

Elektronische Gesundheitskarte und Telematikinfrastruktur

Grobkonzept Vertretungsfunktion (anwendungsübergreifend)

Version: 1.0.0_CC
Revision: 1711118
Stand: 01.09.2026
Status: zur Abstimmung freigegeben
Klassifizierung: öffentlich_Entwurf
Referenzierung: gemKPT_Vertretungsfunktion

Dokumentinformationen

Gender-Hinweis

Aus Gründen der besseren Lesbarkeit wird in diesem Dokument überwiegend die männliche Form verwendet. Sämtliche Personenbezeichnungen gelten gleichermaßen für alle Geschlechter.

Änderungen zur Vorversion

Es handelt sich um eine Erstveröffentlichung.

Dokumentenhistorie

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
1.0.0_CC	24.06.202 6		initiale Erstellung, Version zur Kommentierung	gematik

Inhaltsverzeichnis

1 Management Summary.....	6
2 Einleitung.....	7
2.1 Einordnung des Grobkonzeptes.....	7
2.2 Ausgangslage und Motivation.....	7
2.3 Zielsetzung.....	8
3 Rollen und Begriffe.....	9
3.1 Verwendete Begriffe.....	9
3.2 Rollen.....	9
3.2.1 Rollen und Begriffe im Anwendungsbereich "Sorgerecht".....	10
4 Fachliches Zielbild.....	11
4.1 Fachliche Grundprinzipien der Vertretungsfunktion.....	11
4.2 Grundlegender Ablauf.....	12
4.3 Fachlicher Geltungsbereich.....	13
4.4 Lebenszyklus einer Vertretung.....	13
4.5 Unterstützte Anwendungen.....	14
5 Die Vertretungsfunktion im Überblick.....	16
5.1 Nutzer.....	16
5.2 Funktionsbereiche.....	17
5.2.1 Registrierung.....	17
5.2.2 Gültigkeitsabfrage.....	17
5.2.3 Auskunft.....	17
5.2.4 Protokollierung.....	18
6 Epics und User Stories.....	19
6.1 Anlegen einer Vertretung.....	19
6.1.1 Sorgerecht.....	19
6.1.2 Gewillkürte Vertretung.....	19
6.2 Bereitstellen von Nachweisen.....	19
6.2.1 Sorgerecht.....	19
6.2.2 Gewillkürte Vertretung.....	20
6.3 Bestätigung einer Vertretung.....	20
6.3.1 Sorgerecht.....	20
6.3.2 Gewillkürte Vertretung.....	20
6.4 Bearbeitung einer Vertretung.....	21
6.4.1 Gewillkürte Vertretung.....	21
6.5 Ablehnen, Beenden und Sperren einer Vertretung.....	21

76	6.5.1 Sorgerecht.....	21
77	6.5.2 Gewillkürte Vertretung.....	22
78	6.6 Verwendung von Vertretungen in Anwendungen.....	22
79	6.7 Nutzererlebnis und Transparenz.....	23
80	6.7.1 Hilfestellungen.....	23
81	6.7.2 Übersicht.....	23
82	6.7.3 Benachrichtigungen.....	24
83	6.7.4 Nutzerprotokolle und Nutzerdaten.....	24
84	7 Einordnung in die Telematikinfrastuktur.....	26
85	7.1.1 Allgemeine Sicherheits- und Datenschutzbetrachtung.....	26
86	7.1.1.1 Grundannahmen.....	26
87	7.1.1.2 Erwägung alternativer Lösungen.....	26
88	7.1.2 Ersatzverfahren und barrierefreier/analoger Zugang.....	27
89	8 Technisches Konzept.....	28
90	8.1 Fachliches Informationsmodell.....	28
91	8.1.1 Grundlegende Objekte.....	29
92	8.1.1.1 Vertretung.....	29
93	8.1.1.2 Versicherter.....	29
94	8.1.1.3 Gesundheitsanwendung.....	29
95	8.1.1.4 Nachweis.....	30
96	8.1.1.5 Kostenträger.....	31
97	8.1.1.6 Protokoll-Eintrag.....	31
98	8.1.2 Registrierungstypen.....	32
99	8.1.2.1 Registrierung einer gewillkürten Vertretung.....	32
100	8.1.2.2 Registrierung einer Vertretung aufgrund elterlicher Sorge.....	32
101	8.2 Status und Statusübergänge von Vertretungen.....	33
102	8.3 Umsetzung der Vertretungsfunktion in der TI 2.0.....	36
103	8.3.1 Assets und Schutzbedarfe.....	36
104	8.3.2 Sicherheitsanforderungen an den Systemaufbau.....	37
105	8.3.2.1 Adaption der HCSL für die Bestätigung von Vertretungen.....	37
106	8.3.3 Systemaufbau.....	38
107	8.3.3.1 Vertretungsregister.....	39
108	8.3.3.2 Gesundheitsanwendung FdV.....	40
109	8.3.3.3 Push-Benachrichtigungsdienst.....	41
110	8.3.3.4 Federation Master und sektoraler IdP.....	41
111	8.3.3.5 Gesundheitsanwendung Fachdienst.....	41
112	8.3.3.6 IT-System des Kostenträgers.....	41
113	8.3.4 Schnittstellen.....	41
114	8.3.4.1 Schnittstelle zum Fachdienst.....	41
115	8.3.4.2 Schnittstellen des Vertretungsregisters.....	42
116	8.3.4.2.1 Auskunftsschnittstelle.....	45
117	8.3.4.2.2 Verwendung der Gültigkeitsabfrage.....	47
118	8.4 Integration in die Zero Trust Architektur (ZETA).....	48
119	8.4.1 Erweiterung der ZETA Komponenten.....	48
120	8.4.1.1 Erweiterungen des ZETA Client SDK.....	48
121	8.4.1.2 Erweiterungen des ZETA Guards.....	49
122	8.4.2 Abfrage, Autorisierung und Ausübung einer Vertretung.....	49
123	8.5 Integration in nutzende Gesundheitsanwendungen.....	53
124	8.5.1 Integration in das Gesundheitsanwendung FdV.....	53

125	8.5.1.1 Verwendung des ZETA Client.....	53
126	8.5.1.1.1 Variante 1: Nur Verwendung von Vertretungen.....	53
127	8.5.1.1.2 Variante 2: Registrierung und Verwendung von Vertretungen.....	54
128	8.5.1.2 Integration ohne ZETA.....	55
129	8.5.2 Integration in den Gesundheitsanwendung Fachdienst.....	55
130	8.5.2.1 Verwendung des ZETA Guard.....	55
131	8.5.2.2 Integration ohne ZETA.....	55
132	8.6 Integration in PoPP.....	56
133	8.7 Umsetzung der Registrierungsprozesse.....	56
134	8.7.1 Vollmacht – gewillkürte Vertretung.....	56
135	8.7.1.1 Vollmacht erteilen per FdV.....	57
136	8.7.1.2 Vollmacht erteilen per eGK+PIN.....	57
137	8.7.1.3 Vollmacht erteilen in schriftlicher Form.....	58
138	8.7.2 Einrichten einer Vertretung aufgrund elterlicher Sorge.....	61
139	8.7.2.1 Sorgerecht eintragen mit eGK+PIN des Kindes.....	61
140	8.7.2.2 Sorgerecht eintragen ohne eGK des Kindes.....	61
141	8.8 Aufbau des Nutzerprotokolls.....	62
142	9 Anhang A – Verzeichnisse.....	64
143	9.1 Abkürzungen.....	64
144	9.2 Abbildungsverzeichnis.....	66
145	9.3 Tabellenverzeichnis.....	66
146	9.4 Referenzierte Dokumente.....	66
147	9.4.1 Dokumente der gematik.....	66
148	9.4.2 Weitere Dokumente.....	67
149	10 Anhang C – Offene Punkte, Fragen.....	68
150	10.1 <offener Punkt oder Frage>.....	68
151		

1 Management Summary

Das vorliegende Grobkonzept beschreibt eine anwendungsübergreifende Vertretungsfunktion als zukünftige Plattformleistung der Telematikinfrastruktur (TI). Ziel ist die einheitliche, sichere und nachvollziehbare Verwaltung von Vertretungsbeziehungen zwischen Versicherten, sodass diese in unterschiedlichen digitalen Gesundheitsanwendungen wiederverwendet werden können.

Die Vertretungsfunktion adressiert den steigenden Bedarf, digitale Gesundheitsdienste stellvertretend für andere Personen nutzen zu können. Dies betrifft insbesondere Eltern minderjähriger Kinder sowie Personen, die Angehörige oder vertraute Personen bei der Nutzung digitaler Gesundheitsanwendungen unterstützen. Gleichzeitig leistet die Lösung einen Beitrag zur Umsetzung europäischer Anforderungen an sogenannte Proxy Services im Rahmen des European Health Data Space (EHDS).

Kern des Konzepts ist die zentrale Erfassung und Verwaltung von Vertretungsbeziehungen. Vertretungen sollen möglichst einmalig erfasst und anschließend anwendungsübergreifend nutzbar gemacht werden. Die Vertretungsfunktion bestätigt dabei ausschließlich das Bestehen einer gültigen Vertretungsbeziehung. Die konkrete Ausgestaltung von Berechtigungen und Zugriffsrechten verbleibt weiterhin in der Verantwortung der jeweiligen Fachanwendung.

Im Fokus der ersten Ausbaustufe stehen das Einstellen von Vertretungsbeziehungen durch die Versicherten selbst oder durch die Kostenträger auf Basis festgestellter Vertretungsbeziehungen. Das Konzept definiert die erforderlichen Rollen, Prozesse sowie die Integration in die bestehende TI-Architektur. Die Ausgestaltung der Legitimationsprüfungen von Vertretungen sind explizit nicht Teil dieses Grobkonzeptes und verbleiben in Verantwortung der Kostenträger.

Durch die Einführung einer zentralen Vertretungsfunktion sollen redundante Einrichtungsprozesse reduziert, die Nutzererfahrung verbessert und die Integration von Vertretungsregelungen in bestehende und zukünftige Gesundheitsanwendungen vereinfacht werden. Gleichzeitig schafft das Konzept die Grundlage für zukünftige Erweiterungen auf weitere Vertretungsarten und Anwendungsbereiche.

2 Einleitung

2.1 Einordnung des Grobkonzeptes

Das vorliegende Grobkonzept einer anwendungsübergreifenden Vertretungsfunktion beschreibt eine neue Plattformleistung der Telematikinfrastruktur (TI), die sowohl von TI-Anwendungen als auch von weiteren Anwendungen im Gesundheitswesen genutzt werden kann. Das Konzept dient als Grundlage für die weitere fachliche Abstimmung im Kreis der Gesellschafter der gematik und soll im Anschluss zu einem Feature-Dokument beziehungsweise einer Spezifikation weiterentwickelt werden. Darüber hinaus soll es Stakeholdern bereitgestellt werden, die als Hersteller oder Anbieter von Komponenten, Diensten und Anwendungen der TI die Vertretungsfunktion als Lösungsbaustein umsetzen oder integrieren möchten und aus dieser Perspektive Hinweise zur geeigneten Ausgestaltung der Lösung geben können.

Kapitel 2 beschreibt die Motivation, Zielsetzung und den fachlichen Kontext der anwendungsübergreifenden Vertretungsfunktion.

Kapitel 3 definiert die relevanten Rollen, Begriffe und grundlegenden Prinzipien der Vertretungsregelung.

Kapitel 4 erläutert das fachliche Zielbild, den Geltungsbereich sowie den Lebenszyklus von Vertretungen.

Kapitel 5 gibt einen Überblick über die Vertretungsfunktion, ihre Nutzer und die zentralen Funktionsbereiche.

Kapitel 6 beschreibt die fachlichen Anwendungsfälle und User Stories zur Einrichtung, Verwaltung und Nutzung von Vertretungen.

Kapitel 7 betrachtet die Einordnung der Vertretungsfunktion in die Telematikinfrastruktur sowie Sicherheits- und Datenschutzaspekte.

Kapitel 8 stellt das technische Konzept einschließlich Informationsmodell, Systemarchitektur, Schnittstellen und Integrationsszenarien vor.

2.2 Ausgangslage und Motivation

Mit der zunehmenden Digitalisierung des Gesundheitswesens steigt der Bedarf, digitale Gesundheitsanwendungen auch stellvertretend für andere Personen nutzen zu können. Bereits heute bestehen in unterschiedlichen Kontexten fachliche und rechtliche Anforderungen, bei denen Versicherte durch andere Personen vertreten werden oder Unterstützung bei der Nutzung digitaler Anwendungen benötigen.

Dies betrifft insbesondere:

- Eltern, die für ihre minderjährigen Kinder handeln,
- Angehörige oder vertraute Personen, die unterstützungsbedürftige Versicherte begleiten,
- Versicherte mit eingeschränkter digitaler Teilhabe,

- sowie Personen, die aus praktischen oder gesundheitlichen Gründen Unterstützung bei der Nutzung digitaler Anwendungen wünschen.

Aktuell werden Vertretungsbeziehungen in vielen Anwendungen individuell und anwendungsspezifisch umgesetzt. Dies führt dazu, dass Versicherte Vertretungen für eine Person mehrfach einrichten muss. Darüber hinaus bestehen Unterschiede hinsichtlich der Nutzerführung, der technischen Integration und der Nachvollziehbarkeit bestehender Vertretungen. Mit der zunehmenden Verbreitung digitaler Anwendungen innerhalb und außerhalb der Telematikinfrastruktur entsteht daher der Bedarf nach einer einheitlichen, interoperablen und anwendungsübergreifenden Vertretungsfunktion.

Darüber hinaus verpflichtet Artikel 4 der EHDS-Verordnung die Mitgliedstaaten zur Bereitstellung sogenannter „Proxy Services“, die einen Zugriff auf Gesundheitsdaten in Vertretung ermöglichen sollen. Der Vorschlag zur Umsetzung einer anwendungsübergreifenden Vertretungsfunktion ist damit nicht nur bedarfsorientiert, sondern zugleich eine Voraussetzung zur Erfüllung europäischer Vorgaben.

Die im Konzept beschriebene Vertretungsfunktion soll es Versicherten ermöglichen, eine Vertretung einmalig einzurichten und diese in verschiedenen Anwendungen des Gesundheitswesens nutzen zu können. Dabei müssen besondere Anforderungen an Datenschutz, Informationssicherheit, Nachvollziehbarkeit und Nutzerfreundlichkeit berücksichtigt werden. Vertretungsbeziehungen betreffen regelmäßig besonders schützenswerte Informationen über familiäre, persönliche oder rechtliche Verhältnisse und erfordern daher ein hohes Maß an organisatorischer und technischer Absicherung.

Vor diesem Hintergrund beschreibt das vorliegende Grobkonzept die fachlichen Grundlagen und den möglichen Aufbau einer anwendungsübergreifenden Vertretungsfunktion als zukünftige Plattformleistung der Telematikinfrastruktur.

2.3 Zielsetzung

Ziel der anwendungsübergreifenden Vertretungsfunktion ist die Vereinfachung und Vereinheitlichung der sicheren Einrichtung, Nutzung und Verwaltung von Vertreterberechtigungen in verschiedenen TI-Anwendungen.

Die Vertretungsfunktion ersetzt dabei nicht die anwendungsspezifischen Berechtigungsregeln. Sie stellt vielmehr eine übergreifende Plattformfunktion bereit, mit der Vertretungsbeziehungen anwendungsübergreifend nachgewiesen und gegenüber nutzenden Anwendungen bestätigt werden können.

Vertretungen oder Vollmachten sollen hierzu möglichst nur einmalig erfasst werden, sodass diese den nutzenden Anwendungen bei Bedarf ohne anwendungsspezifische Einrichtung bestätigt werden. Die Vertretungen können dabei durch Kostenträger oder rein digital ohne Beteiligung des Kostenträgers eingerichtet werden. Erfasste Vertretungen sollen von den beteiligten Personen jederzeit eingesehen und verwaltet werden können.

Die Vertretungsfunktion soll sowohl für Nutzer der GesundheitsID als auch für Nutzer der elektronischen Gesundheitskarte (eGK) nutzbar sein. Gleichzeitig soll sie auch Versicherte unterstützen, die über kein eigenes Frontend oder keine eigene eGK verfügen. Darüber hinaus soll die Nutzung vorhandener Identifikationsmittel – beispielsweise der eGK und der PIN der vertretenen Person – eine möglichst einfache Einrichtung von Vertretungen ermöglichen.

3 Rollen und Begriffe

3.1 Verwendete Begriffe

Vertretung, Vertretungsbeziehung

Mit Vertretungsbeziehung - oder kurz Vertretung - ist die formale Beziehung gemeint, die

- zwischen einem Versicherten und seinem Vertreter besteht und
- unabhängig von der Relevanz und tatsächlichen Nutzung in einer bestimmten TI-Anwendung
- und oftmals zeitlich beschränkt gilt.

Im Kontext der technischen Umsetzung wird eine Vertretung durch die Vertretungsfunktion digital erfasst, gespeichert und berechtigten Anwendungen und Nutzern gegenüber bestätigt.

Beispiel: Sorgeberechtigung eines Elternteils für ein leibliches, minderjähriges Kind.

Vertretungsberechtigung

Damit ist eine konkrete Berechtigung gemeint, die

- auf einer Vertretungsbeziehung beruht,
- im Kontext einer Anwendung gilt und
- dem Vertreter die praktische Ausübung seiner Rechte als Vertreter in dieser Anwendung ermöglicht.

Im Kontext der technischen Umsetzung ergeben sich die anwendungsspezifischen Vertretungsberechtigungen ausgehend von den aktuell vorliegenden Vertretungsbeziehungen. Die Ermittlung und ggf. Verwaltung dieser Berechtigungen ist Gegenstand der jeweiligen Anwendung.

Beispiel: Berechtigung eines Elternteils, stellvertretend für sein Kind auf bestimmte Funktionen und Daten der Elektronische Patientenakte (ePA) zuzugreifen.

Zuständiger Kostenträger

In diesem Konzept wird davon ausgegangen, dass der Kostenträger des zu vertretenden Versicherten ggf. den Eintrag einer Vertretung bestätigt, sofern die Vertretung nicht eigenständig durch die beteiligten Versicherten selbst eingerichtet werden kann. Im Folgenden ist daher mit "zuständiger Kostenträger" stets der Kostenträger des zu vertretenden Versicherten gemeint.

3.2 Rollen

Bei der Erfassung und Verwaltung von Vertretungen (siehe auch Kapitel 5) sind verschiedene Akteure in unterschiedlichen Rollen beteiligt:

Vertreter

Ein Versicherter (GKV oder PKV), der stellvertretend für einen anderen Versicherten

gesundheitliche Angelegenheiten erledigt, insbesondere als Nutzer von Gesundheitsanwendungen.

Hinweis: In einer zukünftigen Ausbaustufe könnten hier auch institutionelle Vertreter hinzukommen, etwa Mitarbeiter von Pflegeeinrichtungen.

Vertretener

Der Vertretene - oder auch der zu Vertretende - ist stets ein Versicherter (GKV oder PKV). Dieser kann, aber muss nicht selbst aktiver Nutzer einer Gesundheitsanwendung sein.

3.2.1 Rollen und Begriffe im Anwendungsbereich "Sorgerecht"

Elternteil, Sorgeberechtigter

Der Elternteil - oder der/die Sorgeberechtigte -, hat aufgrund einer gesetzlichen Regelung oder richterlichen Entscheidung das elterliche Sorgerecht für sein versichertes, minderjähriges Kind.

Kind

Der minderjährige Versicherte, der im oben beschriebenen Sinne vertreten wird, also nicht nur leibliche Kinder, sondern auch Kinder im Sinne des elterlichen Sorgerechts bis zur Vollendung des 15. Lebensjahres.

4 Fachliches Zielbild

4.1 Fachliche Grundprinzipien der Vertretungsfunktion

Die anwendungsübergreifende Vertretungsfunktion basiert auf mehreren fachlichen Grundprinzipien, welche die sichere, nachvollziehbare und interoperable Nutzung von Vertretungsbeziehungen in Anwendungen des Gesundheitswesens ermöglichen sollen.

Nutzung der eigenen Identität des Vertreters

Der Vertreter nutzt zur Authentisierung und zur Nutzung von Anwendungen stets seine eigene digitale Identität. Die Vertretungsfunktion ermöglicht dabei keinen Identitätswechsel und keine gemeinsame Nutzung von Benutzerkonten.

Greift ein Vertreter auf Daten oder Funktionen einer Anwendung zu, erfolgt dies nachvollziehbar in seiner Rolle als Vertreter einer anderen Person. Aktionen des Vertreters bleiben dadurch jederzeit einer konkreten natürlichen Person zuordenbar.

Trennung zwischen Vertretungsfunktion und Fachanwendung

Die Vertretungsfunktion stellt ausschließlich die fachliche Information bereit, dass eine gültige Vertretungsbeziehung zwischen zwei Personen besteht.

Die konkrete Entscheidung,

- auf welche Daten zugegriffen werden darf,
- welche Funktionen genutzt werden dürfen,
- und welche Einschränkungen gelten,

verbleibt weiterhin in der Verantwortung der jeweiligen Anwendung.

Die Vertretungsfunktion ersetzt somit keine anwendungsspezifischen Berechtigungs- oder Autorisierungskonzepte.

Wiederverwendung registrierter Vertretungen

Vertretungsbeziehungen sollen möglichst nur einmalig erfasst werden. Anschließend können bestehende Vertretungen gegenüber nutzenden Anwendungen bestätigt werden, ohne dass die zugrunde liegenden Nachweise erneut geprüft werden müssen.

Dadurch sollen:

- wiederholte Prüfprozesse vermieden,
- Verwaltungsaufwände reduziert werden

Nachvollziehbarkeit und Transparenz

Vertretungsbeziehungen sowie deren Nutzung sollen für die betroffenen Versicherten nachvollziehbar sein.

Versicherte sollen insbesondere:

- bestehende Vertretungen einsehen,
- Statusänderungen nachvollziehen,
- sowie Informationen über die Nutzung ihrer Vertretungen erhalten können.

Unterstützung unterschiedlicher Zugangswege

Die Vertretungsfunktion soll sowohl für Nutzer der GesundheitsID als auch für Nutzer der elektronischen Gesundheitskarte (eGK) nutzbar sein.

Darüber hinaus sollen auch Versicherte berücksichtigt werden,

- die über kein eigenes digitales Endgerät verfügen,
- die kein eigenes Frontend nutzen,
- oder die digitale Anwendungen nicht selbst bedienen können oder möchten.

Hierzu können ergänzende organisatorische oder unterstützende Verfahren erforderlich sein.

Erweiterbarkeit der Vertretungsfunktion

Das vorliegende Konzept fokussiert sich zunächst auf ausgewählte Vertreterbeziehungen im familiären Umfeld. Die Vertretungsfunktion soll jedoch grundsätzlich so ausgestaltet werden, dass zukünftige Erweiterungen möglich bleiben.

Dies betrifft insbesondere:

- zusätzliche Vertreterrollen,
- weitere Anwendungskontexte,
- digitale Nachweise,
- europäische Vorgaben,
- sowie zukünftige Wallet- oder Registerlösungen.

Kostenträgerübergreifende Vertretungsbeziehungen

Die Vertretungsfunktion unterstützt in ihrer ersten Ausbaustufe Vertretungsbeziehungen zwischen Versicherten unabhängig von deren Krankenversicherungszugehörigkeit. Sowohl der Vertreter als auch die vertretene Person können bei demselben oder bei unterschiedlichen Kostenträgern versichert sein. Dies umfasst Versicherte der gesetzlichen Krankenversicherung (GKV) ebenso wie Versicherte der privaten Krankenversicherung (PKV).

4.2 Grundlegender Ablauf

Die Vertretungsfunktion ermöglicht die anwendungsübergreifende Erstellung, Bearbeitung, Bestätigung und Nutzung von Vertretungsbeziehungen. Der Vertreter greift dabei mit seiner eigenen Identität auf die Daten und Anwendungsfunktionen des Vertretenen zu. In einem Vertretungsregister sind die verifizierten Vertretungsbeziehungen sicher hinterlegt. Die Anwendung, auf die der Vertreter in Vertretung zugreifen möchte, kann die Information über die Vertretungsbeziehung im Register für die Umsetzung von Zugriffsberechtigungen abrufen. Falls ein Eintrag im Vertretungsregister ungültig wird, verfallen automatisch die darauf beruhenden Zugriffsberechtigungen.

Die Einrichtung einer Vertretung kann dabei auf rein digitalem Weg über das Frontend des Versicherten (FdV) beider Personen oder alternativ durch den zuständigen Kostenträger erfolgen.

Das Konzept lässt die konkrete Ausgestaltung der in den verschiedenen TI-Anwendungen geltenden und aus der Vertretung resultierenden Berechtigungen des Vertreters offen. Wirksamkeit der Vertretung, Umfang und Dauer der konkreten Berechtigungen bleiben Gegenstand der Autorisierung der jeweiligen Anwendung.

4.3 Fachlicher Geltungsbereich

Das vorliegende Konzept unterscheidet grundsätzlich zwischen zwei Vertretungstypen:

Gesetzliche Vertretung: Bei der gesetzlichen Vertretung ist der Vertretene aus rechtlichen und/oder gesundheitlichen Gründen nicht in der Lage, für sich selbst zu entscheiden. In diesen Situationen ist ein gesetzlicher Vertreter vorgesehen. Hier sind verschiedene Typen von Vertretungsbeziehungen zu unterscheiden, insbesondere bei zukünftigen Erweiterungen der Vertretungsfunktion.

Gewillkürte Vertretung: Der Vertretene ist selbst in der Lage, zu entscheiden, ob er durch eine andere Person vertreten werden möchte und in welchem Umfang. Er kann eine entsprechende Vollmacht für den Vertreter erteilen und diese auch jederzeit erweitern, einschränken oder auch widerrufen.

Der fachliche Umfang des Grobkonzeptes beschränkt sich auf die Vertretung im Rahmen des elterlichen Sorgerechts als eine Ausprägung der gesetzlichen Vertretung sowie auf die gewillkürte Vertretung.

Im Falle der Vertretung im Rahmen des elterlichen Sorgerechts wird berücksichtigt, dass beide Elternteile als Vertreter ihrer minderjährigen Kinder Anwendungen der TI nutzen möchten - da die Kinder selbst dafür noch nicht alt genug sind.

- Beispiel: Ein Vater darf aufgrund seines Sorgerechts stellvertretend für seine minderjährige Tochter auf deren Daten in TI-Anwendungen zugreifen.
- Siehe auch BGB §§ 1626 ff. zu den rechtlichen Rahmenbedingungen. In Bezug auf TI-Anwendungen gilt ergänzend § 36 SGB I.

Im Falle der gewillkürten Vertretung nutzt der Vertreter stellvertretend für einen zu unterstützenden Angehörigen Anwendungen der TI, nachdem der zu vertretende Angehörige ihm dazu eine Vollmacht ausgestellt hat. Der Begriff "Angehöriger" umfasst dabei nicht nur Verwandtschaftsbeziehungen, sondern auch sehr vertraute Personen und enge Freunde. Der Vertretene ist in diesen Fällen selbst voll entscheidungsfähig, aber benötigt oder wünscht sich Unterstützung bei der Nutzung von Anwendungen der TI. Typische Gründe sind körperliche Einschränkungen, zu geringe Erfahrung oder Unsicherheit im Umgang mit digitalen Anwendungen oder auch rein praktische Erwägungen. Daher erlaubt der zu Vertretende einem Vertrauten als Vertreter für ihn zu agieren. Hier genügt eine Vollmacht für den Vertreter, ausgestellt vom Vertretenen.

- Beispiel: Eine Großmutter, die kein Handy benutzt, möchte, dass ihre volljährige Enkelin sie bei der Nutzung bestimmter TI-Anwendungen unterstützt, weshalb sie der Enkelin eine entsprechende schriftliche Vollmacht erteilt ("Oma-Enkel-Szenario").
- Siehe auch BGB §§ 164 ff. zu den rechtlichen Rahmenbedingungen.

Mögliche zukünftige Erweiterungen der Vertretungsfunktion - beispielsweise die Integration weiterer Ausprägungen von gesetzlichen Vertretungen - werden durch das vorliegende Konzept nicht ausgeschlossen.

4.4 Lebenszyklus einer Vertretung

Entfernen von Vertretungen

Das Entfernen einer Vertretungsbeziehung lässt ggf. alle darauf beruhenden Berechtigungen unwirksam werden. Einmal entfernt, muss eine Vertretung erneut eingerichtet werden, falls sie wieder erforderlich werden sollte.

Aktives Beenden von Vertretungen

Ein Versicherter kann - als Vertreter oder Vertretener - jederzeit aktiv eine ihn betreffende Vertretung zunächst beenden, womit diese in den Status "ungültig" versetzt wird. Damit bleibt die Vertretung weiterhin sichtbar, jedoch als "ungültig". Auch dies lässt - wie das Entfernen - alle darauf beruhenden Berechtigungen unwirksam werden.

Sperren von Vertretungen

In besonderen Situationen - etwa dem Vorliegen einer Beschwerde, eines Widerrufs o.ä. - kann eine Vertretung gesperrt werden. Das Sperren einer Vertretung lässt die Vertretung weiter sichtbar bleiben, aber sie trägt den Status "gesperrt". Auch dies lässt - wie das Beenden oder Entfernen - alle darauf beruhenden Berechtigungen unwirksam werden. Allerdings gibt es zwei wesentliche Unterschiede:

- Eine gesperrte Vertretung zwischen zwei Versicherten verhindert, dass eine gleichartige Vertretung (gleicher Typ) zwischen eben diesen Versicherten erneut angelegt werden kann. Auf diese Weise kann eine Vertretung nicht nur beendet, sondern auch die Wiederanlage verhindert werden - daher der Status "gesperrt".
- Eine gesperrte Vertretung kann nur durch besonders berechtigte Nutzer (abhängig vom Anwendungsfall) wieder reaktiviert ("entsperrt") oder entfernt werden.

Ablauf von Vertretungen

Vertretungen sind ggf. nur zeitlich befristet gültig, sei es aus rechtlichen Gründen (Beispiel: Sorgerecht für Minderjährige) oder um aus sicherheitstechnischen Gründen eine turnusgemäße Bestätigung ("Refresh") vorzusehen. In diesen Fällen können Vertretungen ungültig werden, wenn die Gültigkeitsdauer erreicht ist und keine erneute Bestätigung erfolgt ist. Ersichtlich ist dies am Status "abgelaufen".

Weitere Details zu Status und Statusübergängen finden sich in Kapitel 8.2 .

4.5 Unterstützte Anwendungen

Die Vertretungsfunktion soll in der ersten Version so umgesetzt werden, dass eine Integration in die folgenden Anwendungen der TI (gemäß SGB V) ermöglicht wird:

- elektronische Patientenakte
- elektronisch verordnungsfähige und veranlasste Leistungen
- Proof of Patient Presence
- Digitale Patientenrechnung

Mittel- und langfristig sollen weitere Anwendungen die Vertretungsfunktion nutzen können. Dies ist Gegenstand zukünftiger Ausbaustufen.

Offener Punkt:

Es ist denkbar, dass Anwendungen außerhalb der TI eine Integration der Vertretungsfunktion über ein Bestätigungsverfahren ermöglicht wird. So könnte beispielsweise die Integration der Vertretungsfunktion in den 116117-Terminservice der Kassenärztlichen Bundesvereinigung eine Online-Buchung von Terminen durch einen Vertreter ermöglichen.

Offener Punkt:

Bei gesetzlich Versicherten können Eltern alleine durch Verwenden der eGK des Kindes - jedoch ohne Eingabe der zugehörigen PIN - bei einem Leistungserbringer den „Proof of Patient Presence“ (PoPP) für das Kind durchführen. Damit können Eltern dem Leistungserbringer den Zugriff auf die Daten des Kindes ermöglichen, ohne selbst den Zugriff darauf zu erhalten.

Bei PKV-Versicherten ist dieses in der alltäglichen Versorgung sehr wichtige Anwendungsszenario so nicht möglich. Daher sollte analysiert werden, ob mittels der Vertretungsfunktion ein vergleichbares Verfahren angeboten werden kann.

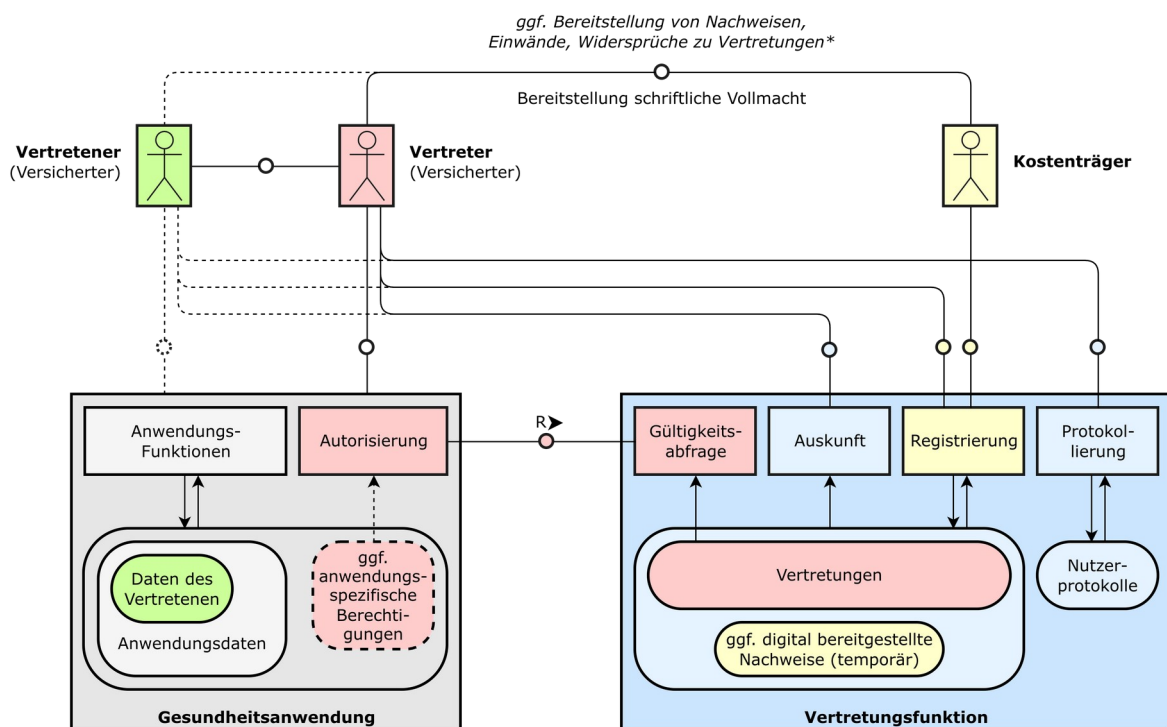
Kern dieser Idee ist die Einrichtung einer eingeschränkten Sorgerechts-Vertretung, bei der ausschließlich eine Vertretung bei PoPP möglich ist.

Die Registrierung dieser Vertretung entspricht weitgehend der Registrierung einer „vollwertigen“ Sorgerechts-Vertretung per FdV ohne eGK (siehe Kapitel 8.7.2.2). Unterschiede bestünden in diesen Punkten:

- Die registrierte Vertretung hätte einen eigenen Typ - „eingeschränkte Sorgerechts-Vertretung“ oder „PoPP-Vertretung“.
- Die Vertretung ist grundsätzlich auf PoPP beschränkt, das Elternteil erhält damit keinen Zugriff auf die medizinischen Daten des Kindes.
- Für den Kostenträger gelten bezüglich der Bestätigung der Vertretung die gleichen Bedingungen wie für die Ausgabe einer eGK des Kindes ohne PIN.

5 Die Vertretungsfunktion im Überblick

Abbildung 1 unten zeigt den funktionalen Aufbau der Vertretungsfunktion im Überblick, einschließlich der Nutzer in den verschiedenen Rollen sowie die Verbindung mit einer Gesundheitsanwendung, die die Vertretungsfunktion nutzt. Die Darstellung dient der Einordnung der weiter unten beschriebenen User Stories. Sie stellt noch nicht die Zerlegung und technische Umsetzung der Vertretungsfunktion in Form von TI-Diensten, Client-Systemen und technischen Schnittstellen dar. Auch die Nutzung vorhandener TI-Dienste, etwa den Identity Providern, ist noch nicht berücksichtigt.



*) nicht Gegenstand des Konzeptes

Abbildung 1 Vertretungsfunktion - Überblick

5.1 Nutzer

Versicherte

Als direkte Nutzer der Vertretungsfunktion sind zunächst Versicherte in der Rolle Vertreter oder Vertretener gegeben. Um Anwendungsfunktionen einer Gesundheitsanwendung in der Vertreterrolle nutzen zu können und auf die Daten des Vertretenen zugreifen zu können, benötigt der Vertreter einen Zugang zur Anwendung. Der Vertretene selbst hat ggf. auch einen Zugang zur Anwendung - es sei denn, er möchte oder kann die Anwendung aus rechtlichen oder sonstigen Gründen (z.B. Minderjährigkeit, körperliche Beeinträchtigungen) nicht selbst aktiv nutzen.

Kostenträger

Mitarbeiter des Kostenträgers benötigen einen direkten Zugang zur Vertretungsfunktion, um dort angelegte Vertretungen bearbeiten zu können. Bei Bedarf können Kostenträger dabei Nachweise von Versicherten anfordern.

Ob ein Kostenträger Nachweise vom Versicherten einfordert, welche dies ggf. sind, auf welchem Weg und in welcher Form, ist nicht Gegenstand der Vertretungsfunktion. Die Vertretungsfunktion bietet jedoch optional die Möglichkeit, Nachweise in digitaler Form vom Versicherten anzufordern und zu beziehen. Diese werden daher nur temporär und zu diesem Zweck gespeichert.

5.2 Funktionsbereiche

Die Vertretungsfunktion umfasst folgende Funktionsbereiche:

5.2.1 Registrierung

Die Registrierung bei der Vertretungsfunktion dient dazu, Vertretungsbeziehungen (im Folgenden auch kurz: Vertretungen) anzulegen, zu bearbeiten und zu löschen sowie bei Bedarf Nachweise anzufordern und bereitzustellen. Als Nutzer kommen hier nur der Kostenträger, der Vertretene und der Vertreter in Betracht. Die Anlage einer Vertretung initiieren können dabei ausschließlich betroffene Versicherte. (siehe auch Abschnitt 8.7 zur Beteiligung von Vertreter und Vertretenem bei der Registrierung) Der Kostenträger bearbeitet und bestätigt bei Bedarf vorhandene Vertretungen. Versicherte können sie betreffende Vertretungen bearbeiten, soweit sie dazu berechtigt sind.

Registrierungsprozesse können je nach Typ der Vertretung, den verwendeten Authentisierungsverfahren und der Art der ggf. genutzten Nachweise unterschiedlich aufwändig sein. Abschnitt 8.7 bietet eine Übersicht über die verschiedenen Registrierungsverfahren.

5.2.2 Gültigkeitsabfrage

Die Gültigkeit einer Vertretung kann von nutzenden Anwendungen über die Gültigkeitsabfrage ermittelt werden, falls der Nutzer Funktionen als Vertreter nutzen möchte. Dazu müssen die Daten über den Vertreter - also den Nutzer -, den zu Vertretenden, die Art der Vertretungsbeziehung (Sorgerecht, per Vollmacht ...) sowie die Auswahl der Gesundheitsanwendung, bei der die Vertretung ausgeübt werden soll, gegeben sein. Die Gültigkeitsabfrage ermöglicht dann ggf. eine Bestätigung dieser Vertretung. Die Gültigkeitsabfrage kann nur von Anwendungen genutzt werden, die als nutzende Anwendungen vorgesehen und authentifiziert sind.

5.2.3 Auskunft

Die Auskunft bietet Versicherten die Möglichkeit, aktuell bestehende und sie betreffende Vertretungen, ggf. angeforderte Nachweise jederzeit einsehen zu können und ausgehend davon ggf. Veränderungen (mittels der Registrierung, siehe oben) vornehmen zu können. Die Möglichkeit zur Einsicht in aktuell vorliegende Vertretungen mittels der Auskunft muss auf die betroffenen Versicherten beschränkt sein. Die Auskunft für Versicherte umfasst ggf. auch Vertretungen, die nicht - oder nicht mehr - gültig sind.

Die Auskunft wird insbesondere auch benötigt, um dem Versicherten im Frontend einer Gesundheitsanwendung eine aktuelle Liste der vertretenen Personen (Kinder,

557 Angehörige) anzeigen zu können, damit der Versicherte daraus eine Auswahl treffen kann
558 zur Durchführung von Anwendungsfällen in Vertretung der ausgewählten Person.

559 *Hinweis:*

560 *In einer zukünftigen Ausbaustufe wäre es denkbar, eine Auskunft zu Vertretungen auch*
561 *Leistungserbringern zu ermöglichen, beispielsweise im Behandlungskontext bei*
562 *Notfallsituationen.*

563 **5.2.4 Protokollierung**

564 Die Protokollierung erfasst alle Aktionen von Nutzern und trägt diese in ein
565 Nutzerprotokoll ein, damit ein Versicherter alle ihn betreffenden Vorgänge im
566 Zusammenhang mit der Vertretungsfunktion auch nachträglich noch einsehen und
567 nachvollziehen kann.

6 Epics und User Stories

6.1 Anlegen einer Vertretung

6.1.1 Sorgerecht

Als Elternteil möchte ich mein Sorgerecht in meinem FdV eintragen, nachweisen und bestätigen lassen, um danach stellvertretend für mein Kind TI-Anwendungen nutzen zu können.

6.1.2 Gewillkürte Vertretung

Als Versicherter möchte ich in meinem FdV eine Vertretung *für* einen Angehörigen anlegen, um diesem eine Unterstützung bei der Nutzung von TI-Anwendungen anbieten zu können.

Als Versicherter möchte ich im FdV eine Vertretung *durch* einen Angehörigen anlegen können, um bei diesem eine Unterstützung bei der Nutzung von TI-Anwendungen anfragen zu können.

6.2 Bereitstellen von Nachweisen

6.2.1 Sorgerecht

Als Elternteil möchte ich beim Eintragen meines Sorgerechts im FdV unterstützende Hinweise zu den dazu erforderlichen Nachweisen erhalten können, um möglichst einfach diese Nachweise dem zuständigen Kostenträger zur Verfügung stellen zu können.

Als zuständiger Kostenträger möchte ich dem Versicherten per FdV direkte Hinweise geben können, wenn Nachweise ggf. für die Bestätigung des Sorgerechts erforderlich sind, um den Versicherten bestmöglich zu unterstützen.

Hinweis: Die Anforderung von Nachweisen durch den Kostenträger über die Vertretungsfunktion ist optional. Dieser Weg bietet sich insbesondere dann an, wenn der Versicherte direkt über sein FdV informiert werden soll.

Verwendung der eGK des Kindes

Als Elternteil möchte ich das Sorgerecht für mein Kind im FdV durch einmalige Verwendung der eGK meines Kindes und Eingabe der zugehörigen PIN registrieren, um keine weiteren Aufwände zur Registrierung zu haben.

Als Elternteil möchte ich ein mittels eGK und PIN des Kindes einmal eingetragenes Sorgerecht in Anwendungen nutzen können, ohne jedes Mal erneut die eGK meines Kindes zu benötigen.

Als gesetzliche Krankenkasse möchte ich die Eintragung eines Sorgerechts durch den Sorgeberechtigten selbst mittels der durch mich bereitgestellten eGK und PIN des Kindes ermöglichen, um die Nachnutzung einer vorhandenen eGK zu ermöglichen und weitere Aufwände zur Registrierung zu vermeiden.

Hinweis: Verfügt ein Elternteil bereits über die eGK mit PIN für ein Kind, so hat das Elternteil zurzeit auch den Zugriff auf die Daten des Kindes. Nach dem vorliegenden Konzept soll es ermöglicht werden, dass dieser bereits vorhandene Zugriff durch Einrichtung einer Vertretung möglichst einfach erhalten werden kann - siehe auch Abschnitt 8.7.2.1.

6.2.2 Gewillkürte Vertretung

Ausstellen der Vollmacht

Als Versicherter möchte ich eine mir von einem Angehörigen per FdV angebotene Vertretung einfach und direkt im FdV bestätigen, um eine Vollmacht ohne aufwändiges schriftliches Verfahren und ohne Umweg über den Kostenträger zu erteilen.

Als nicht digital affiner Versicherter möchte ich eine schriftlich verfasste Vollmacht für einen Angehörigen an meinen Kostenträger senden, damit ich ohne Nutzung eines FdV die Einrichtung einer Vertretung veranlassen kann.

Ausstellen der Vollmacht mittels eigener eGK

Als nicht digital affiner, gesetzlich Versicherter möchte ich eine mir von einem Angehörigen angebotene Vertretung im FdV des Angehörigen mittels meiner eGK und PIN bestätigen können, um auch ohne eigenes FdV die Aufwände eines schriftlichen Verfahrens und den Umweg über den zuständigen Kostenträger zu vermeiden.

6.3 Bestätigung einer Vertretung

6.3.1 Sorgerecht

Als gesetzliche Krankenkasse möchte ich, dass eine Vertretung aufgrund des Sorgerechts eines Versicherten automatisch gültig wird, wenn dieser bei der Eintragung die eGK und PIN seines Kindes als Nachweis verwendet hat, damit ich keine erneuten Aufwände für die Bestätigung erbringen muss.

Als zuständiger Kostenträger möchte ich eine durch einen Versicherten per FdV eingetragene Vertretung aufgrund seines Sorgerechts digital bestätigen können, um auch ohne Ausgabe einer eGK für das Kind dem Versicherten die Ausübung seines Sorgerechts in TI-Anwendungen zu ermöglichen.

6.3.2 Gewillkürte Vertretung

Als zuständiger Kostenträger möchte ich, dass eine durch einen vertretenden Versicherten per FdV angelegte Vertretung automatisch gültig wird, wenn die Vollmacht durch den zu vertretenden Versicherten per FdV bestätigt wurde, damit ich keine Aufwände für die Bestätigung erbringen muss.

Als zuständiger Kostenträger möchte ich, dass eine durch einen vertretenden Versicherten per FdV angelegte Vertretung automatisch gültig wird, wenn der zu

vertretende Versicherte seine eGK und PIN für die Bestätigung der Vollmacht verwendet hat, damit ich keine Aufwände für die Bestätigung erbringen muss.

Als zuständiger Kostenträger möchte ich Versicherten, die weder über eine eGK mit PIN noch über eine GesundheitsID verfügen, die Möglichkeit bieten, in einem strukturierten und sicheren Prozess eine schriftliche Vollmacht auszustellen, damit insbesondere nicht digital affine Versicherte sich bei digitalen Anwendungen vertreten lassen können.

6.4 Bearbeitung einer Vertretung

6.4.1 Gewillkürte Vertretung

Anpassen des Umfangs einer Vollmacht

Als Vertretener möchte ich bei der Erstellung einer Vollmacht - egal ob auf schriftlichem Weg oder per FdV - die Gesundheitsanwendungen auswählen, in denen mein Vertreter mich vertreten darf, um den Umfang der Vollmacht zu bestimmen.

Als Vertretener möchte ich bei einer bereits erteilten Vollmacht - egal ob auf schriftlichem Weg oder per FdV - die Auswahl der Gesundheitsanwendungen jederzeit anpassen können, in denen mein Vertreter mich vertreten darf, um den Umfang der Vollmacht zu bestimmen.

Anpassen der zeitlichen Befristung einer Vollmacht

Als Vertretener möchte ich bei der Erstellung einer Vollmacht - egal ob auf schriftlichem Weg oder per FdV - die zeitliche Befristung setzen, um die Dauer der Vollmacht zu bestimmen.

Als Vertretener möchte ich bei einer bereits erteilten Vollmacht - egal ob auf schriftlichem Weg oder per FdV - die zeitliche Befristung jederzeit ändern können, um die Dauer der Vollmacht zu bestimmen.

6.5 Ablehnen, Beenden und Sperren einer Vertretung

6.5.1 Sorgerecht

Aktiver Verzicht auf die Vertretung

Als Sorgeberechtigter möchte ich mein eingetragenes Sorgerecht jederzeit im FdV oder per schriftlichem Verfahren beenden oder entfernen können, um mein Selbstbestimmungsrecht zu wahren.

Intervention durch den Kostenträger

Als zuständiger Kostenträger möchte ich ein eingetragenes Sorgerecht jederzeit vorübergehend sperren oder endgültig entfernen können, damit ich bei fehlerhaft angelegten Einträgen, Missbrauchsfällen, Beschwerden o.ä. reagieren kann.

Automatisches Ablaufen nach gesetzlicher Befristung

Als junger Versicherter möchte ich, dass ein mich betreffendes Sorgerecht ggf. automatisch unwirksam wird, wenn ich die entsprechende gesetzliche Altersgrenze überschreite, damit ich mein mir dann zustehendes Selbstbestimmungsrecht ausüben kann.

6.5.2 Gewillkürte Vertretung

Ablehnen einer neu angelegten Vertretung

Als Versicherter möchte ich eine mir von einem Angehörigen angebotene Vertretung im FdV ablehnen können, um mein Selbstbestimmungsrecht zu wahren.

Als Versicherter möchte ich eine durch einen Angehörigen angefragte Vertretung im FdV ablehnen können, um mein Selbstbestimmungsrecht zu wahren.

Unterbinden von unerwünschten Anfragen

Als Versicherter möchte ich, dass unerwünschte Anfragen zur Einrichtung einer Vertretung unterbunden werden, sodass ich nicht mit einer hohen Zahl von Anfragen konfrontiert bin.

Aktiver Verzicht auf bzw. Beendigung einer Vertretung

Als Vertreter möchte ich eine bereits eingetragene gewillkürte Vertretung jederzeit im FdV oder per schriftlichem Verfahren beenden oder entfernen können, um mein Selbstbestimmungsrecht zu wahren.

Als Vertretener möchte ich eine bereits eingetragene gewillkürte Vertretung jederzeit im FdV oder per schriftlichem Verfahren beenden oder entfernen können, um mein Selbstbestimmungsrecht zu wahren.

Intervention durch den Kostenträger

Als zuständiger Kostenträger möchte ich eine eingetragene gewillkürte Vertretung jederzeit sperren oder entfernen können, damit ich bei fehlerhaft angelegten Einträgen, Missbrauchsfällen, Beschwerden o.ä. reagieren kann.

Automatisches Ablaufen gemäß eingestellter Befristung

Als Vertretener möchte ich, dass eine mich betreffende Vertretung ggf. automatisch unwirksam wird, wenn deren eingetragene Befristung erreicht wird, damit mein Selbstbestimmungsrecht gewahrt wird.

6.6 Verwendung von Vertretungen in Anwendungen

Als Vertreter möchte ich meine Rechte als Vertreter in einer Gesundheitsanwendung auf einfache Weise konfigurieren und nutzen können, um Hürden oder Aufwände durch erneute Erbringung von Nachweisen möglichst zu vermeiden.

Hinweise:

- 1. Die Möglichkeit und der Umfang einer weitergehenden, anwendungsspezifischen Konfiguration obliegt den jeweiligen Anwendungen.*
- 2. Die Umsetzung der anwendungsspezifischen Berechtigungen obliegt den jeweiligen Anwendungen.*

Als Sorgeberechtigter meines Kindes möchte ich als Vertreter für mein Kind - unter Verwendung meiner eigenen eGK oder GesundheitsID - die Behandlung/Versorgung bei einer Leistungserbringerinstitution (LEI) initiieren können, damit die LEI den benötigten Zugriff auf die Daten meines Kindes erhält.

Als Bevollmächtigter (gewillkürte Vertretung) möchte ich als Vertreter für den von mir vertretenen Versicherten - unter Verwendung meiner eigenen eGK oder GesundheitsID - die Behandlung bei einer Leistungserbringerinstitution initiieren können, damit die LEI den benötigten Zugriff auf die Daten des Vertretenen erhält.

Hinweise zu den beiden obigen User Stories:

1. *Die Umsetzung würde Anpassungen beim PoPP-Dienst und dem PoPP-Modul (FdV) erfordern. Siehe dazu auch Abschnitt 8.6.*
2. *Der Zugriff des LE auf die Daten des Vertretenen betrifft Daten des Vertretenen in Diensten der Telematikinfrastruktur, insbesondere die Stammdaten (VSDM), die ePA, Patientenrechnungen (DiPag) und E-Rezepte.*
3. *Der Umfang der Autorisierung der LEI ist bei gewillkürter Vertretung beschränkt auf die Anwendungen, für die der Vertreter selbst eine Berechtigung per Vollmacht hat.*

Als Versicherter möchte ich, dass bei Anpassung oder Beendigung einer mich betreffenden Vertretungsbeziehung die darauf beruhenden Berechtigungen in Gesundheitsanwendungen automatisch und unverzüglich angepasst oder außer Kraft gesetzt werden.

Als Hersteller, Anbieter oder interner Produktverantwortlicher der gematik möchte ich die Vertretungsfunktion möglichst einfach und sicher in meine Anwendung integrieren können, um schnell und kostengünstig einen Mehrwert für die Nutzer meiner Anwendung bieten zu können.

6.7 Nutzererlebnis und Transparenz

6.7.1 Hilfestellungen

Als Versicherter möchte ich bei der Nutzung der Vertretungsfunktion durch umfassende und auf den Anwendungsfall zugeschnittene Hilfestellungen in Form von erläuternden Texten und angebotenen Bedienmöglichkeiten unterstützt werden, um keine unnötigen Hürden bei der Nutzung der Vertretungsfunktion zu haben.

6.7.2 Übersicht

Als Versicherter möchte ich im FdV auf meinem Endgerät alle mich betreffenden Vertretungsbeziehungen jederzeit einsehen können, damit ich stets weiß,

- wen ich als Sorgeberechtigter oder per Vollmacht vertrete,
- wer mich als Sorgeberechtigter oder per Vollmacht vertritt,
- welche Vertretungen abgelaufen sind, gesperrt, beendet oder noch nicht bestätigt wurden,
- welchen Umfang Vertretungen haben² - d.h. auf welche Anwendungen sie sich jeweils erstrecken - und
- wie lange Vertretungen jeweils noch gültig sind gemäß eingetragener oder gesetzlicher Befristung.

Hinweis: Die Darstellung weitergehender, anwendungsspezifischer Details - beispielsweise für welche Anwendungsfälle der Vertreter bei einer nutzenden Anwendung berechtigt ist - obliegt den jeweiligen Anwendungen.

Als berechtigter Versicherter möchte ich ausgehend von der Übersicht der Vertretungen diese auf einfache Weise beenden oder bearbeiten können, um keine unnötigen Hürden oder Aufwände bei der Nutzung der Vertretungsfunktion zu haben.

6.7.3 Benachrichtigungen

Als Versicherter möchte ich im FdV auf meinem Endgerät zeitnah benachrichtigt werden, wenn zu einer von mir angelegten oder mich betreffenden Vertretung eines der folgenden Ereignisse eintritt:

- es wurde eine Vertretung durch einen anderen Nutzer angelegt, die mich betrifft
- es liegt eine Information seitens des zuständigen Kostenträgers für mich vor zu einem von mir bereitzustellenden Nachweis
- die Bestätigung für eine Vertretung ist erfolgt oder wurde abgelehnt
- eine automatische Beendigung einer Vertretung (Ablauf gemäß Befristung) wird in Kürze erfolgen
- eine automatische Beendigung einer Vertretung (Ablauf gemäß Befristung) ist erfolgt
- jegliche weitere Statusänderung einer Vertretung, die nicht durch mich selbst verursacht wurde

Hinweise:

- *Die Ausgestaltung ggf. weitergehender, anwendungsspezifischer Benachrichtigungen obliegt den jeweiligen Anwendungen.*
- *Benachrichtigungen zu Nachweisen betreffen nur Nachweise, die per Vertretungsfunktion angefordert oder bereitgestellt werden.*

Als Versicherter möchte ich im FdV auf meinem Endgerät einstellen, welche Benachrichtigungen ich erhalte, um den Umfang der mich erreichenden Information selber bestimmen zu können.

6.7.4 Nutzerprotokolle und Nutzerdaten

Als Versicherter möchte ich, dass Zugriffe auf meine Daten im Kontext der Vertretungsfunktion in Form eines Nutzerprotokolls so erfasst werden, dass ich jederzeit einsehen und nachvollziehen kann,

- wer
- wann
- zu welchem Zweck
- in welcher Anwendung
- welche mich betreffenden Vertretungen bearbeitet oder verwendet und
- auf welche meiner Daten zugegriffen hat.

Als Versicherter möchte ich die Möglichkeit haben, eine Kopie meines Nutzerprotokolls zur Vertretungsfunktion herunterzuladen, um dieses unabhängig von der Vertretungsfunktion aufbewahren und einsehen zu können.

Hinweis: Dies zielt insbesondere auch auf das Sichern des Nutzerprotokolls vor einer Löschung des Nutzerprotokolls ab.

Als Versicherter möchte ich jederzeit ausgewählte - oder sämtliche - mich betreffenden Daten der Vertretungsfunktion, d.h.

- mich betreffenden Vertretungen und
- Einträge im Nutzerprotokoll

801 löschen können, um mein informationelles Selbstbestimmungsrecht zu wahren.

7 Einordnung in die Telematikinfrastruktur

Die anwendungsübergreifende Vertretungsfunktion wird umgesetzt als

1. einmalig vorhandener Dienst - Vertretungsregister genannt
Dieser Dienst wird von der gematik beauftragt und betrieben (Gruppe 1)
2. Erweiterung des ZETA Client SDK
Einbindung des Features in nutzende Primärsysteme und FdV
3. Erweiterung des ZETA Guard
Einbindung des Features in nutzende Fachdienste

Das Vertretungsregister kann zunächst - im Rahmen der ersten Version - von ausgewählten TI Anwendungen genutzt werden. Siehe dazu auch Kapitel 4.2. Die Nutzung erfolgt, indem die nutzende Anwendung die oben genannten ZETA Komponenten und den zentralen Dienst verwendet, siehe auch das folgende Kapitel.

7.1.1 Allgemeine Sicherheits- und Datenschutzbetrachtung

7.1.1.1 Grundannahmen

Mit einem Vertretungsregister entstünde voraussichtlich eine Abbildung der Beziehungsgeflechte eines großen Teils der Bevölkerung. Darin wären nicht nur viele verwandtschaftliche Verhältnisse, sondern auch Vertrauens- und Abhängigkeitsbeziehungen gespeichert.

Das Auslesen eines solchen Registers (eine Verletzung des Sicherheitsziels Vertraulichkeit) gäbe potentiellen Angreifern den oben beschriebenen Einblick in Vertrauens- und Abhängigkeitsverhältnisse und damit die Möglichkeit, diese vielfältig auszunutzen.

Das Manipulieren eines solchen Registers (eine Verletzung des Sicherheitsziels Integrität/Authentizität) gäbe potentiellen Angreifern die Möglichkeit, sich unbefugt als Vertreter einer anderen Person auszugeben und damit weitreichend als diese Person zu agieren.

7.1.1.2 Erwägung alternativer Lösungen

Da ein zentrales Register mit bedeutenden Sicherheits- und Datenschutzrisiken einhergeht, müssen alternative, dezentrale Lösungen erwogen werden.

- Speicherung der **Vertretung auf der eGK** ähnlich den Stammdaten bei VSDM: Unabhängig von der technischen Umsetzbarkeit auf der Karte selbst besteht die Notwendigkeit der zeitnahen Aktualisierung der Vertretung auf der Karte, wofür es wiederum eine zentrale oder föderierte Instanz bräuchte. Es gäbe keine Lösung für die GesundheitsID.
- Abbildung der **Vertretung in einer Wallet** (z.B. auf dem Smartphone): Die Nutzung der in einer Wallet lagernden Vertretungsbeziehung wäre dezentral und offline möglich. Die Aktualisierung und Verifizierung bräuchte aber ähnlich wie bei der eGK eine zentrale oder föderierte Instanz. Der oder die Nutzer:in bräuchte ein elektronisches Endgerät. Die EUDI-Wallet ist noch nicht abschließend spezifiziert, ihre Einführung liegt mittelfristig in der Zukunft und die Nutzung ist optional - was

bedeutet, dass die Wallet nur eine Alternative, aber nicht die einzige Lösung sein kann.

- **Föderation von einzelnen Registern**, z.B. bei den Krankenkassen: Es gibt zwar Stand 2026 knapp 100 gesetzliche Krankenkassen (+ ungefähr 40 private Krankenkassen), diese werden aber in der Regel (z.B. bei der ePA) von wenigen technischen Dienstleistern abgedeckt. Es besteht die Gefahr (vor allem bei hohen Sicherheitsanforderungen), dass es auch bei einem föderierten Vertretungsregister nur 2-4 Betreiber gäbe, was die Föderation wenig sinnvoll machen würde. Negativ würde sich außerdem der gestiegene Aufwand bei der Betriebssteuerung und ein höheres Ausfallrisiko auswirken.

Aus der Diskussion der Alternativen heraus gibt es aus aktueller Sicht keine bessere Umsetzung der Vertretungsfunktion als in einem zentralen Register.

Ein zentrales Register muss auf Grund der Risiken (siehe "Grundannahmen") besonders hohen Sicherheitsanforderungen gerecht werden. Mehr zu den Anforderungen im Kapitel "Sicherheitsanforderungen an den Systemaufbau".

7.1.2 Ersatzverfahren und barrierefreier/analoger Zugang

Es gibt mindestens zwei Gründe, um Alternativen zu den Standardverfahren des Vertretungsregisters vorzusehen. Der erste Grund ist die Verfügbarkeit- Vertretungen müssen noch ausgeübt werden können, wenn das Vertretungsregister temporär ausgefallen ist.

Der zweite Grund ist die *allgemeine Barrierefreiheit* im Sinne des "Rechts auf analogen Zugang". Es sollte immer Verfahren geben, welche bestimmte Endgeräte oder Zugänge für den Endnutzer nicht voraussetzen (kein "Digitalzwang"). Die Nutzung dieser alternativen Verfahren muss diskriminierungsfrei möglich sein.

Beides lässt sich oft vereinbaren - das Ersatzverfahren für einen Ausfall kann gleichzeitig die analoge Lösung ohne Digitalzwang sein. Bei der Nutzung dieses Ersatzverfahrens kann es aber Abstriche in der Bequemlichkeit oder Geschwindigkeit geben.

Beim Vertretungsregister betrifft dies Versicherte, die nicht über ein eigenes digitales Endgerät (FdV) verfügen oder ein solches nicht nutzen können oder wollen. Hier sind als alternative Verfahren die Verwendung der eGK mit PIN (siehe Kapitel 8.7.1.2) sowie die Erteilung einer Vollmacht auf dem Postweg (siehe Kapitel 8.7.1.3) vorgesehen. Des Weiteren kann sich der Versicherte an den zuständigen Kostenträger wenden.

Es gibt in dieser Projektphase noch kein Ersatzverfahren für jede Art von Ausfall oder gewünschtem analogen Zugang, es wird aber angestrebt, mit fortschreitender Entwicklung weitere Lösungen zu finden.

8 Technisches Konzept

8.1 Fachliches Informationsmodell

Die Vertretungsfunktion muss verschiedene Informationen erfassen, um die oben beschriebenen Anwendungsszenarien und Funktionen umsetzen zu können. Die Abbildung unten zeigt diese Informationen als Informationsmodell mit den wesentlichen Objekttypen, Beziehungen und Attributen - ohne jedoch eine bestimmte technische Umsetzung oder die dazu gehörigen Details festzulegen. Des Weiteren stellt das Diagramm nicht dar, welche Informationen ggf. durch Schutzmaßnahmen wie Verschlüsselung, Pseudonymisierung, Nutzung von Hash-Werten o.ä. geschützt werden.

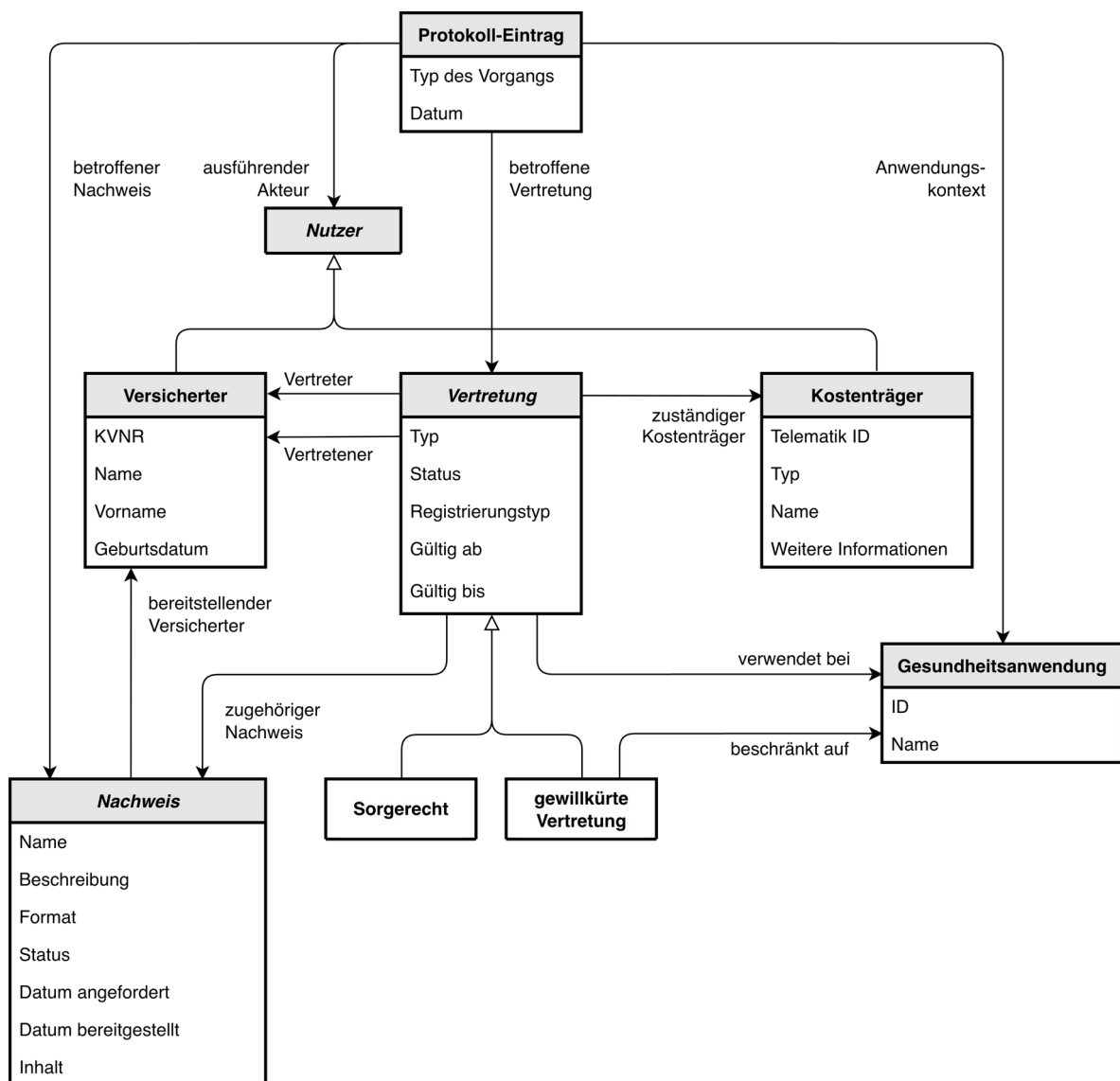


Abbildung 2 Informationsmodell zur Vertretungsfunktion

Die folgenden Unterkapitel bieten eine Erläuterung der Darstellung.

8.1.1 Grundlegende Objekte

Für das Grundverständnis sind zunächst die nicht eingefärbten, im oberen Bereich gezeigten Objekte relevant. Diese umfassen alle wesentlichen Informationen, die bei Vertretungen von Versicherten durch Versicherte relevant sind - unabhängig von der Art der Vertretung.

8.1.1.1 Vertretung

Diese ist das zentrale Element und weist folgende Attribute und Bezüge auf:

Der Typ gibt an, um welche Art der Vertretungsbeziehung es sich handelt:

- gewillkürte Vertretung,
- elterliches Sorgerecht

Der Status gibt den Stand der Bearbeitung und der Gültigkeit der Vertretung wieder. Näheres zu den verschiedenen Status findet sich in Kapitel 8.2.

Der Registrierungstyp bestimmt den bei der Registrierung durchlaufenen Prozess - also z.B. Vollmacht erstellen per FdV, Sorgerecht eintragen mit eGK+PIN usw. Näheres zu den verschiedenen Registrierungsprozessen findet sich in Kapitel 8.7.

Über Zeitpunkte "Gültig ab" und "Gültig bis" lässt sich für eine Vertretung ein Gültigkeitszeitraum festlegen. Dies kann bei gesetzlichen Vertretungen zweckdienlich sein oder bei gewillkürten Vertretungen genutzt werden, um eine zeitliche Befristung vorzusehen.

Jede Vertretung verweist auf einen Vertreter und einen Vertretenen, die in der ersten Version der Vertretungsfunktion ausschließlich Versicherte sein können.

Jeder Vertretung ist außerdem ein Kostenträger zugeordnet als zuständiger Kostenträger. Dieser entspricht dem Kostenträger des vertretenen Versicherten.

8.1.1.2 Versicherter

Um berechtigten Nutzern eine eindeutige Beauskunftung zu vorliegenden Vertretungen bieten zu können, werden für Vertreter und Vertretene

- KVN
- Name
- Vorname
- Geburtsdatum

erfasst. Diese Daten sollen ferner sicherstellen, dass es bei der Erfassung von Vertretungsbeziehungen zu keinen Verwechslungen kommt.

8.1.1.3 Gesundheitsanwendung

Jede Gesundheitsanwendung, die die Vertretungsfunktion unterstützt, wird erfasst. Dazu werden deren ID und Name gemäß der Registrierung in der TI-Föderation hinterlegt.

Bei gewillkürten Vertretungen werden die Gesundheitsanwendungen vermerkt, auf die sich die Vertretung bezieht. Gesundheitsanwendungen, die eine eingetragene Vertretung tatsächlich auch abfragen - also "verwenden" -, werden vermerkt, damit für den

927 betroffenen Versicherten nachvollziehbar ist, bei welchen Gesundheitsanwendungen eine
928 ihn betreffende Vertretung wirksam ist.

929 **8.1.1.4 Nachweis**

930 Werden Vertretungen unter Beteiligung des zuständigen Kostenträgers registriert, so
931 kann dieser vom Vertreter Nachweise anfordern, beispielsweise eine Geburtsurkunde
932 oder eine vom Vertreter verfasste schriftliche Vollmacht. Die Anforderung eines
933 Nachweises kann - aber muss nicht - mittels des Vertretungsregisters geschehen. In
934 diesem Fall erfasst das Vertretungsregister Informationen über den angeforderten
935 Nachweis, sodass der betroffene Versicherte im FdV sehen kann, welcher Nachweis von
936 ihm angefordert wird. Das Vertretungsregister ermöglicht es außerdem dem
937 Versicherten, einen Nachweis digital über das Vertretungsregister bereitzustellen - etwa
938 durch Einscannen oder "Hochladen" in der App seines Kostenträgers. In diesem Fall wird
939 auch der eigentliche Nachweis (d.h. der Inhalt) im Vertretungsregister gespeichert.

940 *Hinweise:*

941 *Daten zu einem Nachweis werden*

- 942 • *nur bei Bedarf (d.h. wenn der Nachweis über das Vertretungsregister angefordert*
943 *wird),*
- 944 • *nur vorübergehend und*
- 945 • *ausschließlich zum Zweck der Übertragung an den anfordernden Kostenträger*
946 *gespeichert.*

947 Als Angaben zu einem Nachweises sind vorgesehen:

- 948 • **Name**
949 Eine Bezeichnung des Nachweises, als Hilfestellung für den Versicherten. Kann durch
950 den Kostenträger gesetzt werden.
- 951 • **Beschreibung**
952 Ergänzende Informationen als Hilfestellung für den Versicherten. Kann durch den
953 Kostenträger gesetzt werden.
- 954 • **Format¹**
955 Nur bei Nachweisen, die in digitaler Form bereitgestellt werden, z.B. PDF oder gängige
956 Bildformate.
- 957 • **Inhalt¹**
958 Nur bei Nachweisen, die in digitaler Form bereitgestellt werden. Dies können z.B. vom
959 Versicherten per mobiler App abfotografierte oder bereits digital vorliegende
960 Dokumente sein.
- 961 • **Status²**
962 Mögliche Status sind:
 - 963 • **angefordert**
964 Ein Nachweis wurde durch den Kostenträger angefordert, aber noch nicht
965 bereitgestellt. Dies wird durch den Zustand "angefordert" explizit festgehalten.
 - 966 • **bereitgestellt**
967 Ein Nachweis wurde bereitgestellt. Je nach Art des Nachweises wird der Zustand
968 automatisch gesetzt oder manuell.
- 969 • **Datum angefordert**
970 Der Zeitpunkt, zu dem der Nachweis angefordert wurde.
- 971 • **Datum bereitgestellt**
972 Der Zeitpunkt, zu dem der Nachweis ggf. bereitgestellt wurde.

- bereitstellender Versicherter (Referenz)
Ein Verweis auf denjenigen Versicherten, von dem der Nachweis angefordert und ggf. bereitgestellt wird.

Hinweise:

1. *Die detaillierte und abschließende Festlegung der unterstützten Formate erfolgt im Rahmen der Spezifikation.*
2. *Der Status eines Nachweises dient dazu, dem Versicherten eine Übersicht über noch zu erbringende bzw. bereits erledigte Nachweise zu bieten. Er sagt nichts über die Prüfung durch den Kostenträger aus.*

8.1.1.5 Kostenträger

Kostenträger sind neben den Versicherten Nutzer des Vertretungsregisters. Hier werden erfasst:

- Telematik-ID
- Typ des Kostenträgers
- Name des Kostenträgers
Zur Anzeige im FdV.
- weitere Informationen
Weitere Angaben zum Kostenträger soweit diese für die Versicherten zur Nutzung der Vertretungsfunktion relevant sind.

Hinweis: Die detaillierte und abschließende Festlegung der Typen und weiteren Informationen erfolgt im Rahmen der Spezifikation.

8.1.1.6 Protokoll-Eintrag

Um dem Versicherten eine Transparenz bezüglich der Zugriffe auf seine Daten zu gewährleisten, müssen die Zugriffe durch die verschiedenen Nutzer im Nutzerprotokoll vermerkt werden. Dazu wird erfasst, welcher Nutzer wann und zu welchem Zweck (ausgeführte Operation) auf welche Daten zugegriffen hat.

Die Einträge im Nutzerprotokoll umfassen:

- Typ des Vorgangs
Welche Aktion wurde vorgenommen?
- Datum
Wann geschah dies?
- Nutzer
Wer hat den Vorgang durchgeführt? Der jeweils ausführende Akteur wird im Protokolleinträgen erfasst. Dies ist ggf. ein Versicherter oder der zuständige Kostenträger.
- betroffene Vertretung
Es wird festgehalten, welche Vertretung von dem Vorgang betroffen war.
- betroffener Nachweis
Ggf. wird vermerkt, welcher Nachweis von dem Vorgang betroffen war.
- Anwendungskontext
Ggf. wird erfasst, bei welcher Gesundheitsanwendung ein Vorgang initiiert wurde.

Eine Festlegung der einzelnen Typen von Einträgen erfolgt in Kapitel 8.8.

8.1.2 Registrierungstypen

Dieses Kapitel bietet einen Überblick über die vorgesehenen Registrierungstypen. Eine detailliertere Betrachtung erfolgt in Kapitel [8.7](#).

Hinweis:

Je nachdem, auf welche Weise eine Vertretung registriert wird, können verschiedene Nachweise relevant sein. Eine eingehende Betrachtung der rechtlich erforderlichen Nachweise ist nicht Gegenstand dieses Konzeptes. Im Folgenden werden diese daher nur soweit betrachtet, wie sie für die Verarbeitung im Vertretungsregister technisch relevant sind.

8.1.2.1 Registrierung einer gewillkürten Vertretung

Hier sind drei Verfahren vorgesehen, wie diese registriert werden können:

- Vollmacht per eigenem FdV
Der Vertretene bestätigt die vom Vertreter angebotene Vertretung durch eine Bestätigung mit seinem eigenen FdV, nach Anmeldung mit eGK+PIN oder GesundheitsID. Siehe auch Kapitel [8.7.1.1](#).
- Vollmacht per eGK+PIN
Der Vertretene bestätigt direkt im Rahmen der Erstellung der Vertretung durch den Vertreter seine Vollmacht durch Verwendung seiner eigenen eGK und PIN - jedoch am FdV des Vertreters. Siehe auch Kapitel [8.7.1.2](#).
- Schriftliche Vollmacht
Hier wird eine schriftliche Vollmacht mit Hilfe der Vertretungsfunktion erstellt und vom Vertretenen als unterschriebenes Dokument an den zuständigen Kostenträger gegeben. Dieser gleicht die Vollmacht mit Daten im Vertretungsregister ab. Anschließend stellt der Kostenträger dem Vertretenen einen Bestätigungscode zu, den dieser an den Vertreter als Bestätigung der Vollmacht übergibt. Der durch Barcode und Ident-Verfahren abgesicherte Prozess wird in Kapitel [8.7.1.3](#) beschrieben.

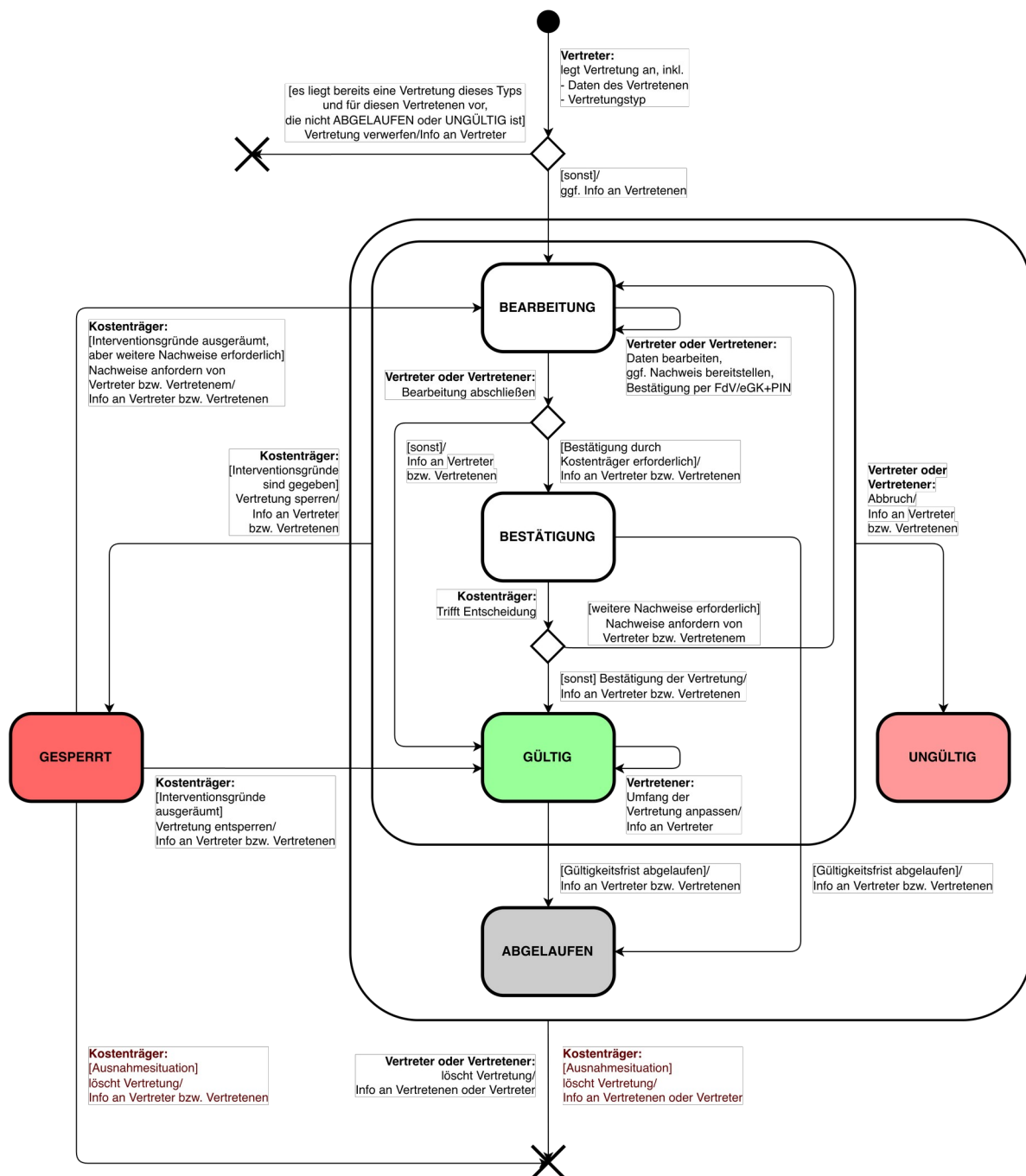
8.1.2.2 Registrierung einer Vertretung aufgrund elterlicher Sorge

Hier sind zwei Verfahren zur Registrierung vorgesehen:

- Registrierung per eGK und PIN des Kindes
Eine vom zuständigen Kostenträger an ein Elternteil ausgegebene eGK mit PIN des Kindes soll vom Elternteil beim Einrichten der Vertretung zur Bestätigung am FdV verwendet werden können. Siehe dazu auch Kapitel [8.7.2.1](#).
- Registrierung ohne eGK des Kindes
Ein Elternteil legt eine Vertretung für sein Kind im Vertretungsregister an, unter Angabe von Vorname, Name, Geburtsdatum und KVNR des Kindes. Die Vertretung muss vom zuständigen Kostenträger bestätigt werden. Dazu kann dieser Nachweise vom Elternteil über das Vertretungsregister (oder einem anderen Weg) anfordern. Siehe dazu auch Kapitel [8.7.2.2](#).

8.2 Status und Statusübergänge von Vertretungen

Das folgende Diagramm zeigt die verschiedenen Status, die eine erfasste Vertretung von der Anlage bis zur Löschung durchläuft sowie deren mögliche Übergänge.



Das Modell ist so allgemein gehalten, dass es alle derzeit vorgesehenen Vertretungstypen abdeckt. Die für die spezifischen Vertretungstypen geltenden Besonderheiten und Einschränkungen werden später noch behandelt. Hier werden zunächst die verschiedenen Status und Übergänge des allgemeinen Modells betrachtet. Auch die im Modell dargestellten "Infos an Vertreter bzw. Vertretenen" werden im Rahmen der Registrierungsprozesse (siehe Abschnitt 8.7) konkretisiert - dort wird beschrieben, wann ein Vertreter oder Vertretener welche Information erhält per Push-Nachricht oder als Anzeige im FdV.

BEARBEITUNG

Eine Vertretung kann - zumindest initial - nur durch den Vertreter angelegt werden, der dazu angemeldet sein muss. Auf diese Weise wird erreicht, dass dessen Identität mit der Anlage der Vertretung bereits sicher erfasst wurde. So kann der Vertretene sicher sein, wer der Vertreter ist, bevor er die Vertretung bestätigt. Der Vertreter muss für die Eintragung die Daten des zu Vertretenden erfassen sowie den Typ der anzulegenden Vertretung.

Eine neue Vertretung kann jedoch nicht angelegt werden, wenn für den Vertreter bereits eine Vertretung dieses Typs und den zu Vertretenden vorliegt und diese noch nicht "ABGELAUFEN" oder "UNGÜLTIG" ist. Damit wird erreicht, dass keine unerwünschten Dubletten zu Vertretungen angelegt werden können.

Im Zustand "BEARBEITUNG" ist die Vertretung noch unwirksam, da eventuell noch unvollständig und nicht bestätigt. Der Zustand kann erst verlassen werden, wenn

- alle Daten zur Vertretung erfasst wurden und
- die für den Vertretungstyp ggf. erforderliche Bestätigung durch den Vertretenen erteilt wurde

Falls der zu vertretene Versicherte eine Bestätigung per FdV geben muss, so wird dieser per Push-Nachricht und Anzeige im FdV informiert.

Bei Vertretungen, die korrekt erfasst wurden und nicht durch den zuständigen Kostenträger bearbeitet werden müssen, wechselt der Zustand nach "GÜLTIG". Dies betrifft Vertretungen, die digital per eGK und PIN oder per FdV bestätigt werden können.

Vertretungen, die vom Kostenträger bearbeitet werden müssen, wechseln zunächst in den Zustand "BESTÄTIGUNG".

Der Zustand "BEARBEITUNG" kann auch aus dem Zustand "BESTÄTIGUNG" erreicht werden - nämlich genau dann, wenn der Kostenträger unter Verwendung des Vertretungsregisters Nachweise von einem der beteiligten Versicherten anfordert. Diese werden dann vom Kostenträger vorgegeben (Name, Beschreibung) und als "angefordert" (Status) eingetragen. Nachweise in digitaler Form können vom Versicherten per Vertretungsregister bereitgestellt werden, womit deren Zustand automatisch auf "bereitgestellt" wechselt. Wird ein so angeforderter Nachweis auf einem Weg außerhalb des Vertretungsregisters an den Kostenträger gegeben - etwa per Postversand -, so kann der Versicherte den Status des Nachweises manuell auf "bereitgestellt" setzen.

Sind die angeforderten Nachweise bereitgestellt, so kann der Versicherte die Bearbeitung wieder abschließen und zurück an den Kostenträger geben - der Zustand wechselt wieder in "BESTÄTIGUNG".

Hinweis:

Nachweise, die auf einem Weg abseits des Vertretungsregisters angefordert und bereitgestellt werden, werden nicht betrachtet.

BESTÄTIGUNG

Der Eintrag der Vertretung ist noch ungültig, aber soweit bearbeitet, dass eine Bearbeitung durch den zuständigen Kostenträger erfolgen kann.

Der Kostenträger kann zu einer Vertretung Nachweise vom Versicherten (Vertreter oder Vertretener) anfordern. Dies kann optional über das Vertretungsregister erfolgen, indem die benötigten Nachweise bei der Vertretung eingetragen werden und die Vertretung wieder zurück an den Versicherten gegeben wird. Derjenige Versicherte, der den Nachweis bereitstellen soll, wird ebenfalls eingetragen (Referenz: "bereitstellender Versicherter", siehe Informationsmodell). Die Vertretung wechselt dann wieder in den Zustand "BEARBEITUNG" (siehe oben) zurück und der betroffene Versicherte erhält entsprechende Hinweise per Push-Benachrichtigung und im FdV.

Kann der Kostenträger die Vertretung bestätigen, so geht diese in den Zustand "GÜLTIG" über.

Hinweis:

Es bleibt dem Kostenträger überlassen, zu entscheiden

- *ob und welche Nachweise erforderlich sind,*
- *in welcher Form diese bereitzustellen sind,*
- *von wem und wie diese angefordert werden und*
- *auf welchem Weg diese bereitzustellen sind.*

GÜLTIG

Der Eintrag wurde erfolgreich bestätigt, entweder durch den Kostenträger oder - wo dies möglich ist - automatisch.

Im Zustand "GÜLTIG" besteht bei gewillkürten Vertretungen die Möglichkeit für den Vertretenen, den Umfang der Vollmacht anzupassen. Dies betrifft

- das Setzen oder Anpassen der Gültigkeitsdauer der Vertretung im Sinne einer befristeten Vollmacht, oder
- das Hinzufügen oder Entfernen von Gesundheitsanwendungen, für die eine gewillkürte Vertretung gilt - also eine Erweiterung oder Einschränkung der Vollmacht.

Hinweis:

Nur im Zustand "GÜLTIG" ergibt eine Gültigkeitsabfrage einer Vertretung eine positive Auskunft, d.h. eine Ausübung von Vertretungsberechtigungen in Gesundheitsanwendungen ist nur dann möglich.

UNGÜLTIG

Der Vertreter oder der Vertretene kann eine Vertretung ablehnen, wenn sie bereits "GÜLTIG" ist oder deren Erstellung abbrechen, wenn sie noch in "BEARBEITUNG" oder "BESTÄTIGUNG" ist. Letzteres kann auch dadurch geschehen, dass eine Bearbeitung durch den Versicherten in der vorgesehenen Zeit ausbleibt (Zeitüberschreitung).

In diesen Fällen wechselt die Vertretung in den Zustand "UNGÜLTIG" und betroffene Versicherte werden per Push-Benachrichtigung oder per FdV informiert. In diesem Zustand bleibt die Vertretung, bis sie aktiv gelöscht wird.

ABGELAUFEN

Sobald für eine Vertretung im Zustand "GÜLTIG" oder "BESTÄTIGUNG" die ggf. vorhandene Gültigkeitsfrist überschritten ist, wechselt diese in den Status "ABGELAUFEN". Dies kann zum Beispiel bei einer Vertretung aufgrund des Sorgerechts erfolgen, wenn das Kind das 15. Lebensjahr vollendet hat, oder auch bei Vollmachten, die nur befristet erteilt wurden. Die betroffenen Versicherten werden ausreichend früh vor Ablauf benachrichtigt, damit diese ggf. darauf reagieren können.

GESPERRT

In bestimmten Situationen kann der Kostenträger erkennen, dass eine Vertretung aufgrund rechtlicher oder sicherheitstechnischer Gründe nicht mehr gültig sein darf oder gar nicht erst zustande kommen darf - siehe im Bild: "Interventionsgründe sind gegeben". Bei einer solchen Intervention durch den Kostenträger kann diese die betroffene Vertretung vorübergehend oder dauerhaft in den Zustand "GESPERRT" versetzen.

Hinweis:

Eine derartige Intervention durch den Kostenträger ist nur für kritische Situationen vorgesehen - etwa bei sicherheitstechnischen Vorfällen, einer Beschwerde gegen eine Vertretung, usw.

Nur der Kostenträger kann den Zustand "GESPERRT" wieder aufheben, wodurch dieser Zustand (in Kombination mit der Verhinderung von Dubletten) als "Sperrung" gegen eine Bearbeitung oder Neu-Anlage dieser Vertretung durch einen Versicherten wirkt.

Falls aus Sicht des Kostenträgers keine Gründe mehr vorliegen für eine Sperrung (siehe im Bild: "Interventionsgründe ausgeräumt"), so kann dieser

- den Eintrag auf "GÜLTIG" setzen oder
- dem Versicherten zur "BEARBEITUNG" übergeben, falls noch Nachweise angefordert werden.

Hinweis:

Eine derartige Rücknahme einer Sperrung könnte zum Beispiel erfolgen, wenn sich eine Beschwerde gegen eine Vertretung als unbegründet erwiesen hat, ein sicherheitstechnisches Problem behoben wurde, usw.

Löschen von Vertretungen

Ein Versicherter - als Vertreter oder Vertretener - kann sich jederzeit entscheiden, eine ihn betreffende Vertretung per FdV zu entfernen - sofern diese nicht gesperrt, d.h. im Zustand "GESPERRT", ist.

In Ausnahmesituationen soll auch der Kostenträger eine Vertretung löschen können, zum Beispiel auf Wunsch des Vertreters oder Vertretenen, wenn diese dies nicht per FdV selbst tun können.

Hinweis:

Eine Löschung durch den Kostenträger ist ansonsten nur für Situationen vorgesehen, in denen dies aus rechtlichen oder sicherheitstechnischen Gründen zwingend erforderlich ist und keine alternative Handlungsoption besteht.

8.3 Umsetzung der Vertretungsfunktion in der TI 2.0

8.3.1 Assets und Schutzbedarfe

Im Folgenden werden die Assets (Informationsobjekte) der Vertretungsfunktion mit ihrem zugewiesenen Schutzbedarf aufgeführt.

Asset	Vertraulichkeit	Integrität	Verfügbarkeit
Beziehung Vertreter - Vertretener	sehr hoch	sehr hoch	hoch
einzelne KVNRS	hoch	hoch - sehr hoch (abhängig von Verwendung)	hoch
gehashte KVNRS oder Beziehungen	normal	sehr hoch	hoch
Flags für Anwendungen einer	normal	sehr hoch	hoch

Vertretung			
------------	--	--	--

8.3.2 Sicherheitsanforderungen an den Systemaufbau

Direkt beauftragter Betreiber: Um ein besseres Durchgriffsrecht zu haben, sollte der Betrieb direkt beauftragt werden.

VAU: Um auszuschließen, dass der Betreiber auf die Daten des Registers zugreifen kann, muss eine VAU mit Schlüsselzeremonien unter gematik-Beteiligung genutzt werden. Es muss so eingerichtet sein, dass weder der Betreiber noch die gematik allein neue Hauptschlüssel erstellen können. Die TLS-Endpunkte befinden sich in der VAU.

Zertifikatsüberwachung: Um einen Angriff durch neu ausgestellte Zertifikate zu bemerken, muss eine Zertifikatsüberwachung (Certificate Transparency) durchgeführt werden.

ASL: Bei der Übertragung von Klardaten muss Additional Security Layer (ASL) eingesetzt werden, wo es der Schutzbedarf erfordert.

mTLS: Die Verbindungen zwischen allen festen/bekannten Servern/Diensten müssen über wechselseitig abgesichertes ("mutual") TLS erfolgen.

Die Verbindungen zwischen FdV und den Diensten werden über die Zero-Trust-Architektur (ZETA) hergestellt und unterliegen deren Anforderungen.

Um die Gefahren eines zentralen Registers so gering wie möglich zu halten, dürfen **Klardaten nur verwendet, übertragen und gespeichert werden, wo es unbedingt notwendig ist.**

8.3.2.1 Adaption der HCSL für die Bestätigung von Vertretungen

Wie im Kapitel zur Umsetzung der Vertretungsfunktion in einem Vertretungsregister und der Erwägung alternativer Lösungen bereits angemerkt wurde, benötigt jeder Mechanismus die Möglichkeit, Vertretungen wieder zurückzuziehen, als ungültig oder vorzeitig abgelaufen zu kennzeichnen. Die Fachanwendung muss sicher sein können, dass eine vom FdV präsentierte Vertretung zum aktuellen Zeitpunkt (noch) gültig ist.

Darin unterscheiden sich Vertretungen nicht von Zertifikaten - auch sie werden einmal für einen bestimmten Zeitraum ausgestellt, können aber vor Ablauf des Zeitraums zurückgezogen bzw. gesperrt werden. Aus dieser Überlegung heraus entstand die Idee, die "hashbasierten Zertifikats-Statuslisten" (HCSL, siehe [gemF_HCSL]) für die Nutzung im Vertretungsregister zu adaptieren. Diese adaptierte Liste enthält Hashwerte zu gültigen Vertretungen und wird hier hashbasierte Positivliste (HPL) genannt. Wie die HCSL basiert diese Liste auf Merkle Hash Trees, siehe [MerkleHashTrees] [RFC 6962].

Die Grundidee ist, dass der ZETA-Guard (allgemein: die Autorisierungskomponente) jeder Fachanwendung jederzeit weiß, welche Vertretungen gültig sind. Der Client erhält die Liste möglicher Vertretungen über die Auskunftsschnittstelle (oder bewahrt sie bereits lokal auf). Sobald eine Vertretung ausgeübt werden soll, präsentiert der Client die gewünschte Vertretung anhand einiger Attribute (darunter die vom Register zufällig erzeugte ID, welche für jede Vertretung einzigartig ist). Der ZETA-Guard der Fachanwendung berechnet aus den Attributen einen Hash, vergleicht diesen mit der hashbasierte Positivliste (HPL) und lässt den Client bei einer Übereinstimmung passieren.

Updates der HPL ruft der ZETA-Guard der Fachanwendung regelmäßig (z.B. alle 10 Minuten) vom Vertretungsregister - genauer: der *Gültigkeitsabfrage* - ab. Nur die ZETA-Guards der Fachanwendungen, welche die Vertretungsfunktion unterstützen, dürfen die HPL beim Register abrufen.

Die neue Methode hat gegenüber einer Attestierungs-Schnittstelle beim Vertretungsregister mehrere Vorteile:

- Einsparung einer separaten Attestierungsschnittstelle und/oder eines Dienstes (die HPL kann lediglich per statischem Webserver bereitgestellt werden),
- Wesentlich schneller: Es werden mehrere Roundtrips gegenüber einzelnen Attestierungstoken eingespart,
- Datenschutzfreundlich: Durch den Wegfall der zugriffsbezogenen Anfragen fallen keine (Meta-)Daten und kein Netzwerkverkehr an, der überwacht und ausgewertet werden könnte.

Hinweis:

Detaillierte Festlegungen zur technischen Umsetzung der HPL erfolgen im Rahmen der Spezifikation.

8.3.3 Systemaufbau

Das Diagramm unten zeigt die Umsetzung der Vertretungsfunktion und deren Integration anhand einer fiktiven Gesundheitsanwendung. Diese Gesundheitsanwendung besteht aus einem Fachdienst und zugehörigem Frontend des Versicherten, siehe links. Diese Gesundheitsanwendung ist als "Platzhalter" für zukünftige, die Vertretungsfunktion nutzende Anwendungen der TI zu verstehen. Dies könnten bereits heute bestehende Anwendungen sein, die auf die Vertretungsfunktion umgestellt werden oder komplett neue Gesundheitsanwendungen. Der Einfachheit halber wird der Fall betrachtet, dass die Gesundheitsanwendung nur einen Fachdienst umfasst. Das technische Konzept ermöglicht jedoch auch Lösungen, bei denen mehrere Fachdienste über ein einziges "umfassendes" FdV genutzt werden können (z.B. eine "Kassen-App").

Die Vertretungsfunktion wird umgesetzt über ein FdV, welches in das FdV einer Anwendung integriert werden kann und einen zentralen Dienst zur Speicherung und Bereitstellung von Daten zu Vertretungen - im Folgenden auch Vertretungsregister genannt.

Das technische Konzept ist auf die TI 2.0 ausgerichtet. Es beruht darauf, dass die Umsetzung unter Verwendung von ZETA Komponenten erfolgt, d.h. ZETA Stufe 2, mit mobilen Zugängen für Versicherte. Dies betrifft einerseits die Umsetzung der Vertretungsfunktion selbst, andererseits die Integration der Vertretungsfunktion in eine nutzende Gesundheitsanwendung. Daher sieht das Konzept punktuelle Ergänzungen an ZETA-Komponenten vor, mit dem Ziel einer möglichst aufwandsarmen Integration der Vertretungsfunktion in nutzenden Anwendungen. Die Anpassungen an den ZETA-Komponenten erweitern deren Autorisierungsfunktionen um die Möglichkeit, eine Autorisierung per Vertretung zu nutzen.

Eine Integration ohne Verwendung von ZETA ist möglich, aber erfordert dann weitergehende, anwendungsspezifische Maßnahmen zur Integration in die nutzende Anwendung. Siehe auch Kapitel 8.5 zu den möglichen Integrationsvarianten.

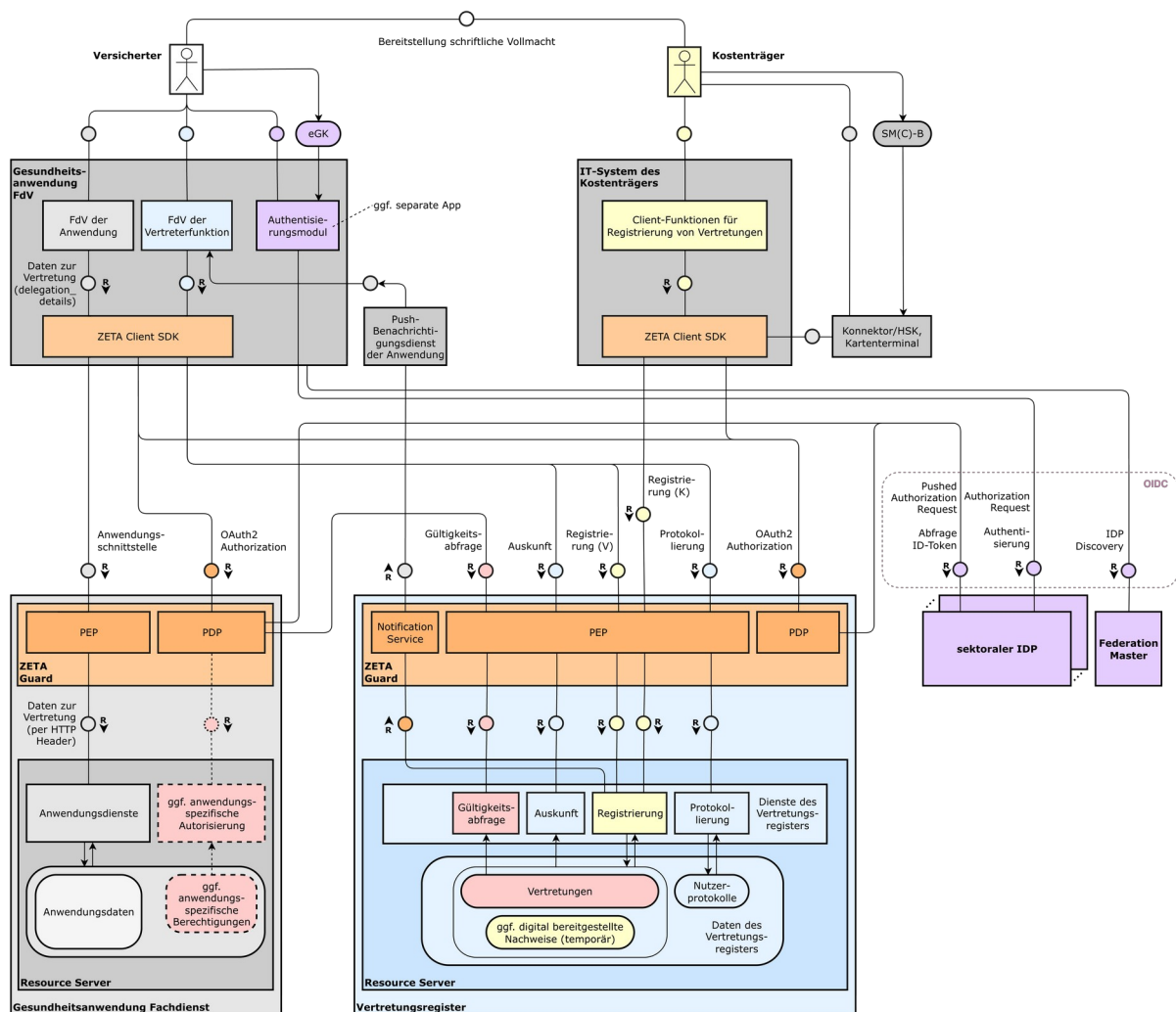


Abbildung 4 Systemaufbau der Vertretungsfunktion

Die im Diagramm gezeigten Komponenten werden im Folgenden beschrieben.

8.3.3.1 Vertretungsregister

Das Vertretungsregister besteht im Kern aus einem über interne Schnittstellen erreichbaren Resource Server, der gemäß [gemSpec_ZETA] durch den vorgelagerten ZETA Guard vor unzulässigen Zugriffen geschützt wird. Der Resource Server speichert Vertretungen und deren Status sowie Daten zu Nachweisen, soweit diese über das Vertretungsregister ausgetauscht werden. Der Inhalt eines Nachweises wird nur gespeichert - und auch nur temporär -, sofern ein Dokument als Nachweis durch den Versicherten digital erfasst wird, um es dem Kostenträger auf diesem Wege zur Prüfung zu übergeben. Des Weiteren setzt der Resource Server die Verarbeitungsfunktionen für die Gültigkeitsabfrage, Auskunft, Registrierung und Protokollierung um.

Sollte es im Rahmen der Registrierung erforderlich sein, dass der Versicherte aktiv informiert wird, so greift der Resource Server auf die im ZETA Guard vorgesehene Benachrichtigungsfunktion (Notification Service) zurück, um ihm eine Push-Nachricht auf seinem registrierten Endgerät (Client Registration des FdV der Anwendung im ZETA Guard) zukommen zu lassen.

Der ZETA Guard stellt die externen Schnittstellen des Vertretungsregisters bereit, siehe auch Abschnitt 8.3.4. Dies sind die spezifischen REST-Endpunkte für das Gesundheitsanwendung-FdV und das IT-System des Kostenträgers (siehe auch Abschnitt 8.3.4) sowie die durch ZETA vorgegebenen Schnittstellen, insbesondere für die Autorisierung mittels OAuth2. Einzelheiten zu den durch ZETA vorgegebenen Schnittstellen finden sich in [gemSpec_ZETA].

8.3.3.2 Gesundheitsanwendung FdV

Dies ist das auf einem ggf. mobilen Endgerät verfügbare Frontend des Versicherten (FdV) für die fiktive Gesundheitsanwendung. Darin enthalten sind:

- FdV der Anwendung

Dies sind die anwendungsspezifischen Frontend-Anteile, von wo aus ggf. ein Vertreter einen Zugriff auf Anwendungsdaten des Vertretenen initiiert, die im Fachdienst der Gesundheitsanwendung gespeichert sind.

- FdV der Vertretungsfunktion

Die Frontend-Funktionen der Vertretungsfunktion für den Versicherten. Diese sind anwendungsunabhängig und bieten dem Versicherten eine Übersicht "an einer Stelle" über ihn betreffende Vertretungen sowie die Möglichkeit, die Neuanlage von Vertretungen zu initiieren, bestehende Vertretungen zu bearbeiten sowie den Zugriff auf sein Nutzerprotokoll.

- ZETA Client SDK (oder kurz: ZETA Client)

Der ZETA Client leitet die Aufrufe der beiden o.g. FdV-Anteile weiter an den Fachdienst der Gesundheitsanwendung und das Vertretungsregister. Dabei setzt er auch FdV-seitige Anteile für die Client-Registrierung, Autorisierung usw. um. Näheres dazu siehe [gemSpec_ZETA].

Für die Vertretungsfunktion sind im ZETA Client Erweiterungen vorgesehen, die eine Ausübung von Vertretungen beim Zugriff auf einen Fachdienst ermöglichen. Dazu übergibt der ZETA Client die Angaben der ggf. auszuübenden Vertretung (delegation_details) an den Fachdienst - genauer: an die dort vorhandene Autorisierungskomponente, idealerweise den ZETA Guard. Dieser prüft mit Hilfe der Gültigkeitsabfrage des Vertretungsregisters die Gültigkeit, bevor die Vertretung in der Fachanwendung ausgeübt werden kann. Eine genauere Beschreibung dazu folgt im Kapitel 8.4.

- Authentisierungsmodul

Für die Authentisierung des Versicherten wird das Authentisierungsmodul des zuständigen sektoralen Identity Provider (IdP) verwendet, entweder als Teil der gleichen oder einer separat zu nutzenden App. Damit wird Versicherten eine Authentisierung sowohl mittels eGK als auch GesundheitsID ermöglicht.

8.3.3.3 Push-Benachrichtigungsdienst

Der Push-Benachrichtigungsdienst der Anwendung wird mit der Gesundheitsanwendung bereitgestellt und ermöglicht dem Notification Service im ZETA Guard des Vertretungsregisters eine aktive Benachrichtigung des Versicherten.

8.3.3.4 Federation Master und sektoraler IdP

Der Federation Master wird ggf. benötigt, um die Liste der verfügbaren sektoralen IdP abzufragen (IdP Discovery) und dem Versicherten zur Auswahl zu geben. Dieser muss

sich gegenüber dem sektoralen IdP seines Kostenträgers authentisieren, um auf den Fachdienst der Gesundheitsanwendung und das Vertretungsregister zuzugreifen.

8.3.3.5 Gesundheitsanwendung Fachdienst

Entsprechend [gemSpec_ZETA] besteht der Fachdienst aus dem eigentlichen Resource Server und dem vorgelagerten ZETA Guard.

Der ZETA Guard führt per OAuth2 die Autorisierung des Nutzers durch (PDP - Policy Decision Point) - wobei auf den sektoralen IdP für den Versicherten zurückgegriffen wird - und setzt die resultierenden Zugriffsberechtigungen durch (PEP - Policy Enforcement Point). Nur berechtigte Zugriffe auf den Resource Server werden dabei zugelassen. Eine detaillierte Beschreibung des ZETA Guard findet sich in [gemSpec_ZETA].

Für die Vertretungsfunktion sind *im ZETA Guard* Erweiterungen vorgesehen, die eine Ausübung von Vertretungen bei Zugriff auf einen Fachdienst ermöglichen. Dazu werden die vom ZETA Client bereitgestellten Angaben zur auszuübenden Vertretung (*delegation_details*) vom PDP im Rahmen der Autorisierung ausgewertet und mittels der hashbasierte Positivliste aus der Gültigkeitsabfrage des Vertretungsregisters überprüft. Erst danach werden Daten zur Vertretung über den PEP an die Anwendung und an die ggf. vorhandene anwendungsspezifische Autorisierung (siehe auch Application Authorization Backend in [gemSpec_ZETA]) weitergegeben.

Eine genauere Beschreibung der Erweiterung des ZETA Guard folgt im Kapitel 8.4.

8.3.3.6 IT-System des Kostenträgers

Mitarbeiter des zuständigen Kostenträgers können die Registrierungsfunktionen des Vertretungsregisters nutzen, um Vertretungen zu bearbeiten und optional Nachweise vom Versicherten anzufordern oder abzurufen (Client-Funktionen für die Registrierung von Vertretungen).

Dazu müssen sie sich mittels SM(C)-B gegenüber dem Vertretungsregister authentisieren. Hierfür ist die Verwendung des ZETA Client vorgesehen, welcher die Ermittlung der Nutzeridentität mittels Inbox-Konnektor (oder High Speed Konnektor) durchführt, siehe auch [gemSpec_ZETA].

8.3.4 Schnittstellen

8.3.4.1 Schnittstelle zum Fachdienst

Die Systemarchitektur der Vertretungsfunktion beruht auf der Annahme, dass der Fachdienst selbst die eigentliche Ausübung der Vertretung autorisiert und umsetzt, also den Zugriff auf Daten und Funktionen für den Vertretenen durch den aktuellen Nutzer. Die Auswahl, welcher Versicherte vertreten werden soll, erfolgt über das FdV.

Auswahldatensatz (*delegation_details*)

Zur Ausübung einer Vertretung übergibt das FdV (genauer: der ZETA Client) einen Datensatz - die *delegation_details* - an den Fachdienst (genauer: den ZETA Guard). Die Übergabe der *delegation_details* erfolgt per OAuth2 Pushed Authorization Requests als Bestandteil der *authorization_details*. Der Fachdienst (ZETA Guard) führt zunächst die Autorisierung der Vertretung durch, unter Verwendung der Gültigkeitsabfrage des Vertretungsregisters. Näheres dazu siehe Abschnitt 8.3.4.2.2.

Hinweis:

*Dies gilt in Bezug auf Anwendungen die ZETA verwenden oder zumindest einen OAuth2 Authorization Server nutzen. Die *delegation_details* könnten auch auf anderem Wege*

an den Fachdienst übergeben werden, solange dieser die Autorisierung unter Verwendung der hashbasierte Positivliste aus der Gültigkeitsabfrage des Vertretungsregisters vornimmt.

Der Datensatz der authorization_details umfasst:

- delegation_id: Ein eindeutiger, nicht erratbarer Zufallswert, über den der Eintrag im Vertretungsregister identifiziert werden kann. (Dieser wird einmalig im Rahmen der Registrierung erzeugt und kann über die Auskunftsschnittstelle des Vertretungsregisters abgefragt werden, siehe dazu auch Kapitel 8.3.4.2.1.)
- Die KVNR des Vertretenen
- Der Typ der Vertretung (Vollmacht oder elterliches Sorgerecht)
- Die Anwendung, bei der die Vertretung ausgeübt werden soll.

Die angegebene Anwendung muss zu dem Fachdienst passen, an den der Datensatz übergeben wird. Der Fachdienst muss dies überprüfen. Außerdem muss die angegebene Anwendung durch die registrierte Vertretung abgedeckt sein, was mittels Gültigkeitsabfrage geprüft wird.

Beispiel

Hier ist ein Beispiel (informativ) für die delegation_details (JSON kodiert):

```
{
  "delegation_details": [
    {
      "delegation_id": "x45Wrt7hkT...", // eindeutiger Wert
      "type": "Vollmacht",             // Typ der Vertretung
      "principal_id": "981981989181",  // KVNR des Vertretenen
      "application": "DiPag"           // Anwendung
    }
  ]
}
```

8.3.4.2 Schnittstellen des Vertretungsregisters

Die folgende Tabelle bietet einen Überblick über die Schnittstellen des Vertretungsregisters, jedoch ohne die Schnittstellen für die Autorisierung. Letztere sind durch [gemSpec_ZETA] vorgegeben. In der Spalte "Client" wird angegeben, welches Client-System diese Schnittstelle nutzt und aus welcher Komponente des Clients heraus Aufrufe der Schnittstelle initiiert werden. Siehe auch die Legende unter der Tabelle zu den Abkürzungen.

Tabelle 1 Schnittstellen des Vertretungsregisters (ohne Autorisierungsschnittstelle)

Client*	Schnittstelle*	verfügbare Funktionen/ Beschreibung	Nutzer/ Zugriffsbeschränkungen
Fachdienst	Gültigkeitsabfrage	Abfrage der Liste der Hashwerte der aktuell gültigen registrierten Vertretungen. Die Liste ermöglicht dem Fachdienst (ZETA Guard) die Prüfung, ob	Ein Eintrag in der Liste ist nur vorhanden für Vertretungen im Status GÜLTIG, siehe 8.2

		eine vom Client System vorgegebene Vertretung für den aktuellen Nutzer zurzeit gültig ist. Siehe Abschnitt <u>8.3.4.2.2</u> für weitere Details.	
GA FdV (A)	Auskunft	Abfrage von Einträgen im Vertretungsregister: • "wen vertrete ich?" Zu jedem gefundenen Eintrag wird ein Datensatz (delegation_info) ausgegeben.	Die Abfrage ist nur möglich für Vertretungen, bei denen <i>der aktuelle Nutzer der Vertreter ist</i>. Die Identität des anfragenden Nutzers wird über den sektoralen IdP ermittelt.
GA FdV (V)	Auskunft	Abfrage von Einträgen im Vertretungsregister • "wer vertritt mich?" und • "wen vertrete ich?" Zu jedem gefundenen Eintrag wird ein Datensatz (delegation_info) ausgegeben.	Die Abfrage ist nur möglich für Vertretungen, bei denen <i>der aktuelle Nutzer der Vertreter oder der Vertretene ist</i>. Die Identität des anfragenden Nutzers wird über den sektoralen IdP ermittelt.
	Registrierung (V)	Neuanlage von Vertretungen	Versicherter (Vertreter)
		Bearbeiten von Vertretungen - Ergänzen von Nachweisen	Vertreter oder Vertretener Nur in bestimmten Status der Vertretung möglich, siehe <u>8.2</u>
		Bearbeiten von Vertretungen - Ändern des Umfangs der Vertretung (bei Vollmacht)	Vertretener Nur in bestimmten Status der Vertretung möglich, siehe <u>8.2</u>
		Löschen von Vertretungen	Versicherter (Vertreter oder Vertretener) Nur in bestimmten Status der Vertretung möglich, siehe <u>8.2</u>

	Protokollierung	Abruf von Einträgen des eigenen Nutzerprotokolls, zwecks Einsicht in das Protokoll.	Versicherter
		Laden des gesamten eigenen Nutzerprotokolls. Dies wird benötigt für das Speichern per FdV, falls der Nutzer einen "Abzug" des Protokolls benötigt für eigene Nachweiszwecke.	Versicherter
		Löschen von Einträgen des eigenen Nutzerprotokolls, vollständig oder für einen Zeitraum	Versicherter
IT-System des Kostenträgers	Registrierung (K)	Bearbeiten von Vertretungen - Setzen des Status	MA des Kostenträgers, sofern für den Vertretenen zuständig. Nur in bestimmten Status der Vertretung möglich, siehe8.2
		Abrufen von Vertretungen	MA des Kostenträgers, sofern für den Vertretenen zuständig. Nur in bestimmten Status der Vertretung möglich, siehe8.2
		Anfordern und Abrufen von Nachweisen, die bei einer Vertretung hinterlegt wurden	MA des Kostenträgers, sofern für den Vertretenen zuständig. Nur in bestimmten Status der Vertretung möglich, siehe8.2
		Löschen von Vertretungen	MA des Kostenträgers, sofern für den Vertretenen zuständig. Nur in Ausnahmesituationen

*) Abkürzungen:

1413

GA FdV (A) = Gesundheitsanwendung Frontend des Versicherten, Anteil FdV der
Anwendung

GA FdV (V) = Gesundheitsanwendung Frontend des Versicherten, Anteil FdV der
Vertretungsfunktion

Registrierung (V) = Registrierungsschnittstelle für den **Versicherten**

Registrierung (K) = Registrierungsschnittstelle für Mitarbeiter des **Kostenträgers**

Offener Punkt:

Überall, wo in der obigen Tabelle Aktionen vom Versicherten ausgehen, könnte wie bei der ePA mit Hilfe des ID-Tokens der Weg bis ins VAU-HSM verschlüsselt werden, um vor der Kompromittierung der VAU zu schützen.

Im Folgenden werden die Daten, die über die Auskunftsschnittstelle bzw. die Gültigkeitsabfrage abgefragt werden können, zum besseren Verständnis kurz dargestellt.

Hinweis: Die abschließende Festlegung der Datenformate erfolgt im Rahmen der Spezifikation.

8.3.4.2.1 Auskunftsschnittstelle

Eine Abfrage der Auskunftsschnittstelle ist nur möglich für Nutzer, die im Vertretungsregister als Vertreter oder Vertretener registriert sind. Eine Übergabe von Daten an das Vertretungsregister bei Abfrage durch das FdV ist nicht erforderlich, da das Vertretungsregister die Identität des aufrufenden Nutzers mit Hilfe des IdP ermittelt.

Auskunftsdatensatz (delegation_info)

Falls es für einen Nutzer einen Eintrag gibt - er darin also Vertreter oder Vertretener ist -, dann liefert das Vertretungsregister einen Datensatz (delegation_info) mit folgenden Angaben zurück:

- delegation_id: Ein eindeutiger, nicht erratbarer Zufallswert, über den der Eintrag im Vertretungsregister identifiziert werden kann. Dieser wird einmalig im Rahmen der Registrierung erzeugt.
- Der aktuelle Status der Vertretung (siehe auch Abschnitt 8.2)
- Die Daten des Vertretenen bzw. des Vertreters
 - Name, Vorname
 - KVNR
 - Geburtsdatum
- Der Typ der Vertretung
- Gültig bis
- bei Vollmachten: Anwendungen, auf die die Vertretung beschränkt ist

Der Datensatz ist signiert mit der Signatur des Vertretungsregisters.

Beispiele

Die folgenden Beispiele gelten für den Fall, dass der Nutzer der Vertreter ist.

Hier ist ein Beispiel (informativ) für die delegation_info (JSON kodiert) für eine Vertretung auf Basis einer Vollmacht:

```
{  
  "delegation_info": [  

```

```
1455     {
1456         "delegation_id": "x45Wrt7hkT...", // eindeutiger Wert
1457         "status": "GÜLTIG",                // Status der Vertretung
1458         "type": "Vollmacht",                // Typ der Vertretung
1459         "principal": {
1460             "name": "Max",                  // Vorname des Vertretenen
1461             "family_name": "Mustermann",    // Nachname des Vertretenen
1462             "id": "981981989181",           // KVNDR des Vertretenen
1463             "birth_date": "1965-06-17"      // Geburtsdatum des Vertretenen
1464         },
1465         "applications": [                  // Liste der Anwendungen, für die
1466                                     // die Vertretung gilt
1467             "ePA",
1468             "E-Rezept",
1469             "DiPag"
1470         ]
1471     }
1472 }
1473 }
```

Bei mehreren Einträgen für einen Nutzer werden diese als Liste ausgegeben. Eine Vertretung für zwei Kinder auf Basis elterlichen Sorgerechts würde wie folgt aussehen:

```
1476 {
1477     "delegation_info": [
1478     {
1479         "delegation_id": "aX45qPrz34...", // eindeutiger Wert
1480         "status": "GÜLTIG",                // Status der Vertretung
1481         "type": "elterliches Sorgerecht",  // Typ der Vertretung
1482         "principal": {
1483             "name": "Kevin",                // Vorname des 1. Kindes
1484             "family_name": "Mustermann",    // Nachname des 1. Kindes
1485             "id": "741985817984",           // KVNDR des 1. Kindes
1486             "birth_date": "2020-02-13"      // Geburtsdatum des 1. Kindes
1487         }
1488     },
1489     {
1490         "delegation_id": "R61rTq6wPl...", // eindeutiger Wert
1491         "status": "GÜLTIG",                // Status der Vertretung
1492         "type": "elterliches Sorgerecht",  // Typ der Vertretung
1493         "principal": {
1494             "name": "Lisa",                 // Vorname des 2. Kindes
1495             "family_name": "Mustermann",    // Nachname des 2. Kindes
1496             "id": "179847419858",           // KVNDR des 2. Kindes
1497             "birth_date": "2022-08-19"      // Geburtsdatum des 2. Kindes
1498         }
1499     }
1500 ]
1501 }
```

8.3.4.2.2 Verwendung der Gültigkeitsabfrage

Um vom FdV vorgegebene Vertretungen überprüfen zu können, fragt der Fachdienst regelmäßig die Liste der Hashwerte der gültigen Vertretungen über die Gültigkeitsabfrage des Vertretungsregisters ab und hält diese Liste in einem sicheren Bereich lokal gespeichert vor. Die Liste kann in Gänze oder als Differenzliste abgefragt werden, wobei

letztere Variante nur die Veränderungen seit der zuletzt bereitgestellten Version umfasst und somit eine datensparsame Übertragung und fortlaufende Aktualisierung ermöglicht. Siehe auch Abschnitt 8.3.2.1.

Inhalt der Liste (delegation_element)

Die über die Gültigkeitsabfrage abrufbare Liste enthält für jede zurzeit gültige registrierte Vertretung einen oder mehrere zugehörige Hashwerte.

Ein Hashwert identifiziert eindeutig ein delegation_element - d.h. einen Datensatz, der folgende Angaben umfasst:

- delegation_id: Ein eindeutiger, nicht erratbarer Zufallswert, über den der Eintrag im Vertretungsregister identifiziert werden kann. Dieser wird einmalig im Rahmen der Registrierung erzeugt.
- Die KVNR des Vertreters
- Die KVNR des Vertretenen
- Der Typ der Vertretung
- Die Anwendung (genaue eine), auf die sich die Vertretung bezieht.

Da eine Vertretung unter Umständen für mehrere Anwendungen gültig sein kann, ist pro Anwendung ein eigener Eintrag (delegation_element) erforderlich.

Prüfung mittels der Liste

Zur Ausübung einer Vertretung übergibt das FdV einen Datensatz (delegation_details) an den Fachdienst. Dieser Datensatz umfasst bereits die oben aufgeführten Daten - bis auf die KVNR des Vertreters. Diese KVNR wird aus dem ID-Token entnommen, welches der Fachdienst vom sektoralen IdP für den aktuellen Nutzer abrufen muss.

Zu dem so vervollständigten Datensatz (delegation_element) wird dann der Hashwert gebildet und anschließend geprüft, ob dieser in der Liste enthalten ist.

Beispiel

Hier ein Beispiel für einen Datensatz (delegation_element), der für die Prüfung gegen die Liste verwendet werden kann:

```
{
  "delegation_element": [
    {
      "delegation_id": "x45Wrt7hkT...", // übernommen aus
      delegation_details
      "type": "Vollmacht", // übernommen aus
      delegation_details
      "delegate_id": "905284651844", // KVNR des Vertreters, aus dem
      ID-Token
      // des Nutzers entnommen
      "principal_id": "981981989181", // KVNR des Vertretenen,
      // übernommen aus
      delegation_details
      "application": "DiPag" // Anwendung, übernommen aus
      delegation_details
    }
  ]
}
```

Hinweise:

- Für die erste Version der Vertretungsfunktion (MVP) wird davon ausgegangen, dass nur eine Vertretung für eine einzelne vertretene Person per `delegation_details` angefragt werden kann - auch wenn es im Vertretungsregister Einträge für mehrere Vertretene geben kann (siehe `delegation_info`). Sollen mehrere Personen vertreten werden, so können diese Vertretungen also nur hintereinander ausgeübt werden. In einer zukünftigen Ausbaustufe der Vertretungsfunktion könnte diese Beschränkung aufgehoben werden.
- Die verbindliche Festlegung der Datenformate sowie ggf. zu ergänzender Schutzmaßnahmen erfolgen im Rahmen der Spezifikation.
- Für die Identifikation der Anwendungen (Abschnitt "applications") werden im Rahmen der Spezifikation geeignete Identifier festgelegt.

8.4 Integration in die Zero Trust Architektur (ZETA)

8.4.1 Erweiterung der ZETA Komponenten

8.4.1.1 Erweiterungen des ZETA Client SDK

Für die Vertretungsfunktion sind *im ZETA Client SDK* diese Erweiterungen vorgesehen:

- Das FdV der Anwendung kann über den ZETA Client die auszuübende Vertretung vorgeben in Form eines strukturierten Aufrufparameters, `dendelegation_details`.
- Der ZETA Client übergibt diese Daten an den ZETA Guard des Fachdienstes, sodass dieser den Zugriff als Vertreter autorisieren kann.

Eine ausführlichere Beschreibung des Ablaufs der Autorisierung mit Erweiterung des ZETA Client folgt im Kapitel 8.4.2.

8.4.1.2 Erweiterungen des ZETA Guards

Für die Vertretungsfunktion sind *im ZETA Guard* Erweiterungen vorgesehen, die eine Ausübung von Vertretungen bei Zugriff auf einen Fachdienst ermöglichen:

- Die vom ZETA Client bereitgestellten Daten zur auszuübenden Vertretung (`delegation_details`) werden zunächst vom PDP überprüft. Der PDP prüft dazu mittels des Vertretungsregisters, ob die vom FdV vorgegebene Vertretung für den aktuellen Nutzer und den angesprochenen Fachdienst aktuell gilt.
- Danach werden die anwendungsspezifischen Berechtigungen, die sich aus der Vertretung ergeben, mittels Ausführung der Policies der jeweiligen Anwendung ermittelt, der Grundkonzeption von ZETA folgend.
- Außerdem werden die Daten zur Vertretung an die Anwendung weitergegeben. Dies geschieht dadurch, dass der PDP im ZETA Guard die Daten der Vertretung aus der `delegation_details` entnimmt und geschützt im Access-Token speichert. Von dort können sie später durch den PEP entnommen und in einem eigenen Request-Header an den Resource Server der Gesundheitsanwendung übermittelt werden.
- Des Weiteren können Daten zur Vertretung an eine ggf. vorhandene anwendungsspezifische Autorisierung übergeben werden. Siehe auch Application Authorization Backend in `[gemSpec_ZETA]`.

Eine ausführlichere Beschreibung des Ablaufs der Autorisierung mit Erweiterung des ZETA Guards folgt im Kapitel 8.4.2.

8.4.2 Abfrage, Autorisierung und Ausübung einer Vertretung

Die beiden Diagramme unten stellen den gesamten Ablauf zur Ausübung einer Vertretung in einer Gesundheitsanwendung dar. Zunächst werden die registrierten Vertretungen abgefragt (erstes Diagramm), danach erfolgt die Autorisierung und Ausübung der Vertretung (zweites Diagramm). Der Ablauf der Autorisierung basiert auf ZETA [gemSpec_ZETA], ist jedoch erweitert um die Gültigkeitsprüfung der Vertretungsfunktion.

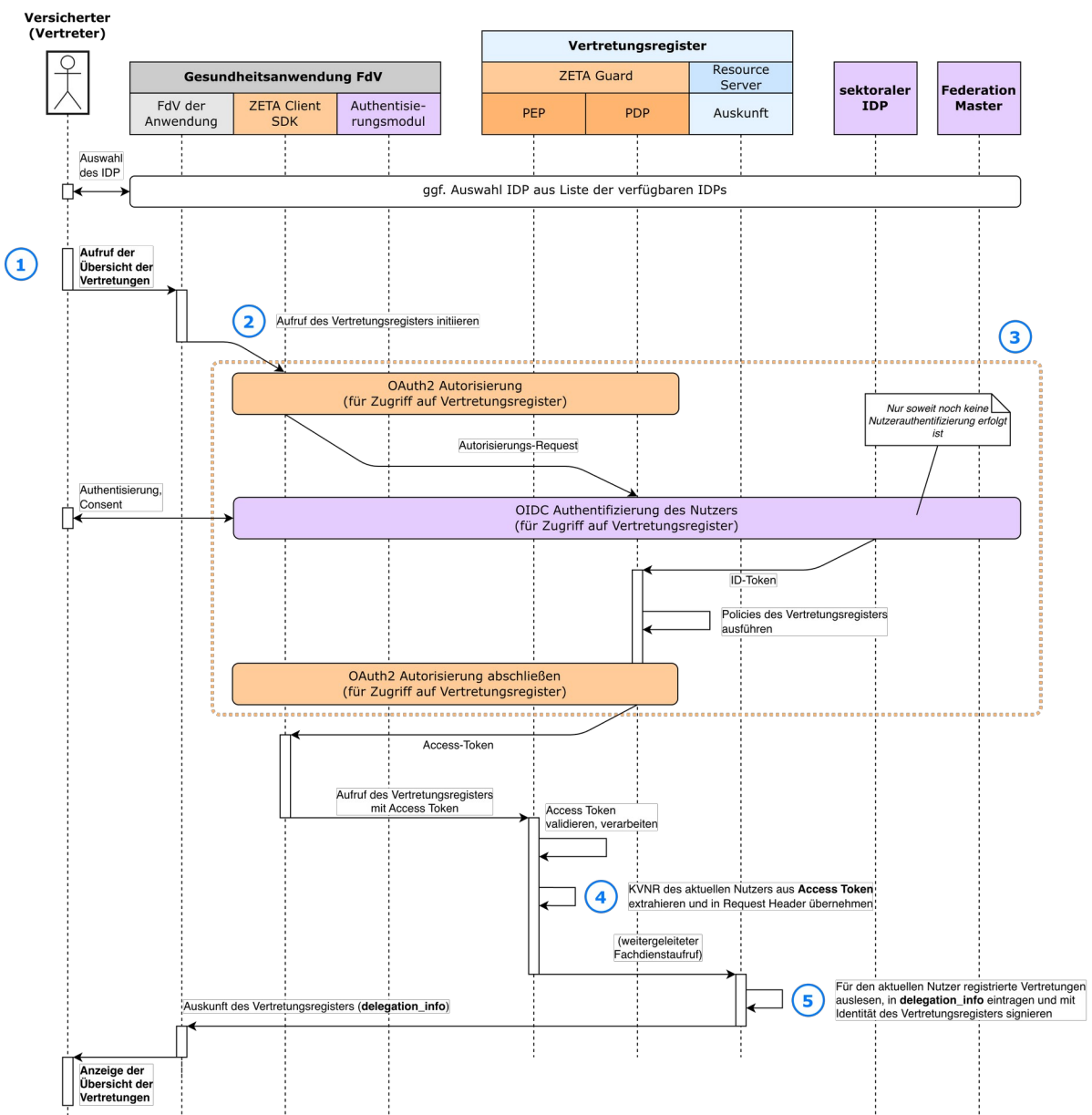


Abbildung 5 Abfrage registrierter Vertretungen

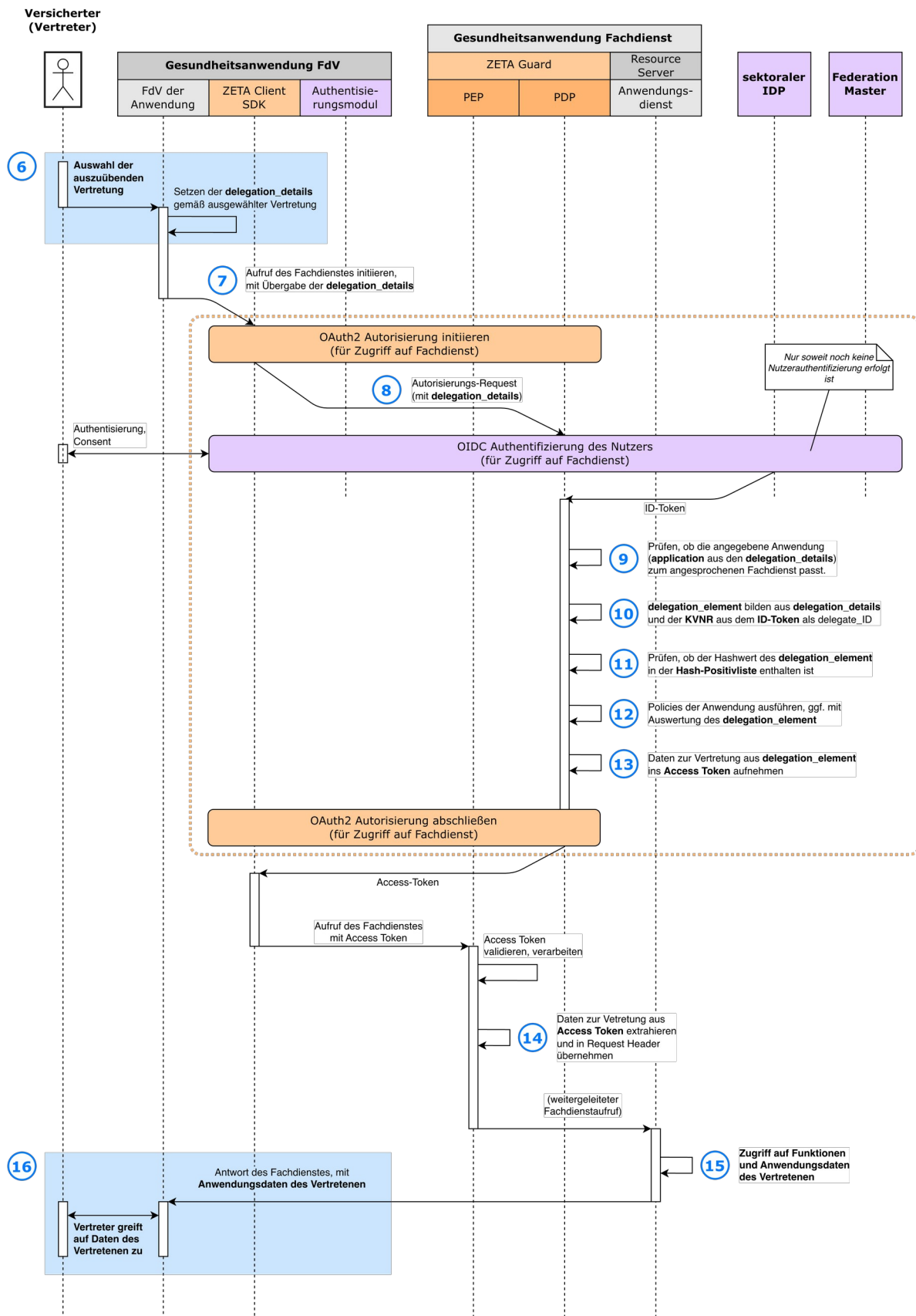


Abbildung 6 Autorisierung und Ausübung einer Vertretung

Zu Beginn des Ablaufs kann es erforderlich sein, dass der Versicherte den für ihn zuständigen Identity Provider auswählen muss. Dies ist nur dann der Fall, wenn das FdV der Gesundheitsanwendung diese Auswahl offen lässt, siehe [gemSpec_IdP_FedMaster].

Des Weiteren wird davon ausgegangen,

- dass für den Versicherten eine registrierte, gültige Vertretung im Vertretungsregister hinterlegt ist, die in der Gesundheitsanwendung verwendet werden soll.
- sowie dass der ZETA Guard des Fachdienstes über eine aktuelle HPL der gültigen Vertretungen (siehe auch Abschnitt 8.3.4.2.2) verfügt, die er vom Vertretungsregister (Gültigkeitsabfrage) bezogen hat.

Im Folgenden werden die einzelnen Schritte und Teilprozesse entsprechend der Nummerierung in den beiden Diagrammen oben erläutert:

Erstes Diagramm - Abfrage der registrierten Vertretungen:

1. Der Versicherte ruft im FdV die Übersicht "seiner" Vertretungen auf, d.h. die Liste derjenigen Personen, für die er als Vertreter im Vertretungsregister eingetragen ist.
2. Über den ZETA Guard wird der Aufruf an das Vertretungsregister initiiert.
3. Im Rahmen der Autorisierung des Versicherten durch das Vertretungsregister (ZETA Guard) wird über den sektoralen IdP die Nutzeridentität des Versicherten ermittelt. Die Policies des Vertretungsregisters werden ausgeführt und als Ergebnis der erfolgreichen Autorisierung wird ein Access-Token an das FdV (den ZETA Client) ausgegeben. Nun erfolgt die Abfrage des Vertretungsregisters (Auskunftsschnittstelle).
4. Im PEP des Vertretungsregister wird das Access-Token validiert und die Identität des aktuellen Nutzers an das Backend (Resource Server) des Vertretungsregisters weitergegeben.
5. Dort wird die Menge der für diesen Nutzer registrierten Vertretungen ausgelesen und als `delegation_info` an das FdV zurückgegeben, welches nun eine Übersicht der registrierten Vertretungen anzeigen kann.

Zweites Diagramm - Autorisierung und Ausübung einer Vertretung:

6. Der Versicherte wählt im FdV den Versicherten aus, den er vertreten möchte. Im FdV werden die `delegation_details` entsprechend der getroffenen Auswahl gesetzt.
7. Ein Aufruf des Fachdienstes der Gesundheitsanwendung wird ausgelöst. Dabei werden auch die `delegation_details` an den ZETA Client übergeben.
8. Der Zeta Client initiiert über den ZETA Guard des Fachdienstes die Autorisierung des Nutzers für den Zugriff auf den Fachdienst. Die Identität des Nutzers wird per sektorialem IdP authentifiziert und als ID Token an den ZETA Guard übergeben. Dies erfolgt per Rich Authorization Request [RFC 9396], wobei die `delegation_details` als Teil der `authorization_details` übergeben werden.
9. Der ZETA Guard (PDP) prüft, ob die in den `delegation_details` angegebene Anwendung zum Fachdienst passt.
10. Die KVN-R des Nutzers aus dem ID Token und die `delegation_details` werden in einem `delegation_element` zusammengeführt.
11. Es wird geprüft, ob die Vertretung gemäß `delegation_element` aktuell gültig ist. Dazu wird der Hashwert des `delegation_element` gebildet und gegen die im ZETA Guard vorliegende HPL aus dem Vertretungsregister geprüft.

12. Die Policies der Anwendung werden ausgeführt, dabei können die Daten der Vertretung ausgewertet werden.
13. Der ZETA Guard des Fachdienstes - d.h. der PDP - speichert die Daten der Vertretung geschützt im Access-Token.
Die Autorisierung für den Fachdienst ist damit abgeschlossen und das daraus resultierende Access-Token wird an den ZETA Client übergeben. Dieser kann dann mit diesem Token den eigentlichen Aufruf des Fachdienstes durchführen.
14. Der ZETA Guard des Fachdienstes - genauer der PEP - extrahiert die im Daten der Vertretung aus dem Access-Token und trägt diese in einen eigenen Request Header ein, der anschließend beim Aufruf an den Resource Server im Fachdienst übergeben wird.
15. Der Resource Server führt den Zugriff auf die Anwendungsdaten durch, wobei auch die Daten der Vertretung aus dem Request Header ausgewertet werden.
16. Die abgefragten Daten werden an das FdV zurückgegeben, womit der Versicherte Zugriff darauf erhält.

8.5 Integration in nutzende Gesundheitsanwendungen

Die Vertretungsfunktion baut auf der Zero Trust Architektur der TI 2.0 auf, insbesondere auf einer Erweiterung der ZETA Komponenten, siehe Kapitel 8.4. Eine Integration in nutzende Anwendungen erfolgt daher vorzugsweise unter Verwendung dieser Komponenten. Durch die Integration in die ZETA Komponenten verringert sich der Integrationsaufwand für nutzende Anwendungen.

Im Folgenden wird davon ausgegangen, dass eine fiktive Gesundheitsanwendung, bestehend aus Gesundheitsanwendung FdV und Gesundheitsanwendung Fachdienst, die Vertretungsfunktion nutzen soll, siehe auch die Darstellung in Kapitel 8.3.3.

8.5.1 Integration in das Gesundheitsanwendung FdV

8.5.1.1 Verwendung des ZETA Client

Bei der Integration in das FdV mittels ZETA sind zwei Varianten zu unterscheiden.

8.5.1.1.1 Variante 1: Nur Verwendung von Vertretungen

Diese - einfache - Variante betrifft Anwendungen, in denen Vertretungen nur genutzt werden sollen. Voraussetzung ist, dass der Versicherte die Verwaltung von Vertretungen und die Einsicht ins Nutzerprotokoll der Vertretungsfunktion über ein anderes FdV (siehe Variante 2) vornehmen kann.

Es werden daher nur Teile der Auskunft verwendet.

Benötigte Erweiterung des FdV der Anwendung sind:

1. Auswahl einer zu vertretenden Person - Auskunfts-Schnittstelle
 - Abfrage von Vertretungen - wen vertrete ich?
 - Darstellung der gefundenen Einträge
 - Auswahl und Übernahme in die delegation_details
2. Übergabe der ausgewählten Vertretung (delegation_details) an den ZETA Client

- bei den Aufrufen des Fachdienstes
- der ZETA Guard prüft die Gültigkeit der Vertretung anhand der HPL, die er regelmäßig vom Vertretungsregister (Gültigkeitsabfrage) bezieht.

8.5.1.1.2 Variante 2: Registrierung und Verwendung von Vertretungen

Diese Variante betrifft z.B. eine App eines Kostenträgers, die einem Versicherten eine "zentrale", anwendungsübergreifende Verwaltung seiner Vertretungen und deren Nutzung bei verschiedenen, integrierten Fachanwendungen bietet.

Diese Variante nutzt daher vollumfänglich die Schnittstellen des Vertretungsregisters für Versicherte.

Die technische Integration der Vertretungsfunktion umfasst:

1. Umsetzung des FdV der Vertretungsfunktion

- a. "zentrale", anwendungsübergreifende Übersicht über alle Vertretungen - Schnittstelle der Auskunft
 - Abfrage von Vertretungen - wen vertrete ich, wer vertritt mich?
 - Darstellung der gefundenen Einträge
- b. Funktionen zur Bearbeitung von Vertretungen - Registrierungs-Schnittstelle für Versicherte
 - Anlegen neuer Vertretungen
 - Eingabe von Daten zur Vertretung
 - Bearbeiten von Nachweisen ("Hochladen", Status setzen)
 - Löschen von Vertretungen
- c. Nutzerprotokoll - Protokollierungs-Schnittstelle
 - Einsicht ins Nutzerprotokoll
 - "Herunterladen" des Protokolls
 - Löschen des Nutzerprotokolls
- d. Push-Benachrichtungen des Vertretungsregisters
 - Empfang und Darstellung von Nachrichten zur Vertretungsfunktion
- e. Sonstiges
 - Einlesen eGK mit PIN - per "Guest Login" der sektoralen IdP
 - Einscannen von Bestätigungs-Codes (Schriftliche Vollmacht, Postweg)

2. Erweiterung des FdV der Anwendung - siehe Variante 1, Abschnitt 8.5.1.1.1.

8.5.1.2 Integration ohne ZETA

Verwendet ein FdV keinen ZETA Client, so ergibt sich daraus ein zusätzlicher Aufwand in Bezug auf die Übergabe einer auszuführenden Vertretung an den Fachdienst:

- Die Daten zur Vertretung müssen ähnlich den `delegation_details` an die Autorisierungskomponente des Fachdienstes übergeben werden, sofern die Prüfung der Gültigkeit der Vertretung im Rahmen der Autorisierung im Fachdienst erfolgen soll. Das Ergebnis der Autorisierung muss dann beim Aufruf der eigentlichen Fachfunktionen berücksichtigt werden. Sofern die Anwendung einen OAuth2

Authorization Server verwendet, liegt es nahe, die Gültigkeitsprüfung der Vertretung dort mit zu integrieren und das Ergebnis über das Access-Token dem FdV bereitzustellen, welches dieses dann bei Aufruf der eigentlichen Fachfunktionen nutzen kann.

- Alternativ könnten die Daten zur Vertretung auch erst beim Aufruf der fachlichen Funktionen übergeben werden, damit die Autorisierung der Vertretung (d.h. die Gültigkeitsprüfung) im Rahmen der Anwendungslogik im Fachdienst erfolgen kann.

8.5.2 Integration in den Gesundheitsanwendung Fachdienst

8.5.2.1 Verwendung des ZETA Guard

Bei Nutzung des ZETA Guards für die Umsetzung eines Fachdienstes übernimmt der dort enthaltene PDP die Berechtigungsprüfung für die Anwendung gemäß den anwendungsspezifischen Policies. Der PEP gewährt den Zugriff auf den Resource Server des Fachdienstes. Daten aus dem Request Context - wie etwa die Daten aus der Nutzeridentität - erhält der Resource Server vom PEP in Form von HTTP Request Headers.

Nutzt eine Gesundheitsanwendung die Vertretungsfunktion, so sind folgende Erweiterungen für den Fachdienst vorzunehmen:

1. Erweiterung der anwendungsspezifischen Policies um Berechtigungsregeln für Vertreter.
Zusätzliche Policies können anwendungsspezifische Regeln abbilden, wobei die Daten aus `dendelegation_details` ausgewertet werden können.
2. Entgegennahme und Verarbeitung der vom ZETA Guard übergebenen Daten zur Vertretung.
Falls der Zugriff durch den ZETA Guard erlaubt wird, werden die Daten der vertretenen Person (aus `dendelegation_details`) per HTTP Header an den Resource Server übergeben. Der Resource Server kann diese auswerten, um zum Beispiel die Daten des Vertretenen - statt der des aktuellen Nutzers - zu selektieren.

8.5.2.2 Integration ohne ZETA

Wird im Fachdienst kein ZETA Guard verwendet, so entstehen dort zusätzliche Aufwände durch die Umsetzung der Autorisierung einer auszuübenden Vertretung. Unabhängig davon, wie das FdV der Anwendung die Daten einer auszuführenden Vertretung übergibt (siehe Abschnitt 8.5.1.2), muss der Fachdienst diese bei der Autorisierung verarbeiten.

Dies betrifft insbesondere die Anbindung und Verwendung der Gültigkeitsabfrage des Vertretungsregisters:

- Der Fachdienst muss sich gegenüber dem Vertretungsregister authentisieren und von dort die HPL beziehen sowie regelmäßig die Aktualisierungen der Delta-Listen abfragen.
- Die HPL muss validiert werden (Signaturprüfung) und lokal geschützt gespeichert werden.
- Der Fachdienst muss die Identität des Nutzers (Vertreter) sicher ermitteln, um dessen KVN-R zu erhalten.
- Er muss die Daten der auszuübenden Vertretung (vergleichbar mit den `delegation_details`) vom FdV beziehen
- Er muss sicherstellen, dass die dort angegebene Anwendung, für die die Vertretung ausgeführt werden soll, zum Fachdienst passt.

- Diese Daten (KVNR des Nutzers, weitere Daten der Vertretung) müssen für die Gültigkeitsprüfung zu einem Datensatz zusammengeführt und der Hashwert dazu gebildet werden. Dieser muss gegen die lokal vorgehaltene HPL geprüft werden.

8.6 Integration in PoPP

Der PoPP Service ermöglicht dem Versicherten, die eigene Behandlung (allgemeiner: Versorgung) bei einer Leistungserbringerinstitution zu initiieren und dieser den Zugriff auf die eigenen Daten in Diensten der TI zu ermöglichen. Es besteht grundsätzlich auch die Möglichkeit, hier die eGK des eigenen Kindes einzusetzen, um die Behandlung/Versorgung für das Kind zu initiieren.

Mit der Vertretungsfunktion soll es ermöglicht werden, als Vertreter für einen Vertretenen dessen Behandlung/Versorgung zu initiieren - ohne darauf angewiesen zu sein, dass man über die eGK des Vertretenen verfügt.

Ein Lösungsansatz besteht darin, den PoPP Service dahingehend zu erweitern, dass der Versicherte den PoPP Service als Vertreter eines ausgewählten anderen Versicherten nutzen kann. Dabei würde das PoPP-Token als Nachweis des Versorgungskontextes ggf. zusätzlich die Information aufnehmen, welchen anderen Versicherten der nutzende Versicherte gerade vertritt und aufgrund welcher Vertretungsbeziehung (elterliche Sorge oder Vollmacht). Mit diesem erweiterten PoPP-Token würde der LEI dann der Zugriff auf die Daten des Vertretenen ermöglicht.

Offener Punkt:

Die Ausarbeitung dieses Lösungsansatzes ist Gegenstand laufender Konzeptionsarbeit und soll im Rahmen der Spezifikation abgeschlossen werden.

8.7 Umsetzung der Registrierungsprozesse

8.7.1 Vollmacht - gewillkürte Vertretung

Bei allen in diesem Konzept dargestellten Anwendungsszenarien wird davon ausgegangen, dass der Vertreter über ein eigenes FdV verfügt, d.h. ein eigenes Endgerät mit App seines Kostenträgers. Der Vertretene (also der Vollmachtgeber) verfügt je nach Szenario über

- ein eigenes FdV (Endgerät mit App seines Kostenträgers),
- nur eGK mit PIN oder
- kein FdV und keine eGK mit PIN.

8.7.1.1 Vollmacht erteilen per FdV

Bei diesem Szenario wird davon ausgegangen, dass Vertreter und Vertretener jeweils über ein eigenes FdV verfügen. Beide können bei verschiedenen Kostenträgern versichert sein - PKV oder GKV - und eGK mit PIN oder eine GesundheitsID nutzen.

Ablauf:

1. Der Vertreter meldet sich in seinem FdV an.
2. Der Vertreter erfasst die Daten des zu Vertretenden (Geburtsdatum, Name, KVNR).
3. Der zu Vertretende meldet sich in seinem FdV an.

4. Der zu Vertretende erhält in seinem FdV eine Nachricht über die Vertretungsanfrage, aus der die Identität des Vertreters hervorgeht.
5. Der zu Vertretende wählt aus, für welche Anwendungen (ePA, E-Rezept usw.) die Anwendung gelten soll. Er kann auch eine Befristung für die Vollmacht insgesamt vorgeben.
6. Der zu Vertretende bestätigt abschließend die Vertretung. Damit ist die Vollmacht registriert.
7. Der Vertreter erhält eine Nachricht im FdV über die erfolgreiche Einrichtung der Vertretung.
8. Der Vertreter kann ab dann für den Vertretenen agieren.

Hinweise:

Die manuelle Erfassung der Daten in Schritt 2 könnte vereinfacht werden, indem der Vertreter auf seinem FdV einen QR-Code erzeugt, den der zu Vertretende mit seinem FdV einliest - oder umgekehrt. Auf diesem Weg könnten die Daten der beiden sicher authentifizierten Personen bei der neu zu registrierenden Vertretung ohne manuelle Eingabe eingetragen werden. Danach ginge der Prozess ab Schritt 4 weiter.

Da beide - Vertreter und Vertretener - über ein FdV verfügen, wäre es auch denkbar, dass der Prozess durch den Vertretenen als Vollmachtgeber gestartet wird und der Vertreter die Vollmacht als Vollmachtnehmer bestätigt. Der oben beschriebene Ablauf hat allerdings den Vorteil, dass im ersten Schritt die Identität des Vertreters sicher festgestellt wird und diese dem Vertretenen angezeigt werden kann, sodass der Vertretene verlässlich erkennen kann, wem er eine Vollmacht erteilt.

8.7.1.2 Vollmacht erteilen per eGK+PIN

Bei diesem Szenario wird davon ausgegangen, dass

- der zu Vertretende nicht digital affin ist, d.h. kein eigenes FdV hat,
- der zu Vertretende über seine eGK und PIN verfügt und
- Vertreter und zu Vertretender sich räumlich zusammenfinden, sodass der Vertreter dem zu Vertretenden temporär Zugang zu seinem FdV geben kann.

Ablauf:

1. Der Vertreter meldet sich in seinem FdV an.
2. Der Vertreter erfasst gemäß den Wünschen des zu Vertretenden den Umfang der Vollmacht (welche Anwendungen, welche Befristung).
3. Der Vertreter händigt sein FdV dem zu Vertretenden aus zur Bestätigung der Vollmacht.
4. Der zu Vertretende sieht auf dem FdV die Angaben zur Vertretung
 - a. die Identität des Vertreters und
 - b. die oben erfassten Daten zum Umfang der Vollmacht.
5. Der zu Vertretende prüft die Angaben
 - a. Falls einverstanden, bestätigt er die Vollmacht, indem er seine eGK an das FdV des Vertreters hält und die zugehörige PIN eingibt. Weiter mit dem nächsten Schritt.
 - b. Ansonsten geht es zurück zu Schritt 2 zwecks Korrektur.
6. Der zu Vertretende gibt das FdV zurück an den Vertreter.

7. Der Vertreter erhält im FdV eine Nachricht über die erfolgreiche Einrichtung der Vertretung.

8. Der Vertreter kann ab dann für den Vertretenen agieren.

Hinweise:

Dieses Verfahren zielt auf zu vertretende GKV-Versicherte ab, die nicht digital affin sind, jedoch über eGK mit PIN verfügen. Der Vertreter kann PKV- oder GKV-versichert sein.

Zu vertretende PKV-Versicherte können das Verfahren per FdV mit GesundheitsID nutzen (siehe oben) oder das Verfahren mit schriftlicher Vollmacht, das im Folgenden beschrieben wird.

8.7.1.3 Vollmacht erteilen in schriftlicher Form

Bei diesem Szenario wird davon ausgegangen, dass

- der zu Vertretende *nicht* digital affin ist, d.h. *kein* eigenes FdV hat und
- der zu Vertretende *nicht* über eine eGK mit PIN verfügt.

Hinweis:

Sofern zumindest eine eGK vorliegt, kann der zu Vertretende alternativ zu nachfolgendem Ablauf auch die dazugehörige PIN bei seinem Kostenträger anfordern und den Ablauf nach Abschnitt 8.7.1.2 ausführen.

Das im Folgenden beschriebene Verfahren zielt darauf ab, dem zu Vertretenden die Ausstellung einer Vollmacht in Papierform zu ermöglichen, jedoch systemseitig unterstützt und abgesichert durch einen digitalen Prozess.

Ablauf:

1. Der Vertreter meldet sich an seinem FdV an.
2. Der Vertreter erfasst gemäß den Angaben des zu Vertretenden
 - a. die Daten des zu Vertretenden (Geburtsdatum, Name, KVNR, Adresse)
 - b. den Umfang der Vollmacht (welche Anwendungen, welche Befristung)
3. Die Vertretungsfunktion speichert diese Daten, inklusive der sicher ermittelten Identität des Vertreters aus Schritt 1.
4. Die Vertretungsfunktion generiert einen Vordruck für die Vollmacht, die der Vertreter per FdV herunterladen, ausdrucken und dem zu Vertretenden aushändigen kann.¹ Dieser Vordruck enthält einen vorbereiteten Text für die Vollmachtserteilung.² Darin enthalten sind
 - a. die Daten des Vertreters gemäß seiner Identität (aus Schritt 1), also des zu Bevollmächtigenden,
 - b. die Daten des zu Vertretenden (aus Schritt 2a), also des Vollmachtgebers,
 - c. die Daten zum Umfang der Vollmacht (aus Schritt 2b) sowie
 - d. einen Bar-Code, der den eingetragenen Datensatz im Vertretungsregister (siehe Schritt 3) eindeutig identifiziert.
5. Der zu Vertretende unterschreibt die Vollmacht und sendet diese postalisch an den für ihn zuständigen Kostenträger.
6. Der Kostenträger empfängt und erfasst das Schreiben. Er kann durch den in der Vollmacht enthaltenen Code den gespeicherten Eintrag (aus Schritt 3) mit den zugehörigen Daten auslesen und im Folgenden bearbeiten.

- 1895 7. Der Kostenträger prüft,
- 1896 a. ob er den im Schreiben aufgeführten Vollmachtgeber eindeutig einem in ihren
- 1897 Bestandsdaten erfassten Versicherten zuordnen kann,
- 1898 b. ob die Vollmacht unterschrieben wurde und - soweit dies prüfbar ist³ - durch den
- 1899 Vollmachtgeber,
- 1900 c. ob alle im Schreiben aufgeführten Daten mit den im Vertretungsregister
- 1901 angelegten Eintrag übereinstimmen, um Manipulationen am Text der Vollmacht
- 1902 auszuschließen,⁴
- 1903 d. ob keine handschriftlichen Veränderungen vorgenommen wurden.
- 1904 8. Nach erfolgreicher Prüfung vermerkt der Kostenträger dies bei der (gemäß Bar-Code)
- 1905 zugehörigen im Vertretungsregister angelegten Vertretung (noch nicht gültiger
- 1906 Datensatz, siehe Statusmodell der Vertretung).
- 1907 9. Das Vertretungsregister generiert daraufhin einen Vordruck für ein
- 1908 Bestätigungsschreiben mit einem Bestätigungscode, d.h. einem nicht erratbaren,
- 1909 eindeutigen Zufallswert, der als Bar-Code in dem Vordruck enthalten ist.⁵
- 1910 10. Der Kostenträgersendet diese Bestätigung an die Meldeadresse des Vollmachtgebers,
- 1911 wobei eine Zustellung mit Identitätsprüfung erforderlich ist, die ein geeignetes
- 1912 Sicherheitsniveau aufweisen muss.⁶
- 1913 11. Der Vollmachtgeber empfängt nach erfolgter Identitätsprüfung das
- 1914 Bestätigungsschreiben. Diesem kann er entnehmen, um welche Vollmacht es geht
- 1915 und dass er zur Aktivierung der Vollmacht den Bestätigungscode an den Vertreter
- 1916 aushändigen muss, sofern er die Vollmacht abschließend bestätigen möchte.
- 1917 12. Der Vollmachtgeber händigt das Schreiben mit dem Bestätigungscode an den
- 1918 Vertreter aus.
- 1919 13. Der Vertreter meldet sich im FdV an und scannt den Bestätigungscode mit seinem
- 1920 FdV ein.
- 1921 14. Das Vertretungsregister prüft,
- 1922 a. ob der Bestätigungscode gültig ist,
- 1923 b. auf welche Vertretung sich der Code bezieht und
- 1924 c. ob der angemeldete Nutzer dem in der Vertretung eingetragenen Vertreter
- 1925 entspricht.
- 1926 15. Bei erfolgreicher Prüfung wird die im Vertretungsregister eingetragene Vertretung auf
- 1927 "GÜLTIG" gesetzt. Erst jetzt ist die digital erfasste Vollmacht wirksam.
- 1928 16. Der Vertreter erhält im FdV eine Nachricht über die erfolgreiche Einrichtung der
- 1929 Vertretung.
- 1930 17. Der Vertreter kann ab dann für den Vertretenen agieren.

Wichtige Hinweise:

- 1932 1) Der in Schritt 4 generierte Vordruck könnte auch vom zuständigen Kostenträger in
- 1933 Papierform per Post an den Vollmachtgeber gesendet oder diesem persönlich
- 1934 ausgehändigt werden, falls die Verwendung einer heruntergeladenen Druckvorlage durch
- 1935 den Nutzer nicht möglich ist.
- 1936 2) Der Vordruck dient dazu, die Formulierung einer eindeutigen und für den
- 1937 Vollmachtgeber - und den Kostenträger - nachvollziehbaren Willensbekundung
- 1938 sicherzustellen, die alle relevanten Daten enthält und mit dem entsprechenden Datensatz
- 1939 im Vertretungsregister übereinstimmt.

3) Die Prüfung der Unterschrift ist eine Plausibilitätsprüfung und ersetzt nicht die Identitätsprüfung. Siehe dazu Schritt 10.

4) Der Abgleich mit den im Vertretungsregister bereits erfassten Daten soll sicherstellen, dass der Vollmachtstext nicht manipuliert wurde - und dass

- kein anderer als der im Vertretungsregister eingetragene Vertreter benannt wird,
- kein anderer als der im Vertretungsregister eingetragene Vollmachtgeber benannt wird und
- kein anderer als der im Vertretungsregister eingetragene Umfang der Vollmacht beschrieben wird, d.h. dass Befristung und Auswahl der Gesundheitsanwendungen übereinstimmen.

5) Der Bestätigungscode muss so gewählt und verarbeitet werden, dass er

- nicht erraten werden kann,
- nur einmal eingesetzt werden kann,
- nur zeitlich beschränkt einlösbar ist,
- nur zur Bestätigung der zugehörigen Vertretung verwendet werden kann und
- nur durch den Nutzer, der als Vertreter eingetragen ist, eingelöst werden kann.

6) Anstelle eines Postversands mit Meldeadresse kann auch eine persönliche Aushändigung mit Identitätsprüfung des Empfängers erfolgen.

Offener Punkt:

Das oben beschriebene Verfahren kann ggf. noch angepasst und optimiert werden, solange folgende Eckpunkte gewährleistet bleiben:

- Das Verfahren - insbesondere die Bereitstellung des Bestätigungscode für den Vollmachtgeber - muss generell ein ausreichendes Sicherheitsniveau aufweisen, vergleichbar dem bei Ausgabe einer PIN für eine eGK.
- Der Vollmachtgeber muss sicher nachvollziehen können, welche Vollmacht für ihn digital eingerichtet wird.
- Vollmachtgeber und Vertreter müssen eindeutig und auf ausreichend hohem Sicherheitsniveau identifiziert werden.
- Manipulationen an den Schreiben und den darin enthaltenen Daten müssen möglichst verhindert oder ggf. erkannt werden können.

Die abschließende Festlegung der technisch-organisatorischen Maßnahmen erfolgt im Rahmen der Spezifikation.

8.7.2 Einrichten einer Vertretung aufgrund elterlicher Sorge

Es wird davon ausgegangen, dass der Vertreter (Elternteil) über ein eigenes FdV verfügt, d.h. ein mobiles Endgerät inklusive der App seines Kostenträgers. Elternteil und zu vertretendes Kind können bei verschiedenen Kostenträgern versichert sein, GKV oder PKV.

Im Gegensatz zur gewillkürten Vertretung ist hier keine explizite Eingabe einer Befristung vorgesehen, denn die Befristung ergibt sich bereits aus dem Umstand, dass ein Minderjähriger ab Vollendung des 15. Lebensjahres bei Gesundheitsangelegenheiten selbst entscheiden darf. Zu diesem Zeitpunkt wird ein Eintrag der Bevollmächtigung aufgrund eines eingetragenen Sorgerechts im Vertretungsregister automatisch unwirksam.

Im Fall von GKV-versicherten Kindern kann eine an ein Elternteil ausgegebene eGK mit PIN des Kindes für die Einrichtung der Vertretung genutzt werden. Ansonsten erfordert die Einrichtung einer Vertretung aufgrund elterlicher Sorge eine Bestätigung durch den

1986 zuständigen Kostenträger. Dieser entscheidet, ob und welche Nachweise ggf. dazu vom
1987 Vertreter angefordert werden.

8.7.2.1 Sorgerecht eintragen mit eGK+PIN des Kindes

Dieses Szenario zielt auf GKV-versicherte Kinder ab, deren Eltern über eine eGK mit PIN des Kindes verfügen.

Ablauf:

1. Das Elternteil meldet sich in seinem FdV an.
2. Das Elternteil wählt die Registrierung des Sorgerechts per eGK des Kindes aus.
3. Das FdV gibt Hinweise zur Handhabung der eGK.
4. Das Elternteil hält die eGK des Kindes an das FdV und gibt die zugehörige PIN ein.
5. Die Daten des Kindes werden ausgelesen und im FdV angezeigt (Name, Geburtsdatum, KVNR)
6. Das Elternteil bestätigt, dass ein Sorgerecht eingetragen werden soll.
7. Die Vertretungsfunktion setzt den Status des Sorgerechteintrags auf "GÜLTIG".
8. Das Elternteil erhält im FdV eine Nachricht über die erfolgreiche Einrichtung der Vertretung.
9. Das Elternteil kann ab dann für das Kind agieren.

8.7.2.2 Sorgerecht eintragen ohne eGK des Kindes

Bei diesem Szenario wird davon ausgegangen, dass das Elternteil nicht über die eGK und PIN des Kindes verfügt.

Ablauf:

1. Das Elternteil meldet sich in seinem FdV an
2. Das Elternteil wählt die Registrierung des Sorgerechts ohne eGK des Kindes aus.
3. Das Elternteil gibt die Daten des Kindes ein (Name, Geburtsdatum, KVNR)
4. Das Elternteil bestätigt, dass eine Vertretung für dieses Kind eingetragen werden soll.
5. Der für das Kind zuständige Kostenträger bearbeitet die angelegte Vertretung:
 - Falls aus Sicht des Kostenträgers die Voraussetzungen für eine Bestätigung gegeben sind, geht es weiter mit Schritt 8.
 - Falls der Kostenträger unter Verwendung des Vertretungsregisters Nachweise anfordern möchte, geht es weiter mit dem nächsten Schritt:
6. Der Kostenträger trägt benötigte Nachweise bei der Vertretung als "angefordert" ein und weist diese dem Elternteil zu. Das Elternteil erhält eine Push-Nachricht per FdV.
7. Das Elternteil stellt die angeforderten Nachweise bereit. Der Ablauf geht zurück zu Schritt 5.
8. Der für das Kind zuständige Kostenträger bestätigt die Vertretung und setzt dadurch den Status auf "GÜLTIG".
9. Das Elternteil erhält im FdV eine Nachricht über die erfolgreiche Einrichtung der Vertretung.
10. Das Elternteil kann ab dann als Vertreter für das Kind agieren.

8.8 Aufbau des Nutzerprotokolls

Für den Nachvollzug von Zugriffen auf Dokumente und Daten von Versicherten sollen vom Vertretungsregister Protokolle geschrieben und z.B. für die Einsicht durch den Versicherten über das FdV zur Verfügung gestellt werden.

Diese sollen mindestens enthalten:

Tabelle 2 Mögliche Einträge im Nutzerprotokoll

Typ des Zugriffs	Zeitpunkt des Zugriffs	Akteur [Darstellung]	Betroffene Daten [Darstellung]
Anlegen einer Vertretung	Datum und Uhrzeit	Versicherter [Name, KVNR]	Vertretung [Typ der Vertretung, Name des Vertreters und des Vertretenen]
Löschen einer Vertretung	Datum und Uhrzeit	Versicherter [Name, KVNR] oder Kostenträger [Name, Telematik-ID]	Vertretung [Typ der Vertretung, Name des Vertreters und des Vertretenen]
Änderung des Status einer Vertretung	Datum und Uhrzeit	Versicherter [Name, KVNR] oder Kostenträger [Name, Telematik-ID] oder Vertretungsregister ["automatisch"]	Vertretung [Typ der Vertretung, Name des Vertreters und des Vertretenen, neuer Status]
Änderung des Umfangs einer Vertretung (Auswahl der Anwendungen bei Vollmacht)	Datum und Uhrzeit	Versicherter [Name, KVNR]	Vertretung [Typ der Vertretung, Name des Vertreters und des Vertretenen, zusätzliche oder entfallene Anwendungen]
Änderung der Gültigkeitsdauer einer Vertretung (Ablaufdatum bei Vollmacht)	Datum und Uhrzeit	Versicherter [Name, KVNR]	Vertretung [Typ der Vertretung, Name des Vertreters und des Vertretenen, neues Ablaufdatum]
Hinzufügen eines Nachweises zu einer Vertretung	Datum und Uhrzeit	Versicherter [Name, KVNR] oder Kostenträger [Name, Telematik-ID]	Vertretung [Typ der Vertretung, Name des Vertreters und des Vertretenen] Nachweis [Name des Nachweises]

Ändern des Status eines Nachweises zu einer Vertretung	Datum und Uhrzeit	Kostenträger [Name, Telematik-ID]	Vertretung [Typ der Vertretung, Name des Vertreters und des Vertretenen] Nachweis [Name des Nachweises, neuer Status]
Speichern des Inhalts eines Nachweises (z.B. Upload eines eingescannten Dokuments) zu einer Vertretung	Datum und Uhrzeit	Versicherter [Name, KVNR] oder Kostenträger [Name, Telematik-ID]	Vertretung [Typ der Vertretung, Name des Vertreters und des Vertretenen] Nachweis [Name des Nachweises]

2032

9 Anhang A - Verzeichnisse

2033

9.1 Abkürzungen

Kürzel	Erläuterung
ASL	Additional Security Layer
BGB	Bürgerliches Gesetzbuch
DiPag	Digitale Patientenrechnung
eGK	Elektronische Gesundheitskarte
EHDS	European Health Data Space (Europäischer Gesundheitsdatenraum)
E-Rezept	Elektronisches Rezept
ePA	Elektronische Patientenakte
FdV	Frontend des Versicherten
GA	Gesundheitsanwendung
GKV	Gesetzliche Krankenversicherung
HCSL	Hash based Certificate Status List (Hashbasierte Zertifikatsstatusliste)
HPL	Hashbasierte Positivliste
HSM	Hardware Security Module
HTTP	Hypertext Transfer Protocol
ID	Identifizier
IdP	Identity Provider
IETF	Internet Engineering Task Force
IT	Informationstechnologie
JSON	JavaScript Object Notation
KVNR	Krankenversicherungsnummer

LE	Leistungserbringer
LEI	Leistungserbringereinstitution
MA	Mitarbeiter
mTLS	Mutual Transport Layer Security
MVP	Minimum Viable Product (Minimal funktionsfähige Erstversion)
OAuth	Open Authorization
OAuth2	Open Authorization 2.0
PDF	Portable Document Format
PDP	Policy Decision Point
PEP	Policy Enforcement Point
PIN	Persönliche Identifikationsnummer
PKV	Private Krankenversicherung
PoPP	Proof of Patient Presence
QR	Quick Response (Zweidimensionaler Matrixcode)
QR-Code	Quick Response Code (Maschinenlesbarer zweidimensionaler Code)
REST	Representational State Transfer
RFC	Request for Comments
SDK	Software Development Kit
SGB I	Sozialgesetzbuch, Erstes Buch
SGB V	Sozialgesetzbuch, Fünftes Buch
SM(C)-B	Security Module Card Typ B
TI	Telematikinfrastruktur
TLS	Transport Layer Security
VAU	Vertrauenswürdige Ausführungsumgebung

VSDM	Versichertenstammdatenmanagement
ZETA	Zero Trust Access (Sicherheitsarchitektur der TI 2.0 zur Authentifizierung und Autorisierung)
ZETA Client	Zero Trust Access Client (Client-Komponente der ZETA-Architektur)
ZETA Guard	Zero Trust Access Guard (Autorisierungs- und Sicherheitskomponente der ZETA-Architektur)

9.2 Abbildungsverzeichnis

Abbildung 1 Vertretungsfunktion - Überblick.....	16
Abbildung 2 Informationsmodell zur Vertretungsfunktion.....	28
Abbildung 3 Status und Statusübergänge von Vertretungen.....	33
Abbildung 4 Systemaufbau der Vertretungsfunktion.....	39
Abbildung 5 Abfrage registrierter Vertretungen.....	50
Abbildung 6 Autorisierung und Ausübung einer Vertretung.....	52

9.3 Tabellenverzeichnis

Tabelle 1 Schnittstellen des Vertretungsregisters (ohne Autorisierungsschnittstelle).....	43
Tabelle 2 Mögliche Einträge im Nutzerprotokoll.....	62

9.4 Referenzierte Dokumente

9.4.1 Dokumente der gematik

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

[Quelle]	Herausgeber: Titel
[gemF_HCSL]	gematik: Feature Hash based Certificate Status List (HCSL) https://gemspec.gematik.de/prereleases/Draft_gemF_HCSL/gemF_HCSL_V1.0.0_CC/
[gemGlossar]	gematik: Glossar der Telematikinfrastruktur

	https://fachportal.gematik.de/fileadmin/Fachportal/Glossar/gemGlossar_V5.2.0.pdf
[gemSpec_IdP_FedMaster]	gematik: Spezifikation Federation Master https://gemspec.gematik.de/docs/gemSpec/gemSpec_IdP_FedMaster/latest/
[gemSpec_ZETA]	gematik: Spezifikation Zero Trust Access (ZETA) https://gemspec.gematik.de/docs/gemSpec/gemSpec_ZETA/latest/

2050

9.4.2 Weitere Dokumente

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[MerkleHashTrees]	Ralph Merkle (1987): "A Digital Signature Based on a Conventional Encryption Function" In: Pomerance, C. (eds) Advances in Cryptology — CRYPTO '87. CRYPTO 1987. Lecture Notes in Computer Science, vol 293. Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-48184-2_32 , https://rdcu.be/VBpYbPAnEnJa (aufgerufen am 01.09.2026)
[RFC6962]	IETF (2013): RFC 6962 – Certificate Transparency https://www.rfc-editor.org/info/rfc6962/ (aufgerufen am 01.09.2026)
[RFC9396]	IETF (2023): RFC 9396 – OAuth 2.0 Rich Authorization Requests https://www.rfc-editor.org/info/rfc9396/ (aufgerufen am 01.09.2026)

2051 **10 Anhang C - Offene Punkte, Fragen**

2052 **10.1 <offener Punkt oder Frage>**

2053