Elektronische Gesundheitskarte und Telematikinfrastruktur

Richtlinie Verzeichnisdienst Datenübermittlung und Befüllung

Version:	1.0.0
Revision:	830482
Stand:	26.01.2024
Status:	freigegeben
Klassifizierung:	öffentlich
Referenzierung:	gemRL_VZD_DatUeb

Dokumentinformationen

Änderungen zur Vorversion

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

Dokumentenhistorie

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
1.0.0	26.01.2024		Erste Version	gematik

Inhaltsverzeichnis

1 Einordnung und Begriffsbestimmung 4
1.1 Zielsetzung 4
1.2 Zielgruppe 4
1.3 Rechtliche Einordnung 4
1.4 Abgrenzungen und mitgeltende Dokumentation 5
1.5 Methodik 5
2 Überblick des Verzeichnisdienstes 7
2.1 Architektur 7
2.2 Akteure und Rollen 7
2.3 Basis- und Fachdaten 9
2.3.1 Für die Administration wichtige Felder in den Basis- und Fachdaten 11
3 Erstbefüllung und Pflege 13
3.1 Schutzbedarf der Daten 13
3.2 Übergreifende technische und organisatorische Anforderungen 13
3.3 Überblick über die Prozesse 14
3.4 Erstbefüllung mit Basisdaten 15
3.5 Änderungen der Basisdaten 16
3.6 Hinzufügen, Ändern und Löschen von Fachdaten 17
3.6.1 KIM-Adresse im LDAP-VZD 17
3.6.2 TI-Messenger-ID im FHIR-VZD 18
3.7 Deaktivieren und Löschen eines Basisdatensatzes 19
4 Nutzung von Echtdaten in den Umgebungen 20
5 Anhang A – Verzeichnisse 21
5.1 Abkürzungen 21
5.2 Glossar 21
5.3 Abbildungsverzeichnis 21
5.4 Tabellenverzeichnis 21
5.5 Referenzierte Dokumente 22
5.5.1 Dokumente der gematik 22
5.5.2 Weitere Dokumente 22
6 Anhang B –Erläuterungen zum Schutzbedarf 24

1 Einordnung und Begriffsbestimmung

Der Verzeichnisdienst ist das elektronische Telefonbuch der Telematikinfrastruktur (TI). Der zentrale Dienst ermöglicht die Suche, Identifikation und Adressierung von angeschlossenen Nutzern. Im Verzeichnisdienst (VZD) werden die Namen, Adressen und andere öffentliche Daten von Leistungserbringern wie Ärzten, Apothekern und Krankenhäusern gespeichert, um sie durch andere Leistungserbringer und Versicherte auffindbar zu machen.

Die Suche findet beispielsweise innerhalb des TI-Messengers, der KIM-Anwendungen, des ePA-Clients und der E-Rezept-App statt. Ohne den VZD können in den Diensten keine Ärzte oder Apotheken gefunden und verschlüsselten E-Mails mit KIM versendet werden.

Authentizität und Integrität der gespeicherten und übermittelten Daten sind hierbei von überragender Bedeutung – ein Versicherter oder Leistungserbringer muss sich darauf verlassen können, dass der Name keine Schreibfehler enthält, Adresse und Fachgebiet aktuell sind und die gespeicherte KIM-E-Mail-Adresse zur richtigen Person oder Institution gehört.

1.1 Zielsetzung

Mit dem Erlass dieser Richtlinie erfüllt die Gesellschaft für Telematikinfrastruktur (gematik) ihren gesetzlichen Auftrag. Dazu gehört insbesondere der Betrieb des VZD, die Gewährleistung seiner bestimmungsgemäßen Nutzbarkeit, und die Sicherstellung der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der im VZD gespeicherten Daten. Indem die gematik geeignete organisatorische Maßnahmen trifft und bestimmte Regeln unter anderem für die Datenübermittlung an den VZD vorgibt, verbessert sie zugleich die Qualität der Nutzerdaten, die Sicherheit des VZD und den Schutz personenbezogener Daten.

1.2 Zielgruppe

Das vorliegende Dokument richtet sich an alle Institutionen oder Personen, welche Einträge im Verzeichnisdienst anlegen, ändern, löschen oder dies in Auftrag geben. Dies sind insbesondere die „Landesärztekammern, die Landeszahnärztekammern, die Kassenärztlichen Vereinigungen, die Kassenzahnärztlichen Vereinigungen, die Apothekerkammern der Länder, die Psychotherapeutenkammern, die Deutsche Krankenhausgesellschaft und die von den Ländern nach § 340 Fünftes Sozialgesetzbuch [SGB V] sowie von der [gematik] nach § 315 Abs. 1 SGB V bestimmten Stellen […] oder ein von ihnen beauftragter Dritter […]“ (Kartenherausgeber).

1.3 Rechtliche Einordnung

Im VZD werden zum Teil personenbezogene Gesundheits- und Sozialdaten verarbeitet. Der rechtliche Rahmen ergibt sich daher in erster Linie aus den Vorgaben des Sozialgesetzbuches (SGB), der Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung, [DSGVO]) und dem Bundesdatenschutzgesetz [BDSG].

Spezifische Vorgaben für den Betrieb des VZD und die an den VZD zu übermittelnden und im VZD zu speichernden Daten finden sich in § 313 SGB V. Dort ist geregelt, dass die oben unter 1.1 und 1.2 genannten Kartenhausgeber fortlaufend und in einem automatisierten Verfahren die bei ihnen vorliegenden Nutzer-Daten an den VZD übermitteln, § 313 Abs. 5 S. 1 SGB V. Die gematik legt die Vorgaben für diese Datenübermittlung in dieser verbindlichen Richtlinie fest, § 313 Abs. 4 S. 2 SGB V.

Die Kartenherausgeber werden durch § 340 [SGB V], die Heilberufsgesetze der Länder und die jeweiligen Spitzenorganisationen der Leistungserbringer näher bestimmt.

1.4 Abgrenzungen und mitgeltende Dokumentation

Diese Richtlinie enthält keine Hinweise zur lesenden Nutzung oder zur Suche im Verzeichnisdienst sowie keine Vorgaben zur Ausgabe von SMC-B (Security Module Card – Type B) oder Heilberufsausweisen (HBA).

Die HBA-Herausgaberichtlinie („Gemeinsame Policy für die Ausgabe der Heilberufsausweise, Zertifikatsrichtlinie Heilberufsausweis") enthält Sicherheitsanforderungen zur Ausstellung von Zertifikaten und Ausgabe elektronischer Heilberufsausweise.

Die Spezifikationen für den (FHIR-)VZD [gemSpec_VZD] und [gemSpec_VZD_FHIR_Directory] definieren die Funktionalität, Prozesse, Schnittstellen und das Informationsmodell des Verzeichnisdienstes. In der Übergreifenden Spezifikation PKI [gemSpec_PKI] werden grundlegende Festlegungen, unter anderem zur Telematik-ID, getroffen.

Der „Implementierungsleitfaden zur Pflege der Daten des Verzeichnisdienstes" [gemILF_Pflege_VZD] beschreibt, wie die Schnittstelle zur Pflege der Daten des Verzeichnisdienstes der TI clientseitig implementiert und genutzt werden kann.

Die verschiedenen Kartenherausgeber von HBA und SM(C)-B haben ihrerseits Anforderungskataloge zur Befüllung des VZD veröffentlicht, welche die Vorgaben für ihren Bereich detaillieren.

Diese Richtlinie gilt für die Produktivumgebung (PU) der TI und trifft, sofern nicht anders beschrieben, keine Aussagen über die Referenzumgebung (RU) und die Testumgebung (TU).

1.5 Methodik

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

Anwendungsfälle und Anforderungen werden im Dokument wie folgt dargestellt:
<AF-ID> - <Titel des Anwendungsfalles>

Text / Beschreibung
[<=]

bzw.

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

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

2 Überblick des Verzeichnisdienstes

2.1 Architektur

Der Verzeichnisdienst existiert zurzeit in zwei technischen Ausprägungen. Die erste verwendet das Lightweight Directory Access Protocol (LDAP) und wird vor allem von KIM-Anwendungen genutzt. Die zweite basiert auf Fast Healthcare Interoperability Resources (FHIR) und wird vom TI-Messenger zuerst verwendet. Im Laufe der Zeit sollen alle Anwendungen auf den FHIR-VZD migrieren, die LDAP-Variante wird perspektivisch nach 2026 außer Betrieb genommen und bis dahin nur noch begrenzt weiterentwickelt.

Die Erläuterungen in dieser Richtlinie beziehen sich vorwiegend auf die LDAP-Variante, auf Abweichungen beim FHIR-VZD wird explizit hingewiesen.

2.2 Akteure und Rollen

Beim Befüllen und der Pflege der Daten im Verzeichnisdienst gibt es die folgenden Akteure/Rollen und Verpflichtungen.

Tabelle 1 - Akteure und ihre Verpflichtungen im VZD

Akteur/Rolle	Beschreibung	Verpflichtungen im Rahmen des Verzeichnisdienstes
Kartenherausgeber	Zuständige Stelle gemäß § 340 [SGB V] für die Ausgabe einer SMC-B oder eines Heilberufsausweises (i.d.R. sind das die Länderberufskammern).	Der Kartenherausgeber ist für die korrekte Befüllung und Pflege der Basisdaten und der Zertifikate (für KIM) verantwortlich. (Er kann allerdings nicht die KIM-Adresse eintragen, das tut der Fachdienstanbieter.) Der Kartenherausgeber kann die Tätigkeit an einen TSP delegieren, er bleibt allerdings Verantwortlicher und Ansprechstelle.
TSP	Auch Vertrauensdiensteanbieter (VDA) genannt, ist für einen Kartenherausgeber tätig und für die Ausstellung, Überprüfung, Bewahrung und Sperrung von Zertifikaten zuständig. Ein TSP kann für mehrere Kartenherausgeber, auch unterschiedlicher Sektoren, tätig sein.	Der TSP kann bei Beauftragung dem Kartenherausgeber die Arbeit der Pflege von Basisdaten und Zertifikaten abnehmen.

Akteur/Rolle	Beschreibung	Verpflichtungen im Rahmen des Verzeichnisdienstes
Antragsteller	Natürliche Person (für einen HBA) oder eine Institution (für eine SMC-B), die eine Karte bei dem für sie zuständigen Kartenherausgeber beantragt.	siehe Ausweisinhaber
Ausweisinhaber	Natürliche Person oder Institution, die einen ausgegebenen Heilberufsausweis oder SMC-B erhält und für dessen Verwendung alleinig verantwortlich ist. Aufgrund der persönlichen oder institutionellen Bindung sind Ausweisinhaber, Zertifikatsinhaber und Antragsteller gewöhnlich identisch.	Ein Ausweisinhaber kann die im Verzeichnisdienst über ihn gespeicherten Daten bei seinem Kartenherausgeber einsehen oder anfragen.
Zertifikatsinhaber	Natürliche Person oder Institution, auf die ein Zertifikat ausgestellt wurde und in der alleinigen Kontrolle über den diesem Zertifikat zugeordneten privaten Schlüssel ist.	siehe Ausweisinhaber
Leistungserbringer und Institutionen	Ein **Leistungserbringer** (LE) im Sinne dieser Richtlinie ist eine durch einen HBA dargestellte Einzelperson des Gesundheitswesens, deren Daten im Verzeichnisdienst gespeichert sind oder werden sollen. Eine **Institution** (oder Leistungserbringer-Institution, LEI) ist eine durch eine SMC-B dargestellte Einheit des Gesundheitswesens (z.B. eine Arztpraxis, ein Krankenhaus, eine Apotheke), deren Daten im Verzeichnisdienst gespeichert sind oder werden sollen. *In dieser Richtlinie wird im Folgenden nur noch die Bezeichnung "Ausweisinhaber" verwendet.*	siehe Ausweisinhaber

Akteur/Rolle	Beschreibung	Verpflichtungen im Rahmen des Verzeichnisdienstes
Fachdienstanbieter	Anbieter eines Fachdienstes wie KIM oder TI-Messenger.	Die Rechte und Pflichten der Anbieter unterscheiden sich ja nach Fachdienst. Der KIM-Anbieter trägt die Daten der Ausweisinhaber (z.B. die KIM-E-Mail-Adresse) selbst ein und ändert diese bei Bedarf. Beim TI-Messenger sind die Ausweisinhaber selbst dazu in der Lage.
gematik	Die gematik ist die Koordinationsstelle und Aufsicht über den Verzeichnisdienst und für den Betrieb des Verzeichnisdienstes verantwortlich. Sie koordiniert das Zusammenspiel der verschiedenen Kartenherausgeber und stellt die Regeln für Befüllung und Pflege der Daten im VZD auf.	Die gematik koordiniert das Zusammenspiel der verschiedenen Kartenherausgeber, stellt die Regeln für Befüllung und Pflege der Daten auf und kontrolliert die Datenqualität im VZD im Sinne der gesetzlichen Governance.
Betreiber	Technischer Dienstleister, welcher im Auftrag der gematik den Verzeichnisdienst betreibt.	Der technische Betreiber des VZD nimmt im Normalfall lediglich Aufträge der gematik entgegen. Bei der Registrierung eines neuen Kartenherausgebers kann dieser aber auch mit dem Betreiber in Kontakt treten, um Probleme schneller zu lösen. Weitere Anforderungen an den Betreiber sind in den Spezifikationen des VZD geregelt. Darüber hinaus werden in dieser Richtlinie dem Betreiber keine Vorgaben gemacht.

2.3 Basis- und Fachdaten

Im Verzeichnisdienst gibt es zu jedem Ausweisinhaber (Leistungserbringer oder Institution) einen Basisdatensatz, welcher durch die Telematik-ID eindeutig identifiziert werden kann. Die Basisdaten enthalten zum Beispiel den Namen, die Postadresse und die Berufsgruppe des Leistungserbringers.

Die Fachdaten sind ihrem Namen entsprechend fachdienstspezifische Erweiterungen der Basisdaten. Für KIM (in den LDAP-Fachdaten als "KOM-LE" bezeichnet) wird eine E-Mail-

Adresse gespeichert, für den TI-Messenger eine entsprechende Adresse. Das System ist für Fachdaten weiterer Anwendungen erweiterbar. Die folgende Abbildung stellt ein Beispiel dar, die aktuelle Ausprägung befindet sich in der Spezifikation [gemSpec_VZD].

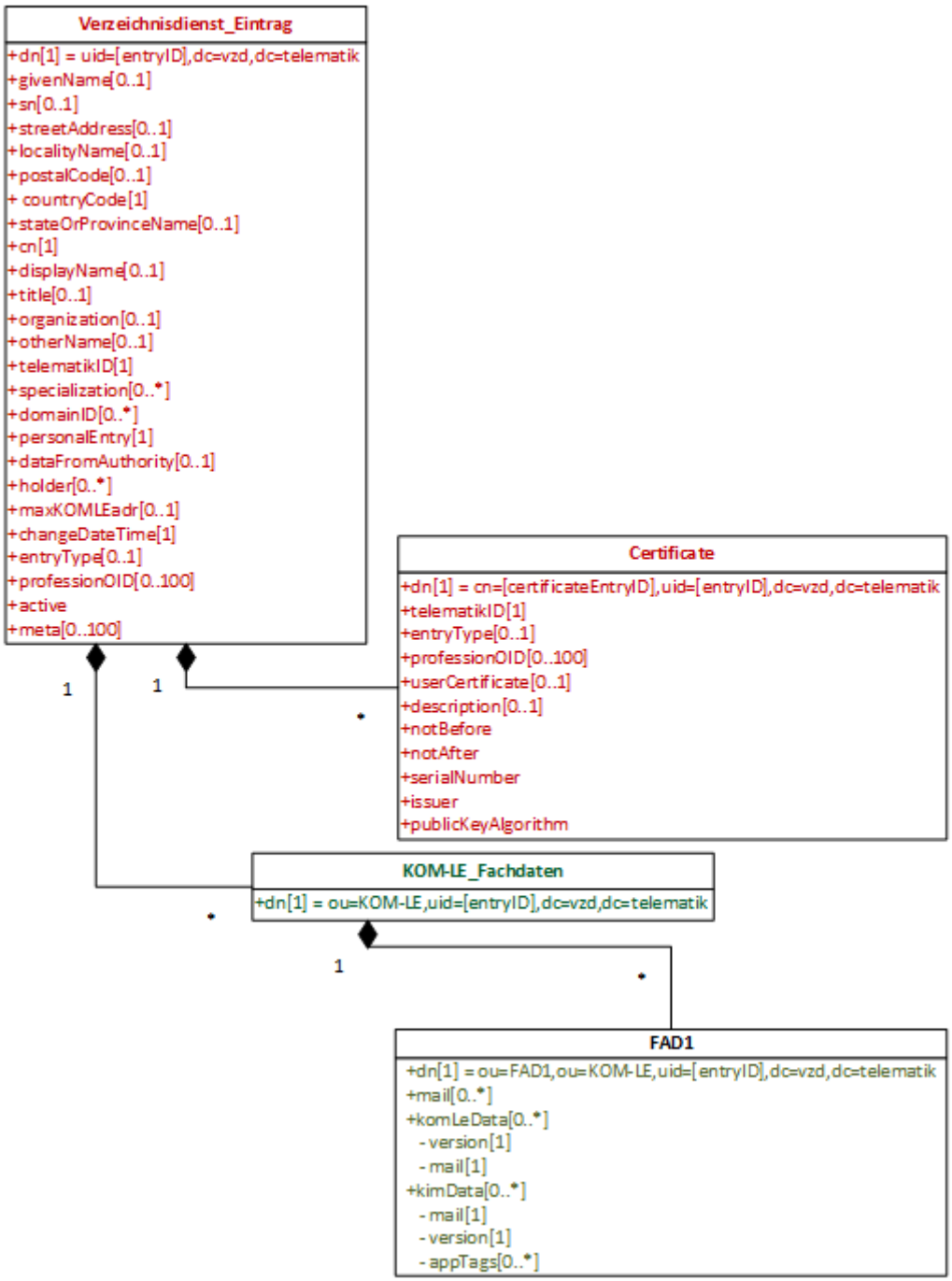

Abbildung 1 - Ein Datensatz im VZD mit Basisdaten (rot) und Fachdaten (grün)

2.3.1 Für die Administration wichtige Felder in den Basis- und Fachdaten

telematikID:

Die Telematik-ID ist ein eindeutiger Identifikator einer Institution oder einer Person in der TI, spezifiziert in [gemSpec_PKI#4.7].

domainID:

Die domainID ist die sektorspezifische Kennung einer Institution oder einer Person. Per Eintrag können mehrere Kennungen angeben werden. Im Gegensatz zur telematikID sind die domainID *nicht eindeutig* und können in mehreren Einträgen gleichzeitig vorkommen. Nur im Zusammenhang mit dem Feld "entryType" (welches aus dem Feld "professionOID" abgeleitet wird) kann die domainID eine Person oder Institution eindeutig identifizieren. Die Nutzung für die Sektoren wird in Kapitel**Attributtabellen** von Dokument [gemILF_Pflege_VZD] beschrieben.

displayName:

Dieses Attribut wird verwendet um vollen Namen einer Institution oder Person in der graphischen Oberfläche anzuzeigen. Die unterschiedliche Verwendung für Institutionen und Personen sowie Beispiele sind im Dokument [LDAP_Attribute] beschrieben.

userCertificate:

X509-Zertifikate werden für die Verschlüsselung der KIM-Nachrichten sowie bei der Berechtigungserteilung in der ePA verwendet.

komLeData:

Die komLeData enthält die Liste von KIM-Adressen mit der zugehörigen KIM-Version.

kimData:

Die kimData ist die neuere Version des Feldes komLeData und enthält wie diese eine Liste von KIM-Adressen mit KIM-Version, ergänzt durch Anwendungskennzeichen (appTags).

active:

Mit diesem Attribut im Basiseintrag kann der Kartenherausgeber oder TSP die Aufnahme des VZD-Eintrags in die flache Liste (in welcher die Suche stattfindet) steuern. Steht das Attribut auf "FALSE", wird der Basiseintrag aus der flachen Liste entfernt beziehungsweise nicht übertragen.

holder:

Enthält eine Liste von Organisationen, die für die Administration dieses Datensatzes berechtigt sind.

Das Holder-Attribut hat eine besondere Funktion bei der Steuerung der Schreibzugriffe auf die Basisdaten. Ein Datensatz mit leerem Holder-Attribut darf von jedem verändert werden. Für eine wirksame Berechtigungskontrolle ist es daher nötig, den Holder beim ersten Anlegen des Basisdatensatzes zu setzen - mindestens auf den verantwortlichen Kartenherausgeber und wenn beteiligt, den eintragenden TSP. Das Holder-Attribut fasst bis zu 100 Einträge. Damit können auch kooperierende Kartenherausgeber eingetragen oder ein Transfer eines

Datensatzes von einem Kartenherausgeber oder TSP zu einem anderen vorbereitet werden.

Auch die gematik hat keine Schreibrechte auf einen Basisdatensatz, wenn sie nicht als Holder eingetragen ist. Tritt der unwahrscheinliche Fall ein, dass sich ein Kartenherausgeber oder TSP aussperrt und der letzte eingetragene Holder nicht bei der Fehlerbehebung kooperiert, muss die gematik per Auftrag an den Betreiber das Holder-Attribut löschen lassen.

Eine weitergehende Erklärung der Wirkweise des „Holder"-Attributs findet sich im Kapitel 3.6 „Berechtigungen" im Implementierungsleitfaden [gemILF_Pflege_VZD].

Da die Fachdaten nicht durch das Holder-Attribut geschützt werden, können Fachdienstanbieter ihre Daten selbst ändern.

Änderungen am Zertifikat unterliegen nicht dem Schutz durch das Holder-Attribut. Der VZD lässt aber nur Zertifikate mit der passenden Telematik-ID zu.

Bei der Beantragung (Registrierung) des Zugangs zur „I_Directory_Administration"-Schnittstelle werden unter anderem die Art des Zugangs („nur lesen" oder „lesen und schreiben") und die Bezeichnung des Kartenherausgebers (die „Client-ID") für das Holder-Attribut festgelegt.

Eine komplette Liste der Attribute und weitere Erläuterungen finden sich im Implementierungsleitfaden [gemILF_Pflege_VZD].

3 Erstbefüllung und Pflege

3.1 Schutzbedarf der Daten

Die verarbeitende Stelle muss die Daten während der Verarbeitung und Speicherung sowohl mit technischen als auch organisatorischen Maßnahmen nach dem Stand der Technik entsprechend den festgelegen Schutzbedarfen schützen. Dabei ist besonders auf die korrekte (im Sinne der Authentizität und Integrität) Verarbeitung, Weitergabe und Eintragung der Daten zu achten. (Zum "Stand der Technik" kann die aktuelle "Handreichung zum Stand der Technik - Technische und organisatorische Maßnahmen" vom Bundesverband IT-Sicherheit e.V. / Teletrust herangezogen werden.)
Für die vorliegende Richtlinie ist nur die Einstufung der im Verzeichnisdienst gespeicherten oder zu speichernden Basisdaten und Fachdaten wichtig. Diese Daten und deren vorgesehene Verwendung im Sinne eines Telefonbuches oder einer Kontakt-Datenbank geben den Schutzbedarf vor. Entsprechend hat die gematik den Schutzbedarf der Daten wie folgt bestimmt; eine Erläuterung und Begründung findet sich im Anhang B.

Tabelle 2 - Schutzbedarf der Basis- und Fachdaten im VZD

Schutzziel	**Schutzbedarf der Basisdaten und Fachdaten**
Vertraulichkeit	**niedrig**
Integrität	**hoch**
Verfügbarkeit	**hoch**
Authentizität	**hoch**

Für die Übertragung innerhalb der TI und über die Administrations-Schnittstelle werden TLS-verschlüsselte Verbindungen nach dem Stand der Technik eingesetzt. Die entsprechenden Anforderungen wurden in den Produkttypsteckbriefen für den VZD und FHIR-VZD festgelegt.

3.2 Übergreifende technische und organisatorische Anforderungen

Für die Verarbeitungsschritte im Zuge der Befüllung und Pflege der Daten im Verzeichnisdienst sind einige grundlegende Anforderungen zu beachten.

A_24412 - Schutz der Zugangsdaten [Vertraulichkeit]
Die verarbeitende Stelle MUSS das Client-Secret für die Administrations-Schnittstelle so schützen, dass es nur wenigen, benannten und mit der Administration beauftragten Personen zur Kenntnis gelangt.**[<=]**

A_24413 - Nachverfolgbarkeit der Nutzung der Zugangsdaten
Die verarbeitende Stelle MUSS die Nutzung des Client-Secrets innerhalb ihrer Organisation audit-sicher dokumentieren.**[<=]**

Es sollte schriftlich festgehalten werden, welchen Personen das Client-Secret bekanntgegeben wurde, beziehungsweise wer es wann genutzt hat.

A_24414 - Vertrauenswürdiges und fachkundiges Personal
Die verarbeitende Stelle MUSS für die Verarbeitung von Daten des Verzeichnisdienstes vertrauenswürdiges und fachkundiges Personal einsetzen.**[<=]**

3.3 Überblick über die Prozesse

In der Befüllung und Pflege des Verzeichnisdienstes nimmt der Kartenherausgeber die wichtigste Rolle ein. Er ist verantwortlich für den Basisdatensatz. Er befüllt diesen nach Freigabe der Karte und ändert auf Wunsch des Antragstellers z.B. die Postadresse nach einer Verlegung des Praxissitzes. Der TSP steuert in den meisten Fällen das Zertifikat der Karte bei. Der Fachdienstanbieter (z.B. für KIM) verantwortet den Eintrag seiner Daten, wie der KIM-Adresse. Alle Beteiligten, welche Schreibzugriff auf den Verzeichnisdienst haben, können sich an den gematik Service-Desk wenden, um bei Problemen Hilfe zu erhalten.

Die folgende Graphik illustriert beispielhaft die Zusammenarbeit der einzelnen Akteure.

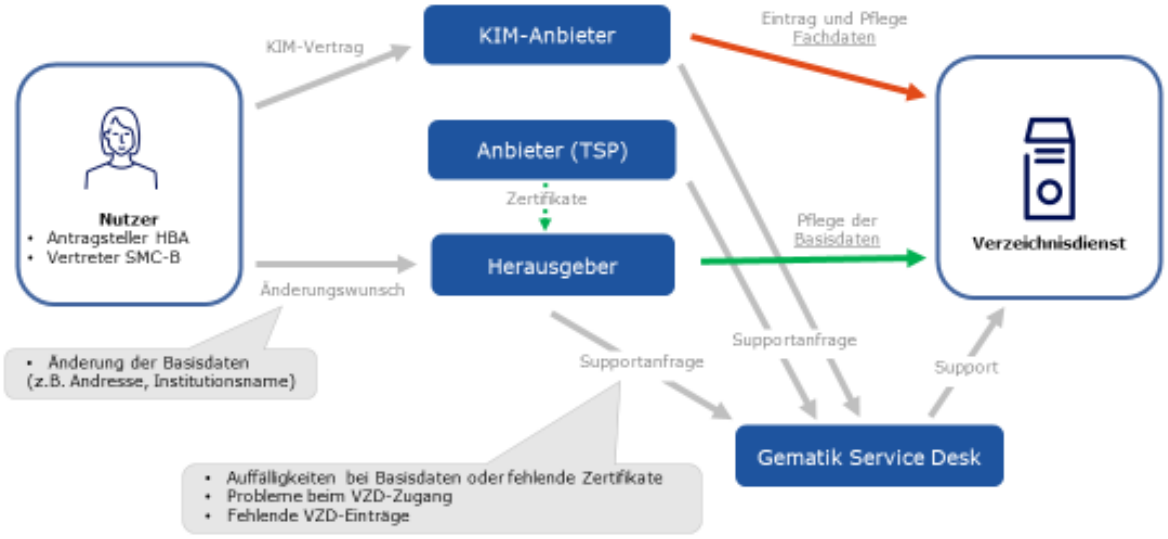

Abbildung 2 - Überblick über die Zusammenarbeit von Nutzern, Kartenherausgebern, TSPs, KIM-Anbietern und gematik beim Verzeichnisdienst

3.4 Erstbefüllung mit Basisdaten

Ein Basiseintrag ist die Grundlage für alle weiteren Operationen im Verzeichnisdienst und wird vom Kartenherausgeber (oder von einem TSP in dessen Auftrag) angelegt. Im folgenden Diagramm ist beispielhaft der Ablauf der Antragstellung für eine Karte einschließlich der Erstbefüllung dargestellt.

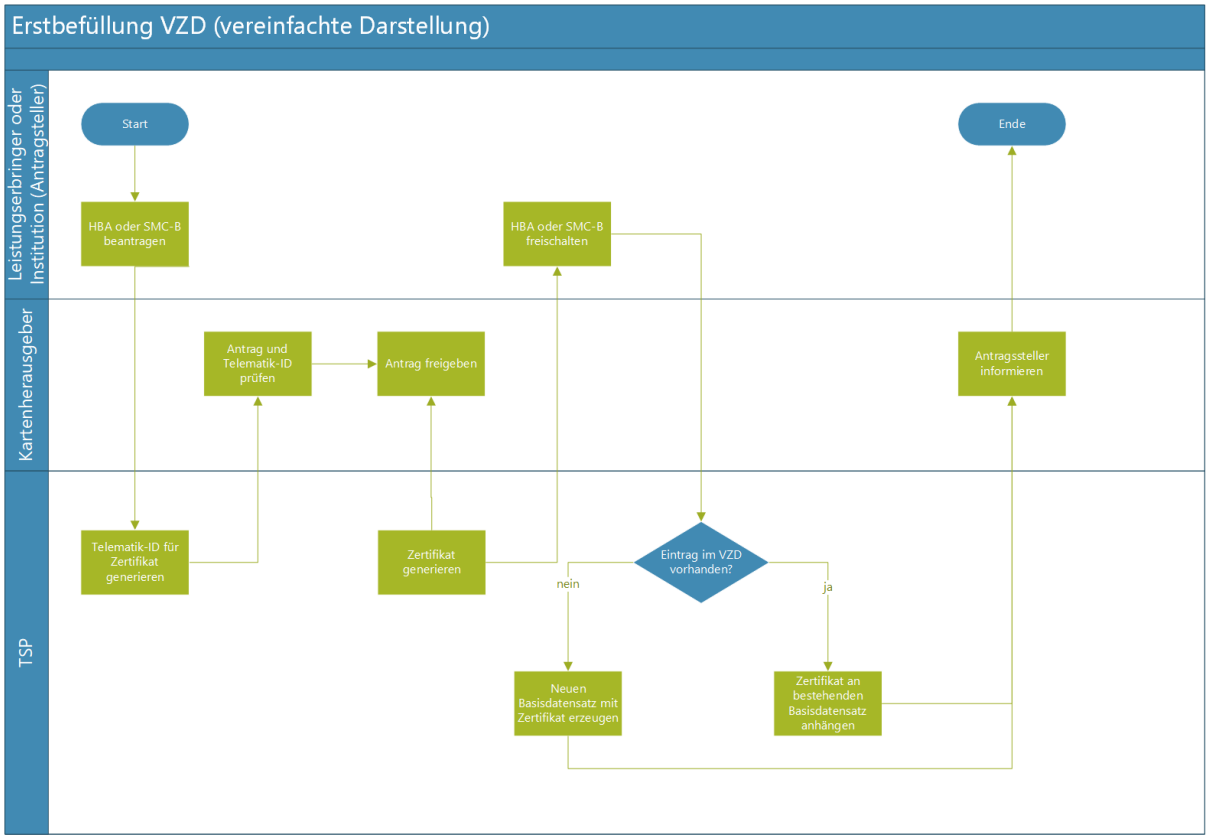

Abbildung 3 - Beispielhafter Ablauf der Kartenherausgabe und Erstbefüllung des VZD

Der Antragsteller startet den Prozess durch seinen Kartenantrag. Direkt im Anschluss wird eine Telematik-ID erzeugt und nach erfolgter Prüfung und Freigabe ein Zertifikat generiert. Nach der Freischaltung der Karte durch den Antragsteller wird üblicherweise ein neuer Basiseintrag mit den Zertifikaten im VZD angelegt oder, wenn es sich nur um eine Kartenerneuerung handelt, lediglich die Zertifikate an einen bestehenden Eintrag gehängt. Es ist aber auch möglich, das oder die Zertifikate zuerst hochzuladen - der VZD erzeugt dabei einen halbleeren Basiseintrag mit aus dem Zertifikat entnommenen Feldern, welcher inaktiv ist, bis der Basiseintrag weiter befüllt und aktiv geschaltet wird.

Die Pflege der Basisdaten erfolgt über die I_Directory_Administration-Schnittstelle.

Die Natur eines Kontaktverzeichnisses bedingt, dass Informationen für alle Teilnehmer abrufbar sind. Den beteiligten Ausweisinhabern muss klar sein, dass alle Daten, die sie für ihren HBA oder ihre SMC-B angegeben haben, auch über die TI einsehbar sein werden (siehe Erläuterung der Basisdaten). Fehlerfälle sind z.B. möglich, wenn Institutionsadressen mit Privatadressen von Ausweisinhabern vermischt werden, die für die Kartenherausgeber im Rahmen der Mitgliederverwaltung geführt werden.

A_24407 - Nur Institutionsadressen im VZD [Vertraulichkeit]
Im Verzeichnisdienst DÜRFEN AUSSCHLIESSLICH Institutionsadressen eingetragen werden.**[**<=**]**

A_24408 - Transparenz der Veröffentlichung im VZD [Integrität, Authentizität, Verfügbarkeit]
Der Kartenherausgeber oder TSP MUSS die Ausweisinhaber darauf hinweisen, welche Daten wie und wo von ihnen veröffentlicht werden.**[**<=**]**

A_24415 - Befüllung der obligatorischen Felder [Authentizität, Verfügbarkeit]
Bei der Erstbefüllung MÜSSEN alle Felder, die im Implementierungsleitfaden mit der Angabe "obligatorisch" geführt werden, befüllt werden, bevor der Basiseintrag per Flag aktiv geschaltet wird.**[**<=**]**

A_24416 - Setzen des Holder-Attributs auf Kartenherausgeber [Integrität, Verfügbarkeit]
Das Holder-Attribut MUSS mindestens auf den verantwortlichen Kartenherausgeber gesetzt werden.**[**<=**]**

A_24417 - Setzen des Holder-Attributs auf TSP [Integrität, Verfügbarkeit]
Übernimmt ein TSP im Auftrag eines Kartenherausgebers die Befüllung, SOLL er das Holder-Attribut **zusätzlich** auf sich selbst setzen.**[**<=**]**

A_24418 - Inkenntnissetzung des Antragsteller [Integrität, Authentizität, Verfügbarkeit]
Nach dem erfolgreichen Ersteintrag oder einer anderen Änderung in den Basisdaten oder Löschung des Basiseintrags MUSS der Antragsteller über die Änderung (inklusive der veränderten Daten) nachvollziehbar in Kenntnis gesetzt werden.**[**<=**]**

3.5 Änderungen der Basisdaten

Eine Änderung der Basisdaten wird im Normalfall durch den Kartenherausgeber veranlasst, welcher über den Zulassungsprozess Kenntnis von Namens-, Adress- und sonstigen Änderungen erlangt. Bei fehlerhaften Einträgen kann der Ausweisinhaber aber auch selbst an den Kartenherausgeber herantreten.

A_24419 - Frist für Korrekturanträge [Authentizität, Integrität]
Der Kartenherausgeber MUSS die vom Ausweisinhaber vorgebrachten Korrekturanträge binnen eines Monats auf Plausibilität prüfen und bei positivem Ergebnis in den Verzeichnisdienst übernehmen.**[**<=**]**

Die Basisdaten können nur durch den Kartenherausgeber oder einen vom ihm beauftragten TSP geändert werden. Dazu sollte das Holder-Attribut im Basisdatensatz entsprechend gesetzt worden sein (siehe oben). Auf Möglichkeiten von Änderungen bei anderen Holder-Attribut-Einträgen geht der Implementierungsleitfaden [gemILF_Pflege_VZD] ein.

A_24420 - Zusammenarbeit und Koordinationsstelle [Integrität, Authentizität, Verfügbarkeit]
Bei Änderungen, die ein Kartenherausgeber oder TSP nicht allein bewerkstelligen kann, MÜSSEN andere direkt Beteiligte (z.B. über das Holder-Attribut eingetragene) Kartenherausgeber oder TSP helfen. Die gematik ist dabei Koordinations- und Schlichtungsstelle.**[<=]**

In Ausnahmefällen, wenn es keinem Kartenherausgeber oder TSP möglich ist, die nötigen Korrekturen vorzunehmen, kann die gematik über einen Service-Request beauftragt werden, Änderungen oder eine Löschung von bestimmten Einträgen durchzuführen. Der Service-Request hat die Nummer SR 715.

3.6 Hinzufügen, Ändern und Löschen von Fachdaten

Die Aufnahme von Fachdaten in den Verzeichnisdienst ist freiwillig. Sie sorgt für eine bessere Erreichbarkeit der Ausweisinhaber. Fachdaten können erst nach dem Anlegen eines Basisdatensatzes im VZD eingetragen werden, da sie an diesen angehängt werden. Die Aufnahme von KIM- und TI-Messenger-Fachdaten unterscheidet sich wie folgt.

3.6.1 KIM-Adresse im LDAP-VZD

Die einzigen im LDAP-VZD genutzten Fachdaten sind Daten für KIM, darunter vor allem die KIM-E-Mail-Adresse. Die Daten werden durch den KIM-Anbieter an einen bestehenden Basisdatensatz angehängt. Besteht noch kein Basisdatensatz, schlägt die Operation fehl. Ein KIM-Anbieter kann keinen Basisdatensatz anlegen. Der KIM-Anbieter nutzt dazu die Schnittstelle "I_Directory_Application_Maintenance". Vor der erstmaligen Nutzung der Schnittstelle muss sich der KIM-Anbieter über die Prozess-Schnittstelle "P_Directory_Application_Registration" als zugelassener KIM-Anbieter registrieren.

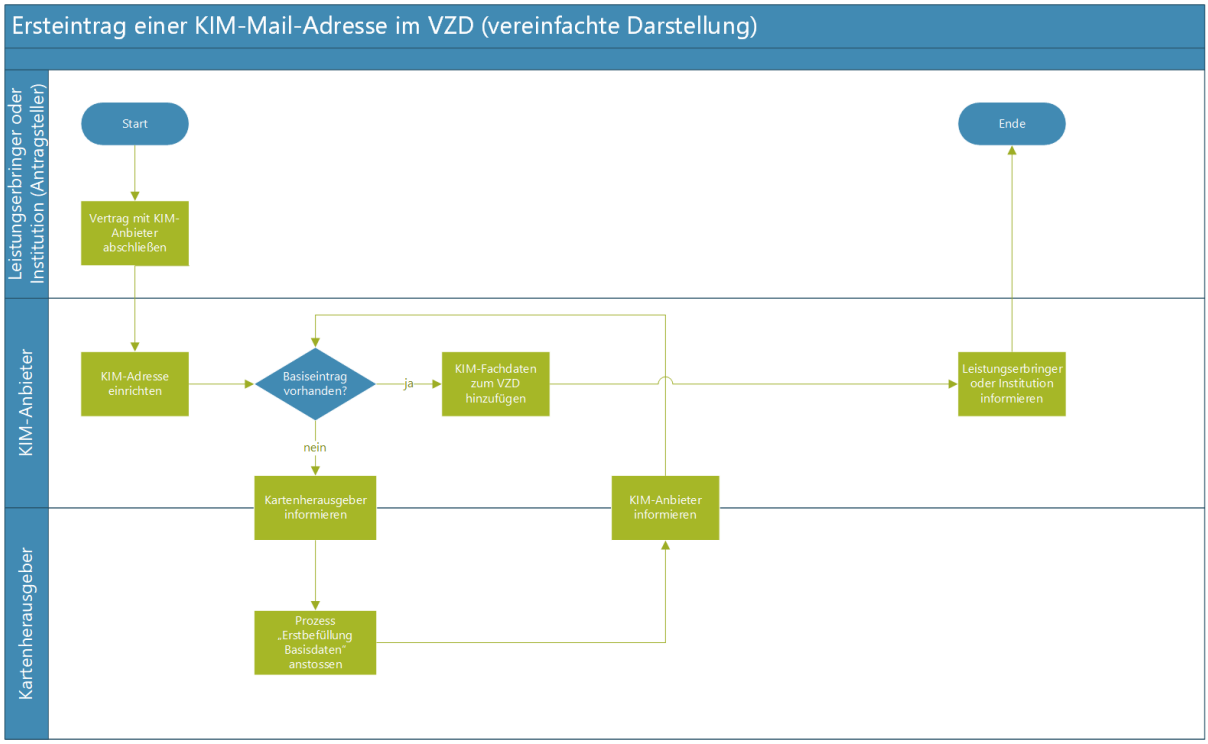

Abbildung 4 - Ersteintrag einer KIM-E-Mail-Adresse im VZD

A_24421 - Zuordnung der KIM-Adresse zum Basiseintrag [Integrität]
Der KIM-Anbieter MUSS die KIM-Adresse des Ausweisinhabers anhand der entsprechenden Telematik-ID an den korrekten Basiseintrag anhängen.**[<=]**

Der KIM-Anbieter übernimmt für den Ausweisinhaber auch Änderungen oder das Löschen der KIM-Fachdaten.

ACHTUNG: Die angehängten Fachdaten gehen beim Löschen des Basiseintrags ebenfalls verloren.

Weitere Hinweise zum Vorgehen geben die KIM-Spezifikationen und die Spezifikationen des Verzeichnisdienstes [gemSpec_VZD] und [gemSpec_VZD_FHIR_Directory].

3.6.2 TI-Messenger-ID im FHIR-VZD

Die TI-Messenger-ID (MXID, Adresse zum Erreichen eines anderen Messenger-Teilnehmers) kann im FHIR-VZD eingetragen werden. (Im LDAP-VZD gibt es dafür keine Möglichkeit.)

Im Gegensatz zur KIM-Adresse beim LDAP-VZD trägt der Ausweisinhaber die TI-Messenger-ID selbst in den FHIR-VZD ein. Dazu wird die Schnittstelle "FHIRDirectoryOwnerAPI" verwendet.

A_24422 - Eintragen der TI-Messenger-ID [Integrität, Authentizität, Verfügbarkeit]
Der Ausweisinhaber KANN seine TI-Messenger-ID selbst in den VZD eintragen.**[<=]**

Entscheidet sich der Ausweisinhaber gegen eine Veröffentlichung seiner TI-Messenger-ID, kann diese nicht über den Verzeichnisdienst gefunden werden. Der Ausweisinhaber

kann seine eigenen TI-Messenger-IDs über die oben genannte Schnittstelle auch selbst ändern und löschen.

3.7 Deaktivieren und Löschen eines Basisdatensatzes

A_24423 - Inaktiv-Setzen des Basisdatensatzes [Integrität, Authentizität, Verfügbarkeit]
Bei gelöschtem oder gesperrtem Zertifikat MUSS der Basisdatensatz per "active"-Attribut auf "inaktiv" (FALSE) gesetzt werden, sollte kein aktives Zertifikat mehr dem Basisdatensatz zugeordnet sein.**[**<=**]**

Der Kartenherausgeber entscheidet nach eigenem Ermessen und anhand der Situation des Ausweisinhaber, ob der Basisdatensatz lediglich deaktiviert oder endgültig gelöscht wird.

Ein Basisdatensatz kann technisch auf zwei Arten gelöscht werden. Die eine ist das manuelle Entfernen durch jemanden, der im Holder-Attribut vermerkt ist. (Ist das Holder-Attribut leer, kann den Eintrag allerdings jeder mit generellen Schreibrechten im VZD löschen.) Die andere Art des Löschens geschieht durch den VZD selbst - ist ein Basisdatensatz ein Jahr ohne Zertifikat, wird er automatisch entfernt.

Wird der Basisdatensatz gelöscht, werden alle angehängten Fachdaten ebenfalls gelöscht.

4 Nutzung von Echtdaten in den Umgebungen

Seitens der Kartenherausgeber gibt es den Bedarf, den Import von Echtdaten zu testen, bevor sie diese Echtdaten ins Produktivsystem des VZDs einspielen. Die normalen Referenz- und Testumgebungen sind allerdings für diesen Zweck ungeeignet, weshalb die gematik eine "virtuelle" Referenzumgebung bereitstellt, in der Echtdaten erlaubt sind.

Generell existiert die Telematikinfrastruktur in drei Ausprägungen:

- Produktivumgebung (PU): für die produktive Nutzung mit Echtdaten durch Kartenherausgeber (HBA und SMC-B) sowie von ihnen berechtigte Dritte,
- Referenzumgebung (RU): für den Test durch Kartenherausgeber (HBA und SMC-B) sowie von ihnen berechtigte Dritte,
- Testumgebung (TU): für den Test durch gematik-Mitarbeiter.

Für den VZD gestaltet sich die Übersicht der Umgebungen folgendermaßen:

- Die **PU** ist die Umgebung, welche den "echten" Verzeichnisdienst für die Nutzer bereitstellt. Kartenherausgeber und Fachdienstanbieter tragen hier die Echtdaten der Ausweisinhaber ein, welche anschließend von anderen Nutzern gefunden werden können.
- Die **RU** ist für technische Tests von Kartenherausgebern gedacht, Ausweisinhaber haben keinen Zugriff darauf. Die Anforderung TIP1-A_4191 aus dem "Testkonzept der TI" [gemKPT_Test] schließt die Nutzung von Echtdaten in RU und TU aus. Alle Datensätze ohne Testzertifikat werden regelmäßig gelöscht. (Dies betrifft Datensätze mit PU-Zertifikat als auch Datensätze ohne Zertifikat.)
- Die **vRU** (virtuelle Referenzumgebung) wird den Kartenherausgebern und TSP bei Bedarf bereitgestellt. Sie ist ausschließlich für den jeweiligen Antragsteller zugreifbar und gegen andere Zugriffe abgeschottet ist.

Der Kartenherausgeber oder TSP beantragt die Nutzung der vRU per E-Mail an das VZD-Postfach (vzd@gematik.de). Dabei kann der Antragsteller selbst bestimmen, wie lange seine vRU existieren soll (mindestens 10 Tage), eine Dauer von 10 Tagen ist voreingestellt. Die gematik erhält innerhalb von drei Werktagen den Zugang vom Betreiber und leitet ihn an den Antragsteller weiter.

Die vRU wird dem Kartenherausgeber oder TSP exklusiv zugewiesen, hochgefahren und nach dem Test wieder heruntergefahren und gelöscht.

5 Anhang A – Verzeichnisse

5.1 Abkürzungen

Kürzel	Erläuterung
IDP	Identity Provider - Bereitsteller einer (digitalen) Identität
LDAP	Lightweight Directory Access Protocol
TU	Testumgebung
PU	Produktivumgebung
RU	Referenzumgebung
vRU	virtuelle Referenzumgebung
FHIR	Fast Healthcare Interoperability Resources

5.2 Glossar

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

5.3 Abbildungsverzeichnis

Abbildung 1 - Ein Datensatz im VZD mit Basisdaten (rot) und Fachdaten (grün) 10
Abbildung 2 - Überblick über die Zusammenarbeit von Nutzern, Kartenherausgebern, TSPs, KIM-Anbietern und gematik beim Verzeichnisdienst 14
Abbildung 3 - Beispielhafter Ablauf der Kartenherausgabe und Erstbefüllung des VZD ...15
Abbildung 4 - Ersteintrag einer KIM-E-Mail-Adresse im VZD 18

5.4 Tabellenverzeichnis

Tabelle 1 - Akteure und ihre Verpflichtungen im VZD 7
Tabelle 2 - Schutzbedarf der Basis- und Fachdaten im VZD.....13

Tabelle 3 - Mögliche Einstufungen des Schutzbedarfs von niedrig bis sehr hoch 24

Tabelle 4 - Schutzbedarfsfeststellung der Basis- und Fachdaten im VZD mit Begründung 26

5.5 Referenzierte Dokumente

5.5.1 Dokumente der gematik

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

[Quelle]	Herausgeber: Titel
[gemGlossar]	gematik: Einführung der Gesundheitskarte – Glossar
[gemILF_Pflege_VZD]	gematik: Implementierungsleitfaden zur Pflege der Daten des Verzeichnisdienstes; https://github.com/gematik/api-vzd/blob/main/docs/gemILF_Pflege_VZD.adoc
[LDAP_Attribute]	gematik: LDAP-Attribute im gematik Verzeichnisdienst; https://github.com/gematik/api-vzd/blob/main/docs/LDAP_Attribute.adoc
[gemSpec_PKI]	Übergreifende Spezifikation PKI
[gemSpec_VZD]	Spezifikation Verzeichnisdienst
[gemSpec_VZD_FHIR_Directory]	Spezifikation Verzeichnisdienst FHIR-Directory
[gemKPT_Test]	Testkonzept der TI

5.5.2 Weitere Dokumente

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[HBA-Herausgaberichtlinie]	Gemeinsame Policy für die Ausgabe der Heilberufsausweise, Zertifikatsrichtlinie Heilberufsausweis
[SGB V]	Sozialgesetzbuch, Fünftes Buch, Gesetzliche Krankenversicherung
[DSGVO]	VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)
[BDSG]	Bundesdatenschutzgesetz (BDSG), Ausfertigungsdatum: 30.06.2017

6 Anhang B –Erläuterungen zum Schutzbedarf

Die vier vom Gesetzgeber für den Verzeichnisdienst geforderten Schutzziele sind:

- **Vertraulichkeit** bezeichnet den Schutz von Informationen vor unberechtigter Einsicht oder Offenlegung.
- **Integrität** beinhaltet den Schutz vor unautorisierten Änderungen an und vor dem Löschen von Informationen.
- **Verfügbarkeit** bedeutet, dass Informationen stets wie vorgesehen genutzt werden können.
- **Authentizität** umfasst die Echtheit, Überprüfbarkeit, Vollständigkeit und Vertrauenswürdigkeit von Informationen.

Die gematik nutzt bei der Einordnung des Schutzbedarfs die 4 Stufen „niedrig", „mittel", „hoch" und „sehr hoch". Potentielle Schäden werden in die 6 Kategorien

- Operative Auswirkungen
- Finanzielle Auswirkungen
- Auswirkungen auf die Reputation
- Compliance / rechtliche Auswirkungen
- Auswirkungen auf die informationelle Selbstbestimmung
- Auswirkungen auf Gesundheit und Sicherheit

gegliedert.

Die Stufen werden in der Risiko-Richtlinie näher erläutert, für das allgemeine Verständnis folgt hier eine Kurzfassung.

Tabelle 3 - Mögliche Einstufungen des Schutzbedarfs von niedrig bis sehr hoch

Schutzbedarf-Stufe	Erklärung
niedrig	Aus einem Verlust des Schutzziels folgt eine unwesentliche Beeinträchtigung des Geschäftsbetriebes. Ein möglicher finanzieller Schaden liegt unter 50.000 EUR. Ein Reputationsschaden wäre gering und nicht nachhaltig. Mögliche Verstöße gegen gesetzliche Vorgaben bewegen sich auf einem sehr geringen Niveau. Es gäbe tolerierbare Beeinträchtigungen des Selbstbestimmungsrechtes eines oder mehrerer Betroffener. Die Auswirkungen auf Gesundheit und Sicherheit können von Unbehagen bis zu leichten Verletzungen einer Person reichen.

Schutzbedarf-Stufe	Erklärung
mittel	Aus einem Verlust des Schutzziels folgt eine spürbare Beeinträchtigungen der Telematikinfrastruktur, die auch durch Stakeholder wahrgenommen wird mit wahrnehmbaren Funktionseinschränkungen für den Endnutzer. Ein möglicher finanzieller Schaden liegt unter 1.000.000 EUR. Die negativen Folgen auf die Reputation der gematik und/oder Telematikinfrastruktur werden als spürbar wahrgenommen, das Thema ist kurzzeitig, aber wahrnehmbar in den Medien. Die Folgen eines Verstoßes gegen gesetzliche, organisatorische bzw. vertragliche Vorgaben werden als spürbar, aber noch tolerierbar, eingeordnet. Es gäbe mäßige Beeinträchtigungen des Selbstbestimmungsrechtes eines oder mehrerer Betroffener. Die Auswirkungen auf Gesundheit und Sicherheit könnten erhelbliche Verletzungen einer Person oder Personengruppe sein.
hoch	Aus einem Verlust des Schutzziels folgt eine starke Beeinträchtigungen der Funktionsfähigkeit der Telematikinfrastruktur mit starken Auswirkungen auf die Zielerreichung oder starken Verzögerungen bei der Aufgabenerfüllung der gematik. Die Nutzerakzeptanz der Anwendung ist gefährdet. Für die gematik entsteht ein erheblicher und nachhaltiger Schaden unter 10.000.000 EUR. Eine negative Berichterstattung ist flächendeckend in landesweiten Medien zu erwarten, das Vertrauen in die gematik und/oder Anwendungen und Dienste der Telematikinfrastruktur würde für einen abgrenzbaren Zeitraum beschädigt sein. Verstöße gegen Gesetze führten zu erheblichen Konsequenzen für die gematik. Der Eintritt des Schadensereignisses hätte gravierende Beeinträchtigungen für das informationelle Selbstbestimmungsrecht eines oder mehrerer Betroffener zur Folge. Es könnte schwere Verletzungen oder Todesfälle geben.
sehr hoch	Aus einem Verlust des Schutzziels folgt eine sehr starke Beeinträchtigung der Funktionsfähigkeit der Telematikinfrastruktur bzw. massive Funktionseinschränkungen für einen überwiegenden Teil der Endnutzer. Die Nutzerakzeptanz ist möglicherweise langfristig beschädigt. Für die gematik entsteht ein Schaden gößer als 10.000.000 EUR, für institutionelle Teilnehmer der TI eventuell mehr. Die Reputation der gematik und der Telematikinfrastruktur ist gravierend und dauerhaft geschädigt. Die Folgen eines Verstoßes gegen gesetzliche bzw. vertragliche Vorgaben wären sehr hohe Strafzahlungen oder Freiheitsstrafen. Nicht tolerierbare Beeinträchtigungen für das informationelle Selbstbestimmungsrecht eines oder mehrerer Betroffener wären die Folge. Es bestünde akute Gefahr für Leib und Leben.

Für die vorliegende Richtlinie ist nur die Einstufung der im Verzeichnisdienst gespeicherten oder zu speichernden Basisdaten und Fachdaten wichtig. Die gematik hat den Schutzbedarf der Daten wie folgt bestimmt:

Tabelle 4 - Schutzbedarfsfeststellung der Basis- und Fachdaten im VZD mit Begründung

Schutzziel mit Einschätzung	**Begründung**
Vertraulichkeit: **niedrig**	Die Daten des VZD sind für alle Zugriffsberechtigten öffentlich. Ein Verlust der Vertraulichkeit führt absehbar weder zu einem Verstoß gegen Gesetze, einer Beeinträchtigung der persönlichen Unversehrtheit oder informationellen Selbstbestimmung und auch nicht zu finanziellen Auswirkungen.
Integrität: **hoch**	Der Verzeichnisdienst enthält postalische Adressen, KIM-Mail-Adressen und andere Kontaktdaten, Zertifikate und andere Fachdaten. Ein Verlust der Integrität dieser Informationen kann zu Datenschutzvorfällen, falschen Berechtigungsvergaben, falscher Zuordnung von postalischen Adressen und Fachrichtungen und letztlich einem Ansehensverlust des Dienstes (und der gematik) führen, die den Betrieb des Dienstes gefährdet. Ein Verstoß gegen Gesetze, eine Beeinträchtigung der persönlichen Unversehrtheit, eine Beeinträchtigung der informationellen Selbstbestimmung sowie finanzielle Auswirkungen wären mögliche Folgen.

Schutzziel mit Einschätzung	Begründung
Verfügbarkeit: **hoch**	Die Nicht-Verfügbarkeit kann dazu führen, dass benötigte Verschlüsselungszertifikate nicht verfügbar sind. Diese auf anderem Wege zur Verfügung zustellen, kann sehr aufwändig sein. Im schlimmsten Fall wird auf die verschlüsselte Übermittlung der Daten verzichtet. Die Nicht-Verfügbarkeit kann dazu führen, dass Informationen auf dem Verzeichnisdienst nicht aktualisiert oder gelöscht werden können (z.B. nicht mehr aktuelle Verschlüsselungszertifikate). Daher könnten ggf. in Prozessen ungültige Informationen verwendet werden, die Auswirkungen auf die Sicherheit haben bzw. Arbeitsabläufe negativ beeinflussen ((Schadensszenario Beeinträchtigung der Aufgabenerfüllung). Der VZD wird weiterhin für die Erteilung von Berechtigungen durch den Versicherten in der ePA genutzt. Hieraus ergibt sich ein sehr hoher Schutzbedarf im Schutzziel Verfügbarkeit. Ein Verstoß gegen Gesetze, eine Beeinträchtigung der persönlichen Unversehrtheit, eine Beeinträchtigung informationellen Selbstbestimmung sowie finanzielle Auswirkungen sind aufgrund des Verlustes der Verfügbarkeit nicht zu erwarten.
Authentizität: **hoch**	Der Verzeichnisdienst enthält postalische Adressen, KIM-Mail-Adressen und andere Kontaktdaten, Zertifikate und andere Fachdaten. Er ist „das Telefonbuch der TI", welches die oben genannten Daten für KIM, ePA, E-Rezept, den TI-Messenger und kommende Anwendungen bereitstellt. Als zentrale Instanz hängt von ihm die korrekte Zuordnung der Suche zu den Suchergebnissen ab, wann immer ein Patient oder Ausweisinhaber eine KIM-Mail verschicken, eine Berechtigung vergeben, eine Postadresse aufsuchen oder anschreiben möchte. Ein Verlust der Integrität dieser Informationen kann zu Datenschutzvorfällen, falschen Berechtigungsvergaben, falscher Zuordnung von postalischen Adressen und Fachrichtungen und letztlich einem Ansehensverlust des Dienstes (und der gematik) führen, die den Betrieb des Dienstes gefährdet. Ein Verstoß gegen Gesetze, eine Beeinträchtigung der persönlichen Unversehrtheit, eine Beeinträchtigung der informationellen Selbstbestimmung sowie finanzielle Auswirkungen wären mögliche Folgen. Mit der Authentizität eines Verzeichnisses steht und fällt seine Daseinsberechtigung.