komponente "Authorization Server" des ZETA Guard 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 "ZETA Client" realisiert und durch den VSDM Authorization-Server (SW-Komponente des ZETA Guard) 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_ZETA] und dem Produkttypsteckbrief [gemProdT_VSDM_2_FD] zu entnehmen.

6.66.7 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_ZETA]	
Authorization-Server	
siehe [gemSpec_ZETA]	
HTTP-Proxy	
siehe [gemSpec_ZETA]	
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 Prüfziffer sind in der Antwort enthalten.
304	Anfrage konnte erfolgreich bearbeitet werden. Das Clientsystem besitzt schon die aktuellsten Versichertenstammdaten und es erfolgt keine Aktualisierung. Der Prüfziffer ist in der Antwort enthalten.
400	79010 79011 79030 79031 79032 79205 79206 79207 79400 79401 79402
403	79041
404	79020

Resource-Server GET /vdservice/v1/vsdbundle	
405	79040
428	79033
500	79100
502	79110
504	79111

6.76.8 ZETA Guard

A_26809 -Anbieter VSDM - ZETA Guard Informationspflicht via Betriebshandbuch

Der Anbieter eines Fachdienst VSDM MUSS alle Informationen und Regelungen zu Bereitstellung, Konfiguration und Verwendung des ZETA Guard dem Betriebshandbuch des ZETA Guard Herstellers entnehmen und anwenden. [~~≤~~, ~~Anb_VSDM_2_FD~~, ~~Sich.techn. Eignung: Gutachten (Anbieter) ≤~~]

A_26810 -Anbieter VSDM - ZETA Guard VSDM Policy erstellen

Der Anbieter eines Fachdienst VSDM MUSS bei der Erstellung der Policy für einen Fachdienst VSDM mit der gematik zusammenarbeiten. [~~≤~~ [~~≤~~, ~~Anb_VSDM_2_FD~~, ~~funkt. Eignung: Anbietererklärung~~]

Hinweis: Die Erstellung und das Deployment der VSDM-Policy werden durch einen CID-Prozess gesteuert. Näheres zu diesem Prozess wird in [gemSpec_ZETA] definiert werden.

A_26811 -Anbieter VSDM - ZETA Guard Konfigurationsdateien erstellen

Der Anbieter eines Fachdienst VSDM MUSS die Konfigurationen (Manifest-Dateien) des ZETA Guard für alle VSDM-Umgebungen (Produktiv-, Referenz-, Test-, Entwicklungsumgebung) erstellen und der gematik zur Prüfung und Freigabe bereitstellen. [~~≤~~, ~~Anb_VSDM_2_FD~~, ~~funkt. Eignung: Anbietererklärung ≤~~]

Hinweis: Die Erstellung und das Deployment der Manifest-Dateien werden durch einen CID-Prozess gesteuert. Näheres zu diesem Prozess wird in [gemSpec_ZETA] definiert werden.

6.86.9 Sicherheit und Datenschutz

Ein VSDM2-FD bewahrt Zugriffsprotokolle für Versicherte drei Jahre auf (vgl. Abschnitt ~~6.4.3-5~~) 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 eines Fachdienst VSDM DARF KEINE Profile bilden. [~~=, Anb_VSDM_2_FD, Sich.techn. Eignung: Gutachten (Anbieter)<=~~]

A_26970 -Anbieter VSDM - Verarbeitung von Profildaten

Der Anbieter eines Fachdienst VSDM MUSS Daten zum Zwecke des Logging oder Monitoring, 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 eines Fachdienst VSDM DARF NICHT Daten an Dritte weitergeben. Dies betrifft insbesondere personenbeziehbare (medizinische) Daten oder Daten, die für eine Profilbildung genutzt werden können. [~~=, 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.

A_27404 -Anbieter VSDM - Sicherung der Datenverbindung zwischen HTTP-Proxy und Resource-Server

Der Anbieter eines Fachdienst VSDM MUSS die Datenverbindung zwischen HTTP-Proxy und Resource-Server entsprechend der in seiner Betreiberumgebung vorhandenen Umgebungsbedingungen sicherheitstechnisch ausreichend absichern.

[~~=, Anb_VSDM_2_FD, Sich.techn. Eignung: Anbietererklärung<=~~]

Erläuterung zu A_27404:

Verschiedene Umsetzungsvarianten erfordern unterschiedlich starke Sicherheitsmechanismen.

6.96.10 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:

6.9.16.10.1 Schnittstellen und Anwendungsfälle

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

6.9.26.10.2 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.

6.9.36.10.3 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. In dieser Zeit wird es notwendig sein, dass die angestrebte Transition mittels qualifizierter Unterstützungsleistungen von gematik und den Anbietern intensiv betreut wird.

Die Terminplanung sieht derzeit folgende Meilensteine ab einem Zeitpunkt T=0 vor (T wird zu einem späteren Zeitpunkt definiert):

- T=0: Beginn der kontrollierten Inbetriebnahme (KIB) von VSDM 2.
- T+1 Monat: Ende der KIB und Start 'Fokus auf die Modellregion'.
- T+3 Monate: Ende des Fokus auf die Modellregion.
- T+7 Monate: Offboarding der Fachdienste UFS, VSDD und CMS (VSDM 1).

Der Start (T=0) und das Erreichen der Meilensteine (T+) haben unterschiedliche Abhängigkeiten, die bis zu demjenigen Zeitpunkt vollständig aufgelöst werden müssen. Diese Abhängigkeiten und ein beispielhafter Ablauf werden nachfolgend kurz skizziert.

Die KIB wird intensiv von mindestens einem Transition-Manager der gematik begleitet, der u.a. bei der Anbieterzulassung VSDM 2 und abhängigen Nachweisführung ein Ansprechpartner ist. In der KIB MÜSSEN alle Instrumente des betrieblichen und sicherheitstechnischen Monitorings nachgewiesen werden. Dies gilt sowohl für PoPP, als auch für VSDM 2. Der Anbieter VSDM ist angehalten, das KIB-Verfahren binnen eines Monats mit Unterstützung der gematik vollständig abzuschließen.

Beginn der kontrollierten Inbetriebnahme (T=0):

Ab diesem Zeitpunkt findet dann ein Parallelbetrieb von VSDM 1 und VSDM 2 statt.

- Der PoPP-Service muss für den produktiven Betrieb bereit sein.
- Der Anbieter VSDM muss im Rahmen der KIB mindestens eine LEI suchen, in der die KIB durchgeführt werden kann.
- Der Anbieter VSDM muss im Rahmen der KIB mindestens zwei Versicherte suchen, die mit ihm diese KIB in der Praxis durchführen.
- Die Primärsysteme der KIB-Praxen müssen die VSDM2-, Zero-Trust und PoPP-Funktionen implementiert haben.
- Die Konnektorversion PTV 6 läuft erfolgreich in den KIB-Praxen.
- Bei der KIB müssen auch alle PoPP-Anwendungsfälle ausprobiert und validiert werden (eGK stecken, eGK kontaktlos, GesundheitsID-Versicherter, etc.), um den PoPP-Token zu erhalten und damit den Versichertenstammdatensatz abzurufen.

Ende der KIB und Start 'Fokus auf die Modellregion' (T+1 Monat):

Wenn eine Praxis bereits Software-seitig auf VSDM 2 umgestellt ist, kann die eGK dennoch mit der Konnektorfunktion "ReadVSD" ausgelesen werden. Dabei ist jedoch die Einschränkung vom PS-Hersteller "per default" vorzunehmen, sodass KEINE Onlineprüfung für VSDM 1 durchgeführt wird. Der Parameter "PerformOnlineCheck" muss gemäß [VSDM-A_2693] auf 'false' gesetzt werden.

Ende des Fokus auf die Modellregion (T+3 Monate):

Der Fokus auf die Modellregion wird in Rücksprache mit den Gesellschaftern beendet. Alternativ kann der Zeitraum erweitert werden. Die Empfehlung nach einem erfolgreichen Ende des Fokus auf die Modellregion kann z.B. ein bundesweiter Rollout sein.

Offboarding der Fachdienste UFS, VSDD und CMS - VSDM 1 (T+7 Monate):

Dieser Zeitpunkt ist der früheste Beginn der Ausgabe von eGKs mit verkürzten VSD. Das Offboarding der Fachdienste VSDM 1 kann beginnen.

~~6.9.3.16.10.3.1~~ Verfahren zum Umgang mit der strukturierten Prüzfiffer

Das Verfahren der strukturierten Prüzfiffer als Zugriffselement auf andere TI-Dienste aus dem Vorgängersystem VSDM 1 wird nicht weitergeführt. Stattdessen wird der originäre Sinn der Prüzfiffer 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 Prüzfiffer 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 Prüzfiffer) als Nachweismerkmal des Versorgungskontextes den Zugriff auf andere TI 2.0 Dienste mit ermöglicht.

~~6.106.11~~ 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.

Die Festlegungen hierzu werden in einem späteren Release nachgeführt.

~~6.116.12~~ Zulassung Fachdienste

Der konkrete Zulassungsschnitt und Zulassungsprozess für die VSDM Fachdienste inkl. der genutzten ZETA Guards befindet sich aktuell noch in Abstimmung.

Die Festlegungen hierzu werden in einem späteren Release nachgeführt.

~~6.126.13~~ 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.

Die Festlegungen hierzu werden in einem späteren Release nachgeführt.

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.

Die konkrete Ausgestaltung des Datensatzes befindet sich noch in Absprache zwischen den Gesellschaftern. Die in Abstimmung befindlichen Felder sind im logical model auf Simplifier mit "WIP" gekennzeichnet.

Die Festlegungen hierzu werden in einem späteren Release nachgeführt.

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.
	WOP	Kennzeichen für die Kassenärztliche Vereinigung, in deren Bezirk der Versicherte seinen Wohnsitz hat.
Persönliche Versicherungsdaten	Versicherten_ID	Die Versicherten-ID ist der 10-stellige unveränderliche Teil der 30-stelligen Krankenversichertennummer.
	Vorname	Gibt den Vornamen des Versicherten an.

Container	Feld	Beschreibung
	Nachname	Gibt den Nachnamen des Versicherten an.
	Geburtsdatum	Gibt das Geburtsdatum des Versicherten an.

7.3 Zugriffsprotokoll für Versicherte

A_26812-01 -Fachdienst VSDM - Zugriffsprotokoll Versicherte - Protokolleintrag ~~**A_26812 - VSDM Resource Server - Zugriffsprotokoll Versicherte -**~~

Protokolleintrag Der **Fachdienst VSDM Resource Server** MUSS bei jedem Aufruf der HTTP-GET Operation auf den Endpunkt `/vdservice/v1/vsdbundle` und damit auf die dedizierten Versichertenstammdaten sowie bei Zugriffen auf das Zugriffsprotokoll eines Versicherten **mindestens** folgende Informationen protokollieren:

Tabelle 10 : Informationsmodell_Zugriffsprotokoll

Information	Protokollelement	Protokollwert
Wann ist der Zugriff erfolgt? (Zugriff auf die VSD bspw. durch eine LEI, oder Zugriff auf die Zugriffsprotokolldaten)	Zugriffszeitpunkt	Zeitangabe kodiert im Format nach ISO-8601 Beispiel: "2024-11-22T10:00:00.123456" Zeitangabe als Unix-Zeit kodiert als natürliche Zahl (Nachkommastellen (d. h. Sekundenbruchteile) werden ggf. abgeschnitten.) Beispiel: 1750836932 Diese Angabe würde 25.06.2025 um 09:35:32 (MESZ) repräsentieren.
Wer hat zugegriffen?	Organisation	<commonName> (aus dem HTTP Header ZETA-User-Info oder ein menschenlesbares Äquivalent für Zugriffe von Kostenträgern oder Ombudsstellen, welches diesen eindeutig zugeordnet werden kann)

Information	Protokollelement	Protokollwert
	Organisationsbezeichnung	<organizationName> (optional, wenn vorhanden: aus dem HTTP-Header ZETA-User-Info oder ein menschenlesbares Äquivalent für Zugriffe von Kostenträgern oder Ombudsstellen)
	Organisationskennung	<Telematik-ID> (Feld identifiziert aus dem HTTP-Header ZETA-User-Info ; Institutionskennzeichen für Zugriffe von Kostenträger oder ein eindeutiges Äquivalent für Zugriffe von Ombudsstellen, wenn vorhanden)
Worauf wurde zugegriffen?	Daten	"Versichertenstammdaten" ODER "Zugriffsprotokoll"
Wer hat zugegriffen?	Zugreifender	<Vor- und Nachname des Versicherten> (für Protokoll-Zugriffe des Versicherten bspw. mittels App des Krankenversicherers) <commonName> (für VSD-Zugriffe einer LEI: aus dem HTTP-Header ZETA-User-Info ; für Protokoll-Zugriffe von Kostenträgern oder Ombudsstellen ein menschenlesbares Äquivalent, welches diesen eindeutig zugeordnet werden kann)
	Zusatz	<> (für Protokoll-Zugriffe des Versicherten: leeres Feld oder Element "Zusatz" kann auch entfallen) <organizationName> (für VSD-Zugriffe einer LEI und wenn vorhanden aus dem HTTP-Header ZETA-User-Info sonst "nicht bekannt"; für Protokoll-Zugriffe von Kostenträgern oder Ombudsstellen ein menschenlesbares Äquivalent)

Information	Protokollelement	Protokollwert
	Kennung	<p><KVNR> (für Protokoll-Zugriffe des Versicherten)</p> <p><Telematik-ID> (für VSD-Zugriffe einer LEI: Feld <i>identifier</i> aus dem HTTP-Header <i>ZETA-User-Info</i>)</p> <p><IK-NR> (Institutionskennzeichen für Protokoll-Zugriffe vom Kostenträger oder ein eindeutiges Äquivalent für Protokoll-Zugriffe von Ombudsstellen, wenn vorhanden)</p>
War der Zugriff erfolgreich?	Ergebnis	<p>"Versichertenstammdaten übermittelt." ODER "Versichertenstammdaten angefragt - Versichertenstammdatenübermittlung nicht notwendig." ODER "Übermittlung der Versichertenstammdaten nicht durchgeführt." ODER "Zugriffsprotokoll übermittelt." ODER "Übermittlung des Zugriffsprotokoll nicht durchgeführt."</p>

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

*Hinweis: Die Informationen <commonName> und <organizationName> Im Kontext VSDM werden über das Feld *additionalProperties* des mittels ZETA-User-Info übertragen Info Header die Nutzerinformationen gemäß [user-info-vsdm.yaml] übertragen.*

Hilfestellung zu ISO-8601 zur Unix-Zeit:

Code-Beispiel in python

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

```
$ python
Python 3.9.16 (main, Mar 8 2023, 22:47:22) [GCC 11.3.0] on cygwin
Type "help", "copyright", "credits" or "license" for more information.
>>> import time
>>> zugriffszeit=int(time.time())
>>> print(zugriffszeit)
1750839460
>>> # Nur zur Veranschaulichung in menschenlesbare Zeit konvertieren
```



```
>>> from datetime import datetime
>>> import tzlocal
>>> local_timezone = tzlocal.get_localzone()
>>> local_time = datetime.fromtimestamp(zugriffszeit, local_timezone)
>>> print(f"{zugriffszeit}:", local_time.strftime('Das entspricht %d.%m.%Y
um %H:%M:%S.'))
1750839460: Das entspricht 25.06.2025 um 10:17:40.
>>>
```

7.4 VSDM-Policy

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

7.5 VSDM-spezifische Konfigurationsdaten ZETA Guard

Die VSDM-spezifische Konfigurationen für die Komponenten des ZETA Guard müssen von dem Anbieter eines VSDM Fachdienstes nach dem Verfahren gemäß [gemSpec_ZETA] erstellt werden. Die zugehörigen Konfigurationsdateien (Manifest-Dateien) werden dem Anbieter eines Fachdienstes VSDM über das ZETA Git-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
ZETA	Zero Trust Access

Kürzel	Erläuterung
ZT	Zero-Trust
ZETA/ASL	Zero Trust/Additional Security Layer (ehemals VAU-Protokoll) Eine auf HTTP und basierende zusätzliche Verschlüsselung der Daten zwischen ZETA Client und ZETA Guard PEP. Die verschlüsselte Verbindung wird auch ZETA/ASL-Kanal genannt.

8.2 Glossar

Begriff	Erläuterung
Authorization-Server	Ist im Kontext VSDM eine Komponente des ZETA Guard 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	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.

Begriff	Erläuterung
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 § 352 SGB 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 Personen zusammengefassten Leistungserbringer (z.B. Arztpraxen, 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 Krankenhausinformationssystem (KIS) oder eine Apothekensoftware (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

Abbildung 1 : Kontextdiagramm VSDM	12
Abbildung 2 : Systemdiagramm VSDM	20
Abbildung 3: Sequenzdiagramm VSDM	49
Abbildung 1: Kontextdiagramm VSDM	12
Abbildung 2: Systemdiagramm VSDM	20
Abbildung 3: Sequenzdiagramm VSDM	49

8.4 Tabellenverzeichnis

Tabelle 1 : TAB_FACHDIENST_VSDM_FEHLERMELDUNGEN_FÜR_CLIENTSYSTEM	27
Tabelle 2 : TAB_VSDM_KONFIGURATIONSÜBERSICHT_ZETA_GUARD	29
Tabelle 3 : TAB_FACHDIENST_VSDM_ERLAUBTE_PROFESSION_OID	31
Tabelle 4 : TAB_FACHDIENST_VSDM_RESSOURCEN	33
Tabelle 5 : TAB_FACHDIENST_VSDM_FEHLER-REFERENZEN_UND_BDE-CODES	42
Tabelle 6 : TAB_FACHDIENST_VSDM_LOKALISIERUNG	51
Tabelle 7 : TAB_FACHDIENST_VSDM_BERECHTIGUNGSREGELN	54
Tabelle 8 : TAB_FACHDIENST_VSDM_HTTP_STATUS_CODES	56
Tabelle 9 : Übersicht der auf der eGK bereitgestellten Daten	61
Tabelle 10 : Informationsmodell_Zugriffsprotokoll	62
Tabelle 1 : TAB_FACHDIENST_VSDM_FEHLERMELDUNGEN_FÜR_CLIENTSYSTEM	27
Tabelle 2 : TAB_VSDM_KONFIGURATIONSÜBERSICHT_ZETA_GUARD	29
Tabelle 3 : TAB_FACHDIENST_VSDM_ERLAUBTE_PROFESSION_OID	31
Tabelle 4: TAB_FACHDIENST_VSDM_RESSOURCEN	33
Tabelle 5 : TAB_FACHDIENST_VSDM_FEHLER-REFERENZEN_UND_BDE-CODES	42
Tabelle 6 : TAB_FACHDIENST_VSDM_LOKALISIERUNG	51
Tabelle 7 : TAB_FACHDIENST_VSDM_BERECHTIGUNGSREGELN	54
Tabelle 8: TAB_FACHDIENST_VSDM_HTTP_STATUS_CODES	56
Tabelle 9: Übersicht der auf der eGK bereitgestellten Daten	61
Tabelle 10 : Informationsmodell_Zugriffsprotokoll	62

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
[ILF_VSDM_2]	gematik: Implementierungsleitfaden VSDM 2 https://github.com/gematik/spec-VSDM2
[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_ZETA]	gematik: Spezifikation Zero Trust Access (ZETA)
[gemAnbT_VSDM_2_FD]	gematik: Anbietertypsteckbrief Anbieter VSDM 2 Fachdienst
[gemProdT_VSDM_2_FD]	gematik: Produkttypsteckbrief VSDM 2 Fachdienst
[gemSST_PS_ZETA]	gematik: Steckbrief Prüfvorschrift Primärsystem-Schnittstelle Zero Trust Access
[VSDMErrorcodeVS]	gematik: FHIR ValueSet für die Anwendung VSDM https://simplifier.net/vsdm2/vsdm-errorcode-vs
[VSDM-Konfigurationsdatei]	gematik: Konfigurationsdatei(en) für den ZETA Guard 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.]

[Quelle]	Herausgeber: Titel
[OpenAPI_VSDM_2]	gematik: OpenAPI Spezifikation VSDM https://github.com/gematik/spec-VSDM2/blob/main/src/openapi/vsdm2.yaml
[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
[user-info-vsdm.yaml]	https://raw.githubusercontent.com/gematik/spec-VSDM2/refs/heads/main/src/schemas/user-info-vsdm2.yaml

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

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[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