Elektronische Gesundheitskarte und Telematikinfrastruktur

Systemdesign der Telematikinfrastruktur - Release 4.0 -

Version:	1.0.~~9.~~0 CC
Revision:	
Stand:	~~20.03~~30.04.2020
Status:	zur Abstimmung freigegeben
Klassifizierung:	~~vertraulich_TI-Ausschuss~~öffentlich
Referenzierung:	[gemKPT_SysD_TI]

Dokumenteninformationen

Änderungen zur Vorversion

Es handelt sich um die Erstversion des Dokumentes.

Dokumentenhistorie

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
1.0.~~9.~~0 CC	~~20.03~~28.04.20		Zur Abstimmung freigegeben	

Inhaltsverzeichnis

1 Einordnung des Dokuments

Beginnend mit Release 4.0 stellt die gematik ihr Vorgehen in Bezug auf die Erfassung von fachlichen Anforderungen für die TI (vormals geschehen über Lastenhefte) und die Betrachtung auf System-Ebene der TI (vormals geschehen über Systemlösungen) um.
Beide Anteile werden gemeinsam in einem releasebezogenen und anwendungsübergreifenden Systemdesign-Dokument betrachtet, welches die Grundlage für die weitere Umsetzung auf Detailebene ist. Das Systemdesign fixiert dabei den Umfang des Releases auf fachlicher Ebene und auf Systemebene.
Die vorliegende Version des Systemdesigns für R4.0 stellt eine initiale Fassung dar. Sie dient neben einer inhaltlichen Abstimmung auch zur Abstimmung des neuen Vorgehens der gematik. Parallel zu dieser ersten Abstimmung wird die gematik das Dokument methodisch weiterentwickeln und ggf. inhaltlich nachjustieren, wenn sich neue Erkenntnisse im Entwicklung- und Abstimmungsprozess ergeben. Anschließend erfolgt eine erneute Verteilung des Dokuments.

1.1 Zielsetzung des Dokuments

Das vorliegende Konzept zum Systemdesign der Telematikinfrastruktur (TI) definiert den Funktionsumfang der TI für das Release 4.0. Hierzu erfolgt eine Festlegung dieses Funktionsumfangs im Vergleich zum letzten TI-Release mit dem Stand 3.1. Betrachtet wird sowohl der funktionale Umfang aus Nutzersicht als auch die sich ableitende Systemebene mit den Komponenten und Diensten der TI (Produkttypen), angrenzenden IT-Systemen sowie den operativen Betriebsleistungen für Dienste der TI (Anbietertypen).

Kapitel 2 legt zunächst den funktionalen Umfang für das Release 4.0 fest. Der Fokus liegt auf den Nutzern der TI und den hierbei zu betrachtenden Versorgungsprozessen im Gesundheitswesen. Diese Versorgungsprozesse werden durch die verschiedenen Fachanwendungen der TI bzw. deren Zusammenspiel unterstützt. Hierbei werden neue Fachanwendungen in das Release aufgenommen oder bestehende Fachanwendungen weiterentwickelt.

Darüber hinaus können sich weitere funktionale Änderungen außerhalb dieser Anwendungsebene ergeben, beispielsweise aufgrund von technologischen Weiterentwicklungen, aufgrund von Änderungen regulativer Rahmenbedingungen oder aufgrund von Erkenntnissen aus dem operativen Betrieb der TI. Mit dem Release 4.0 werden die Fachanwendung E-Rezept eingeführt sowie die Fachwendungen ePA und KOM-LE weiterentwickelt. Der Umfang dieser Anpassungen wird als Delta zum Release 3.1 dargestellt.

In Kapitel 1.1.1 wird ein informativer Gesamtüberblick der TI gegeben, wobei neue und geänderte Anteile ausgewiesen werden.

In Kapitel 4 erfolgt, ausgehend vom funktionalen Umfang des Releases aus Kapitel 2, die Umsetzung auf Systemebene der TI und angrenzender IT-Systeme. Betrachtungsgegenstand sind hierbei die Produkttypen und Anbietertypen der TI sowie angrenzende IT-Systeme und ihr Zusammenspiel untereinander. Die Systemebene ~~betrachtete~~betrachtet neben fachlichen und technischen Aspekten auch Aspekte aus IT-Sicherheit, Datenschutz und Betrieb. Ebenfalls erfolgt eine Betrachtung des Betreibermodells für die Produkttypen der TI und der Zulassungsverfahren gematik. In der Betrachtung der Systemebene wird ~~als~~das Delta zum Release 3.1 dargestellt.

Das vorliegende Konzept dient als Ausgangspunkt für spätere Detailregelungen bezüglich der Entwicklung von TI-Komponenten und -Diensten (Produkttypen) sowie deren Betrieb (Anbietertypen) durch Industriepartner der gematik. Hierzu zählen insbesondere die Spezifikationen, Produkttyp- und Anbietertypsteckbriefe sowie Test-, Zulassungs- und Bestätigungsverfahren.

1.2 Zielgruppe des Dokuments

Das vorliegende Dokument stellt die normative Grundlage zur Weiterentwicklung der TI für das Release 4.0 dar und richtet sich vorrangig an folgende Zielgruppen:

- Gesellschafter der gematik
- Hersteller von Komponenten und Diensten der TI sowie angrenzenden IT-Systemen
- Anbieter operativer Betriebsleistungen für die TI
- Mitarbeiter der gematik.

Hersteller und Anbieter können sich via Systemdesign einen Überblick der Änderungen und Erweiterungen der TI für das Release 4.0 verschaffen. Ferner soll es das Dokument ermöglichen, die Industrie bei Überlegungen zur Weiterentwicklung der TI einzubinden.

Abschließend fungiert das Systemdesign als Basis für die Entwicklung aller normativen Detailregelungen innerhalb des Releases 4.0.

1.1 Geltungsbereich

Dieses Dokument enthält normative Festlegungen für die TI und definiert den Umfang für das TI-Release 4.0 auf fachlicher und systemischer Ebene.

Insofern sich im laufenden Entwicklungsprozess notwendige Anpassungsbedarfe mit Auswirkungen auf das Systemdesign ergeben, wird die gematik diese in einer aktualisierten Fassung des Dokuments publizieren.

Dieses Dokument berücksichtigt Inhalte des ~~Referentenentwurfs~~Kabinettsentwurfs zum Patientendaten-~~Schutzgesetz~~Schutz-Gesetz (PDSG) vom ~~30.01~~31.03.2020. Sofern sich im weiteren Gesetzgebungsverfahren Änderungen am PDSG ergeben, werden diese Änderungen in einer Folgeversion dieses Dokuments berücksichtigt.

1.2 Abgrenzung des Dokuments

Nicht Bestandteil des Dokumentes sind Korrekturen und Optimierung für das Release, sofern diese für eine Betrachtung auf funktionaler Ebene bzw. Systemebene nicht relevant sind. Derartige Änderungen im Release werden unmittelbar in den Detaildokumenten (bspw. Spezifikationen) der gematik adressiert.

2 Fachlicher Umfang für das Release

Dieses Kapitel stellt dar, welche neuen oder veränderten Funktionsumfänge das Release aus fachlicher Sicht bietet und welche Faktoren zu einem Änderungs- oder Weiterentwicklungsbedarf geführt haben.

2.1 Anwendungsübergreifender Umfang

2.1.1 Einführung eines Identity Provider

2.1.1.1 Authentifizierung als anwendungsübergreifender Dienst

Die sichere Authentifizierung der Nutzer der TI ist eine für alle Anwendungen benötigte Funktion. Daher liegt es nahe, diese Funktion als anwendungsübergreifenden Dienst (Identity Provider, kurz IdP) in der TI zu etablieren, um Wiederverwendung, Einheitlichkeit und Modularisierung zu unterstützen.

Fachliche Darstellung

- Anwendungen können die Authentifizierung als Dienst einbinden, sodass sich der umzusetzende Funktionsumfang der Anwendung reduziert. Das E-Rezept soll in diesem Zusammenhang die erste Anwendung sein, weitere sollen folgen.
- Mit der Auslagerung der Authentifizierung vereinfachen sich Test und Zulassung einer Anwendung. Authentisierungslösungen können zentral geprüft und ihr Vertrauensniveau transparent ermittelt und festgehalten werden.
- Die Entkopplung der Authentifizierung von der Fachlogik ermöglicht es, Anwendungen unabhängig vom verwendeten Authentifizierungsverfahren zu entwickeln.
- Die Entkopplung ermöglicht es außerdem, in Folge-Releases neue Authentisierungslösungen einfacher zu integrieren und allen Anwendungen zur Verfügung zu stellen.

2.1.1.2 Nutzer-Komfort

Der IdP soll den Komfort für den Nutzer erhöhen, indem die Anmeldung, bei gegebener Sicherheit, aus Nutzersicht einfach durchzuführen ist und nur so oft wie nötig erfolgen muss. Weiterhin kann der Nutzerkomfort durch eine anwendungsübergreifend genutzte Anmeldung verbessert werden.

Fachliche Darstellung

- Der IdP schafft die Voraussetzung für Single Sign-On, wodurch der Nutzer sich nur so oft authentisieren muss wie unbedingt nötig.
- Der IdP ermöglicht es, neben einer Smart Card in Folge-Releases alternative Authentisierungsverfahren anzubieten, die für den Nutzer einen höheren Komfort bieten.

2.1.1.3 Kompatibilität

Der IdP muss den Betrieb bestehender Dienste und Anwendungen weiter ermöglichen und mit aktuell in der TI genutzten Standards kompatibel sein.

Fachliche Darstellung

- Der IdP muss mit den bereits vorhanden PKI-Diensten der TI integrierbar sein.
- Der IdP muss auf Standards und Produkten basieren, die im e-Health-Bereich verbreitet oder zumindest leicht integrierbar sind.
- Der IdP muss in Folge-Releases die Integration vorhandener IdP-Lösungen ermöglichen.
- Der IdP muss in Folge-Releases eine Interoperabilität mit weiteren Anwendungen ermöglichen.
- Der IdP muss in Folge-Releases eine Interoperabilität mit der elektronischen Patientenakte ermöglichen.

2.1.1.4 Zukunftssicherheit

Der IdP sollte auf Standards und Produkten aufbauen, die nicht nur aktuell etabliert sind, sondern auf absehbare Zeit ihre Relevanz behalten, um unnötige kostenintensive Umstellungen auf andere Technologien zu vermeiden.

Fachliche Darstellung

- Der IdP muss auf Standards aufbauen, die im e-Health-Bereich etabliert sind und auf absehbare Zeit ihre Bedeutung behalten werden.
- Der IdP muss unterschiedliche Deployment-Modelle der nutzenden Anwendungen ermöglichen, insbesondere native Clients im dezentralen Bereich sowie Applikationsserver im zentralen Bereich.
- Der IdP muss gleichermaßen mobile wie nicht-mobile Anwendungen ermöglichen.
- Der IdP muss in Folge-Releases eine geeignete Basis für die Entwicklung einer zukünftigen neuen TI-Zugangslösung bieten.
- Der IdP muss in Folge-Releases eine geeignete Basis für den Aufbau eines zukünftigen, nationalen oder EU-weiten föderierten Identity Managements bieten.

2.1.1.5 Sicherheit und Datenschutz

Der Zugriff auf sensible und schützenswerte Daten oder Funktionen erfolgt erst nach einer sicheren Authentifizierung des Nutzers. Der IdP muss daher entsprechende Anforderungen bezüglich Datenschutz und Informationssicherheit erfüllen.

Fachliche Darstellung

- Im Sinne der Privacy by Design stellt der IdP einer Anwendung nur diejenigen Identitätsattribute bereit, die diese auch tatsächlich benötigt.
- Im Sinne der Privacy by Design kann eine Anwendung für einzelne Anwendungsfälle vorgeben, welche Identitätsattribute der IdP bereitstellt.
- Der IdP bietet dem Nutzer die Möglichkeit, seine Sitzungen jederzeit zu beenden.

- Der IdP bietet dem Betreiber die Möglichkeit, Sitzungen eines Nutzers zu beenden oder die Authentifizierung zu verweigern, falls dies aus Sicherheitsgründen (z.B. kompromittierte Identität des Nutzers) erforderlich ist.

- Der IdP ermöglicht es einer Anwendung, das Sicherheitsniveau der Authentifizierung vorzugeben und abzufragen.

2.1.1.6 Betrieb

Der IdP wird für neue oder weiterentwickelte Anwendungen als Authentisierungsdienst Voraussetzung für deren Nutzung und muss daher sicher, zuverlässig, hoch verfügbar und performant in der TI betrieben werden.

Der Anbieter bzw. Betreiber des IdP ist in das übergreifende TI-ITSM einzubinden und muss die für ihn in der weiteren Spezifikation definierten betrieblichen Anforderungen erfüllen. Insbesondere muss er einen 24/7 TI-ITSM-Teilnehmer-Support bereitstellen. Zur Wahrnehmung der betrieblichen Aufgaben der gematik ist eine angemessene Überwachung des Dienstes und seiner Anwendungsfälle durch die gematik zu ermöglichen

2.1.2 Anbindung neuer Berufsgruppen an die TI

Mitarbeiterinnen und Mitarbeiter in Institutionen neuer Nutzergruppen möchten die Anwendungen der Telematikinfrastruktur nutzen, um eine bessere Patientenversorgung zu ermöglichen und durch digitale Anwendungen den Arbeitsalltag zu erleichtern.

So müssen durch Festlegungen des § 352 PDSG einige neue Berufsgruppen technisch in der Lage sein, auf Dokumente und Datensätze der ePA zuzugreifen und diese zu verarbeiten, insofern sie dafür vom Versicherten berechtigt worden sind.

Fachliche Darstellung

Für die folgenden Berufsgruppen bzw. Nutzerkreise sind die technischen Voraussetzungen für den Zugang zur Telematikinfrastruktur zu schaffen, um diesen die Nutzung der Fachanwendungen zu ermöglichen.

Neue Berufsgruppen bzw. Nutzerkreise gemäß § 352 PDSG:

- Gesundheits- und Krankenpflegerinnen und Gesundheits- und Krankenpfleger

- Gesundheits- und Kinderkrankenpflegerinnen und Gesundheits- und Kinderkrankenpfleger

- Altenpflegerinnen und Altenpfleger

- Pflegefachfrauen und Pflegefachmänner sowie Pflegehilfskräfte

- Hebammen und Entbindungspfleger

- Physiotherapeutinnen und Physiotherapeuten

- berufsmäßige Gehilfen von Ärzten, Zahnärzten und Psychotherapeuten oder zur Vorbereitung auf den Beruf bei genannten Heilberuflern Tätige in Vorsorge- oder Rehabilitationseinrichtungen nach § 107 Absatz 2 SGB V oder bei einem Leistungserbringer der medizinischen Rehabilitation des SGB VI oder der Heilbehandlung einschließlich medizinischer Rehabilitation des SGB VII

- Ärzte und Ärztinnen und berechtigte Personen in Behörden des Öffentlichen Gesundheitsdienstes

- Fachärztinnen und Fachärzte für Arbeitsmedizin und Betriebsärztinnen und Betriebsärzte

Neue Berufsgruppen bzw. Nutzerkreise gemäß § 340 Absatz 2 PDSG:

- Augenoptiker, Hörakustiker, Orthopädieschuhmacher, Orthopädietechniker und Zahntechniker

Berufsgruppen bzw. Nutzerkreise, für deren Anbindung an die TI nach § 340 Absatz 4 PDSG die gematik die elektronischer Heilberufs- und Berufsausweise sowie die Komponenten zur Authentifizierung von Leistungserbringerinstitutionen (SMC-B) ausgeben muss:

- Apotheker und berechtigtes pharmazeutisches Personal in EU-Versandapotheken
- berechtigte Berufsgruppen in Eigeneinrichtungen der Krankenkassen nach § 140 SGB V (z.B. Centrum für Gesundheit der AOK Nordost)
- Ärzte, Zahnärzte und Psychotherapeuten und deren berufsmäßige Gehilfen im Sanitätsdienst der Bundeswehr
- (zukünftig werden weitere Nutzerkreise zu berücksichtigen sein)

Berufsgruppen bzw. Nutzerkreise gemäß dem Gesetz zur Reform der Notfallversorgung § 133b Absatz 4:

- berechtigte Mitarbeiter von Rettungsleitstellen

Die anwendungsspezifischen Berechtigungskonzepte sind dann zu berücksichtigen, wenn darauf aufbauend spezifische Vorgaben für identitätsbezogene Datenstrukturen für die genannten Berufsgruppen zu entwickeln sind.

Im Hinblick auf die Erweiterung der Nutzergruppen soll die Möglichkeit einer zukünftigen kontaktlosen, ggf. auch mobilen Nutzung der SMC-B, berücksichtigt werden.

Randbedingungen

Die notwendigen Voraussetzungen für die Nutzung der Anwendungen der Telematikinfrastruktur durch die oben genannten Berufsgruppen umfassen:

- technische Voraussetzungen gemäß § 311 PDSG für die Anbindung der jeweiligen Institutionen an die Telematikinfrastruktur und den Zugriff der dort Tätigen auf medizinische Daten
- organisatorische Voraussetzungen für die Ausgabe elektronischer Heilberufs- und Berufsausweise und Komponenten zur Authentifizierung von Leistungserbringerinstitutionen (SMC-B) durch die gematik gemäß § **XXX** PDSG.

Weitere Quellen

Gesetzentwurf PDSG § 312 Aufträge an die Gesellschaft für Telematik

Gesetzentwurf PDSG § 311 Aufgaben der Gesellschaft für Telematik

Gesetzentwurf PDSG § 340 Ausgabe von elektronischen Heilberufs- und Berufsausweisen sowie von Komponenten zur Authentifizierung von Leistungserbringerinstitutionen

Gesetzentwurf PDSG § 342 Angebot und Nutzung der elektronischen Patientenakte

Gesetzentwurf PDSG § 352 Verarbeitung von Daten in der elektronischen Patientenakte durch Leistungserbringer und andere zugriffsberechtigte Personen

Gesetz zur Reform der Notfallversorgung § 133b Gemeinsames Notfallleitsystem

2.1.3 Betriebliche Regelungen

2.1.3.1 Erfassung und Lieferung technischer Performance-Rohdaten

Die Lieferung betrieblicher Performance-Kennzahlen (Produkt-Performance, Produkt-Verfügbarkeit) erfolgt vom Anbieter eines zugelassenen Produktes bisher in Form monatlicher Zustellungen aggregierter Performance- und Service-Level-Berichte. Parallel dazu sind bisher von den betroffenen Produkttypen aggregierte Performancedaten in einer 5-Minuten-Frequenz an die Störungsampel der TI zu senden.

Aufgrund der zahlreichen Erschwernisse, Ungenauigkeiten und technischen Probleme sowie der mangelnden automatisierten Verwertbarkeit der Daten, die diese Lieferungen in der betrieblichen Praxis gezeigt haben, wurde beginnend mit dem Release 3.0 für neue Produkt- und Anbietertypen die Erhebung und Lieferung von Performance-Rohdaten verpflichtend. Ziel dieser Rohdaten-Lieferungen ist es, mit einer automatisierten Erhebung und Lieferung der Daten ohne weitere Aggregation eine störungsresistente und verlässliche Datenquelle zu schaffen, auf derer Basis eine automatisierte Verifizierung, Auswertung und Darstellung betrieblicher Steuerungsgrößen flexibel und tagesaktuell sowie zielgruppengenau möglich ist.

Fachliche Darstellung

Bereits seit Release 3.1 werden bestimmte bestehende Produkttypen verpflichtet, Rohdaten zu liefern. Mit Release 4.0 wird die Erhebung und Lieferung von Rohdaten für weitere Produkt- und Anbietertypen verpflichtend (siehe Kapitel 4.1.6.2). Im Gegenzug entfallen die Lieferung von Daten an die Störungsampel und die Lieferung der monatlichen Performance- und Service Level-Berichte. Die erhobenen Performance-Rohdaten sind vom Anbieter in einer frei konfigurierbaren Frequenz an die definierte Betriebsdatenschnittstelle zu liefern.

~~2.1~~2.2 Elektronische Patientenakte ePA (Stufe 2.0)

Mit der elektronischen Patientenakte ePA 1.1. wurde eine Anwendung ins Feld geführt, die eine sektoren- und einrichtungsübergreifende Kommunikation zwischen Versicherten und ihren Leistungserbringern ermöglicht. Mit ePA 2.0 soll das Beziehungsgeflecht aus Patienten und Apotheken, Krankenhäusern und niedergelassenen Arzt-, Psychotherapeuten- und Zahnarztpraxen auf nicht-approbierte Berufsgruppen wie bspw. Hebammen und Entbindungspfleger, Pflegepersonal und Physiotherapeuten ausgeweitet werden, die auf Wunsch des Versicherten bzw. ggf. seines Vertreters ebenfalls Zugriff auf die elektronische Patientenakte erhalten.

Im Kontext der Erweiterung der möglichen zugriffsberechtigten Leistungserbringerinstitutionen ist es notwendig, dass das Berechtigungskonzept verfeinert wird und ein Versicherter sowie dessen Vertreter die Vergabe von Zugriffsrechten auf einzelne Dokumente und Gruppen von Dokumenten verwalten können. Da fast alle Use Cases, die vom Versicherten durchgeführt werden können, auch von dessen Vertreter durchgeführt werden dürfen, wird nachfolgend nur noch vom Versicherten gesprochen. Ausnahmefälle, in den der Vertreter Use Cases nicht durchführen können darf, werden explizit benannt.

~~Die Kassenärztliche Bundesvereinigung (KBV) verfolgt gemäß § 355 PDSG die Aufgabe, die Formate der Dokumente in der ePA zu standardisieren. Für strukturierte Dokumententypen~~

~~muss sichergestellt werden, dass das bestehende Datenmodell Metadaten und Wertebereich der neu hinzukommenden Dokumentenkategorien unterstützt.~~

Gemeinsam mit neuen Funktionalitäten werden mit der ePA Stufe 2 einige Leistungsmerkmale erstmals bereitgestellt, welche zwar in den Spezifikationen zur ePA 1.1. definiert, aber zunächst zurückgestellt wurden, um eine schnelle Verfügbarkeit zu ermöglichen. Dabei handelt es sich um:

- Anbieterwechsel (bspw. Versicherter wechselt seine Krankenkasse)
- Einstellen von Kassendaten in die ePA durch die Krankenkasse des Versicherten
- Anforderungen an das betriebliche Service Monitoring
- Möglichkeit des Einrichtens von Vertretern durch den Versicherten.

Die Kassenärztliche Bundesvereinigung (KBV) standardisiert gemäß § 355 PDSG die Formate der Dokumente in der ePA. Für strukturierte Dokumententypen muss sichergestellt werden, dass das bestehende Datenmodell Metadaten und Wertebereich der neu hinzukommenden Dokumentenkategorien unterstützt.

Ferner finden mit dem ePA-Frontend des Versicherten für Anwendungen des Versicherten (ePA-FdV AdV) auf dem Terminal für Anwendungen des Versicherten (KTR-AdV-Terminal) ~~bzw. dem TI-Terminal~~ und der Umschlüsselung zwei weitere Funktionalitäten Eingang in die ePA, welche sowohl die Autonomie in der Nutzung der Anwendung als auch die Sicherheit der Anwendung weiter stärken.

~~2.1.1~~2.2.1 Rollenprofile für Berufsgruppen

In § 352 PDSG findet sich eine abschließende Liste von Rollen/Berufsgruppen, die vom Versicherten ein Zugriffsrecht auf ~~die~~seine elektronische Patientenakte ~~zugreifen dürfen~~erhalten können. Für jede Berufsgruppe sieht das PDSG zudem eine Regelung vor, über welche konkreten Rechte ein Leistungserbringer dieser Rolle in den jeweiligen Dokumenten-Kategorien maximal verfügen darf. Diese maximalen Zugriffsrechte dürfen selbst mit Einwilligung des Versicherten nicht erweitert werden.

Fachliche Darstellung

Technisch soll sichergestellt werden, dass die gesetzlichen Regelungen für Berufsgruppen nach § 352 PDSG als Rollen und Berechtigungen bezogen auf Dokumentenkategorien nach § 341(2) PDSG durchgesetzt werden. Bei den zu identifizierenden Berufsgruppen handelt es sich nach § 352 PDSG um:

- Ärztinnen und Ärzte (und deren berufsmäßige Gehilfen)
- Zahnärztinnen und Zahnärzte (und deren berufsmäßige Gehilfen)
- Apothekerinnen und Apotheker (und ~~deren berufsmäßige Gehilfen~~pharmazeutisches Personal)
- Psychotherapeutinnen und Psychotherapeuten (und deren berufsmäßige Gehilfen)
- Gesundheits- und Krankenpfleger sowie Gesundheits- und Kinderkrankenpfleger (und deren berufsmäßige Gehilfen)
- Altenpflegerinnen und Altenpfleger (und deren berufsmäßige Gehilfen)

- Pflegefachfrauen und Pflegefachmänner (und deren berufsmäßige Gehilfen)
- Hebammen und Entbindungspfleger
- Physiotherapeutinnen und Physiotherapeuten (und deren berufsmäßige Gehilfen)
- ~~Ärzte in Gesundheitsbehörden~~
- Ärztinnen und Ärzte in einer für den öffentlichen Gesundheitsdienst zuständigen Behörde
- Fachärztinnen und Fachärzte der Arbeitsmedizin und Betriebsmedizin.

Für einige dieser Berufsgruppen sind Zugriffsrechte auch für in Ausbildung befindliche Personen vorgesehen. Die vollständige Liste ist der konkreten Regelung des § 352 PDSG zu entnehmen. Eine Übersicht – abgeleitet aus dem PDSG – kann dem Anhang A1 entnommen werden.

Für den Versicherten ~~und dessen Vertreter~~ sollte bei der Erteilung einer Zugriffsberechtigung am Frontend des Versicherten (ePA-FdV~~)~~ oder ePA-FdV AdV) ersichtlich sein, welcher Berufsgruppe die ausgewählte Leistungserbringerinstitution zuzuordnen ist. Ebenfalls sollen sich FdV oder AdV so verhalten, dass sie dem Versicherten einen transparenten Überblick darüber ermöglichen, welche gesetzlichen Restriktionen für die Rechtevergabe in Abhängigkeit von der Berufsgruppe der ausgewählten Leistungserbringerinstitution gelten.

Für den FdV- oder AdV-Hersteller kommen folgende Anwendungsfälle zum Tragen:

- Anzeige der Berufsgruppe nach § 352 PDSG, zu der die zu berechtigende Leistungserbringerinstitution gehört
- ~~Reduktion~~Anzeige der ~~angezeigten~~ Anzahl der Dokumente, auf die ~~eine Berechtigung vergeben werden kann~~ – in Abhängigkeit von der ausgewählten Berufsgruppe der zu berechtigenden Leistungserbringerinstitution – eine Berechtigung vergeben werden kann.

Für die Aktensystemhersteller kommt folgender Anwendungsfall zum Tragen:

- Prüfung der Berufsgruppe und Durchsetzung der maximalen Lese- und Schreibrechte, bevor einem Nutzer einer jeweiligen Berufsgruppe eine ~~Menge~~Anzahl an verfügbaren Dokumenten angezeigt wird.

Für den Primärsystemhersteller (PS-Hersteller) kommt folgender Anwendungsfall zum Tragen:

- Reduktion der ~~angezeigten~~verfügbaren Anzahl der Dokumente, auf die eine Berechtigung vergeben werden kann, in Abhängigkeit von der Berufsgruppe respektive Leistungserbringerinstitution, die um Zugriffsberechtigung bittet.

Randbedingungen

--

Weitere Quellen

~~**Randbedingungen**~~

~~Die Umsetzung dieser Anforderung gilt für folgende Nutzerumgebungen:~~

- ~~Primärsysteme der Leistungserbringer~~
- ~~FdV~~

- ~~AdV.~~

~~Weitere Quellen~~

~~Patienten-Datenschutz~~Gesetzentwurf Patientendaten-Schutz-Gesetz (PDSG), Zweiter Teil

~~2.1.2~~2.2.2 Verfeinertes Berechtigungskonzept

Damit ein Versicherter ~~und dessen Vertreter~~ einer Leistungserbringerinstitution ~~sowohl den~~ Zugriff sowohl auf spezifische Dokumente und Datensätze als auch auf Gruppen von Dokumenten und Datensätzen der elektronischen Patientenakte" (§ 342 Abs. 2 Nr. 2 lit. b ~~PDSG~~) erteilen bzw. beschränken kann, wird ein verfeinertes Berechtigungskonzept für die ePA 2.0 benötigt. ~~Dieses~~Das Konzept ~~ersetzt~~ändert das bisherige Berechtigungskonzept der ePA 1.1.

Fachliche Darstellung

~~**Fachliche Darstellung**~~

~~*Die Abstimmungen zum verfeinerten Rechtekonzept der ePA sind auf gesetzlicher Ebene noch nicht soweit abgeschlossen, als dass eine belastbare Grundlage für eine tiefergehende fachliche und technische Analyse gegeben ist. Es bestehen zu hohe Umsetzungsrisiken.*~~

~~Spätestens~~In der ePA 1.1 wurde ein grobgranulares Berechtigungskonzept genutzt, welches dem Versicherten erlaubte, neben der gewünschten Berechtigungsdauer auch auszuwählen, ob eine Zugriffsberechtigung für alle Dokumente in seiner ePA erteilt werden soll oder nur für ausgewählte Datenquellen:

(1) Von Leistungserbringern eingestellte Dokumente

(2) Vom Versicherten (oder seinem Vertreter) selbst eingestellte Dokumente

(3) Von seiner Krankenkasse in der ePA bereitgestellte Dokumente.

Mit der ePA 2.0 wird dieses Berechtigungskonzept abgelöst durch ein Berechtigungskonzept, welches dem Versicherten Berechtigungsmöglichkeiten verschiedener Granularität eröffnet bis hin zur Vergabe von Zugriffsrechten für einzelne Dokumente oder Gruppen von Dokumenten.

Der Gesetzgeber hat mit den Festlegungen der §§ 341 und 352 des Patientendaten-Schutz-Gesetzes (PDSG) darüber hinaus bereits einschränkende Festlegungen getroffen, welche Arten von Dokumenten der ePA für welche Gruppen von Leistungserbringern durch den Versicherten bereitgestellt werden dürfen. Diese gesetzlichen Festlegungen sollen vom Versicherten nicht außer Kraft gesetzt werden können und sind als Rahmenwerk von der ePA technisch durchzusetzen.

Die verschiedenen Granularitätsstufen, mit denen der Versicherte Berechtigungen vornehmen kann, sind im Folgenden kurz erläutert:

(1) Grobgranulare Berechtigung auf Basis ~~des Kabinettsentwurfs~~der Vertraulichkeit von Dokumenten

Die grobgranulare Berechtigung stellt die einfachste Form der Rechtevergabe durch den Versicherten dar und erfolgt mittels Auswahl von Vertraulichkeitsstufen, die Dokumente zugeordnet sind. Jedes Dokument in der ePA ist dabei einer der folgenden drei Vertraulichkeitsstufen zugeordnet. Über die jeweilige Klassifizierung entscheidet der Versicherte.

- „Normal": Dokumente dieser Kategorie sind für Leistungserbringer sichtbar, welche ein sog. „einfaches Zugriffsrecht" durch den Versicherten erhalten haben. Erhält eine Leistungserbringerinstitution ein „einfaches Zugriffsrecht", darf sie Dokumente in die ePA des ~~**PDSG werden die**~~ Versicherten einstellen sowie Dokumente der Vertraulichkeitsstufe „normal" einsehen, welche sich zum Zeitpunkt der Zugriffserteilung in der Akte befinden oder während des Bestehens der Berechtigung eingestellt werden (ggf. mit Einschränkung auf bestimmte Dokumentenarten gemäß §§ 341 und 352 PDSG).

- „Vertraulich": Als „vertraulich" werden nach Ermessen des Versicherten typischerweise Dokumente gekennzeichnet, welche der Versicherte nur ausgewählten, an seiner Behandlung beteiligten Leistungserbringerinstitutionen bereitstellen möchte. Dabei könnte es sich bspw. um Dabei könnte es sich bspw. um Dokumente zu als gegebenenfalls stigmatisierend empfundenen Befunden der Psychotherapie oder Infektiologie handeln. Möchte der Versicherte einer Leistungserbringerinstitution Zugriff auf „vertrauliche" Dokumente gewähren, vergibt er ein sog. „erweitertes Zugriffsrecht". Leistungserbringer mit „erweitertem Zugriffsrecht" dürfen Dokumente in die ePA des Versicherten einstellen (ggf. mit Einschränkung auf bestimmte Dokumentenarten gemäß §§ 341 und 352 PDSG) sowie Dokumente der Vertraulichkeitsstufe „normal" und „vertraulich" einsehen, welche zum Zeitpunkt der Zugriffserteilung in der Akte befinden oder während des Bestehens der Berechtigung eingestellt werden.

- „Streng vertraulich": Als „streng vertraulich" werden nach Ermessen des Versicherten Dokumente gekennzeichnet, die der Versicherte als privat, brisant und gegebenenfalls stigmatisierend empfindet und die er zwar in seiner elektronischen Patientenakte verwalten, aber Leistungserbringern nur im Ausnahmefall zugänglich machen möchte. Ein als „streng vertraulich" eingestelltes Dokument ist zunächst ausschließlich für den Versicherten (und seine Vertreter) sichtbar. Möchte der Versicherte dieses Dokument einem Leistungserbringer zur Verfügung stellen, muss dies durch einen expliziten Berechtigungsvorgang geschehen. Die Freigabe kann direkt im Kontext der Erteilung oder Administration einer Zugriffsberechtigung oder aus dem Kontext der Dokumentenverwaltung (vom Dokument eine Freigabe für eine LEI erteilen) erfolgen. Anders als bei den Vertraulichkeitsstufen „normal" und „vertraulich" ist es bei „streng vertraulichen" Dokumenten nicht möglich, eine generelle und auch für zukünftig eingestellte Dokumente geltende Berechtigung zu erteilen.

Die Möglichkeit der Vergabe grobgranularer Berechtigungen soll für den Versicherten an den ihm zur Verfügung stehenden Frontends und im Ad-hoc-Szenario beim Leistungserbringer möglich sein.

Die Kennzeichnung der Vertraulichkeit muss zu einem späteren Zeitpunkt durch den Versicherten sowie auf Wunsch des Versicherten durch den Leistungserbringer änderbar sein.

(2) Mittelgranulare Berechtigung

Die mittelgranulare Berechtigung stellt dem Versicherten eine Möglichkeit bereit, Dokumente nach festgelegten Fachgebieten und Dokumentenkategorien freizugeben. Die Dokumentenkategorien sind im § 341 PDSG festgelegt:

1) medizinische Informationen über Versicherte für eine einrichtungsübergreifende, fachübergreifende und sektorenübergreifende Nutzung, insbesondere

   a) Daten zu Befunden, Diagnosen, durchgeführten und geplanten Therapiemaßnahmen sowie zu Behandlungsberichten und sonstige untersuchungs- und behandlungsbezogene medizinische Informationen,

   b) Daten des elektronischen Medikationsplans nach § 334 Absatz 1 Nummer 4,

   c) Daten der elektronischen Notfalldaten nach § 334 Absatz 1 Nummer 5,

   d) Daten in elektronischen Briefen zwischen den an der Versorgung der Versicherten teilnehmenden Ärzten und Einrichtungen (elektronische Arztbriefe),

2) Daten zum Nachweis der regelmäßigen Inanspruchnahme zahnärztlicher Vorsorgeuntersuchungen gemäß § 55 Absatz 1 in Verbindung mit § 92 Absatz 1 Satz 2 Nummer 2 (elektronisches Zahn-Bonusheft),

3) Daten gemäß der nach § 92 Absatz 1 Satz 2 Nummer 3 und Absatz 4 in Verbindung mit § 26 beschlossenen Richtlinie des Gemeinsamen Bundesausschusses zur Früherkennung von Krankheiten bei Kindern (elektronisches Untersuchungsheft für Kinder),

4) Daten gemäß der nach § 92 Absatz 1 Satz 2 Nummer 4 in Verbindung mit den §§ 24c bis 24f beschlossenen Richtlinie des Gemeinsamen Bundesausschusses über die ärztliche Betreuung während der Schwangerschaft und nach der Entbindung (elektronischer Mutterpass),

5) Daten der Impfdokumentation nach § 22 des Infektionsschutzgesetzes (elektronische Impfdokumentation),

6) durch die Versicherten zur Verfügung gestellte Daten,

7) Daten der Versicherten aus einer von den Krankenkassen nach § 68 finanzierten elektronischen Akte der Versicherten,

8) bei den Krankenkassen gespeicherte Daten über die in Anspruch genommenen Leistungen der Versicherten,

9) Daten, die die Versicherten ihren Krankenkassen für die Nutzung in zusätzlichen von den Krankenkassen angebotenen Anwendungen nach § 345 zur Verfügung stellen können,

10) Daten zur pflegerischen Versorgung der Versicherten nach §§ 24g, 37, 37b, 37c, 39a und 39c oder nach dem Elften Buch,

11) Daten elektronischer Verordnungen nach § 360,

12) die nach § 73 Absatz 2 Satz 1 Nummer 9 ausgestellte Bescheinigung über eine Arbeitsunfähigkeit und

13) sonstige von den Leistungserbringern für die Versicherten bereitgestellte Daten.

Hinweis zur Kategorie 9:
Der Versicherte soll den Krankenkassen Dokumente seiner ePA über einen Kommunikationsmechanismus bereitstellen können. Dokumente, die über diesen Mechanismus an die Krankenkassen übermittelt wurden, sollen automatisch gekennzeichnet werden, damit eine Filterung und Anzeige dieser Dokumente möglich ist. Es entstehen daher also keine Dokumentenkopien von Dokumenten anderer Kategorien nach §341 PDSG. Ein Zugriffsrecht für Krankenkassen ist nach wie vor gesetzlich explizit nicht vorgesehen.

Gemäß § 354(2)2 PDSG ist die gematik aufgefordert, in Abstimmung mit der Kassenärztlichen Bundesvereinigung sowie der Kassenzahnärztlichen Bundesvereinigung weitere Kategorien in der elektronischen Patientenakte festzulegen, die eine Zuordnung von Dokumenten und Datensätzen der Dokumentenkategorie 1a („Daten zu Befunden, Diagnosen […]“) zu medizinischen Fachrichtungen, die als besonders versorgungsrelevant erachtet werden, zulässt. Aufgrund der Festlegungen in §352 PDSG, Ziffer 14 ist bereits vorgegeben, dass eine Identifikation der sich aus der physiotherapeutischen Behandlung ergebenden Dokumente möglich sein muss. Es ist möglich, dass ein Dokument mehreren Fachgebieten zugeordnet wird. Idealerweise belegt das Primärsystem den Wert mit einem Vorschlagswert für die jeweilige Praxis vor, damit manuelle Pflegeaufwände von Metadaten vermieden werden.

Als Fachgruppen werden vorgeschlagen:

Fachgruppe	**Einschätzung gematik**
Innere Medizin	Empfohlen
Allgemeinmedizin	Empfohlen
Chirurgie	Empfohlen
Anästhesiologie	Nicht empfohlen
Gynäkologie/Frauenheilkunde und Geburtshilfe	Empfohlen
Kinder- und Jugendmedizin	Zur Diskussion
Psychiatrie und Psychotherapie	Empfohlen
Radiologie	Zur Diskussion
Augenheilkunde	Zur Diskussion
Neurologie	Zur Diskussion
HNO-Heilkunde	Zur Diskussion
Urologie	Empfohlen
Haut- und Geschlechtskrankheiten	Empfohlen
Physiotherapie	Empfohlen
Zahnheilkunde	Empfohlen
Andere Fachgebiete	Empfohlen

Die endgültige Festlegung erfolgt bis zur Freigabe und Veröffentlichung der entsprechenden ~~**Punkte ergänzt**~~Spezifikationen.

Die Möglichkeit der Vergabe mittelgranularer Berechtigungen soll für den Versicherten an den ihm zur Verfügung stehenden Frontends und im Ad-hoc-Szenario beim Leistungserbringer möglich sein.

(3) Feingranulare Berechtigung

Feingranulare Berechtigungen erlauben die Berechtigungserteilung von Leistungserbringerinstitutionen durch den Versicherten auf Basis einzelner Dokumente oder mittels Suche und Filterung gewählter Gruppen von Dokumenten.

Feingranulare Berechtigungen können mit einer grob- und mittelgranularen Berechtigung (welche hier als eine Art Schnellfilter betrachtet werden können) kombiniert werden.

Leistungserbringer, welche ausschließlich für den Zugriff auf einzelne Dokumente berechtigt wurden, dürfen diese konkreten Dokumente einsehen sowie selbst Dokumente in die ePA des Versicherten einstellen (ggf. mit Einschränkung auf bestimmte Dokumentenarten gemäß §§ 341 und 352 PDSG).

Die Möglichkeit der Vergabe feingranularer Berechtigungen soll für den Versicherten an den ihm zur Verfügung stehenden Frontends möglich sein.

Im Zusammenspiel der verschiedenen Granularitätsstufen können grobgranulare Zugriffsrechte durch mittel- oder feingranulare Mechanismen eingeschränkt werden.

Für die Ausgestaltung der Zugriffserteilung ergeben sich verschiedene Anforderungen je Benutzeroberfläche.

Für den Versicherten:

- muss beim Erteilen einer Zugriffsberechtigung an den Frontends der Versicherten eine grob-, mittel- und feingranulare Rechtevergabe möglich sein
- soll es möglich sein, Leistungserbringern ein sog. „einfaches Zugriffsrecht" oder ein „erweitertes Zugriffsrecht" erteilen zu können, wobei abhängig von der Nutzerumgebung weitere Einschränkungen auf Dokumentenkategorien und Fachgebiete oder bestimmte Dokumente möglich sind.

Für die LEI:

- müssen beim Einholen einer Ad-hoc-Berechtigung die Berechtigungsdauer sowie der Zugriff auf „normal" oder auch „vertraulich" sichtbare Dokumente abfragt werden.

  muss die Möglichkeit im Primärsystem angeboten werden, über die Auswahl spezifischer Dokumentenkategorien und Fachgebiete eine sog. mittelgranulare Berechtigungsvergabe für den Versicherten durchzuführen.

Randbedingungen

Die verschiedenen Umgebungen, in denen der Versicherte Zugriffsrechte verwalten kann, bieten u. U. nur eine Teilmenge der unterschiedlichen Granularitäten in der Rechtevergabe an, d. h. im Besonderen, dass eine feingranulare Berechtigung durch den Versicherten nur dann umsetzbar ist, wenn der Versicherte die Berechtigung direkt an einem IT-Gerät mit entsprechenden Darstellungsmöglichkeiten vornimmt. Dies ist sowohl beim Frontend des Versicherten (bspw. Smartphone) als auch beim Frontend des Versicherten des KTR-AdV-Terminals der Fall.

Bei Nutzung der dezentralen Infrastruktur der Leistungserbringer (Ad-hoc-Szenario) haben Leistungserbringer die Versicherten vor einer konkreten Zugriffserteilung auf die in dieser technischen Umgebung eingeschränkten Zugriffsmanagementmöglichkeiten hinzuweisen.

Weitere Quellen

~~**Weitere Quellen**~~

Gesetzentwurf Patientendaten-Schutz-Gesetz (PDSG), Zweiter Teil

~~2.1.3~~2.2.3 Erweiterung des Datenmodells ~~und Migration~~

Gemäß § 341(2) und § 354(2)2 PDSG werden eine Reihe von bereits bekannten und noch zu definierenden ~~strukturierten~~ Dokumentenkategorien vorgegeben, die von der ePA zu unterstützen sind. Für die bereits bekannten und bereits strukturierten Dokumentenkategorien muss sichergestellt werden, dass das bestehende Datenmodell die Metadaten und ~~Wertebereich~~Wertebereiche der neu hinzukommenden Dokumentenkategorien unterstützt. Darüber hinaus sind Festlegungen zur Migration des Datenmodells der Stufe 1 zum Datenmodell der Stufe 2 zu treffen.

Fachliche Darstellung

Damit die Dokumente in der ePA einer eindeutigen und der fachlich korrekten Dokumentenkategorie zugeordnet werden können, muss die Akte die dazugehörigen Metadaten und deren Wertebereiche unterstützen. Folgende neue Dokumente sind semantisch und syntaktisch ~~bekannt~~ zum Zeitpunkt der Inbetriebnahme der ePA 2.0 bekannt:

- elektronischer Impfpass
- elektronisches Zahnbonusheft
- elektronisches Untersuchungsheft für Kinder
- elektronischer Mutterpass
- elektronische Verordnungen
- elektronische Arbeitsunfähigkeitsbescheinigung~~.~~

Dazu gehört, dass es eine Aktualisierung der bereits in der ePA vorliegenden Dokumente geben muss, die um die neu hinzukommenden Metadaten und den korrekten Wert angereichert werden. Ebenfalls muss geregelt werden, wie mit als „leistungserbringeräquivalent" und als „~~Patienteninformation~~Versicherteninformation" gekennzeichnete Dokumente umzugehen ist. Mit ePA 2.0 soll die Funktionalität der Kennzeichnung von Dokumenten als „leistungserbringeräquivalent" und als „~~Patienteninformation" entfallen~~Versicherteninformation" entfallen. Für zukünftige Erweiterungen des Datenmodells um weitere standardisierte Datenformate (bspw. MIO), welche über die oben genannten Dokumentenarten hinausgehen, muss darüber hinaus ein entsprechender Prozess definiert werden, wie dies erfolgt.

Für FdV- und AdV-Hersteller kommt folgender Anwendungsfall zum Tragen:

- Zur Inbetriebnahme der ePA 2.0 wird der Versicherte oder dessen Vertreter über die Aktualisierung des Metadatenmodells informiert. Gleichzeitig soll möglichst automatisiert die metadatenbezogene Migration erfolgen, um die bereits in der ePA vorliegenden Dokumente zu aktualisieren. Der zu vergebende Standardwert für das Metadatum „Vertraulichkeit" soll auf „normal" gesetzt werden. Für die zu

vergebenden Werte für die „Dokumentenkategorie“ und dem „Facharztbereich“ wird im Rahmen der Spezifikation ein Mapping erarbeitet.

2.2.4 Durch die KBV standardisierte Dokumentenformate der ePA

Gemäß § 355 PDSG trifft die Kassenärztliche Bundesvereinigung (KBV) die notwendigen Festlegungen für die Inhalte der elektronischen Patientenakte ab Stufe 2.0, um deren semantische und syntaktische Interoperabilität zu gewährleisten. Die dabei entstehenden strukturierten Dokumentenformate werden von der KBV auch Medizinische Informationsobjekte (Abk. MIO) genannt.

Medizinische Informationsobjekte können sowohl Dokumente als Ganzes definieren als auch einzelne Einträge, welche zu einer Dokumentenansicht aggregiert werden können. Die Wahl dieser Ausprägung, welche erst im Rahmen der MIO-Erstellung erfolgt, hat bspw. Auswirkung darauf, in welcher Granularität Einträge durch die Nutzer erstellt oder gelöscht werden dürfen. Die Fachanwendung ePA muss daher einen flexiblen Mechanismus bereitstellen, welcher die Durchsetzung dieser Löschberechtigungen bzw. Löschbeschränkungen in Abhängigkeit der MIO-Ausprägung erlaubt.

Mit der Festlegung neuer standardisierter Datenformate sind ebenfalls folgende Fragestellungen zu betrachten:

- Einbringen dieser Formate in den Versorgungsalltag, wobei aufwändige Neuzulassungen von Produkten vermieden werden sollten
- Durchsetzung der Schemakonformität und Datenqualität
- Bereitstellung von Anzeigehilfsmitteln, damit neue Datenformate an den Frontends umgehend dargestellt werden können
- Ggf. MIO-spezifische Hinweise und Festlegungen

2.2.4.1 Release unabhängiges Einbringen neuer strukturierter Dokumentenformate

Die gemäß § 355 PDSG von der Kassenärztliche Bundesvereinigung (KBV) festgelegten MIOs sollen ohne aufwändige Neuzulassungen von Produkten der ePA unterstützt werden können.

Fachliche Darstellung

Neue MIO sollen möglichst schnell Eingang in die medizinische Versorgung finden und müssen daher von den Produkttypen der ePA unterstützt werden. Das Einbringen neuer standardisierter Dokumentenformate soll unabhängig von Releasezyklen und ohne Notwendigkeit aufwändiger Neuzulassungen der Produkte möglich sein.

Für Primärsystem-, ePA-Aktensystem- und FdV-Hersteller kommen folgende Anwendungsfälle zum Tragen:

- Einstellen von MIOs in die ePA
- Suchen und Anzeigen von MIOs aus der ePA am Client

Randbedingungen

Die KBV plant MIOs quartalsweise zu veröffentlichen in einem Umfang von ca. 15 Spezifikationen pro Jahr. Um die Verfügbarkeit von MIOs im Feld zu gewährleisten, plant

die KBV in jeder MIO-Spezifikation eine Übergangsregelung zu definieren, die sich an die Primärsystemhersteller richtet.

2.2.4.2 Schemakonformität für strukturierte Dokumente

Die Nutzung von Schemata für bekannte und genormte Dokumentenformaten verbessert die Qualität, Interoperabilität und maschinelle Weiterverarbeitbarkeit der in der ePA abgelegten, strukturierten Dokumententypen. Bspw. ist die für Folgestufen vorgesehene automatische Pseudonymisierung/Anonymisierung von Daten für deren Bereitstellung durch den Versicherten zu Forschungszwecken ausschließlich auf Basis standardisierter Datensätze möglich.

Fachliche Darstellung

Um die maschinelle Weiterverarbeitbarkeit von Daten zu ermöglichen, müssen standardisierte Formatvorgaben nicht nur erstellt, sondern ihre Anwendung auch durchgesetzt werden. Hierfür sind geeignete Tools und Mechanismen festzulegen.

Randbedingungen

Auch wenn das Leistungsmerkmal zunächst auf die durch die KBV standardisierten MIOs fokussiert, sind ähnliche Betrachtungen zu gegebener Zeit auch für andere Dokumentenarbeiten, bspw. für vom Versicherten oder die von Krankenkassen bereitgestellten Daten durchzuführen.

Weitere Quellen

--

2.2.4.3 Rendering-Vorlagen für strukturierte Dokumente

Neue standardisierte Datenformate sollen nicht nur abgelegt werden, sondern auch Eingang in den Versorgungsalltag finden. Dies ist in Gänze nur erreicht, wenn für den Anwender auch eine lesbare Anzeige der Daten möglich ist.

Fachliche Darstellung

Eine menschenlesbare Darstellung muss sowohl für den Versicherten als auch für den Leistungserbringer gewährleistet sein. Daher sollen den Herstellern von Primärsystemen oder Frontends des Versicherten (FdV und AdV) Vorlagen für eine Anzeige der MIOs bereitgestellt werden. Den Herstellern ist es jedoch freigestellt, eigene Darstellungsformen zu nutzen.

Für Versicherte und deren Vertreter kommen folgende Anwendungsfälle zum Tragen:

- menschenlesbare Darstellung der Inhalte von strukturierten Standarddokumenten

Für Leistungserbringer kommen folgende Anwendungsfälle zum Tragen:

- menschenlesbare Darstellung und fachlich sinnvolle Anordnung der Inhalte von strukturierten Standarddokumenten

Randbedingungen

~~**Randbedingungen**~~

~~Die Umsetzung dieser Anforderung gilt für folgende Nutzerumgebungen:~~

- ~~Primärsysteme der Leistungserbringer~~
- ~~FdV~~

- ~~AdV~~

~~**Weitere Quellen**~~

~~--~~

Die Kassenärztliche Bundesvereinigung plant, mit Bereitstellung neuer MIOs stets auch eine Anzeigemöglichkeit mittels des MIO-Viewers bereitzustellen.

~~2.1.3.1~~2.2.4.4 MIO „Elektronische Impfdokumentation“

Die elektronische Impfdokumentation (auch: elektronischer Impfpass) ist ein Passdokument des Versicherten, in dem alle durchgeführten Impfungen und damit der Impfstatus des Versicherten digital dokumentiert sind. Rechtsgrundlage in Deutschland ist~~.~~ hierfür der § 22 Infektionsschutzgesetz, in dem die Dokumentationsinhalte konkret vorgegeben werden.
Die Grundlage für den elektronischen Impfpass in der elektronischen Patientenakte findet sich in § 341(2)5 PDSG.

Fachliche Darstellung

~~**Fachliche Darstellung**~~

Der elektronische Impfpass wird durch einen Leistungserbringer (auch Ärzte in Öffentlichen Gesundheitsdiensten oder Fachärzte der Arbeits- und Betriebsmedizin) angelegt und ausschließlich durch ~~einen~~ Leistungserbringer gepflegt.

Für berechtigte Leistungserbringer kommen maximal (je nach Zugriffsrechten) folgende Anwendungsfälle im Rahmen der elektronischen Impfdokumentation zum Tragen:

- ~~Eintragen~~Erstellen von Impfeinträgen
- Einsehen des Impfpasses und einzelner Einträge
- Löschen von Impfeinträgen zum Zwecke der Korrektur
- Signieren von Impfeinträgen
- Abhängig von der Festlegung im Rahmen der MIO-Erstellung: entweder Löschen des Impfpasses in Gänze oder auch Löschen einzelner Impfeinträge

Für den Versicherten kommen folgende Anwendungsfälle im Rahmen der elektronischen Impfdokumentation zum Tragen:

- Einsehen des Impfpasses ~~in der ePA~~und einzelner Einträge mittels FdV/ AdV
- Export des Impfpasses aus der ePA mittels FdV

~~Für Ärzte in Gesundheitsbehörden kommen folgende Anwendungsfälle~~Abhängig von der Festlegung im Rahmen der ~~elektronischen Impfdokumentation zum Tragen:~~

- ~~Einsehen~~MIO-Erstellung: entweder Löschen des Impfpasses

~~**Randbedingungen**~~

~~Die Umsetzung dieser Anforderung gilt für folgende Nutzerumgebungen:~~

- ~~Primärsysteme der Leistungserbringer~~

- in Gänze oder auch Löschen einzelner Impfeinträge mittels FdV
- / AdV

Randbedingungen

Die elektronische Impfdokumentation muss gemäß § 342(2) PDSG spätestens ab dem 01. Januar 2022 in der elektronischen Patientenakte verfügbar sein.

Die semantischen und syntaktischen Vorgaben zur elektronischen Impfdokumentation finden sich in der dazugehörigen Spezifikation der Kassenärztlichen Bundesvereinigung (KBV) wieder (gemäß § 355 PDSG).

~~2.1.3.2~~2.2.4.5 MIO „Elektronisches Zahnbonusheft"

Das elektronische Zahnbonusheft ist ein Passdokument, mit dem der Versicherte nachweisen kann, in welchen Abständen er zahnärztliche Vorsorgeuntersuchungen wahrgenommen hat. Eine lückenlose Dokumentation von jährlichen Prophylaxeterminen erhöht den Festzuschuss für die Kosten eines Zahnersatzes.

Die Grundlage für das Zahnbonusheft in der elektronischen Patientenakte ist § 341(2)2 PDSG.

Fachliche Darstellung

Das elektronische Zahnbonusheft wird üblicherweise in einer Zahnarztpraxis angelegt und durch das Hinzufügen von Einträgen gepflegt.

Für berechtigte Leistungserbringer kommen maximal (je nach Zugriffsrechten) folgende Anwendungsfälle im Rahmen des Zugriffs auf das elektronische Zahnbonusheft zum Tragen:

- ~~Eintragen~~Erstellen von ~~Zahnbonushefteinträgen~~Einträgen
- Signieren des Zahnbonusheftes als Ganzes
- Einsehen des Zahnbonusheftes und einzelner Einträge
- ~~Löschen von Zahnbonushefteinträgen~~
- Abhängig von der Festlegung im Rahmen der MIO-Erstellung: entweder Löschen des Passes in Gänze oder auch Löschen einzelner Einträge

Für den Versicherten kommen folgende Anwendungsfälle im Rahmen des elektronischen Zahnbonusheftes zum Tragen:

- Einsehen des Zahnbonusheftes in der ePA mittels FdV/AdV
- Export des Zahnbonusheftes aus der ePA mittels FdV
- Abhängig von der Festlegung im Rahmen der MIO-Erstellung: entweder Löschen des Passes in Gänze oder auch Löschen einzelner Einträge mittels FdV/AdV

Randbedingungen

~~**Randbedingungen**~~

~~Die Umsetzung dieser Anforderung gilt für folgende Nutzerumgebungen:~~

- ~~Primärsysteme der Leistungserbringer~~
- ~~FdV~~

- ~~AdV~~

Das elektronische Zahnbonusheft muss gemäß § 342(2) PDSG spätestens ab dem 01. Januar 2022 in der elektronischen Patientenakte verfügbar sein.

Die semantischen und syntaktischen Vorgaben zum elektronischen Zahnbonusheft finden sich in der dazugehörigen Spezifikation der Kassenärztlichen Bundesvereinigung (KBV) wieder (gemäß § 355 PDSG).

~~2.1.3.3~~2.2.4.6 MIO „Elektronisches Untersuchungsheft für Kinder"

Das elektronische Untersuchungsheft für Kinder (U-Heft) ist ein Passdokument, welches dem Nachweis von wahrgenommenen Vorsorgeuntersuchungen zur Früherkennung von Krankheiten bei Kindern dient.

Die Grundlage für das elektronische Untersuchungsheft für Kinder in der elektronischen Patientenakte ist § 341(2)3 PDSG.

Fachliche Darstellung

Das elektronische Untersuchungsheft für Kinder wird von (Kinder-)Ärzten oder von Hebammen angelegt. In der Folge wird es durch Hinzufügen von Einträgen und der damit einhergehenden Dokumentation der Kinderuntersuchung von Ärzten gepflegt.

Für berechtigte Leistungserbringer kommen maximal (je nach Zugriffsrechten) folgende Anwendungsfälle im Rahmen des elektronischen Untersuchungsheftes für Kinder zum Tragen:

- ~~Eintragen~~Erstellen von Einträgen ~~im elektronischen Untersuchungsheft für Kinder~~über Untersuchungen
- Einsehen des Passes und einzelner Einträge
- Signieren von Untersuchungsergebnissen
- Abhängig von der Festlegung im Rahmen der MIO-Erstellung: entweder Löschen des Passes in Gänze oder auch Löschen einzelner Einträge

Für Ärzte in Gesundheitsbehörden kommen folgende Anwendungsfälle im Rahmen des elektronischen Untersuchungsheftes für Kinder zum Tragen:

- Einsehen des Untersuchungsheftes für Kinder
- ~~Löschen von U-Heft-Einträgen~~

Für ~~Ärzte in Gesundheitsbehörden~~Versicherte kommen folgende Anwendungsfälle im Rahmen des elektronischen Untersuchungsheftes für Kinder zum Tragen:

- ~~Einsehen des elektronischen Untersuchungsheftes für Kinder~~

~~Für Versicherte kommen folgende Anwendungsfälle im Rahmen des elektronischen Untersuchungsheftes für Kinder zum Tragen:~~

- Einsehen der Einträge des ~~elektronischen~~ Untersuchungsheftes für Kinder in der ePA mittels FdV/AdV
- Export des ~~elektronischen~~ Untersuchungsheftes für Kinder aus der ePA mittels FdV

~~Randbedingungen~~

- Abhängig von der Festlegung im Rahmen der MIO-Erstellung: entweder Löschen des Passes in Gänze oder auch Löschen einzelner Einträge

Randbedingungen

~~Die Umsetzung dieser Anforderung gilt für folgende Nutzerumgebungen:~~

- ~~Primärsysteme der Leistungserbringer~~
- ~~FdV~~
- ~~AdV~~

Das elektronische Untersuchungsheft für Kinder muss gemäß § 342(2) PDSG ab dem 01. Januar 2022 in der elektronischen Patientenakte verfügbar sein.

Die semantischen und syntaktischen Vorgaben zum elektronischen Untersuchungsheft für Kinder finden sich in der dazugehörigen Spezifikation der Kassenärztlichen Bundesvereinigung (KBV) wieder (gemäß § 355 PDSG).

~~2.1.3.4~~2.2.4.7 MIO „Elektronischer Mutterpass"

Der elektronische Mutterpass ist ein Dokument, welches es der Versicherten erlaubt, den Verlauf ihrer Schwangerschaft dokumentieren zu lassen und die enthaltenen Informationen anderen Leistungserbringern während der Betreuung in der Schwangerschaft zukommen zu lassen.

Die Grundlage für den elektronischen Mutterpass in der elektronischen Patientenakte ist § 341(2)4 PDSG.

Fachliche Darstellung

Der elektronische Mutterpass wird in der Regel von Ärzten bzw. von Krankenhäusern oder von Hebammen angelegt. In der Folge wird er durch das Hinzufügen von Einträgen durch Ärzte oder Hebammen gepflegt. Der elektronische Mutterpass dient anderen Leistungserbringern zum Informationsaustausch während der Schwangerschaft.

Für berechtigte Leistungserbringer kommen maximal (je nach Zugriffsrechten) folgende Anwendungsfälle im Rahmen des elektronischen Mutterpasses zum Tragen:

- ~~Eintragen~~Erstellen von Einträgen über Untersuchungen
- Einsehen des Passes und einzelner Einträge
- Signieren von Untersuchungsergebnissen
- ~~Einsehen des Mutterpasses~~
- ~~Löschen von Mutterpasseinträgen~~
- Abhängig von der Festlegung im Rahmen der MIO-Erstellung: entweder Löschen des Passes in Gänze oder auch Löschen einzelner Einträge

Für Versicherte kommen folgende Anwendungsfälle im Rahmen des elektronischen Mutterpasses zum Tragen:

- Einsehen des Mutterpasses in der ePA mittels FdV/AdV
- Export des Mutterpasses aus der ePA mittels FdV
- Abhängig von der Festlegung im Rahmen der MIO-Erstellung: entweder Löschen des Passes in Gänze oder auch Löschen einzelner Einträge

Randbedingungen

~~Die Umsetzung dieser Anforderung gilt für folgende Nutzerumgebungen:~~

- ~~Primärsysteme der Leistungserbringer~~
- ~~FdV~~
- ~~AdV~~

Der elektronische Mutterpass muss gemäß § 342(2) PDSG spätestens ab dem 01. Januar 2022 in der elektronischen Patientenakte verfügbar sein.

Die semantischen und syntaktischen Vorgaben zum elektronischen Mutterpass finden sich in der dazugehörigen Spezifikation der Kassenärztlichen Bundesvereinigung (KBV) wieder (gemäß § 355 PDSG).

~~2.1.4 Releaseunabhängiges Einbringen neuer strukturierter Dokumentenformate~~

~~Gemäß § 355 PDSG trifft die Kassenärztliche Bundesvereinigung (KBV) die notwendigen Festlegungen für die Inhalte der elektronischen Patientenakte ab Stufe 2.0, um deren semantische und syntaktische Interoperabilität zu gewährleisten. Die daraus resultierenden strukturierten Dokumentenformate sollen ohne Neuzulassung von der ePA unterstützt werden können.~~

~~Fachliche Darstellung~~

~~Von der KBV werden die strukturierten Dokumente als medizinische Informationsobjekte (MIO) bezeichnet. Diese spezifizierten Dokumentenformate sollen schnellstmöglich die medizinischen Versorgung unterstützen und in der ePA verwaltet werden können. Daher soll das Einbringen neuer standardisierter Dokumentenformate unabhängig von Releasezyklen und ohne Notwendigkeit einer Neuzulassung der Produkte möglich sein.~~

~~Für Primärsystem-, ePA-Aktensystem- und FdV-Hersteller kommen folgende Anwendungsfälle zum Tragen:~~

- ~~Einstellen von MIOs in die ePA~~
- ~~Anzeigen von MIOs aus der ePA am Client~~

~~Randbedingungen~~

~~Die KBV plant MIOs quartalsweise zu veröffentlichen in einem Umfang von ca. 15 Spezifikationen pro Jahr. Um die Verfügbarkeit von MIOs im Feld zu gewährleisten, plant die KBV in jeder MIO-Spezifikation eine Übergangsregelung zu definieren, die sich an die Primärsystemhersteller richtet. Je nach MIO kann eine Verfügbarmachung bspw. innerhalb eines Jahres umzusetzen.~~

~~2.1.4.1 1.1.1.1 Schemakonformität für strukturierte Dokumente~~

~~Die Nutzung von Schemata für bekannte und genormte Dokumentenformaten verbessert die Qualität, Interoperabilität und maschinelle Weiterverarbeitbarkeit der in der ePA abgelegten, strukturierten Dokumententypen.~~

~~Fachliche Darstellung~~

~~Die KBV definiert die Schemata, welche wiederum von der gematik zur Nutzung durch die Hersteller bereitgestellt werden. Die Hersteller sorgen in ihren Produkten dafür, dass die~~

~~durch das Schema vorgegebenen Strukturen und Formate für Dokumente, die in die ePA eingestellt werden, eingehalten werden. Somit werden für strukturierte Dokumentenformate Fehler vermieden, eine maschinelle Lesbarkeit unterstützt und die Güte der Datenqualität sichergestellt.~~

~~**Randbedingungen**~~

~~Die Umsetzung des fachlichen Bedarfes gilt für folgende Nutzerumgebungen:~~

- ~~Primärsysteme der Leistungserbringer~~

~~**Weitere Quellen**~~

~~–~~

~~2.1.4.21.1.1.1~~ ~~Rendering-Vorschriften für strukturierte Dokumente~~

~~Neue standardisierte Datenformate sollen nicht nur abgelegt werden, sondern auch Eingang in den Versorgungsalltag finden. Dies ist in Gänze nur erreicht, wenn für den Anwender auch eine lesbare Anzeige der Daten möglich ist. Eine menschenlesbare Darstellung muss sowohl für den Versicherten und dessen Vertreter via FdV und AdV als auch für den Leistungserbringer via Primärsystem gewährleistet sein.~~

~~**Fachliche Darstellung**~~

~~Für Versicherte und deren Vertreter kommen folgende Anwendungsfälle zum Tragen:~~

- ~~menschenlesbare Darstellung der Inhalte von strukturierten Standarddokumenten~~

~~Für Leistungserbringer kommen folgende Anwendungsfälle zum Tragen:~~

- ~~menschenlesbare Darstellung und fachlich sinnvolle Anordnung der Inhalte von strukturierten Standarddokumenten~~

~~**Randbedingungen**~~

~~Die Umsetzung des fachlichen Bedarfes gilt für folgende Nutzerumgebungen:~~

- ~~Primärsysteme der Leistungserbringer~~
- ~~ePA-Frontend des Versicherten~~
- ~~ePA-AdV-App~~

~~**Weitere Quellen**~~

~~–~~

~~2.1.5~~2.2.5 Verfahren zur gezielten Umschlüsselung (Akten-/ Kontextschlüssel)

Um ~~auf Kompromittierungen und Abkündigungen~~einer Kompromittierung von kryptographischen ~~Algorithmen~~Schlüsseln vorzubeugen und um in Folge einer erfolgten Kompromittierung reagieren zu können, soll die Möglichkeit zum Wechsel ~~von Akten- und Kontextschlüssel~~relevanter Schlüssel innerhalb der elektronischen Patientenakte geschaffen werden.

Fachliche Darstellung

Dem Versicherten soll die Möglichkeit geboten werden, zu jedem Zeitpunkt die Umschlüsselung der elektronischen Patientenakte veranlassen zu können, damit bei

Verdacht oder tatsächlicher Kompromittierung von Schlüsselmaterial missbräuchliche Zugriffe verhindert werden (analog Passwortwechsel).

Für den Versicherten kommen folgende Anwendungsfälle zum Tragen:

- ~~Wechsel des Akten- und Kontextschlüssels~~Umschlüsselung seiner ePA über ~~FdV~~ein Frontend des Versicherten
- ~~Wechsel des Akten- und Kontextschlüssels~~Umschlüsselung seiner ePA ohne ~~FdV~~ein Frontend des Versicherten

Darüber hinaus soll die Möglichkeit einer Kompromittierung von Schlüsselmaterial auch unabhängig vom Versicherten durch einen regelmäßigen oder anlassbezogenen (z.B. bei Schwachstelle im genutzten kryptographischen Algorithmus) Schlüsselwechsel verringert und damit die aktuellen kryptographischen Vorgaben eingehalten werden:

- durch das Aktensystem initiierter, regelmäßiger Wechsel des Akten- und Kontextschlüssels seiner ePA ~~durch das Aktensystem~~
- durch das Aktensystem initiierter, anlassbezogener Wechsel des Akten- und Kontextschlüssels seiner ePA durch das Aktensystem

Randbedingungen

Bei der Bewertung der Lösungsoptionen muss das Verhalten des Systems aus Nutzersicht betrachtet werden (bspw. Datenvolumen, bei mobilen Endgeräten der Energieverbrauch, Dauer des Prozesses, Notwendigkeit mit der Anwendung aktiv zu interagieren für die Dauer des Prozesses).

Auch nach der Umschlüsselung müssen der Versicherte und alle Berechtigten auf alle Dokumente der Akte weiterhin zugreifen können, damit die Dokumente für die medizinische Behandlung des Versicherten weiterhin genutzt werden können.

~~Nach einem Austausch müssen die bestehenden Zugriffsberechtigungen auf die Akte weiterhin greifen.~~

~~Ein automatisierter Austausch des Akten- und Kontextschlüssels muss alle zwei Jahre sichergestellt werden.~~

~~2.1.6~~2.2.6 ePA-FdV AdV~~-/TI-Terminal~~

Einem Versicherten ohne eigene technische Geräte muss die Möglichkeit geboten werden die Berechtigungen seiner ePA zu verwalten und Dokumente seiner Akte einsehen und löschen zu können. Dafür wird im KTR-AdV-Terminal eine ePA-~~Auch Versicherte und deren Vertreter ohne eigene technische Geräte (Personal Computer, Tablet, Smartphone) müssen ihre ePA verwalten können, damit diese von ihren Leistungserbringern genutzt werden kann.~~

~~Fachliche Darstellung~~

FdV AdV zur Verfügung gestellt.

Fachliche Darstellung

Für den Versicherten kommen folgende Anwendungsfälle durch die Nutzung ~~eines~~einer ePA-FdV AdV~~-/TI-Terminals~~ zum Tragen:

- Nutzerzugang ePA (Login Aktensession, Logout Aktensession)

- Aktenkonto verwalten (Aktenkonto aktivieren, Aktenkonto schließen)
- Dokumente suchen
- Dokumente anzeigen
- Dokumente im Aktenkonto löschen
- Protokolle einsehen
- Protokolle löschen
- Umschlüsselung der Akte
- Änderung der Kennzeichnung der Vertraulichkeit von Dokumenten
- Zugriffsberechtigungen verwalten (Berechtigung für LEI ändern, Berechtigung für Vertreter ändern)

Randbedingungen

Die Bereitstellung ~~dieser technischen Einrichtung (sog. Anwendungen~~ des ~~Versicherten- oder auch Telematikinfrastruktur-Terminal (kurz~~ KTR, AdV ~~-/TI-Terminal))~~ Terminals ist gemäß § 338 PDSG gesetzlich gefordert ~~gemäß § 338 PDSG~~.

Weitere Quellen

--

~~2.2~~2.3 KOM-LE (Stufe 1.5)

Die Erweiterungen der Anwendung KOM-LE im vorliegenden Systemdesign sollen soweit wie möglich abwärtskompatibel ausgestaltet werden, da eine längere Migrationsphase der KOM-LE-IT-Systeme (Komponenten und Dienste der TI, Primärsysteme) erwartet wird.

Es ist davon auszugehen, dass KOM-LE 1.0 bis Ende 2020 mindestens bei allen ärztlichen und zahnärztlichen Leistungserbringern ausgerollt sein wird, insbesondere um ab dem 01.01.2021 die Arbeitsunfähigkeitsbescheinigung (AU) elektronisch mittels KOM-LE zwischen Leistungserbringern und Krankenversicherungen übermitteln zu können. Die Migration auf KOM-LE 1.5 kann nur über einen mehrjährigen Zeitraum erfolgen. Während der Migrationsphase muss weiterhin ein Versand von KOM-LE-Nachrichten zwischen Teilnehmern an KOM-LE 1.0 und KOM-LE 1.5 möglich sein.

~~2.2.1~~2.3.1 Übermittlung von großen Dokumenten

KOM-LE 1.0 wird erweitert um die Möglichkeit zur Übermittlung von großen Dokumenten. Die derzeit bestehende Limitierung auf eine maximale Nachrichtengröße von 25 MB wird somit aufgehoben.

In realen Versorgungs- und Verwaltungsprozessen werden vereinzelt – aber regelmäßig – Dokumente zwischen KOM-LE-Teilnehmern ausgetauscht, die eine Größe von 25 MB deutlich überschreiten (Übermittlung von Bilddateien – z.B. Röntgenbilder – zwischen Leistungserbringern sowie umfangreichen Abrechnungsdaten zwischen Leistungserbringern und KVen/KZVen).

Fachliche Darstellung:

- Es muss eine Übermittlung (senden und empfangen) von Dokumenten bis zu einer Größe von ~~200~~500 MB möglich sein.
- Die Übermittlung großer Dokumente muss bei allen stationären KOM-LE-Endpunkten möglich sein, d.h. für KOM-LE-Teilnehmer mit Zugang zur TI über den Konnektor, Basis-Consumer und KTR-Consumer.
- Zwischen Teilnehmern an KOM-LE 1.0 und KOM-LE 1.5 muss uneingeschränkt ein Nachrichtenaustausch von KOM-LE-Nachrichten bis zu einer Größe vom 25 MB möglich sein.
- Vor einem Versand von KOM-LE-Nachrichten mit einer Nachrichtengröße von über 25 MB soll für den Sender erkennbar sein, ob der Empfänger noch KOM-LE 1.0 verwendet, da der Empfang der Nachricht in diesem Fall nicht möglich ist.

~~2.2.2~~2.3.2 Flexibilisierung KOM-LE-Integration für Clientsysteme (PS)

Für KOM-LE Stufe 1.5 soll es Herstellern von Clientsystemen (PS) ermöglicht werden, die Funktionen des KOM-LE-Clientmoduls eigenständig zu entwickeln und in ihr PS zu integrieren. Bisher ist im KOM-LE-Zulassungsverfahren ein KOM-LE-Clientmodul ausschließlich durch den KOM-LE-Anbieter, gekoppelt mit dem KOM-LE-Fachdienst, zuzulassen und bereitzustellen. Die technischen Schnittstellen zwischen KOM-LE-Clientmodul und KOM-LE-Fachdienst sind bereits in KOM-LE 1.0 weitgehend – bis auf den Account-Manager des KOM-LE-Fachdienstes – interoperabel spezifiziert, eine Prüfung der Interoperabilität ist allerdings nicht Gegenstand der Zulassungsverfahren, da eine feste Kopplung zwischen KOM-LE-Clientmodul und KOM-LE-Fachdienst im Zulassungsverfahren vorgesehen ist.

Durch die Möglichkeit einer direkten Integration der KOM-LE-Clientsystem-Funktionalität durch PS-Hersteller in ihr PS reduziert sich die Komplexität der Praxis-IT sowohl in technischer als auch in betrieblicher Hinsicht.

Fachliche Darstellung:

- Die Kopplung von KOM-LE-Clientmodul und KOM-LE-Fachdienst wird aufgehoben.
- KOM-LE-Clientmodule können unabhängig vom KOM-LE-Anbieter durch Hersteller entwickelt werden.
- Die KOM-LE-Clientsystem-Funktionalität kann auch direkt durch den Hersteller eines Primärsystems in das PS integriert werden.
- Es muss eine Interoperabilität zwischen KOM-LE-Clientmodulen bzw. Primärsystemen, die die KOM-LE-Clientsystem-Funktionalität direkt umsetzen, und KOM-LE-Fachdiensten gegeben sein.
- KOM-LE-Anbieter müssen weiterhin ein KOM-LE-Clientmodul bereitstellen.
- Die Schnittstelle zum Account-Manager des KOM-LE-Fachdienstes muss interoperabel ausgestaltet werden.

~~2.2.3~~2.3.3 Unterstützung von Nachrichten-Kategorien

Für KOM-LE Stufe 1.5 soll eine ~~optionale~~ Nachrichten-Kategorie innerhalb von KOM-LE-Nachrichten eingeführt werden, um eine syntaktische Kategorisierung von KOM-LE-Nachrichten zu ermöglichen.

Insbesondere bei einer automatisierten Verarbeitung von empfangenen KOM-LE-Nachrichten in Clientsystemen unterstützt eine Kategorisierung von KOM-LE-Nachrichten die Weiterverarbeitung von KOM-LE-Nachrichten, die strukturierte Daten enthalten. Hierdurch können Umsetzungen von verarbeitenden IT-Systemen sowie Versorgungs- und Verwaltungsprozesse vereinfacht werden.

Fachliche Darstellung:

- Für KOM-LE-Nachrichten wird ~~als Option~~ ein Datum zur Kategorisierung von Nachrichten aufgenommen.
- Die gematik pflegt eine Liste mit aktuell gültigen Kategorien und veröffentlicht diese.
- Bei berechtigtem Interesse können bei der gematik neue Kategorien beantragt werden. Berechtigt dazu sind die Gesellschafter der gematik und die gematik selbst.
- Innerhalb der TI erfolgt durch Komponenten und Dienste der TI keine inhaltliche Prüfung der Nachrichten-Kategorien.

~~2.2.4 Kompatibilitätseigenschaften~~

~~Die Erweiterungen der Anwendung KOM-LE im vorliegenden Systemdesign sollen soweit wie möglich abwärtskompatibel ausgestaltet werden, da eine längere Migrationsphase der KOM-LE-IT-Systeme (Komponenten und Dienste der TI, Primärsysteme) erwartet wird.~~

~~Es ist davon auszugehen, dass KOM-LE 1.0 bis Ende 2020 mindestens bei allen ärztlichen und zahnärztlichen Leistungserbringern ausgerollt sein wird, insbesondere um ab dem 01.01.2021 die Arbeitsunfähigkeitsbescheinigung (AU) elektronisch mittels KOM-LE zwischen Leistungserbringern und Krankenversicherungen übermitteln zu können. Die Migration auf KOM-LE 1.5 kann nur über einen mehrjährigen Zeitraum erfolgen. Während der Migrationsphase muss weiterhin ein Versand von KOM-LE-Nachrichten zwischen Teilnehmern an KOM-LE 1.0 und KOM-LE 1.5 möglich sein.~~

~~**Fachliche Darstellung:**~~

- ~~Zwischen Teilnehmern an KOM-LE 1.0 und KOM-LE 1.5 muss uneingeschränkt ein Nachrichtenaustausch von KOM-LE-Nachrichten bis zu einer Größe vom 25 MB möglich sein.~~
- ~~Vor einem Versand von KOM-LE-Nachrichten mit einer Nachrichtengröße von über 25 MB soll für den Sender erkennbar sein, ob der Empfänger noch KOM-LE 1.0 verwendet, da der Empfang der Nachricht in diesem Fall nicht möglich ist.~~

- KOM-LE-Nachrichten, die eine Nachrichten-Kategorie enthalten, müssen von KOM-LE 1.0-Teilnehmern uneingeschränkt empfangen werden können.

~~2.2.5~~2.3.4 Betriebliche Änderungen

Für den Fachdienst KOM-LE (Stufe 1.5) werden mit Release 4.0 neue betriebliche Kennzahlen definiert, anhand derer das Last- und Performanceverhalten sowie die Verfügbarkeit des Fachdienstes präziser gemessen und nachgewiesen werden. Des Weiteren wird der Fachdienst KOM-LE Performance-Messdaten erheben, welche die definierten betrieblichen Kenngrößen darstellen.

~~2.3~~2.4 E-Rezept (Stufe 1)

Die Fachanwendung „Elektronische Verordnung von Leistungen“ bzw. „elektronische ärztliche ~~Verordnungen~~Verordnung“ (kurz: E-Rezept) wird mit Release 4.0 (E-Rezept Stufe 1) aufgrund der Regelungen gemäß § 291a SGB V neu eingeführt. Dort wird ausgeführt, „[dass] die Gesellschaft für Telematik [gematik] die Maßnahmen durchzuführen [hat], die erforderlich sind, damit ärztliche Verordnungen für apothekenpflichtige Arzneimittel in elektronischer Form übermittelt werden können.

~~Nach § 31 SGB V~~Gemäß dem Gesetz für mehr Sicherheit in der Arzneimittelversorgung (GSAV) soll die Fachanwendung E-Rezept „"Innovationen in der telemedizinischen Behandlung ermöglichen und zur Entlastung von Ärztinnen und Ärzten, Apothekerinnen und Apothekern sowie Patientinnen und Patienten beitragen.“

2.4.1 Umsetzung gemäß Stufenkonzept

In Stufe 1 werden berücksichtigt:

- ärztliche/zahnärztliche Verordnungen für apothekenpflichtige Arzneimittel
- Die Erweiterbarkeit des E-Rezeptes für Folgestufen ist bereits in diesem Konzept und der Systemlösung zu berücksichtigen.
- Die Abhängigkeiten zu den Anwendungen eMP/AMTS, NFDM sind zu beachten.
- Der Abgleich der Informationsmodelle zwischen E-Rezept und eMP und VSDM muss erfolgen.

In den weiteren Ausbaustufen werden unter anderem berücksichtigt:

- Verordnungen von Hilfsmitteln, die zur Applikation eines Arzneimittels erforderlich sind
- Verordnungen von Betäubungsmitteln
- Verordnungen auf T-Rezepten
- Verordnung von Sprechstundenbedarf
- weitere in die Arzneimittelversorgung einbezogene Produkte gemäß § 31 SGB V
- Verordnungen für Heil- und Hilfsmittel
- Verordnungen zur Einlösung in einem anderen EU-Land nach §2 Abs. 1b AMVV (zunächst ist die Anschlusslösung der TI an den NCPeH zu erarbeiten)
- Privatrezepte für gesetzlich Versicherte
- Verordnungen von digitalen Gesundheitsanwendungen (DiGAs)

Darüber hinaus werden die Abhängigkeiten zur Anwendung ePA berücksichtigt.

Grundsätzlich lässt sich das Konzept auch auf Rezepte für Privatversicherte übertragen. In diesem Zusammenhang sind jedoch insbesondere Fragen zur Abrechnung festzulegen.

2.4.2 Übermittlung ärztlicher Verordnungen für apothekenpflichtige Arzneimittel in elektronischer Form

~~Fachliche Darstellung~~

Die Fachanwendung E-Rezept ermöglicht eine Übermittlung von ärztlichen und zahnärztlichen Verordnungen für apothekenpflichtige Arzneimittel in elektronischer Form. Perspektivisch soll die Anwendung E-Rezept, alle derzeit auf Papier ausgestellten Verordnungen ablösen. Dabei ~~sind~~wird die Digitalisierung der Prozesse von der Ausstellung von Verordnungen bis zur Abgabe der Arzneimittel inkl. der freien Auswahl einer Apotheke durch den Versicherten und die Kommunikation zwischen Versicherten und Apotheken ~~zu digitalisieren.~~betrachtet. Bei der Rezeptabgabe kann sich ein Versicherter grundsätzlich durch eine andere Person vertreten lassen. Eine Abbildung digitaler Prozesse für Pflegeeinrichtungen und -kräfte ~~-~~ist in der E-Rezept Stufe 1 nicht vorgesehen.

Die Fachanwendung E-Rezept betrachtet drei Hauptprozesse, welche in den Umgebungen der (Zahn-)Arztpraxis bzw. im Krankenhaus, der Apotheke und in einem für den Versicherten bereitgestellten Frontend ablaufen. Mit Hilfe eines Frontends hat der Versicherte die Möglichkeit, seine E-Rezepte in dem für ihn zulässigen Rahmen zu verwalten. Im Kontext der Fachanwendung E-Rezept wird das Frontend als App auf einem mobilen Endgerät verstanden; andere Ausprägungen sind jedoch möglich und werden nicht eingeschränkt.

Hauptprozesse der Fachanwendung E-Rezept:

- Ausstellen eines E-Rezepts in der Praxis/im Krankenhaus
- Verwalten der E-Rezepte im Frontend durch den Versicherten
- Abgeben eines Arzneimittels in der Apotheke

Die Beschreibung der Fachanwendung endet mit der Abgabe des Arzneimittels an den Versicherten. Die weiteren Schritte der Abgabe und Abrechnung von E-Rezepten in der Apotheke liegen nicht in der Fachanwendung E-Rezept.

Nach der Ausstellung eines E-Rezeptes in der Praxis/im Krankenhaus wird dieses nun nicht mehr direkt an den Versicherten übergeben, sondern innerhalb der TI gespeichert. Der Versicherte kann über sein Frontend das E-Rezept einsehen. Mit Hilfe eines elektronischen Zugangstokens (E-Rezept-Token) kann er eine Apotheke zur Einlösung berechtigen. Der E-Rezept-Token berechtigt den Besitzer (auch den Vertreter) zur Einlösung in der Apotheke.

Zusätzlich ist ein alternatives Verfahren mittels eines Ausdrucks des E-Rezept-Tokens in Form eines 2D-Codes möglich, um auch Versicherten, die keine mobilen Endgeräte nutzen, die uneingeschränkte Nutzung des Verfahrens zu ermöglichen.

Zur Einlösung des Rezeptes leitet der Versicherte oder sein Vertreter den E-Rezept-Token an die Apotheke weiter oder übergibt ihn direkt vor Ort. Der Apotheker erhält mit Hilfe des E-Rezept-Tokens Zugang zum E-Rezept und kann das Arzneimittel für den Versicherten bereitstellen.

Für das Ausstellen eines E-Rezepts in der Praxis/im Krankenhaus und für das Einlösen in der Apotheke müssen sich Versicherter und Arzt/Zahnarzt bzw. Apotheker nicht am gleichen Ort befinden (Fernbehandlung, Online-Bestellung in einer Apotheke).

Mit Hilfe seines Frontends kann der Versicherte seine E-Rezepte einsehen, löschen und das Protokoll einsehen.

Optional wird es für den Versicherten künftig auch möglich sein, die Inhalte der Verordnung und die abgegebenen Arzneimittel über die ePA einzusehen. Die relevanten Informationen des E-Rezeptes bzw. zur Abgabe in der Apotheke können dazu genutzt werden, in weiteren Fachanwendungen wie dem elektronischen Medikationsplan (eMP/AMTS) die einzunehmenden Arzneimittel zu dokumentieren.

2.4.3 Fachliche Informationsobjekte

Der Verordnungsdatensatz wird in Anlehnung an das Muster 16 „Arzneiverordnungsblatt" der Anlage 2 BMV-Ä bzw. Anlage 14 BMV-Z erstellt. Die fachlichen Inhalte, die hierbei durch den Verordnenden bereitgestellt werden, werden gemäß § 86 SGB V über die Bundesmantelvertragspartner entsprechend der gesetzlichen Vorgaben definiert und nicht im Rahmen der Fachanwendung E-Rezept festgelegt. Seitens BMV-Ä Partner wird das Benehmen mit dem DAV hergestellt.

Ein Verordnungsdatensatz wird in der Praxis/im Krankenhaus qualifiziert elektronisch signiert und an den E-Rezept-Fachdienst übergeben. Dieser signierte Datensatz wird "E-Rezept" genannt.

Alle nachfolgenden Datensätze wie bspw. Abrechnungs- und Dispensierdatensätze sind nicht Bestandteil dieser Betrachtung. Die Regelungen hierzu erfolgen über den Rahmenvertrag § 129 Abs. 2 SGB V sowie über die Arzneimittelabrechnungsvereinbarung nach § 300 SGB V zwischen GKV-Spitzenverband und dem Deutschen Apothekerverband (DAV).

Berücksichtigt wird jedoch, dass der Dispensierdatensatz in der Apotheke mit Komponenten der TI signiert wird. Sofern Korrekturen und Ergänzungen der Verordnung gem. BTMVV, AMVV, ApoBetrVO sowie den Regelungen des Rahmenvertrags § 129 Abs. 2 SGB V erfolgen, wird mittels HBA eine qualifizierte elektronische Signatur (QES) erzeugt; sofern keine Korrekturen und Ergänzungen erfolgen, wird eine fortgeschrittene Signatur mittels SMC-B erstellt.

Daraus ergeben sich die folgenden Informationsobjekte, welche im Rahmen der Fachanwendung E-Rezept verarbeitet werden:

Tabelle 1: Informationsobjekte der Fachanwendung E-Rezept

Informationsobjekt	Erläuterung
Verordnungsdatensatz	wird im Primärsystem des verordnenden Arztes/Zahnarztes erstellt und enthält die folgenden Informationen: • Versichertenstammdaten • Angaben zum verordnenden Arzt/Zahnarzt • Verordnung • weitere Informationen, die zur Belieferung der Verordnung notwendig sind
E-Rezept	• wird aus dem Verordnungsdatensatz mit der QES des verordnenden Arztes/Zahnarztes erstellt • Prämisse ist, ein E-Rezept enthält eine Verordnung (bzw. Arzneimittel)

Informationsobjekt	Erläuterung
E-Rezept-Datensatz	• befindet sich im Fachdienst E-Rezept der TI • enthält das qualifiziert signierte E-Rezept • enthält zusätzliche Informationen zur technischen Verarbeitung des E-Rezepts (z.B. ID, Status etc.)
Dispensierdatensatz	• enthält, sofern in der Apotheke Änderungen bei der Abgabe vorgenommen werden, den QES-signierten Dispensierdatensatz • enthält, sofern in der Apotheke keine Änderungen erfolgen, den fortgeschritten signierten Dispensierdatensatz
E-Rezept-Token	• der E-Rezept-Token steuert den Zugriff auf das E-Rezept; sein Besitz berechtigt zur Einlösung in der Apotheke
Quittung	• wird vom E-Rezept-Fachdienst bereitgestellt • dient der Apotheke bei der Abrechnung als Nachweis, dass ein Arzneimittel auf ein E-Rezept einmalig über die TI abgegeben worden ist

Die folgende Abbildung stellt die Informationsobjekte im zeitlichen Ablauf dar:

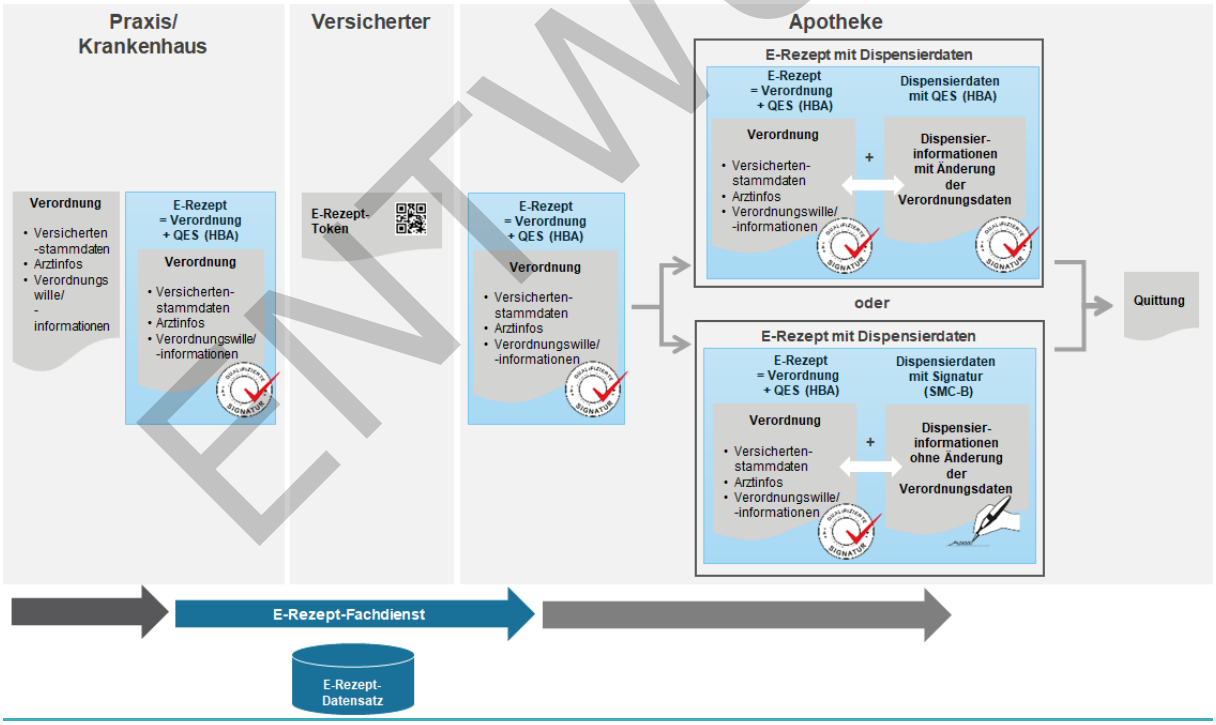


Abbildung 1: ABB_KPTERP_004 Informationsobjekte der Fachanwendung E-Rezept

Hinweis: Die obige Abbildung [ABB_KPTERP_004] stellt lediglich die in der Fachanwendung E-Rezept betrachteten Objekte dar. Es handelt sich hierbei nicht um eine Darstellung des Informationsmodells.

2.4.4 Fachliches Statusmodell

Ein E-Rezept befindet sich im E-Rezept-Fachdienst in unterschiedlichen Status, die im Folgenden dargestellt werden.

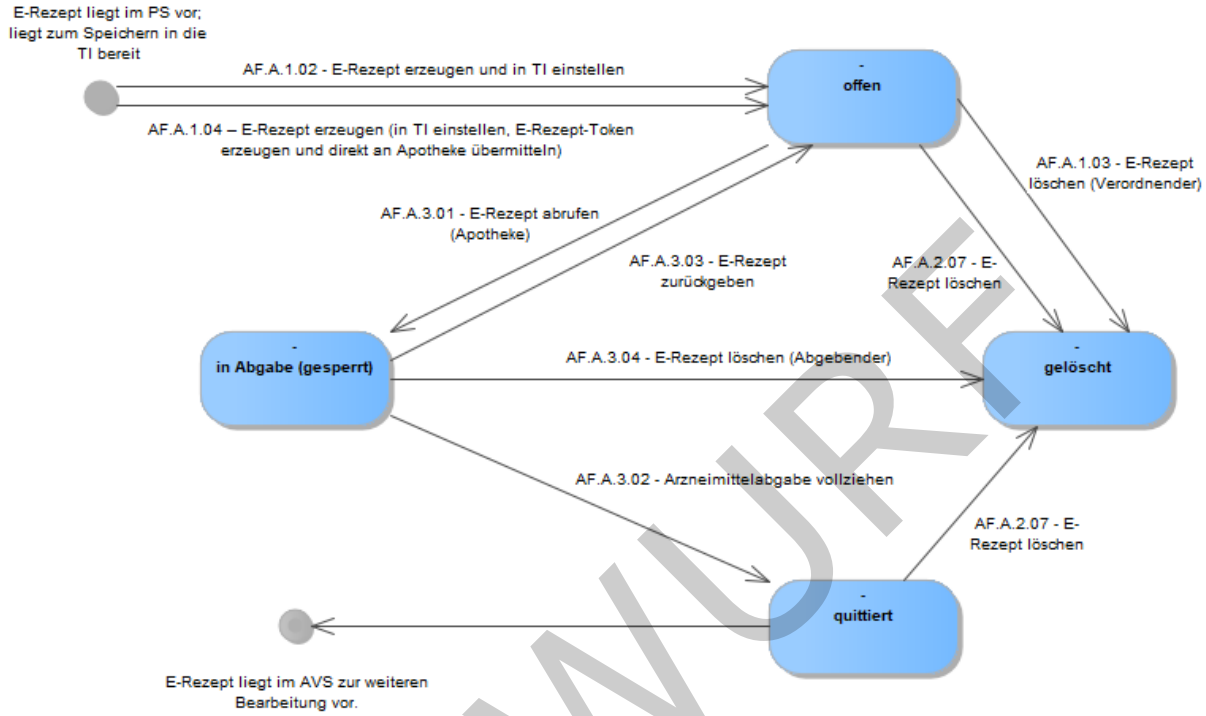


Abbildung 2: ABB_KPTERP_011 Fachliches Statusmodell E-Rezept

Tabelle 2: Status in der Fachanwendung E-Rezept

Status	Beschreibung
offen	• Das E-Rezept ist in den E-Rezept-Fachdienst eingestellt. • Es kann in der Apotheke abgerufen werden und wechselt dann in den Status „in Abgabe (gesperrt)". • Es kann vom verordnenden Arzt gelöscht werden und wechselt dann in den Status „gelöscht". • Es kann vom Versicherten bzw. seinem Vertreter angesehen werden. • Es kann vom Versicherten gelöscht werden.
in Abgabe (gesperrt)	• Das E-Rezept wurde in einer Apotheke abgerufen, eine andere Apotheke kann das E-Rezept nicht einlösen, es kann weder von einer anderen Apotheke noch von Ärzten gelöscht werden. • Es kann zurückgegeben werden und wechselt dann in den Status „offen". • Es kann in der Apotheke gelöscht werden und wechselt dann in den Status "gelöscht". • Nach Anforderung der Quittung vom E-Rezept-Fachdienst durch die Apotheke wechselt es in den Status „quittiert". • Es kann vom Versicherten bzw. seinem Vertreter angesehen werden.

Status	Beschreibung
	• Es kann vom Versicherten nicht gelöscht werden.
quittiert	• Die Arzneimittelabgabe auf dem E-Rezept wurde in der Apotheke vollzogen. • Es kann nicht noch einmal abgegeben werden. • Es kann vom Versicherten bzw. seinem Vertreter angesehen werden. • Es kann vom Versicherten gelöscht werden.
gelöscht	• Das E-Rezept wurde vom verordnenden Arzt, in der Apotheke oder vom Versicherten gelöscht.

2.4.5 Fachliche Darstellung der Hauptprozesse

2.4.5.1 Akteure

Die Akteure des E-Rezepts lassen sich den verschiedenen Rollen zuordnen:

Tabelle 3: TAB_KPTERP_002 Rollen E-Rezept

Rolle	Beschreibung
Versicherter (eGK)	Ein Versicherter ist eine Person, die in einem Versicherungsverhältnis mit einer gesetzlichen Krankenkasse steht und eine eGK besitzt.
Vertreter	Ein Vertreter ist die Person, die für den Versicherten bestimmte Anwendungsfälle in Bezug auf die Anwendung E-Rezept durchführen kann. Die Voraussetzung ist hierfür der jeweilige Besitz des E-Rezept-Tokens. Der Vertreter muss nicht in einem Versicherungsverhältnis mit einer gesetzlichen Krankenkasse stehen. Im Kontext der Fachanwendung E-Rezept ist die technische Autorisierung des Vertreters gegenüber der TI nicht notwendig."
Verordnende Akteure – Arzt, Zahnarzt (HBA)	Ein (Zahn-)Arzt ist ein approbierter Heilberufler und aufgrund seiner Mitgliedschaft in einer (Zahn-)Ärztekammer im Besitz eines HBA. Er ist befugt, vertragsärztliche Verordnungen am PVS zu erzeugen, mit einer QES zu versehen und diese als E-Rezept in der TI bereitzustellen. Die hier zu berücksichtigenden (Zahn-)Ärzte sind immer einer Institution zuzuordnen (z. B. eigene Praxis, med. Berufsausübungsgemeinschaft, MVZ, Krankenhaus).

Rolle	Beschreibung
Verordnende Akteure - Mitarbeiter medizinische Institution	Ein „Mitarbeiter medizinische Institution" arbeitet in einer Institution zur medizinischen Versorgung (z.B. eigene Praxis, med. Berufsausübungsgemeinschaft, MVZ, Krankenhaus) auf Weisung des verantwortlichen Vorgesetzten als berufsmäßiger Gehilfe des Arztes/Zahnarztes oder zur Vorbereitung auf den Beruf.
Abgebende Akteure – Apotheker und pharmazeutisches Personal (HBA)	Ein Apotheker ist ein approbierter Heilberufler, der im Besitz eines HBA ist. Pharmazeutisches Personal – Pharmazieingenieure und Apothekerassistenten, das zur Vertretung des Apothekenleiters gem. § 2 (7) ApBetrO beauftragt ist und im Besitz eines HBA ist. Sie sind befugt, Arzneimittel auf Grundlage eines E-Rezeptes abzugeben und die Abgabe mit einem fortgeschrittenen signierten Dispensierdatensatz im AVS zu dokumentieren. Im Falle einer Änderung am E-Rezept sind sie befugt, diese zusammen mit dem Dispensierdatensatz durch eine QES zu dokumentieren. Die hier benannten Akteure sind immer einer Institution zuzuordnen (z.B. öffentliche Apotheke (Haupt-/ Filialapotheke), Versandapotheke als Bestandteil einer öffentlichen Apotheke, Krankenhausapotheke).
Abgebende Akteure – Mitarbeiter Apotheke	Ein „Mitarbeiter Apotheke (abzeichnungsberechtigt)" arbeitet in einer Apotheke (z.B. öffentliche Apotheke (Haupt-/ Filialapotheke), Versandapotheke als Bestandteil einer öffentlichen Apotheke, Krankenhausapotheke) auf Weisung des verantwortlichen Vorgesetzten und ist zur Abgabe von Arzneimitteln auf Grundlage einer Verordnung befugt sowie abzeichnungsberechtigt. Die Dokumentation der Abgabe erfolgt durch eine fortgeschrittene Signatur des Dispensierdatensatzes. Ein „Mitarbeiter Apotheke (nicht abzeichnungsberechtigt)" arbeitet in einer Apotheke (z.B. öffentliche Apotheke (Haupt-/Filialapotheke), Versandapotheke als Bestandteil einer öffentlichen Apotheke, Krankenhausapotheke) auf Weisung bzw. unter Aufsicht des verantwortlichen Vorgesetzten und ist nicht berechtigt, Verordnungen abzuzeichnen, jedoch zu deren Entgegennahme, zur Vorbereitung der Arzneimittel zur Abgabe und nach Maßgabe des § 3 ApBetrO ggf. zur Abgabe der Arzneimittel befugt.

2.4.5.2 E-Rezept ausstellen

Der ausstellende Arzt/Zahnarzt erstellt analog dem heutigen Prozess einen Verordnungsdatensatz mit Hilfe seines Primärsystems, signiert diesen mittels der qualifizierten elektronischen Signatur des HBA und stellt ihn in den E-Rezept-Fachdienst ein.

Der Versicherte kann elektronisch (z.B. über eine App) auf die Informationen des E-Rezepts zugreifen. Zusätzlich kann dem Versicherten in der Praxis/im Krankenhaus (hier: Entlassrezept), z.B. wenn er nicht über die notwendige technische Ausstattung verfügt, die Information zum E-Rezept papierbasiert übergeben werden.

Das E-Rezept kann in der Praxis/im Krankenhaus auch direkt an einen Vertreter des Versicherten (nach vorhergehender Autorisierung) übergeben werden. Unter Einhaltung des Apothekengesetzes kann ein E-Rezept direkt an eine Apotheke (z.B.: im Falle von Sprechstundenbedarf, parenteralen Zubereitungen nach §11 ApoG (Zytostatika) übergeben werden.

Der verordnende Arzt/Zahnarzt kann ein E-Rezept löschen, z.B. wenn ein Fehler bei der verordneten Packungsgröße festgestellt wird. Voraussetzung ist, dass das E-Rezept von ihm erstellt wurde und dass es noch nicht in einer Apotheke bearbeitet oder das Arzneimittel abgegeben wurde. Sofern eine Korrektur des Fehlers erfolgen soll, muss ein neues E-Rezept ausgestellt werden.

Sofern ein Versicherter die freiwillige Anwendung eMP/AMTS (elektronischer Medikationsplan/Arzneimitteltherapiesicherheit) oder NFDM (Notfalldatenmanagement) nutzt, unterstützt das Primärsystem den Arzt/Zahnarzt dabei, die Daten vor dem Erstellen eines E-Rezepts z.B. im Hinblick auf durch andere Ärzte dokumentierte Diagnosen oder Arzneimittelunverträglichkeiten zu prüfen. Im Falle eines gepflegten eMP kann zudem geprüft werden, welches Arzneimittel zuletzt in der Apotheke abgegeben worden ist. Mit Hilfe der Daten des E-Rezepts können der eMP und der NFD (Notfalldatensatz) aktualisiert und zudem künftig die Daten des E-Rezepts in der ePA abgelegt werden.

2.4.5.3 E-Rezept durch den Versicherten verwalten

Der Versicherte kann die Inhalte seiner E-Rezepte mit Hilfe des Frontends einsehen und verwalten. Er kann den E-Rezept-Token an eine Vor-Ort-Apotheke digital übermitteln bzw. direkt überbringen oder einer Apotheke für eine Online-Bestellung übermitteln. Er kann den E-Rezept-Token auch an einen Vertreter übergeben.

Die Übergabe des E-Rezept-Tokens an eine Apotheke oder einen Vertreter kann mit Hilfe des Frontends über die TI erfolgen oder z.B. indem der E-Rezept-Token an einen Vertreter, der nicht in einer gesetzlichen Krankenkasse versichert sein muss, weitergegeben wird.

Im Kontext eines E-Rezepts kann der Versicherte mithilfe des Frontends auf elektronischem Wege Kontakt mit der Apotheke aufnehmen, und zwar basierend auf asynchroner Kommunikation, die vergleichbar mit marktüblichen Messenger-Diensten ist. Die Kommunikation geht dabei vom Versicherten aus und enthält den Rezeptkontext in maschinell auswertbarer Form.Der Versicherte kann das E-Rezept löschen. Über ein Protokoll kann er sich über alle erfolgten Zugriffe auf das E-Rezept in der TI informieren.

Der Versicherte kann sich auch nach der Abgabe des Arzneimittels in der Apotheke bis zur endgültigen Löschung die Inhalte des E-Rezepts einsehen.

2.4.5.4 E-Rezept einlösen

Die Abgabe in der Apotheke erfolgt nicht personengebunden. Derjenige, der den E-Rezept-Token überbringt, kann das E-Rezept einlösen.

Die Apotheke ruft das E-Rezept aus dem E-Rezept-Fachdienst mittels des übergebenen E-Rezept-Tokens ab. Der E-Rezept-Fachdienst verhindert die doppelte Abgabe eines Arzneimittels auf ein E-Rezept in der Apotheke.

Wenn die Abgabe des Arzneimittels nicht möglich ist, gibt der Apotheker das E-Rezept wieder frei, so dass der Versicherte den E-Rezept-Token an eine andere Apotheke übermitteln kann.

Falls in der Apotheke ein Fehler an der Verordnung festgestellt wird, der sich nur durch die Ausstellung eines neuen E-Rezepts beim (Zahn-)Arzt beheben lässt, kann das E-Rezept auch in der Apotheke gelöscht werden.

Mit der Abgabe des Arzneimittels endet der Prozess in der Fachanwendung E-Rezept. Die Schritte zur weiteren Bearbeitung im Rahmen der Abgabe und Abrechnung finden außerhalb der Fachanwendung E-Rezept statt. Die in der Apotheke erstellten Datensätze werden jedoch mit Hilfe von Komponenten der TI fortgeschritten bzw. qualifiziert elektronisch signiert.

Für die Durchführung der AMTS-Prüfung und die Dokumentation der abgegebenen Arzneimittel bzw. der Einnahmehinweise ist bereits die freiwillige Anwendung eMP/AMTS (elektronischer Medikationsplan/Arzneimitteltherapiesicherheit) vorgesehen. Der Apotheker kann auf Wunsch des Versicherten den eMP aktualisieren und künftig in der ePA ablegen. Hierfür können ggf. auch Daten des E-Rezeptes genutzt werden. Eine dauerhafte Speicherung des E-Rezeptes im Fachdienst der TI ist nicht vorgesehen.

2.4.5.5 Dispensierdaten anbringen

Wenn die Abgabe eines Arzneimittels ohne Änderung vollzogen wurde (gemäß ApoBetrO §17 Abs. 6), signieren der abgebende Apotheker oder seine Mitarbeitenden den Dispensierdatensatz digital mit Hilfe der fortgeschrittenen Signatur des Konnektors.

Wenn die Abgabe eines Arzneimittels mit einer Änderung in Bezug auf die Verordnungsdaten des verordnenden Arztes vollzogen wurde, signiert der Apotheker den Datensatz mittels qualifizierter elektronischer Signatur (QES) gemäß ApoBetrO § 17 Abs. 5.

2.4.6 Anwendungsfälle

Folgende Anwendungsfälle kommen im Rahmen der Fachanwendung E-Rezept zum Tragen:

Tabelle 4: Anwendungsfälle Fachanwendung E-Rezept

Anwendungs-fall	Bezeichnung	Kurzbeschreibung
1. Übergreifend		
AF.A.1.01	Dokument mit QES signieren (Verordnender/Abgebender	Ein im Primärsystem erstelltes Dokument ist qualifiziert elektronisch signiert.
2. E-Rezept ausstellen		
AF.A.1.02	E-Rezept erzeugen und in TI einstellen	Der verordnende Akteur erzeugt aus einer signierten Verordnung (QES) ein E-Rezept und speichert dieses auf dem E-Rezept-Fachdienst.

Anwendungs-fall	Bezeichnung	Kurzbeschreibung
AF.A.1.03	E-Rezept löschen (Verordnender)	Der verordnende Akteur löscht ein E-Rezept vom E-Rezept-Fachdienst.
AF.A.1.04	E-Rezept erzeugen (in TI einstellen, E-Rezept-Token erzeugen und direkt an Apotheke übermitteln)	Der verordnende Akteur erzeugt aus einem E-Rezept ein E-Rezept-Datensatz und speichert diesen auf dem E-Rezept-Fachdienst. Zusätzlich wird ein korrespondierender E-Rezept-Token erzeugt und der versorgenden Apotheke zur Verfügung gestellt. Dieser Anwendungsfall umgeht die Übermittlung des Token an die Apotheke durch den Versicherten bzw. seinen Vertreter und weicht in dieser Hinsicht von AF.A.1.02 ab. AF.A.1.04 ist ausschließlich für besondere Versorgungssituationen wie der Übermittelung von Sprechstundenbedarf, von parenteralen Zubereitungen nach § 11 ApoG (Zytostatika) anzuwenden. Für E-Rezepte, die im Krankenhaus erstellt, krankenhausintern verwendet und gemäß § 129a SGB V abgerechnet werden und für die kein Fremdzuweisungsverbot gilt, können E-Rezept-Token auch außerhalb der TI, z.B. über das KIS, vom Verordnenden an den Abgebenden übermittelt werden.
3. E-Rezept durch den Versicherten verwalten		
AF.A.2.01	E-Rezept-Token an Apotheke übermitteln	Der Versicherte/Vertreter übermittelt einen E-Rezept-Token an die Apotheke seiner Wahl.
AF.A.2.02	E-Rezept-Token in Frontend optisch (2D-Code) darstellen	Dem Versicherten/Vertreter wird ein E-Rezept-Token im Frontend optisch dargestellt.
AF.A.2.03	Protokolle einsehen	Dem Versicherten werden Protokolleinträge für von ihm wählbare Zeiträume angezeigt.
AF.A.2.04	E-Rezept ansehen	Dem Versicherten/Vertreter werden die Inhalte eines E-Rezepts angezeigt.
AF.A.2.07	E-Rezept löschen (Versicherter)	Der Versicherte löscht ein E-Rezept vom E-Rezept-Fachdienst.
4. E-Rezept in der Apotheke einlösen		
AF.A.3.01	E-Rezept abrufen (Apotheke)	Der abgebende Akteur ruft ein E-Rezept mit Hilfe eines übergebenen E-Rezept-Tokens ab.
AF.A.3.02	Arzneimittelabgabe vollziehen	Der abgebende Akteur führt einer Arzneimittelabgabe durch, versetzt den

Anwendungs-fall	Bezeichnung	Kurzbeschreibung
		Status des E-Rezept-Datensatz in den Status "quittiert" und erhält eine Quittung.
AF.A.3.03	E-Rezept zurückgeben	Der abgebende Akteur gibt ein E-Rezept, auf das eine Arzneimittelabgabe oder -versendung nicht erfolgen konnte, zurück.
AF.A.3.04	E-Rezept löschen (Abgebender)	Der abgebende Akteur löscht ein E-Rezept vom E-Rezept-Fachdienst.
5. Signieren in der Apotheke		
AF.A.3.05	Dokument fortgeschritten signieren	Der abgebende Akteur signiert den im AVS erzeugten Dispensierdatensatz.
6. Kommunikation		
AF.A.5.04	Kommunikation mit der Apotheke ausgehend vom Versicherten	Der Versicherte oder sein Vertreter stellt eine Anfrage bei der Apotheke, beispielsweise nach der Verfügbarkeit der im E-Rezept verordneten Arzneimittel.
AF.A.5.05	Versicherten im Kontext des E-Rezepts kontaktieren (Apotheke)	Die Apotheke kontaktiert einen Versicherten im Kontext eines E-Rezepts

Im Folgenden wird der Gesamtablauf für das Ausstellen eines E-Rezepts, seine Verwaltung und das Einlösen in der Apotheke dargestellt.

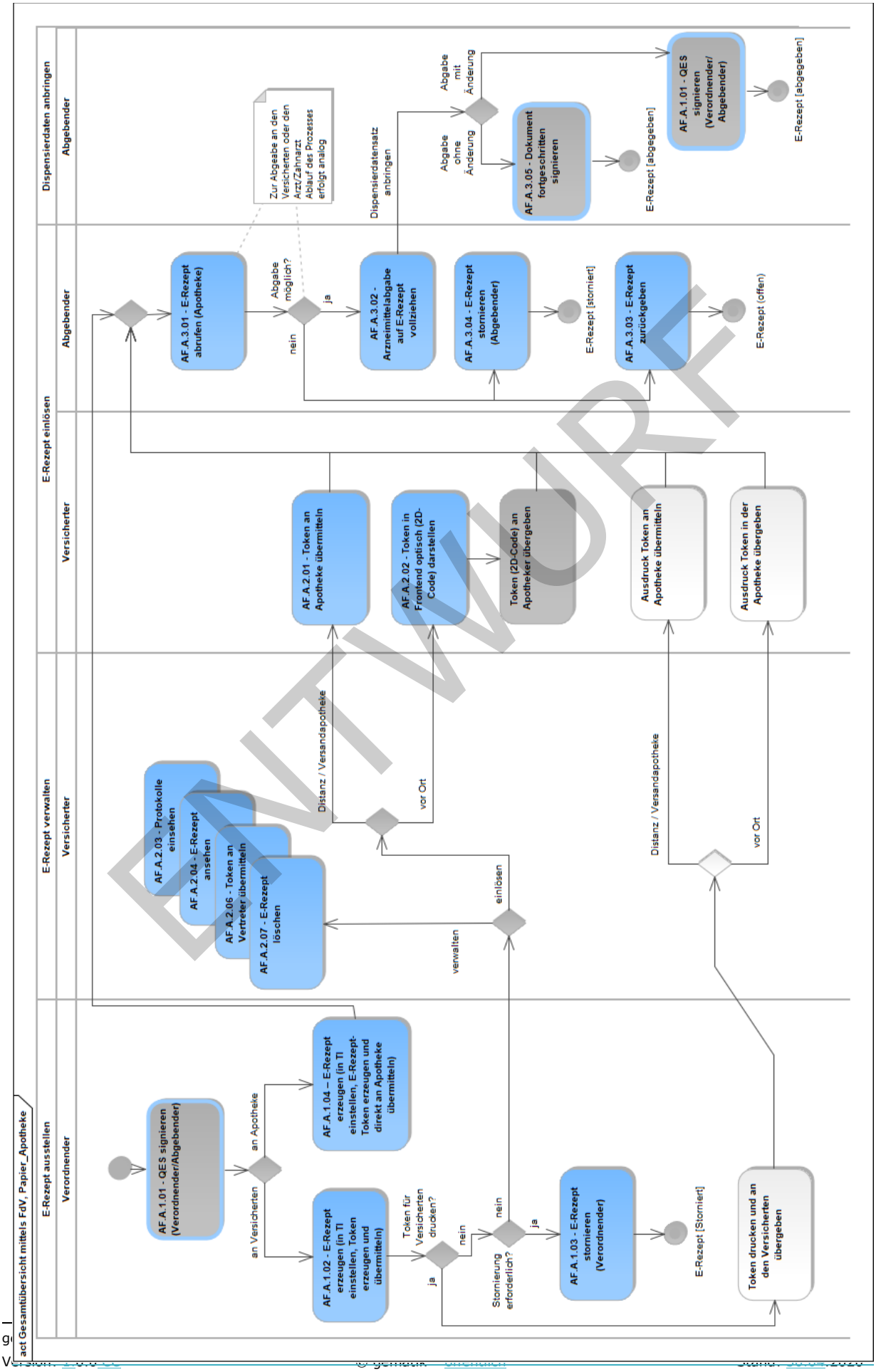

act Gesamtübersicht mittels FdV, Papier_Apotheke
E-Rezept ausstellen
E-Rezept verwalten
E-Rezept einlösen
Dispensierdaten anbringen
Verordnender
Versicherter
Abgebender
Abgebender
AF.A.1.01 - QES signieren (Verordnender/Abgebender)
an Apotheke
an Versicherten
AF.A.1.04 – E-Rezept erzeugen (in TI einstellen, E-Rezept-Token erzeugen und direkt an Apotheke übermitteln)
AF.A.1.02 - E-Rezept erzeugen (in TI einstellen, Token erzeugen und übermitteln)
Token für Versicherten drucken?
ja
nein
Stornierung erforderlich?
nein
ja
AF.A.1.03 - E-Rezept stornieren (Verordnender)
E-Rezept [Storniert]
Token drucken und an den Versicherten übergeben
AF.A.2.03 - Protokolle einsehen
AF.A.2.04 - E-Rezept ansehen
AF.A.2.06 - Token an Vertreter übermitteln
AF.A.2.07 - E-Rezept löschen
verwalten
einlösen
Distanz / Versandapotheke
vor Ort
AF.A.2.01 - Token an Apotheke übermitteln
AF.A.2.02 - Token in Frontend optisch (2D-Code) darstellen
Token (2D-Code) an Apotheker übergeben
Distanz / Versandapotheke
vor Ort
Ausdruck Token an Apotheke übermitteln
Ausdruck Token in der Apotheke übergeben
AF.A.1.01 - E-Rezept abrufen (Apotheke)
Abgabe möglich?
nein
ja
Zur Abgabe an den Versicherten oder den Arzt/Zahnarzt Ablauf des Prozesses erfolgt analog
AF.A.3.02 - Arzneimittelabgabe auf E-Rezept vollziehen
Dispensierdatensatz anbringen
AF.A.3.04 - E-Rezept stornieren (Abgebender)
E-Rezept [storniert]
AF.A.3.03 - E-Rezept zurückgeben
E-Rezept (offen)
Abgabe mit Änderung
Abgabe ohne Änderung
AF.A.3.05 - Dokument fortgeschritten signieren
E-Rezept [abgegeben]
AF.A.1.01 - QES signieren (Verordnender/ Abgebender)
E-Rezept [abgegeben]

Abbildung 3: ABB_KPTERP_010 Übersicht Gesamtablauf E-Rezept (Hinweis: Diese Anwendung stellt eine Übersicht der Abläufe dar und enthält keine vollständige Abbildung aller Prozess-Schritte)

2.4.7 Betrieb

~~Die Anforderungen an die Fachanwendung E-Rezept werden im „Konzept E-Rezept“ ([gemKPT_eRp]) ausführlich beschrieben. Dort sind die umzusetzenden Anwendungsfälle (für die E-Rezept Stufe 1) sowie die nicht-funktionalen und übergreifenden Anforderungen aufgeführt. Der architektonische Aufbau samt Struktur sowie die technische Umsetzung der funktionalen und nicht-funktionalen Anforderungen hingegen werden im Dokument [gemSysL_eRp] beschrieben. An dieser Stelle wird daher mit dem Verweis auf die beiden vorgenannten Dokumente auf die weiterführende fachliche Darstellung der Fachwendung verzichtet.~~

~~Die E-Rezept-Stufe 1 umfasst noch keine Komfort-QES-Funktionen (z.B. zur Einstellung von E-Rezepten in den E-Rezept-Fachdienst).~~

Der Anbieter bzw. Betreiber des Fachdienstes E-Rezept ist in das übergreifende TI-ITSM einzubinden und muss die für ihn in der weiteren Spezifikation definierten betrieblichen Anforderungen erfüllen. Insbesondere muss er einen 24/7 TI-ITSM-Teilnehmer-Support bereitstellen. Darüber hinaus muss er sicherstellen, dass im Störungsfall den Nutzern der Anwendung ein wirksamer 24/7 Support zur Verfügung steht.

Die Fachanwendung E-Rezept muss insgesamt hochverfügbar sein und die Anwendungsfälle für die Nutzer jederzeit wahrnehmbar performant verarbeiten. Zur Wahrnehmung der betrieblichen Aufgaben der gematik ist eine angemessene Überwachung des Fachdienstes und seiner Anwendungsfälle durch die gematik zu ermöglichen.

~~2.4.11 Anwendungsübergreifender Umfang~~

~~2.4.11.1 Identity Provider~~

~~2.4.11.1.1 Authentifizierung als anwendungsübergreifender Dienst~~

~~Die sichere Authentifizierung der Nutzer der TI ist eine für alle Anwendungen benötigte Funktion. Daher liegt es nahe, diese Funktion als anwendungsübergreifenden Dienst (Identity Provider, kurz IdP) in der TI zu etablieren, um Wiederverwendung, Einheitlichkeit und Modularisierung zu unterstützen.~~

~~**Fachliche Darstellung**~~

- ~~Anwendungen können die Authentifizierung als Dienst einbinden, sodass sich der umzusetzende Funktionsumfang der Anwendung reduziert. Das E-Rezept soll in diesem Zusammenhang die erste Anwendung sein, weitere sollen folgen.~~
- ~~Mit der Auslagerung der Authentifizierung vereinfachen sich Test und Zulassung einer Anwendung.~~
- ~~Die Entkopplung der Authentifizierung von der Fachlogik ermöglicht es, Anwendungen unabhängig vom verwendeten Authentifizierungsverfahren zu entwickeln.~~

- Die Entkopplung ermöglicht es außerdem, in Folge-Releases neue Authentisierungslösungen einfacher zu integrieren und allen Anwendungen zur Verfügung zu stellen.

2.4.1.21.1.1.1 Nutzer-Komfort

Der IdP soll den Komfort für den Nutzer erhöhen, indem die Anmeldung mit möglichst einfachen Mitteln und nur so oft wie nötig erfolgen muss.

Fachliche Darstellung

- Der IdP schafft die Voraussetzung für Single Sign-On, wodurch der Nutzer sich nur so oft authentisieren muss wie unbedingt nötig.
- Der IdP ermöglicht es, neben einer Smart Card in Folge-Releases alternative Authentisierungsverfahren anzubieten, die für den Nutzer einen höheren Komfort bieten.

2.4.1.31.1.1.1 Kompatibilität

Der IdP muss den Betrieb bestehender Dienste und Anwendungen weiter ermöglichen und mit aktuell in der TI genutzten Standards kompatibel sein.

Fachliche Darstellung

- Der IdP muss mit den bereits vorhanden PKI-Diensten der TI integrierbar sein.
- Der IdP muss auf Standards und Produkten basieren, die im e-Health-Bereich verbreitet oder zumindest leicht integrierbar sind.
- Der IdP muss in Folge-Releases die Integration vorhandener IdP-Lösungen ermöglichen.
- Der IdP muss in Folge-Releases eine Interoperabilität mit weiteren Anwendungen ermöglichen.
- Der IdP muss in Folge-Releases eine Interoperabilität mit der elektronischen Patientenakte ermöglichen.

2.4.1.41.1.1.1 Zukunftssicherheit

Der IdP sollte auf Standards und Produkten aufbauen, die nicht nur aktuell etabliert sind, sondern auf absehbare Zeit ihre Relevanz behalten, um unnötige kostenintensive Umstellungen auf andere Technologien zu vermeiden.

Fachliche Darstellung

- Der IdP muss auf Standards aufbauen, die im e-Health-Bereich etabliert sind und auf absehbare Zeit ihre Bedeutung behalten werden.
- Der IdP muss unterschiedliche Deployment-Modelle der nutzenden Anwendungen ermöglichen, insbesondere native Clients im dezentralen Bereich sowie Applikationsserver im zentralen Bereich.
- Der IdP muss gleichermaßen mobile wie nicht-mobile Anwendungen ermöglichen.
- Der IdP muss in Folge-Releases eine geeignete Basis für die Entwicklung einer zukünftigen neuen TI-Zugangslösung bieten.

- Der IdP muss in Folge-Releases eine geeignete Basis für den Aufbau eines zukünftigen, nationalen oder EU-weiten föderierten Identity Managements bieten.

2.4.1.51.1.1.1 Sicherheit und Datenschutz

Der Zugriff auf sensible und schützenswerte Daten oder Funktionen erfolgt in der Regel erst nach einer sicheren Authentifizierung des Nutzers. Der IdP muss daher entsprechende Anforderungen bezüglich Datenschutz und Informationssicherheit erfüllen.

Fachliche Darstellung

- Im Sinne der Privacy by Design stellt der IdP einer Anwendung nur diejenigen Identitätsattribute bereit, die diese auch tatsächlich benötigt.
- Im Sinne der Privacy by Design kann eine Anwendung für einzelne Anwendungsfälle vorgeben, welche Identitätsattribute der IdP bereitstellt.
- Der IdP bietet dem Nutzer die Möglichkeit, seine Sitzungen jederzeit zu beenden.
- Der IdP bietet dem Administrator die Möglichkeit, Sitzungen eines Nutzers zu beenden.
- Der IdP ermöglicht es einer Anwendung, das Sicherheitsniveau der Authentifizierung vorzugeben und abzufragen.
- Der IdP weist nicht zugelassene oder als nicht sicher attestierte Versionen des auf dem Gerät des Versicherten betriebenen Authentisierungsmodul ab.

2.4.1.61.1.1.1 Betrieb

Der IdP wird für neue oder weiterentwickelte Anwendungen als Authentisierungsdienst Voraussetzung für deren Nutzung und muss daher sicher, zuverlässig, hoch verfügbar und performant in der TI betrieben werden.

Der IdP wird ein eigenes Authentisierungsmodul für Client-Systeme herstellen und anbieten.

Fachliche Darstellung

Zur Überprüfung der Betriebssicherheit wird der IdP

- bei jedem (Erst-)Aufruf eines Authentisierungsmodul und
- bei jedem (Erst-)Aufruf eines Clients (Token-Anforderung)

die Version des Authentisierungsmoduls bzw. Clients und den Erfolg oder Nicht-Erfolg des Aufrufes protokollieren. Das Protokoll ist mindestens tagesaktuell an die Betriebsdatenschnittstelle zu liefern. Eine Protokollierung personenbezogener oder personenbeziehbarer und medizinischer Daten sowie die Möglichkeit einer Profilbildung ist auszuschließen.

Zur betrieblichen Steuerung erhebt der IdP Performance-Rohdaten und liefert diese in konfigurierbarer Frequenz an die Betriebsdatenschnittstelle.

2.4.2 Verzeichnisdienst (VZD)

Der Verzeichnisdienst (VZD) wird für die Fachanwendung E-Rezept von Versicherten zur Suche von Apotheken zur Abgabe der auf der Verordnung ausgestellten Arzneimittel

genutzt. Der Zugriff erfolgt dabei aus dem Internet über das E-Rezept-Frontend des Versicherten. Der Dienst muss daher auch an der neuen Schnittstelle sicher, zuverlässig, hoch verfügbar und performant in der TI betrieben werden.

Fachliche Darstellung

Zur Überprüfung der Betriebssicherheit wird der VZD bei jedem Aufruf das aufrufende E-Rezept FdV inkl. Version und den Erfolg oder nicht-Erfolg des Aufrufes protokollieren und das Protokoll mindestens tagesaktuell an die Betriebsdatenschnittstelle liefern. Eine Protokollierung personenbezogener oder personenbeziehbarer und medizinischer Daten sowie die Möglichkeit einer Profilbildung ist auszuschließen.

2.4.3 Anbindung neuer Berufsgruppen an die TI

Mitarbeiterinnen und Mitarbeiter in Institutionen neuer Nutzergruppen möchten die Anwendungen der Telematikinfrastruktur nutzen, um eine bessere Patientenversorgung zu ermöglichen und durch digitale Anwendungen den Arbeitsalltag zu erleichtern.

So müssen durch Festlegungen des § 352 PDSG einige neue Berufsgruppen technisch in der Lage sein, auf Dokumente und Datensätze der ePA zuzugreifen und diese zu verarbeiten, insofern sie dafür vom Versicherten berechtigt worden sind.

Fachliche Darstellung

Für die folgenden Berufsgruppen bzw. Nutzerkreise sind die technischen Voraussetzungen für den Zugang zur Telematikinfrastruktur zu schaffen, um diesen die Nutzung der Fachanwendungen zu ermöglichen.

Neue Berufsgruppen bzw. Nutzerkreise gemäß § 352 PDSG:

- Gesundheits- und Krankenpflegerinnen und Gesundheits- und Krankenpfleger
- Gesundheits- und Kinderkrankenpflegerinnen und Gesundheits- und Kinderkrankenpfleger
- Altenpflegerinnen und Altenpfleger
- Pflegefachfrauen und Pflegefachmänner sowie Pflegehilfskräfte
- Hebammen und Entbindungspfleger
- Physiotherapeutinnen und Physiotherapeuten
- berufsmäßige Gehilfen von Ärzten, Zahnärzten und Psychotherapeuten oder zur Vorbereitung auf den Beruf bei genannten Heilberuflern Tätige in Vorsorge- oder Rehabilitationseinrichtungen nach § 107 Absatz 2 SGB V oder bei einem Leistungserbringer der medizinischen Rehabilitation des SGB VI oder der Heilbehandlung einschließlich medizinischer Rehabilitation des SGB VII
- Ärzte und Ärztinnen und berechtigte Personen in Behörden des Öffentlichen Gesundheitsdienstes
- Fachärztinnen und Fachärzte für Arbeitsmedizin und Betriebsärztinnen und Betriebsärzte

Berufsgruppen bzw. Nutzerkreise, für deren Anbindung an die TI nach § 340 Absatz 3 PDSG die gematik die elektronischer Heilberufs- und Berufsausweise sowie die Komponenten zur Authentifizierung von Leistungserbringerinstitutionen (SMC-B) ausgeben muss:

- ~~Apotheker und berechtigtes pharmazeutisches Personal in EU-Versandapotheken~~
- ~~berechtigte Berufsgruppen in Eigeneinrichtungen der Krankenkassen nach § 140 SGB V (z.B. Centrum für Gesundheit der AOK Nordost)~~
- ~~Ärzte, Zahnärzte und Psychotherapeuten und deren berufsmäßige Gehilfen im Sanitätsdienst der Bundeswehr~~
- ~~(zukünftig werden weitere Nutzerkreise zu berücksichtigen sein)~~

~~Berufsgruppen bzw. Nutzerkreise gemäß dem Gesetz zur Reform der Notfallversorgung § 133b Absatz 4:~~

- ~~berechtigte Mitarbeiter von Rettungsleitstellen~~

~~Die anwendungsspezifischen Berechtigungskonzepte sind dann zu berücksichtigen, wenn darauf aufbauend spezifische Vorgaben für identitätsbezogene Datenstrukturen für die genannten Berufsgruppen zu entwickeln sind.~~

~~Randbedingungen~~

~~Die notwendigen Voraussetzungen für die Nutzung der Anwendungen der Telematikinfrastruktur durch die oben genannten Berufsgruppen umfassen:~~

- ~~technische Voraussetzungen gemäß § 311 PDSG für die Anbindung der jeweiligen Institutionen an die Telematikinfrastruktur und den Zugriff der dort Tätigen auf medizinische Daten~~

a) ~~organisatorische Voraussetzungen für die Ausgabe elektronischer Heilberufs- und Berufsausweise und Komponenten zur Authentifizierung von Leistungserbringerinstitutionen (SMC-B) durch die gematik gemäß § 340 Absatz 3 PDSG.~~

~~zu a): Konzepte und Spezifikationen der gematik enthalten anwendungsübergreifend alle notwendigen funktionalen und technischen Vorgaben für Herausgeber und Anbieter von Heilberufs- und Berufsausweise und/oder Komponenten zur Authentifizierung von Leistungserbringerinstitutionen (SMC-B) als Grundlage entsprechender Herausgabeverfahren, inklusive Zertifikatsprofile, OIDs und angepasste Zulassungs- und Bestätigungsverfahren der betroffenen Produkt- und Anbietertypen.~~

~~zu b): Die Herausgabe von Komponenten zur Authentifizierung von Leistungserbringerinstitutionen (SMC-B) und elektronischen Heilberufs- und Berufsausweise kann erfolgen, mindestens ein Anbieter ist vertraglich gebunden und alle erforderlichen Antrags-, Freigabe und Sperrprozesse sind definiert.~~

~~Weitere Quellen~~

~~Referentenentwurf PDSG § 312 Aufträge an die Gesellschaft für Telematik~~

~~Referentenentwurf PDSG § 311 Aufgaben der Gesellschaft für Telematik~~

~~Referentenentwurf PDSG § 340 Ausgabe von elektronischen Heilberufs- und Berufsausweisen sowie von Komponenten zur Authentifizierung von Leistungserbringerinstitutionen~~

~~Referentenentwurf PDSG § 342 Angebot und Nutzung der elektronischen Patientenakte~~

~~Referentenentwurf PDSG § 352 Verarbeitung von Daten in der elektronischen Patientenakte durch Leistungserbringer und andere zugriffsberechtigte Personen~~

~~Gesetz zur Reform der Notfallversorgung § 133b Gemeinsames Notfallleitsystem~~

2.4.41.1.1 Betriebliche Regelungen

2.4.4.11.1.1.1 Erfassung und Lieferung technischer Performance-Rohdaten

Die Lieferung betrieblicher Performance-Kennzahlen (Produkt-Performance, Produkt-Verfügbarkeit) erfolgt vom Anbieter eines zugelassenen Produktes bisher in Form monatlicher Zustellungen aggregierter Performance- und Service-Level-Berichte. Parallel dazu sind bisher von den betroffenen Produkttypen aggregierte Performancedaten in einer 5-Minuten-Frequenz an die Störungsampel der TI zu senden.

Aufgrund der zahlreichen Erschwernisse, Ungenauigkeiten und technischen Probleme sowie der mangelnden automatisierten Verwertbarkeit der Daten, die diese Lieferungen in der betrieblichen Praxis gezeigt haben, wurde beginnend mit dem Release 3.0 für neue Produkt- und Anbietertypen die Erhebung und Lieferung von Performance-Rohdaten verpflichtend. Ziel dieser Rohdaten-Lieferungen ist es, mit einer automatisierten Erhebung und Lieferung der Daten ohne weitere Aggregation eine störungsresistente und verlässliche Datenquelle zu schaffen, auf derer Basis eine automatisierte Verifizierung, Auswertung und Darstellung betrieblicher Steuerungsgrößen flexibel und tagesaktuell sowie zielgruppengenau möglich ist.

Fachliche Darstellung

Seit Release 3.1 werden auch bestimmte bereits bestehende Produkttypen verpflichtet, Rohdaten zu liefern. Mit Release 4.0 werden für die Produkt- und Anbietertypen KOM-LE und VPN-Zugangsdienst (inkl. Intermediär) die Erhebung und Lieferung von Rohdaten verpflichtend. Im Gegenzug entfallen die Lieferung von Daten an die Störungsampel und die Lieferung der monatlichen Performance- und Service-Level-Berichte. Die erhobenen Performance-Rohdaten sind vom Anbieter in einer frei konfigurierbaren Frequenz an die definierte Betriebsdatenschnittstelle zu liefern.

2.4.4.2 Erfassung von Aufruf-Protokolldaten von Diensten mit Internetschnittstelle

Mit Einführung der Fachanwendungen elektronische Patientenakte und E-Rezept wird für Versicherte und deren Vertreter die Nutzung von Anwendungen der Telematikinfrastruktur auf ihren eigenen Endgeräten möglich. Da die Nutzung vornehmlich auf mobilen Geräten erfolgen wird, erstellt die gematik die Rahmenbedingungen für die Entwicklung und für die Zulassung entsprechender Produkte. Zur Gewährung eines sicheren und stabilen Betriebes der Fachanwendungen, deren Nutzung aus dem Internet heraus erfolgt, wird es notwendig, betriebliche Informationen über die verwendeten Produkte, deren Produktversionen und über die Häufigkeit der Nutzung zu erhalten, unabhängig von der sicherheitstechnischen Absicherung der Internetschnittstellen. Daher wird eine Protokollierungspflicht relevanter betrieblicher Informationen für die betroffenen Dienste und Komponenten der Telematikinfrastruktur eingeführt.

Die Protokollierungspflicht erfolgt zur Sicherung und Stabilität des TI-Regelbetriebs. Zur Wahrnehmung dieses gesetzlichen Auftrags ist es notwendig, bei geplanten Abkündigungen zugelassener Produktversionen oder aufgrund kurzzeitig umzusetzender Sicherheitserfordernisse einen Überblick über die im Feld befindlichen Produkte und die Häufigkeit ihrer Nutzung zu erhalten (z.B. Nachhalten und Erfolg der Außerbetriebnahme abgekündigter oder veralteter Produktversionen).

Eine Protokollierung personenbezogener oder personenbeziehbarer Daten sowie von medizinischen Daten ist auszuschließen. Darunter fallen auch netzwerktechnische Informationen (z.B. IP-Adressen). Eine Profilbildung ist ebenfalls auszuschließen.

Fachliche Darstellung

Die Dienste der TI, welche über eine Internetschnittstelle Nutzern für Anwendungen der TI Funktionen bereitstellen, müssen die Aufrufe, die über diese Schnittstelle an den Dienst gelangen, protokollieren und die Protokolle automatisiert an die gematik übermitteln. Die Protokolle sind so zu gestalten, dass sie zur Aufnahme weiterer Daten erweiterbar sind. Sie enthalten in einem ersten Schritt Informationen über die für den Aufruf von den Nutzern verwendeten Produkte (Primärsysteme, FdVs) und deren Versionen sowie über den Erfolg/Nicht-Erfolg der Aufrufe. Zugelassene Produkte und deren Versionen müssen einwandfrei identifiziert werden können. Die Protokolle sind vom jeweiligen Anbieter tagesaktuell an die für Betriebsdaten definierte Lieferschnittstelle zu liefern.

Die Pflicht zur Erhebung und Lieferung der Protokolle wird ab Release 4.0 für die Produkt- und Anbietertypen Identity Provider (IdP), E-Rezept-Fachdienst und Verzeichnisdienst verpflichtend eingeführt.

2.4.5 1.1.1 Übergreifende Datenschutz- und Sicherheitsregelungen

2.4.6 Durchführung regelmäßiger Schwachstellenscans

Motivation und Mehrwert

Das Monitoring der TI-Dienste mittels Schwachstellenscans ist ein essentielles Element, um den gesetzlichen Auftrag der gematik zum sicheren Betrieb der TI zu erfüllen und präventiv Sicherheitslücken wie beispielsweise Fehlkonfigurationen am Dienst zu identifizieren und anschließend eine Behebung zu ermöglichen.

Fachliche Darstellung

Zur Durchführung eines Schwachstellenscans an einem Dienst ist die Kenntnis aktueller IP-Adressen und fully qualified domain names (FQDNs) von Diensten der TI unablässig. Aus diesem Grund ist ein Mechanismus zu etablieren, der die gematik in die Lage versetzt das Monitoring auf Basis der aktuellen IP-Adressen und FQDNs aller Dienste durchzuführen. Dieser Mechanismus muss für alle Dienste der TI etabliert werden, um ein vollständiges Sicherheitslagebild der TI zu erhalten. Um das Sicherheitslagebild mittels regelmäßiger (i. d. R. monatlich) Schwachstellenscans zu erhalten, bedarf es einer Anforderungsgrundlage zur Duldung der Schwachstellenscans durch den Anbieter.

Somit muss die gematik in die Lage versetzt werden

- aktuelle IP-Adressen und FQDNs aller Dienste der TI zu kennen
- regelmäßige Schwachstellenscans an Diensten mit einer TI-Außenschnittstellen durchführen zu können.

3 Überblick über die Telematikinfrastruktur

Die folgenden Abschnitte bieten einen Überblick über die Anwendungen der Telematikinfrastruktur. Für jede Anwendung werden dargelegt:

- die grundlegende Beschreibung der Funktion,
- die grobe Aufteilung der Funktionen auf dezentrale Anteile, ggf. zentrale Fachdienste und zentrale anwendungsübergreifende Dienste,
- die verfügbaren Zugänge (Frontend des Versicherten, Primärsystem, …)
- die genutzten Smart Cards und
- wo die Fachdaten der Anwendung gespeichert werden (Dienst oder Smart Card).

Außerdem wird pro Anwendung aufgezeigt, wo das Systemdesign ggf. neue oder veränderte Anwendungsanteile, inklusive betroffener anwendungsübergreifender Dienste, mit sich bringt.

Technische und betriebliche Details zu Veränderungen und Neuerungen an Produkt- oder Anbietertypen einzelner Anwendungen oder Dienste finden sich ggf. in den jeweiligen vertiefenden Abschnitten in Kapitel 4.

3.1 Anwendungen des Versicherten

Die Nutzung der Anwendungen der TI durch den Versicherten (oder dessen Vertreter) kann in einigen Anwendungsfällen in der Leistungserbringerumgebung unter Nutzung der dort vorhandenen Primärsysteme und Komponenten erfolgen.

Für die Nutzung außerhalb der Leistungserbringerumgebung besteht für den Versicherten und seinen Vertreter zudem die Möglichkeit, über ein eigenes Gerät (z.B. PC, Handy) in seiner persönlichen Umgebung auf die Anwendungsfunktionen zuzugreifen (Frontend des Versicherten).

Im Sinne der Diskriminierungsfreiheit soll der Versicherte (Vertreter) Anwendungen allerdings auch nutzen können, wenn er sich nicht in der Leistungserbringer-Umgebung befindet und auch nicht über ein eigenes Gerät verfügt. Dazu wird ihm – typischerweise von den Krankenversicherungen – mit dem KTR-AdV-Terminal eine eigens vorgesehene Hardware bereitgestellt.

Alle diese Anwendungsfälle werden als Anwendungen des Versicherten (AdV) zusammengefasst.

3.1.1 Funktionsüberblick

Bei den AdV ist zwischen zwei Funktionsbereichen zu unterscheiden:

1. **Fachanwendungsspezifische Funktionen**

   Fachanwendungsspezifische Funktionen sind Funktionen, die den Fachanwendungen (siehe Abschnitte 3.2 bis 3.7) zuzurechnen sind. Sie werden nachfolgend in den entsprechenden Abschnitten näher beschrieben.

2. AdV-Kernfunktionen

Zu den AdV-Kernfunktionen zählen allgemeine Funktionen, die nicht Teil der zuvor erwähnten Fachanwendungen sind (siehe auch Abbildung 4, linke Seite). Dazu zählen u.a.:

- Protokolldaten-Management – das Einsehen des Protokolls auf der eGK, um Zugriffe auf Daten der eGK nachvollziehen zu können.
- PIN-Management – Ändern/Entsperren der PIN der eGK, Aktivieren/Deaktivieren für Fachanwendungen.
- Gültigkeitsprüfung der eGK.

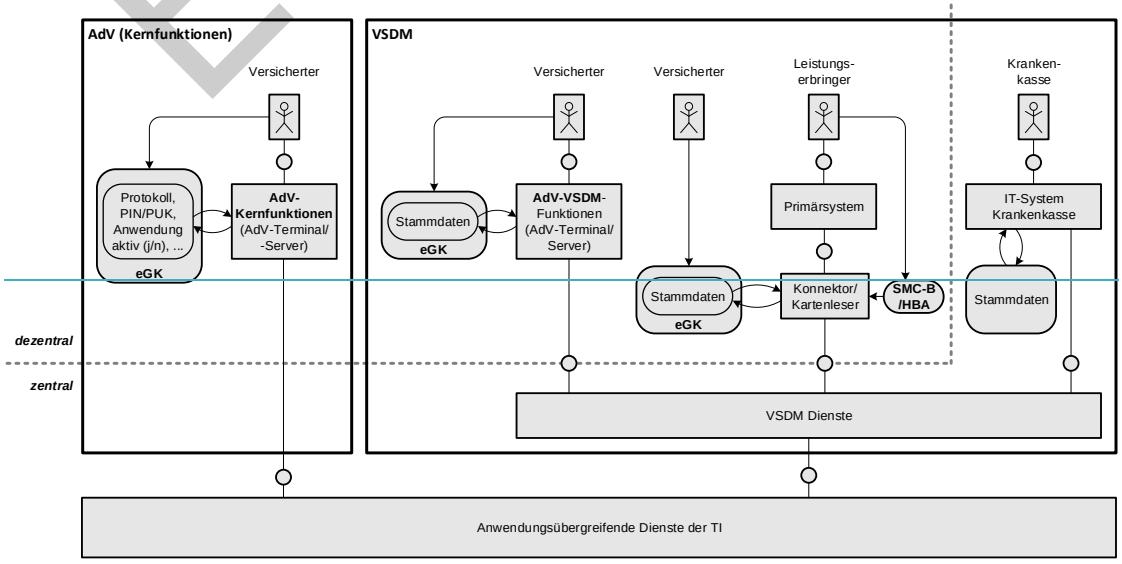
3.1.2 Neuerungen im Systemdesign

Im Rahmen des Releases werden Funktionen der ePA mittels KTR-AdV-Terminal nutzbar gemacht (s. auch Kapitel 3.5). Diese Neuerung betrifft jedoch nicht die AdV-Kernfunktionen, sondern sind ausschließlich anwendungsspezifisch.

3.2 Versicherten-Stammdatenmanagement

3.2.1 Funktionsüberblick

Das Versicherten-Stammdatenmanagement (VSDM) dient primär der Erleichterung des Praxisbetriebs durch die Bereitstellung aktueller digitaler Stammdaten des Versicherten (siehe Abbildung 4, rechte Seite). Der Versicherte stellt mit seiner eGK die darauf befindlichen Stammdaten in der Leistungserbringerumgebung bereit. Der Zugriff muss durch eine SMC-B oder einen HBA freigeschaltet werden. Die Stammdaten können nun via Konnektor/Kartenleser eingelesen und im Primärsystem verarbeitet werden. Um sicher zu stellen, dass diese Daten aktuell sind, bietet das VSDM zentrale Dienste an, die einen Abgleich mit den bei der gesetzlichen Krankenversicherung geführten Stammdaten durchführen. Stimmen die auf der eGK gespeicherten Daten nicht überein, so erfolgt deren Aktualisierung basierend auf den Stammdaten der Krankenkasse. Die Gültigkeit der eGK und der Versichertenstatus werden ebenfalls geprüft. Zugriffe auf die Stammdaten werden auf der eGK protokolliert.



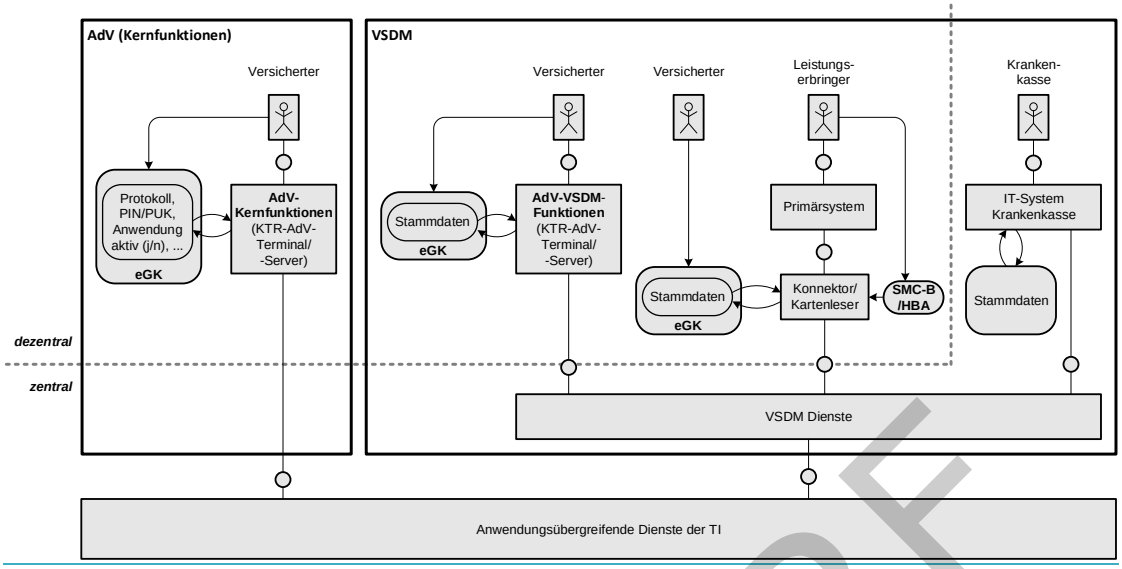


Abbildung 4: Funktionaler Aufbau der AdV-Kernfunktionen und des Versicherten-Stammdatenmanagements (VSDM)

Für den Versicherten besteht im Rahmen der Anwendungen des Versicherten (siehe auch 3.1) die Möglichkeit, VSDM-Funktionen unter Verwendung eines KTR-AdV-Terminals zu nutzen – siehe Abbildung 4. Damit kann er die Stammdaten auf seiner eGK über die VSDM-Dienste einsehen und ggf. aktualisieren. Auch hier erfolgt eine Protokollierung der Zugriffe auf der eGK.

3.2.2 Neuerungen im Systemdesign

Das Versicherten-Stammdatenmanagement bleibt gegenüber dem letzten Release unverändert.

3.3 Notfalldaten-Management

3.3.1 Funktionsüberblick

Mit dem Notfalldaten-Management (NFDM) können Leistungserbringer wichtige medizinische Notfalldaten (NFD) direkt auf der eGK speichern, sofern der Versicherte (oder Vertreter) dem zustimmt. Dies erfolgt mittels Primärsystem. Der Zugriff auf die eGK per Konnektor/Kartenleser muss hierfür per HBA/SMC-B freigeschaltet werden – siehe Abbildung 5, linke Seite. In einer Notsituation, z.B. wenn ein Patient ins Krankenhaus eingeliefert wird, können Ärzte darauf zugreifen. Im Notfalldatensatz können folgende Informationen gespeichert werden:

- Diagnosen, chronische Erkrankungen und frühere Operationen
- regelmäßig eingenommene Medikamente
- Allergien und Unverträglichkeiten
- weitere wichtige medizinische Hinweise (z. B. Schwangerschaft oder Implantate)
- Kontaktdaten von Angehörigen und behandelnden Ärzten, die im Notfall benachrichtigt werden sollen.

Des Weiteren können Informationen zum Aufbewahrungsort für folgende persönliche Erklärungen via Datensatz Persönliche Erklärung (DPE) gespeichert werden:

- Organspendeausweis,
- Patientenverfügung und
- Vorsorgevollmacht.

Für den Versicherten besteht im Rahmen der Anwendungen des Versicherten (siehe auch 3.1) die Möglichkeit, NFDM-Funktionen unter Verwendung eines KTR-AdV-Terminals zu nutzen (siehe Abbildung 5). Dazu gehören:

- NFD auf der eGK verbergen oder sichtbar machen
- DPE auf der eGK verbergen oder sichtbar machen
- DPE bearbeiten (anzeigen, ändern, löschen).

3.3.2 Neuerungen im Systemdesign

Die Anwendung NFDM bleibt gegenüber dem letzten Release unverändert.

3.4 Elektronischer Medikationsplan/Arzneimittel-Therapiesicherheit

3.4.1 Funktionsüberblick

Sofern der Versicherte dem zustimmt, kann ein Leistungserbringer Medikationsdaten sowie medikationsrelevante Daten (z.B. Allergien oder Nierenfunktionswerte) eines Versicherten direkt auf der Karte speichern. Dieser somit erstellte elektronische Medikationsplan (eMP) kann von anderen Leistungserbringern ausgelesen werden, sodass diese bspw. über die medikamentöse Therapie informiert sind. Mögliche Wechselwirkungen der Arzneimittel können so berücksichtigt und die Arzneimittel-Therapiesicherheit (AMTS) erhöht werden. Der E-Medikationsplan enthält folgende Daten:

- Patientenstammdaten, wie Name~~, Adresse~~ und Geburtsdatum (bereits über VSDM erfasst)
- medikationsrelevante Daten, wie Allergien und Unverträglichkeiten und medizinische Individualparameter des Versicherten (z. B. Gewicht, Kreatinin-Wert)
- Angaben zur Medikation, d. h. alle verordneten und frei verkäuflichen Arzneimittel, die ein Patient einnimmt inkl. Informationen zur Anwendung
- Hinweise und Informationen der beteiligten Heilberufler zum interprofessionellen Informationsaustausch (z.B. Hinweise zur gewählten Medikation)
  - Kommentarfeld zum Medikationseintrag
  - übergeordneter Kommentar zum gesamten Medikationsplan.

Das Anlegen und Auslesen dieser Daten erfolgt über die Primärsysteme der Leistungserbringer. Hierzu muss der Zugriff auf die eGK per Konnektor/Kartenleser und HBA/SMC-B freigeschaltet werden (siehe nachfolgende Abbildung, rechte Seite).

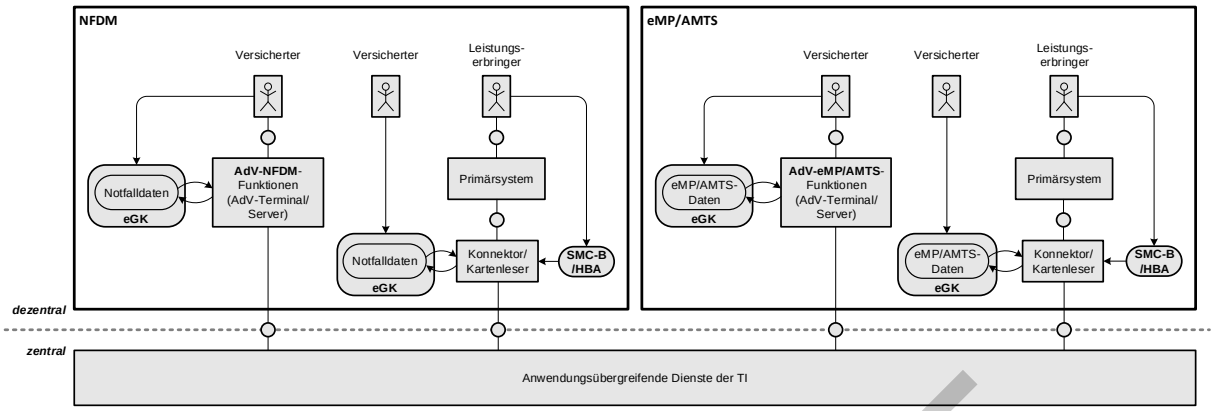


Abbildung 5: Funktionaler Aufbau der ~~fachanwendungsspezifischen Funktionen~~Fachanwendungen NFDM und eMP/AMTS

Für den Versicherten besteht im Rahmen der Anwendungen des Versicherten (AdV, siehe auch 3.1) die Möglichkeit, Funktionen zu eMP/AMTS unter Verwendung eines KTR-AdV-Terminals zu nutzen – siehe Abbildung 5,, AdV-eMP/AMTS-Funktionen. Dazu gehören:

- eMP/AMTS-Daten auf der eGK verbergen oder sichtbar machen
- Vertreter-PIN auf der eGK entsperren oder ändern. Der Versicherte kann auf diese Weise einem Vertreter den Zugriff auf die eMP/AMTS-Daten ermöglichen.

3.4.2 Neuerungen im Systemdesign

Die Anwendung eMP/AMTS bleibt gegenüber dem letzten Release unverändert.

3.5 Elektronische Patientenakte

3.5.1 Funktionsüberblick

Mit der elektronischen Patientenakte (ePA) können medizinische Dokumente zwischen dem Versicherten und von ihm berechtigten Leistungserbringern ausgetauscht werden (siehe Abbildung 6). Durch die ePA kann ein berechtigter Leistungserbringer schneller auf bereits vorhandene medizinische Unterlagen zugreifen und somit den Versicherten gezielter und effizienter behandeln. Die ePA steht dabei unter der Kontrolle des Versicherten, der bestimmen kann, welche Inhalte darin liegen und wem diese zur Verfügung gestellt werden. Zugriffe auf die ePA werden protokolliert, damit der Versicherte diese nachvollziehen kann.

Die berechtigte Krankenkasse kann dem Versicherten via ePA Dokumente bereitstellen, ohne jedoch Zugriff auf ~~die anderen~~ Daten in der ePA zu haben. Die Anbindung erfolgt dabei über den KTR-Consumer.

Leistungserbringer können über ihr Primärsystem auf die ePA zugreifen, wobei dazu eine Authentisierung per ~~HBA/~~SMC-B – mittels Konnektor/Kartenleser – erfolgen muss und zusätzlich noch eine Berechtigung seitens des Versicherten benötigt wird. Letztere vergibt dieser zeitlich befristet und bestätigt diese durch Stecken seiner eGK und Eingabe seiner PIN~~.~~, insofern die Berechtigung nicht schon mittels ePA-FdV oder ePA-FdV AdV erteilt wurde. Leistungserbringer können, abhängig von ihrer Berechtigung:

- Berechtigungen für den Zugriff auf Dokumente vom Versicherten anfordern

- Dokumente suchen, hochladen, herunterladen oder löschen
- ~~die Klassifizierung~~Attribute eines Dokuments beim Wiedereinstellen ändern
- ~~das Übertragungsprotokoll (Primärsystem) einsehen~~

Der Versicherte kann in der Leistungserbringerumgebung:

- Leistungserbringer für den Zugriff auf Dokumente berechtigen
- Ein vom Anbieter bereitgestelltes Aktenkonto aktivieren

Der Versicherte kann mit dem Frontend des Versicherten (ePA-FdV) auf seinem geeigenten eigenen Gerät auf seine ePA zugreifen. Dazu muss er sich mit seiner eGK oder alternativen Versichertenidentität authentisieren. Mit dem ePA-FdV kann er:

- Ein vom Anbieter bereitgestelltes Aktenkonto aktivieren oder schließen
- Den Wechsel des Anbieters seiner ePA vorbereiten
- Dokumente suchen, hochladen, herunterladen oder löschen
- Berechtigungen für Leistungserbringer einsehen, vergeben und entziehen
- Vertreter einrichten
- Das Protokoll der ePA einsehen
- Die Umschlüsselung durchführen

Für den Versicherten besteht im Rahmen der Anwendungen des Versicherten (AdV, siehe auch 3.1) die Möglichkeit, ePA-Funktionen unter Verwendung eines KTR-AdV-Terminals zu nutzen – siehe Abbildung 6, AdV-ePA-Funktionen. Dazu gehören:

- Ein vom Anbieter bereitgestelltes Aktenkonto aktivieren oder schließen
- Den Wechsel des Anbieters seiner ePA vorbereiten
- Dokumente suchen, ansehen oder löschen
- Berechtigungen für Leistungserbringer einsehen, vergeben und entziehen
- Vertreter einrichten
- Das Protokoll der ePA einsehen
- Die Umschlüsselung durchführen

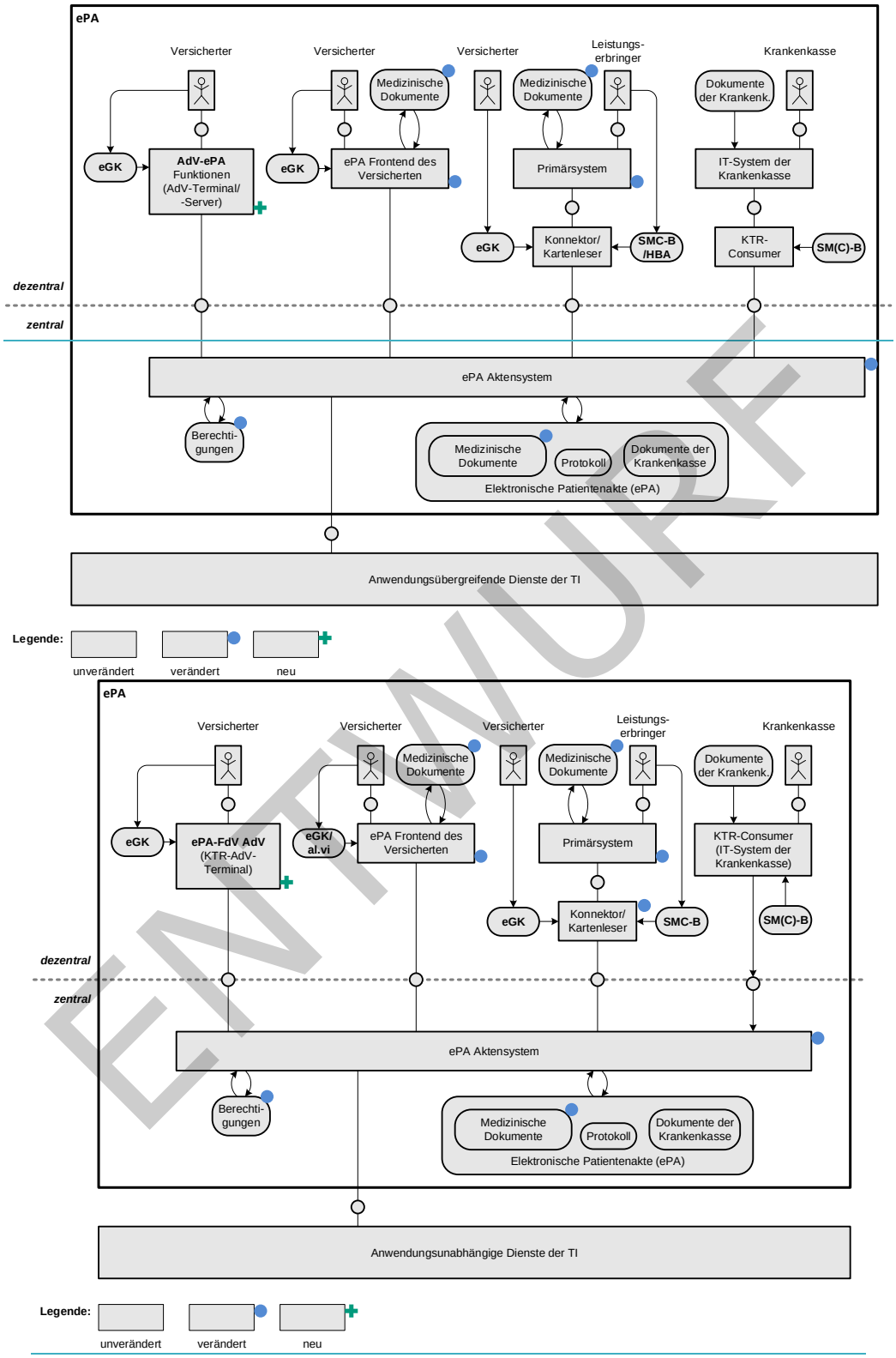


Abbildung 6: Funktionaler Aufbau der ~~fachanwendungsspezifischen Funktion~~Fachanwendung ePA

3.5.2 Neuerungen im Systemdesign

Mit dem aktuellen Systemdesign ergeben sich bei der ePA einige Änderungen, siehe auch die grafischen Markierungen in Abbildung 6:

Neue Anteile:

- ePA-Funktionen im KTR-AdV-Terminal

  Die ePA soll ab Stufe 2.0 auch über die Anwendungen des Versicherten nutzbar sein, d.h. über das KTR-AdV-Terminal. Die dazu erforderlichen Funktionen (AdV-ePA-Funktionen) werden neu eingeführt.

Veränderte Anteile:

- Fachdienste

  Das Aktensystem muss für verschiedene Funktionserweiterungen (siehe 2.2) – z.B. die ~~feingranularen~~verfeinerte Berechtigungen und die neuen strukturierten Dokumententypen – angepasst werden.

- dezentrale Komponenten

  Die verschiedenen Funktionserweiterungen (siehe 2.2) der ePA erfordern außerdem Anpassungen an Primärsystemen, ePA-Fachmodul des Konnektors und dem Frontend des Versicherten.

3.6 Kommunikation Leistungserbringer

3.6.1 Funktionsüberblick

Die Fachanwendung Kommunikation Leistungserbringer (KOM-LE) ermöglicht Leistungserbringern, Leistungserbringerorganisationen (LEO) und Krankenkassen einen sicheren Versand digitaler Nachrichten und Dokumente. KOM-LE basiert auf E-Mail und ergänzt Funktionen für Signatur, Verschlüsselung und das Versenden großer Dokumenten-Anhänge.

Leistungserbringer greifen auf die Anwendung über ein Primärsystem zu, dabei erfolgt eine Authentisierung per SMC-B/HBA über Konnektor/Kartenleser. Krankenkassen und LEO können mittels eigener, über KTR- oder Basis-Consumer an die TI angebundene IT-Systeme, die Anwendung nutzen. Hier kommt eine SMC-B (oder SM-B) für die Authentisierung zum Einsatz.

Für den Versand einer KOM-LE-Nachricht werden vom Sender ein oder mehrere Empfänger ausgewählt. Die Nachricht (und ggf. zugehörige Anhänge) werden auf dem Clientsystem des Senders mit der Sender-Identität signiert (per SMC-B) und für jeden Empfänger verschlüsselt. Erst danach erfolgt die Übertragung zum KOM-LE-Dienst, von wo ein Empfänger die Nachricht abrufen kann. Auf dem lokalen Client-System des Empfängers erfolgt dann die Entschlüsselung (per SM(C)-B oder HBA) und die Prüfung der Signatur.

KOM-LE nutzt anwendungsübergreifende Dienste, insbesondere den Verzeichnisdienst zum Auffinden von Empfängern („Adressbuch-Funktion").

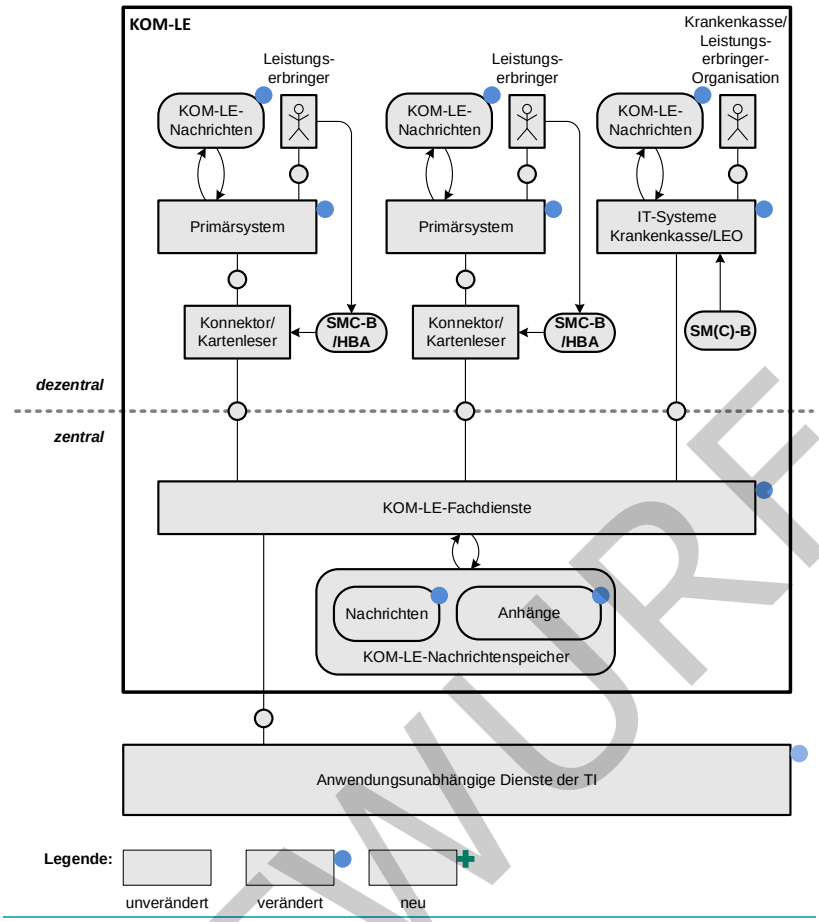


Abbildung 7: Funktionaler Aufbau der Fachanwendung KOM-LE 1.5

3.6.2 Neuerungen im Systemdesign

Veränderte Anteile:

- Flexibilisierung der Integration in Primärsysteme

  Herstellern von Primärsystemen wird es ermöglicht, die Funktionen des KOM-LE-Clientmoduls eigenständig zu entwickeln und entweder als eigenständiges KOM-LE-Clientmodul zuzulassen oder direkt in ihr PS zu integrieren.

- Nachrichtenkategorien

  Die für KOM-LE 1.5 eingeführten Nachrichtenkategorien erfordern Anpassungen an den Client-Systemen (LEO/Krankenkasse und Primärsystem).

- Große Anhänge bis 500 MB

  KOM-LE 1.5 ermöglicht außerdem den Versand von Anhängen bis 500 MB. Auch hier werden Anpassungen an den Client-Systemen und dem Fachdienst KOM-LE erforderlich.

~~3.6~~3.7 Elektronisches Rezept

~~3.6.1~~3.7.1 Funktionsüberblick

Das elektronische Rezept bietet als neue Anwendung erstmals die Möglichkeit, Verordnungen in digitaler Form auszustellen, dem Versicherten zu übergeben und bei einer Apotheke einzulösen. Rezepte werden dazu in einem neuen Fachdienst gespeichert, der auch Zugriffe protokolliert (siehe Abbildung 8). Der Fachdienst speichert neben den eigentlichen Rezeptdaten auch den Bearbeitungsstatus des Rezeptes. Für den Zugriff auf Rezeptdaten eines bestimmten Rezeptes im Fachdienst wird ein Token (E-Rezept-Token) benötigt, welches außerhalb des Fachdienstes weitergegeben werden kann.

Der Leistungserbringer kann mit seinem Primärsystem ein elektronisches Rezept erstellen und im E-Rezept-Fachdienst ablegen. Für den Zugriff auf den Dienst wird eine Authentisierung per SMC-B benötigt; die Signatur des Rezeptes erfolgt via HBA. Wenn der Versicherte die Informationen des elektronischen Rezeptes nicht selbst vom Fachdienst lädt, bleibt die Möglichkeit bestehen, das Rezept als Papierausdruck auszuhändigen, welcher eine codierte Darstellung des E-Rezept-Tokens (Data Matrix Code) enthält. Die Leistungserbringer haben außerdem die Möglichkeit, E-Rezepte zu löschen, z.B. wenn sie versehentlich falsch ~~erstellte Rezepte zu stornieren~~erstellt wurden.

Der Versicherte kann die eigentlichen Rezeptdaten vom Fachdienst mit dem FdV abrufen. Dazu muss er sich beim Dienst mit seiner eGK anmelden. Der Versicherte kann über das E-Rezept-FdV Angaben anzeigen ~~und stornieren~~, E-Rezepte löschen sowie das Protokoll einsehen. Außerdem bietet es die Möglichkeit, den Rezept-Token optisch an das Primärsystem des abgebenden Leistungserbringers (Apotheker) oder das FdV eines anderen Versicherten zu übergeben, damit dieser es als Vertreter bei einer Apotheke einlösen kann. Optional bleibt auch der Papierausdruck für die Übergabe des Rezept-Tokens an eine Apotheke bestehen.

Der abgebende Leistungserbringer nutzt sein Primärsystem für den Zugriff auf Rezeptdaten im Fachdienst. Dazu muss er sich per SMC-B authentisieren und über das entsprechende Rezept-Token im Primärsystem verfügen. Um ggf. ~~Anpassungen am Rezept~~im Rahmen der Abgabe Ergänzungen vornehmen und signieren (QES) zu können, benötigt auch der abgebende Leistungserbringer seinen HBA. Nach Abgabe der verordneten Arzneimittel wird der Status des Rezeptes im Fachdienst vermerkt und eine Quittung für Abrechnungsprozesse ~~erzeugt (diese Prozesse sind~~(Prozess ist nicht Gegenstand der Anwendung~~).~~) erzeugt. Der abgebende Leistungserbringer kann bei Bedarf ein elektronisches Rezept stornieren.

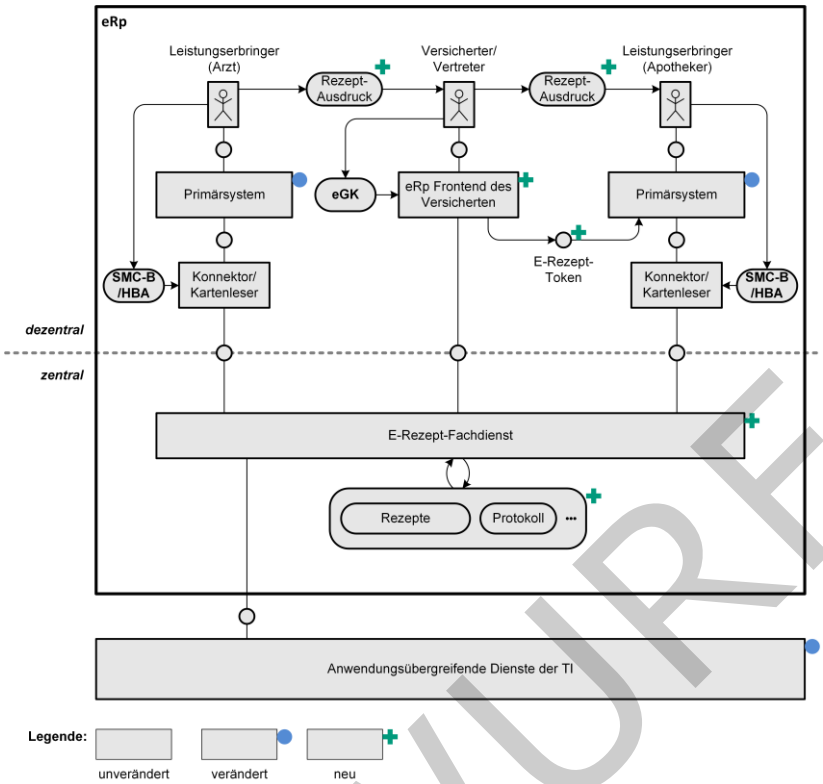


Abbildung 8: Funktionaler Aufbau der ~~fachanwendungsspezifischen Funktion~~Fachanwendung elektronisches Rezept

~~3.6.2~~3.7.2 Neuerungen im Systemdesign

Neue Anteile:

- E-Rezept als neue Fachanwendung

  Das E-Rezept wird erstmalig mit dem vorliegenden Systemdesign eingeführt. Daher werden die meisten Anteile neu eingeführt. Dies umfasst das E-Rezept-FdV sowie den E-Rezept-Fachdienst.

Veränderte Anteile:

- Erweiterung der Primärsysteme

  Für die Nutzung der E-Rezept-Funktionen durch die Leistungserbringer müssen die Primärsysteme erweitert werden.

- Erweiterungen bei den anwendungsübergreifenden Diensten und dezentralen Komponenten

Als neuer anwendungsübergreifender Dienst wird der Identity Provider eingeführt. Im dezentralen Bereich wird das Authentisierungsmodul eingeführt, welches den Identity Provider ergänzt. (Diese Anteile werden zunächst für die Anwendung E-Rezept benötigt.)

Der Verzeichnisdienst wird so angepasst, dass das Frontend des Versicherten darauf sicher zugreifen kann. Außerdem werden die Einträge der abgebenden Leistungserbringer für die Suche seitens der Versicherten um Informationen erweitert.

3.71.1 Kommunikation Leistungserbringer

3.7.11.1.1 Funktionsüberblick

Die Fachanwendung Kommunikation Leistungserbringer (KOM-LE) ermöglicht Leistungserbringern, Leistungserbringerorganisationen (LEO) und Krankenkassen einen sicheren Versand digitaler Nachrichten und Dokumente. KOM-LE basiert auf E-Mail und ergänzt Funktionen für Signatur, Verschlüsselung und das Versenden großer Dokumenten-Anhänge.

Leistungserbringer greifen auf die Anwendung über ein Primärsystem zu, dabei erfolgt eine Authentisierung per SMC-B/HBA über Konnektor/Kartenleser. Krankenkassen und LEO können mittels eigener, über KTR- oder Basis-Consumer an die TI angebundene IT-Systeme, die Anwendung nutzen. Hier kommt eine SMC-B (oder SM-B) für die Authentisierung zum Einsatz.

Für den Versand einer KOM-LE-Nachricht werden vom Sender ein oder mehrere Empfänger ausgewählt. Die Nachricht (und ggf. zugehörige Anhänge) werden auf dem Clientsystem des Senders mit der Sender-Identität signiert (per SMC-B) und für jeden Empfänger verschlüsselt. Erst danach erfolgt die Übertragung zum KOM-LE-Dienst, von wo ein Empfänger die Nachricht abrufen kann. Auf dem lokalen Client-System des Empfängers erfolgt dann die Entschlüsselung (per SM(C)-B oder HBA) und die Prüfung der Signatur.

KOM-LE nutzt anwendungsübergreifende Dienste, insbesondere den Verzeichnisdienst zum Auffinden von Empfängern („Adressbuch-Funktion").

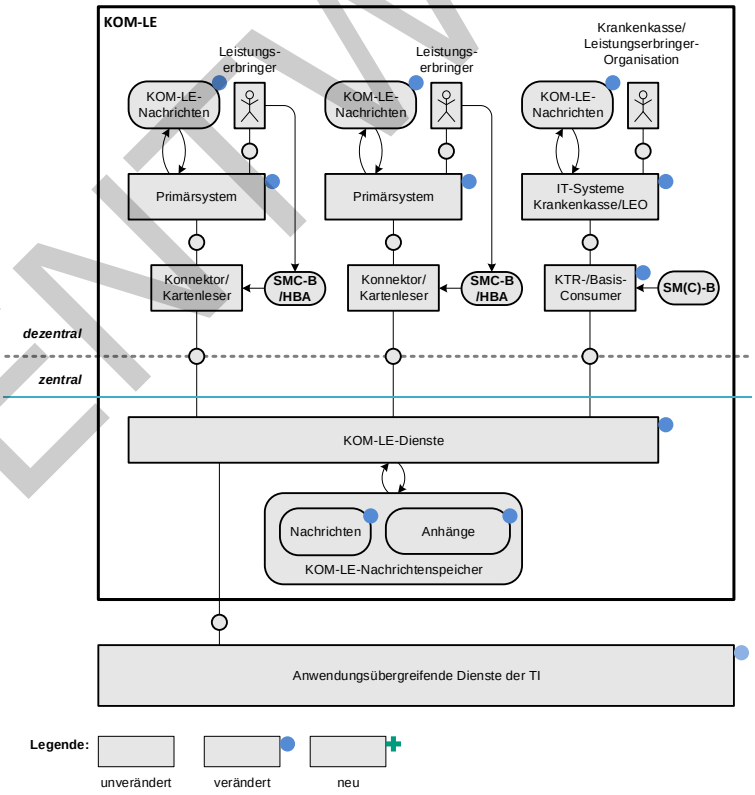


Abbildung 5: Funktionaler Aufbau der fachanwendungsspezifischen Funktion KOM-LE 1.5

~~3.7.21.1.1 Neuerungen im Systemdesign~~

~~Veränderte Anteile:~~

- ~~Flexibilisierung der Integration in Primärsysteme~~

  ~~Herstellern von Primärsystemen wird es ermöglicht, die Funktionen des KOM-LE-Clientmoduls eigenständig zu entwickeln und in ihr PS zu integrieren.~~

- ~~Nachrichtenkategorien~~

  ~~Die für KOM-LE 1.5 eingeführten Nachrichtenkategorien erfordern Anpassungen an den Client-Systemen (LEO/Krankenkasse und Primärsystem), außerdem am Fachdienst KOM-LE und den anwendungsübergreifenden Diensten.~~

- ~~Große Anhänge bis 200 MB~~

  ~~KOM-LE 1.5 ermöglicht außerdem den Versand von Anhängen bis 200 MB. Auch hier werden Anpassungen an den Client-Systemen und dem Fachdienst KOM-LE erforderlich.~~

3.8 Weitere elektronische Anwendungen

Weitere elektronische Anwendungen des Gesundheitswesens sowie für die Gesundheitsforschung sind elektronische Anwendungen im Gesundheitswesen, die die elektronische Gesundheitskarte nicht nutzen und außerhalb der Gesellschaft für Telematik entwickelt werden, insbesondere Anwendungen, die in SGB V und SGB XI geregelt sind.

Die weiteren Anwendungen werden hier nicht betrachtet.

3.9 Anwendungsübergreifende Dienste und dezentrale Komponenten

Die folgenden anwendungsübergreifenden Dienste sind im Systemdesign enthalten:

- Signaturdienst
- Identity Provider
- Zeitdienst
- Namensdienst
- Konfigurationsdienst (KSR)
- Service Monitoring
- Schlüsselgenerierungsdienst Typ 2
- Verzeichnisdienst
- TSP-X.509 nonQES
- TSP-X.509 QES
- TSL-Dienst
- OCSP-Proxy
- VPN-Zugangsdienst
- Sicherheitsgateway Bestandsnetze

- gematik Root-CA
- CVC-Root
- TSP-CVC

Die folgenden dezentralen Komponenten sind im Systemdesign enthalten:

- Authentisierungsmodul
- Konnektor
- eHealth-Kartenterminal
- MobKT (Mobiles Kartenterminal)
- eGK (elektronische Gesundheitskarte)
- HBA (Heilberufsausweis)
- SMC-B/SM-B
- SMC-B Org / SM-B Org
- SMC-B KTR / SM-B KTR
- g-SMC-K
- g-SMC-KT
- KOM-LE Client-Modul
- KTR-Consumer
- Basis-Consumer
- KTR-AdV
- KTR-AdV-Terminal

4 Umsetzung des fachlichen Umfangs

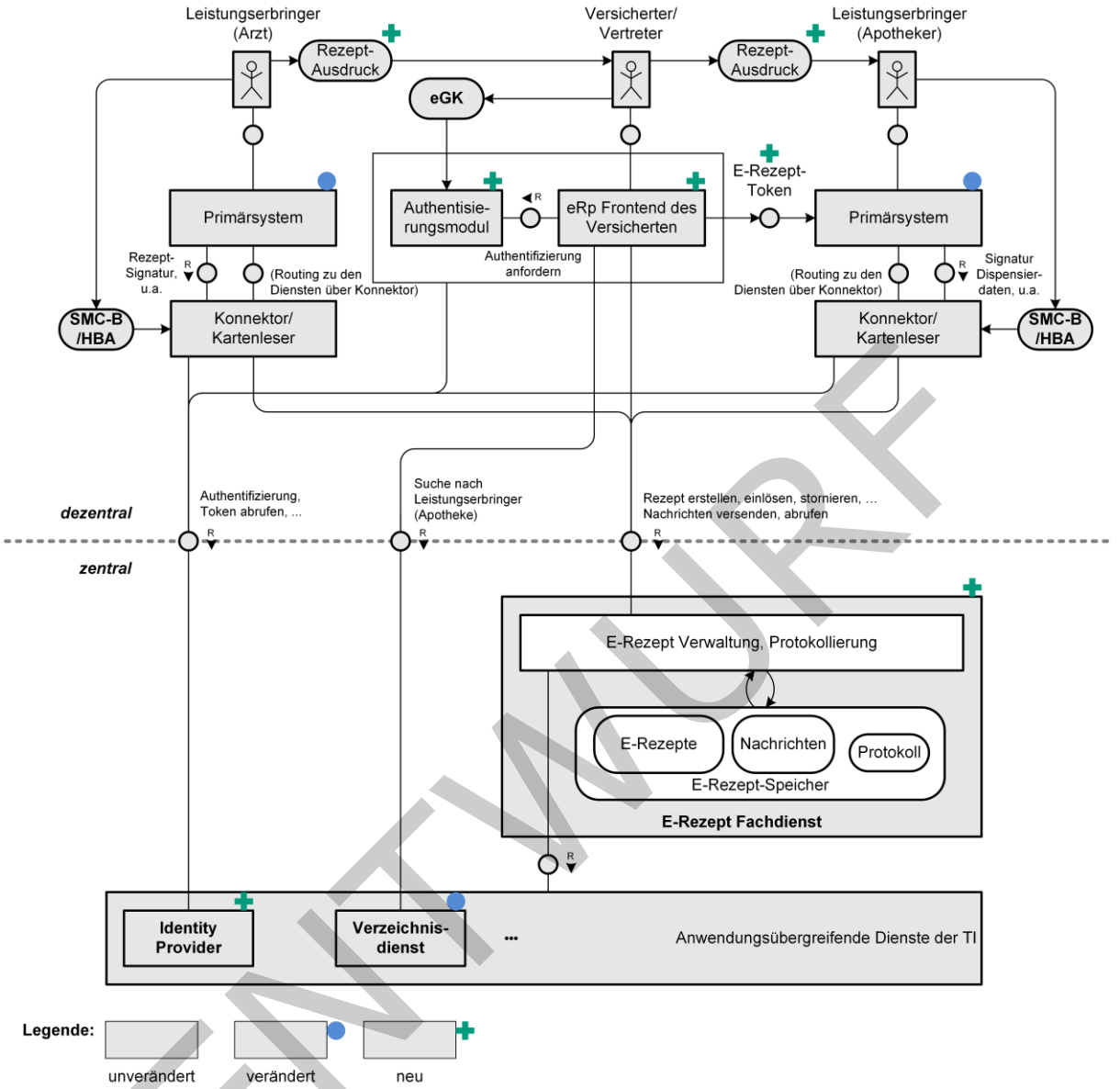
Dieses Kapitel stellt dar, in welcher Weise die in Kapitel 2 beschriebenen fachlichen Neuerungen und Anpassungen auf Systemebene technisch umgesetzt werden. Die Darstellung fokussiert auf neue oder angepasste Anwendungen und die wesentlichen Neuerungen. Dabei werden auch betroffene Produkt- oder Anbietertypen aufgezeigt sowie Aspekte zu Betrieb, Sicherheit, Datenschutz und Zulassung betrachtet. Eine Übersicht über alle Produkt- und Anbietertypen zu diesem Systemdesign bietet Kapitel 5.

4.1 Anwendungsübergreifender Umfang

~~4.1.1 E-Rezept~~

~~4.1.1.1 Aufbau und Funktionsweise~~

~~Der technische Aufbau der Fachanwendung E-Rezept und die dazu gehörigen Abläufe werden im Dokument [gemSysL_eRp] beschrieben. Daher wird im Folgenden auf eine detailliertere technische Beschreibung der Fachanwendung bzw. des E-Rezept-Fachdienst verzichtet. Eine Übersicht über den logischen Aufbau der zusammenwirkenden Komponenten gibt Abbildung 6:~~



~~Abbildung 6: Funktionaler Aufbau der fachanwendungsspezifischen Funktion E-Rezept~~

~~Zur Umsetzung der Anwendungsfälle wird neben dem neuen E-Rezept-Fachdienst auch ein weiterer neuer Dienst Identity Provider (IdP) benötigt. Dieser wird in Kapitel 4.4.1 dieses Dokumentes beschrieben.~~

~~Vom Ablauf her erstellt der verordnende Leistungserbringer für einen Versicherten ein E-Rezept, welches auf dem zentralen E-Rezept-Fachdienst abgelegt wird. Der Standardfall sieht vor, dass der Versicherte seine E-Rezepte mit dem E-Rezept-FdV auf seinem technischen Endgerät verwaltet. Zur Authentisierung nutzen Versicherte bzw. deren Vertreter in der ersten Ausbaustufe NFC-fähige eGKs und NFC-fähige Endgeräte. Der Versicherte kann über sein Frontend im Verzeichnisdienst die Apotheke seiner Wahl aussuchen und sie für die Abgabe der ausgestellten Arzneimittel berechtigen. Die Zugriffs-Berechtigung auf das E-Rezept erfolgt mittels einer elektronischen Übertragung eines für das E-Rezept ausgestellten E-Rezept-Tokens durch den Versicherten an die Apotheke. Für Versicherte ohne eigenes Endgerät bzw. ohne NFC-fähige eGK wird vom verordnenden~~

~~Leistungserbringer der E-Rezept-Token als 2D-Code sowie beschreibende Rezept-Daten ausgedruckt, mit denen sich der Versicherte an eine Apotheke seiner Wahl wenden kann.~~

~~In der E-Rezept-Version 1.0 (Release 4.0) ist eine direkte Kommunikation zwischen dem Versicherten und Apotheken über das E-Rezept vorgesehen (eine im E-Rezept-Fachdienst integrierte Kommunikationsfunktion). Rückfragen zwischen dem abgebenden und dem verordnenden Leistungserbringer können unabhängig davon über KOM-LE erfolgen.~~

~~In der Apotheke wird die Abgabe der Arzneimittel auch elektronisch auf dem E-Rezept-Fachdienst vollzogen und quittiert.~~

~~Die Umsetzung von Komfort-QES-Signatur-Funktionen folgt in einem folgenden Release.~~

~~Versicherte haben jederzeit die Hoheit über auf sie ausgestellte E-Rezepte, da jeglicher Zugriff auf ein konkretes Rezept im E-Rezept-Fachdienst entweder nur den Versicherten selbst, ihren Vertreter oder Apotheken möglich ist, die den entsprechenden E-Rezept-Token erhalten haben.~~

~~4.1.21.1.1 Sicherheit und Datenschutz~~

~~Da der E-Rezept-Fachdienst den Zugriff auf personenbezogene medizinische Daten ermöglicht, ist er bei den Schutzzielen Vertraulichkeit und Integrität mit einem Schutzbedarf von sehr hoch bewertet. Insbesondere dürfen die im E-Rezept-Fachdienst verarbeiteten personenbezogenen Daten nicht zu unzulässigen Verarbeitungszwecken verwendet werden.~~

~~Zur Einhaltung der Vorschriften des Datenschutzes ist technisch sicherzustellen, dass beim E-Rezept-Fachdienst keine Profilbildung erfolgen kann.~~

~~Der Schutzbedarf für die Verfügbarkeit des E-Rezept-Fachdienstes ist hoch.~~

~~Der E-Rezept-Fachdienst erkennt die von dem E-Rezept-FdV mitgeteilte Versionsnummer und kann festgelegte Versionsnummern abweisen (bspw. abgekündigte Versionen oder Versionen mit erheblichen Sicherheitslücken).~~

~~4.1.31.1.1 Betrieb~~

~~Der E-Rezept-Fachdienst ist nur einmalig in der TI vorhanden und wird als neue Servicekomponente in das übergreifende TI-ITSM integriert. Für den Dienst ist aus Akzeptanz- und Versorgungsgründen eine sehr hohe Verfügbarkeit erforderlich, unterteilt nach Haupt- und Nebenzeit.~~

~~Operative Betriebsleistungen werden anhand eines entsprechenden Anbietertypsteckbriefs durch einen von der gematik beauftragten Dienstleister erbracht. Bei Bedarf koordiniert der Anbieter des E-Rezept-Fachdienstes im Rahmen des TI-ITSM alle E-Rezept-fachanwendungsspezifischen Incidents.~~

~~Leistungserbringer können sich im Störungsfall an den User Help Desk des sie betreuenden VPN-Zugangsdienstes wenden. Versicherte wenden sich an einen von der gematik beauftragten Dienstleister, der den User Help Desk für das E-Rezept für Versicherte bereitstellt.~~

~~Zur Überprüfung der Betriebssicherheit wird der E-Rezept-Fachdienst sämtliche mit einem Authentisierungstoken erfolgten Aufrufe durch Client-Systeme zur Identifikation der aufrufenden Client-Systeme und deren Versionen protokollieren und das Protokoll mindestens tagesaktuell an die Betriebsdatenschnittstelle liefern. Unautorisierte Zugriffe werden abgelehnt, die Ablehnung ist ebenfalls zu protokollieren.~~

Zur betrieblichen Steuerung hat der E-Rezept-Fachdienst Performance-Rohdaten zu erheben und in konfigurierbarer Frequenz an die Betriebsdatenschnittstelle zu liefern.

4.1.41.1.1 Zulassungsverfahren der Anwendung

Der Hersteller des Produkttyps E-Rezept-Fachdienst bedarf einer Produktzulassung. Die operativen Betriebsleistungen des Fachdienstes E-Rezept werden von einem durch die gematik beauftragten Dienstleister erbracht. Eine formale Anbieterzulassung nach Anbietertypsteckbrief ist daher nicht vorgesehen.

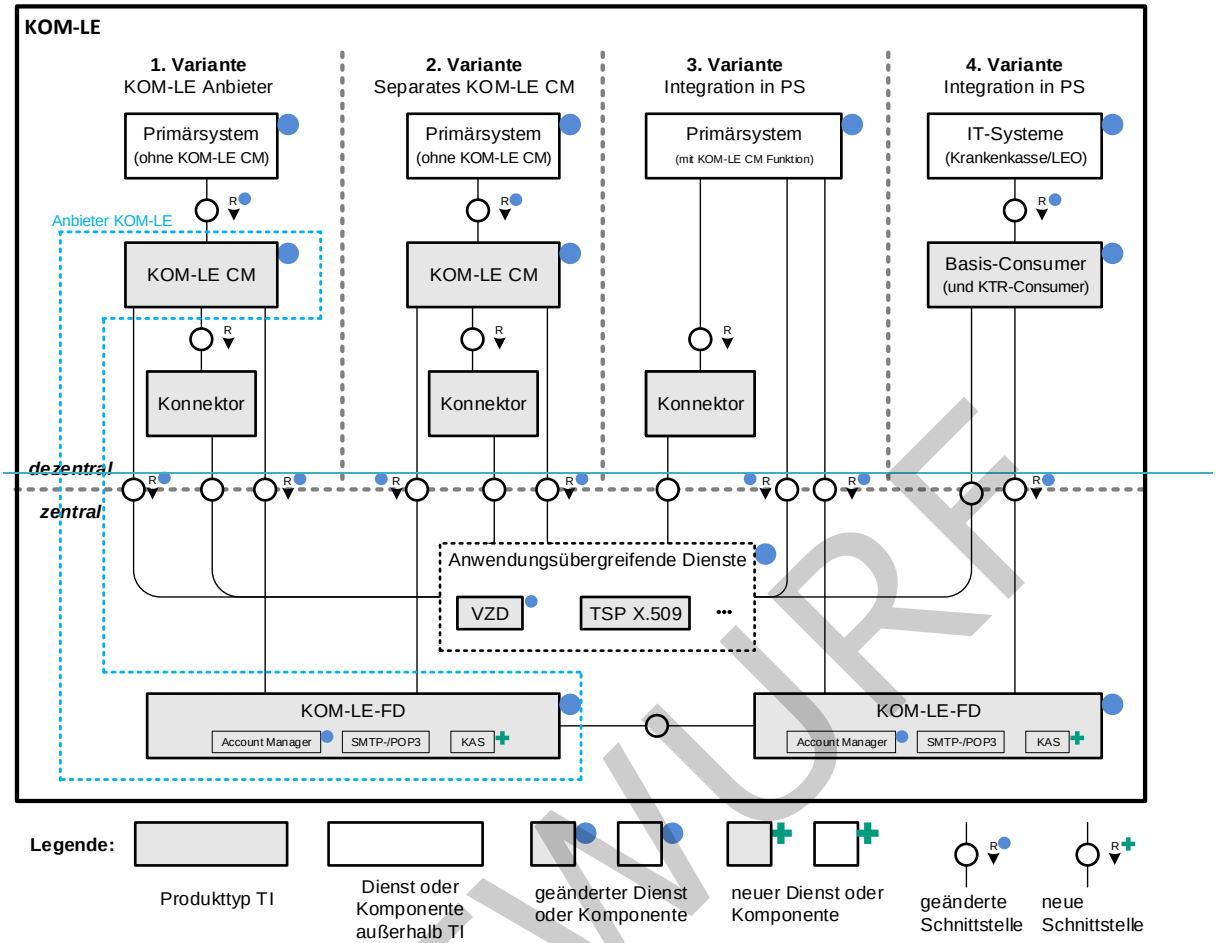
4.2 KOM-LE

4.2.1 Übersicht der Änderungen

Mit KOM-LE 1.5 wird im Release 4.0 der in Kapitel 2.2 definierte fachliche Umfang zusätzlich zu KOM-LE 1.0 (Release 2.1) umgesetzt:

- Flexibilisierung der Integration in Primärsysteme
- Übermittlung von großen Dokumenten bis zu 200 MB
- Unterstützung von Nachrichten-Kategorien

Abbildung 7 zeigt die von den Änderungen betroffenen Produkttypen der TI und der angrenzenden IT-Systeme.



~~**Abbildung 7: Übersicht über Neuerungen für KOM-LE 1.5 inklusive Produkttypen**~~

~~4.2.1.11.1.1.1 Flexibilisierung der Integration in Primärsysteme~~

~~Um es Herstellern von Primärsystemen zu ermöglichen, die Funktionen des KOM-LE-Clientmoduls eigenständig zu entwickeln und in ihr PS zu integrieren, werden folgende Änderungen für KOM-LE 1.5 durchgeführt:~~

~~1. Auf eine Produktzulassung des KOM-LE-Clientmoduls (nach [gemZul_Prod_KOM-LE]) wird verzichtet. Es verbleibt die Produktzulassung des KOM-LE-Fachdienstes.~~

~~2. Für den Produkttyp KOM-LE-Clientmodul wird ein Bestätigungsverfahren eingeführt, welches Hersteller von KOM-LE-Clientmodulen durchlaufen müssen.~~

~~3. Ein KOM-LE-Anbieter (entsprechend [gemZUL_Anbieter] muss weiterhin, neben dem KOM-LE-Fachdienst, ein eigenständiges KOM-LE-Clientmodul umsetzen, bestätigen und für seine KOM-LE-Kunden bereitstellen.~~

~~4. Für PS-Hersteller erfolgt eine Erweiterung (neue Variante) im Bestätigungsverfahrens für KOM-LE 1.5. Falls ein PS-Hersteller die KOM-LE-Clientsystem-Funktionalität direkt in ihr PS integriert, erfolgt eine Prüfung der Funktion gegen die entsprechenden genutzten TI-Schnittstelle (u.a. Konnektor, VZD, KOM-LE-Fachdienst). Als Implementierungsleitfaden für diese Varianten dienen bezüglich der Schnittstellen zur TI die technischen Vorgaben für das KOM-LE-Clientmodul.~~

~~Für die KOM-LE Integration in die LE-Umgebung ergeben sich insgesamt die drei in Abbildung 7 dargestellten Varianten:~~

- ~~Variante 1: Das PS nutzt das vom KOM-LE Anbieter bereitgestellte und durch die gematik bestätigte KOM-LE-Clientmodul.~~
- ~~Variante 2: Das PS nutzt ein unabhängig vom KOM-LE-Anbieter entwickeltes KOM-LE-Clientmodul.~~
- ~~Variante 3: Das PS integriert im Rahmen einer Eigenentwicklung durch den PS-Hersteller die KOM-LE-Clientmodul-Funktionalität. Relevant sind hierbei lediglich die Funktionalitäten bzw. Schnittstellen des KOM-LE-Moduls Richtung TI (d.h. Richtung KOM-LE-FD, Konnektor und VZD).~~

~~Die vierte Variante aus Abbildung 7 zeigt die KOM-LE-Anbindung für Kassen und Leistungserbringerorganisationen mittels KTR-Consumer bzw. Basis-Consumer.~~

~~Die gematik empfiehlt Leistungserbringern ausdrücklich den Einsatz von durch die gematik bestätigten Primärsystemen und – falls im Einsatz – von KOM-LE-Clientmodulen.~~

~~Die technische Schnittstelle zwischen KOM-LE-Clientmodul und KOM-LE-Fachdienst bzw. Konnektor sind bereits weitgehend in KOM-LE 1.0 interoperabel spezifiziert. Lediglich die Übermittlung des Schlüssels und des TLS-Zertifikats für die beidseitig authentisierte TLS-Verbindung zwischen KOM-LE-Clientmodul und KOM-LE-Fachdienst mittels einer passwortgeschützten PKCS#12 Datei und die Übermittlung des Passworts hierfür sind nicht interoperabel spezifiziert. Dies wird in KOM-LE 1.5 soweit wie notwendig nachgeholt.~~

~~Im Rahmen der Bestätigung von KOM-LE-Clientmodulen und der Zulassung von KOM-LE-Fachdiensten sowie dem erwarteten übergangsweisen Parallelbetrieb von KOM-LE 1.0 und KOM-LE 1.5 stellt die gematik im Rahmen der nachzuweisenden eigenverantwortlichen Tests der Hersteller und der Zulassungstests der gematik eine ausreichende Interoperabilität von KOM-LE sicher.~~

~~4.2.1.2 Übermittlung von großen Dokumenten bis zu 200 MB~~

~~Aufgrund einer Limitierung im Konnektor können derzeit nur Dokumente mit einer maximalen Größe von 25 MB signiert und verschlüsselt werden. Da KOM-LE bei der Übermittlung sowohl eine Nachrichtensignatur durch den Konnektor (unter Verwendung von ID.HCI.OSIG der SMC-B des Senders) als auch eine Verschlüsselung durch den Konnektor (unter Verwendung von ID.HCI.ENC der SMC-B bzw. ID.HP.ENC des HBA der Empfänger) durchführt, ergibt sich für KOM-LE 1.0 eine übertragbare maximale Dokumenten- bzw. Nachrichtengröße von 25 MB je Nachricht (E-Mail).~~

~~Mit KOM-LE 1.5 wird der Versand von Nachrichten bis zu einer Größe von 200 MB unterstützt. Bei Nachrichten bis zu einer Größe von 25 MB wird eine vollständige Rückwärtskompatibilität zu KOM-LE 1.0 sichergestellt.~~

~~Große Dokumente werden hierzu nicht mehr über E-Mail (SMTP/POP3) übertragen, sondern zur Übermittlung sicher auf einem Speichersystem des KOM-LE-FD abgelegt. Hierzu werden bei großen Nachrichten über 25 MB, die vom PS an das KOM-LE-CM übertragen werden, alle Anhänge der E-Mail symmetrisch verschlüsselt, beim KOM-LE-FD in einer neuen Komponente KOM-LE-Attached-Service (KAS) abgelegt, und anschließend aus der E-Mail entfernt. Die Verschlüsselung der Anhänge findet über das KOM-LE-CM statt. Die Lokalisierung der Dokumente am KAS ist über eine vergebene URL möglich. In der KOM-LE E-Mail selbst wird die URL und der symmetrische Schlüssel übertragen und hierbei analog zu KOM-LE 1.0 mit den Funktionen des Konnektors mittels SMC-B signiert und mittels SMC-B bzw. HBA für den Empfänger verschlüsselt. Beim Empfang einer derartigen~~

E-Mail durch ein KOM-LE-1.5-Modul werden die über die URL verfügbaren Anhänge vom KAS geladen, entschlüsselt und als Anhang der E-Mail angehängt.

Falls die Funktionalitäten eines KOM-LE-1.5-CM direkt in das PS integriert werden (siehe Variante 3 in Kapitel 4.2.1.1) übernimmt das PS selbst die im vorhergehenden Absatz dargestellt Übermittlung der großen Nachrichten.

Im VZD wird durch den KOM-LE-Anbieter ab KOM-LE 1.5 für jeden KOM-LE-Teilnehmer die unterstützte KOM-LE Version in den fachdienstspezifischen Daten abgelegt. Anhand dieser Information kann ein PS und ein KOM-LE-CM beim bzw. vor dem Versand von großen Nachrichten erkennen, ob die Empfänger diese Nachricht auch empfangen können und eine Rückmeldung hierzu an den Nutzer geben. Das KOM-LE-CM verhindert den Versand von großen Nachrichten, falls der Empfänger nicht mindestens KOM-LE 1.5 einsetzt.

Damit auch Organisationen des Gesundheitswesens, die KOM-LE einsetzen und hierbei über den Basis-Consumer bzw. KTR-Consumer an die TI gebunden sind, die Funktionen von KOM-LE 1.5 nutzen können, werden ebenfalls Basis-Consumer und KTR-Consumer für KOM-LE 1.5 angepasst. Ein einer Übergangszeit bleiben ebenfalls Basis-Consumer und KTR-Consumer mit dem KOM-LE 1.0 Funktionsumfang gültige Zulassungsobjekte.

4.2.1.31.1.1.1 Unterstützung von Nachrichten-Kategorien

Zur Unterstützung von Nachrichten-Kategorien wird ein weiteres KOM-LE-spezifisches Attribut im E-Mail-Header aufgenommen, welches optional vom PS gesetzt werden kann. Das Attribut wird ebenfalls transparent in der äußeren KOM-LE E-Mail Nachricht übertragen, die vom KOM-LE-CM erzeugt wird. Hierdurch ist sichergestellt, dass beim Empfänger der Nachricht bereits vor dem Entschlüsseln der Nachricht eine automatische Vorverarbeitung der Nachricht möglich ist.

Die gematik pflegt eine Liste mit aktuell gültigen Kategorien und veröffentlicht diese. Änderungen zu den gültigen Kategorieneinträgen können durch die gematik und deren Gesellschafter veranlasst werden. Komponenten und Dienste der TI dürfen keine inhaltliche Prüfung der Nachrichten-Kategorien vornehmen. Für Primärsysteme können Regelungen über die PS-Implementierungsleitfäden der gematik aufgenommen werden, falls in einzelnen Anwendungsfällen spezifische Kategorien zu verwenden sind.

Durch die optionale Aufnahme der Nachrichten-Kategorie „Attribut" im E-Mail-Header ist eine vollständige Rückwärtskompatibilität zu KOM-LE 1.0 sichergestellt. KOM-LE-Fachdienste und KOM-LE-Clientmodule aus KOM-LE 1.0 leiten diese Attribut transparent weiter. Empfänger (z.B. Primärsysteme mit KOM-LE 1.0 Unterstützung und Standard-E-Mail-Clients ignorieren dieses Attribut).

4.2.2 Geänderte Komponenten, Dienste

Tabelle 1 gibt eine Übersicht der vom KOM-LE 1.5 betroffen Produkttypen, Anbietertypen und IT-Systemen.

Tabelle 1: Übersicht geänderte Komponenten und Dienste

Art	Bezeichnung	Änderung
Clientsystem	PS	• Möglichkeit zur Integration der KOM-LE-CM Funktionalität, einschl. Bestätigungsverfahren hierzu. • Bei großen (> 25 MB) KOM-LE-Nachrichten, Prüfung ob Empfänger hierzu in der Lage ist (über VZD-Eintrag) • Unterstützung von KOM-LE Nachrichten-Kategorien
Produkttyp	KOM-LE-CM	• Umgang mit großen (> 25 MB) Nachrichten beim Versand und Empfang

		• Weiterleitung der KOM-LE Nachrichten Kategorien • Bestätigungsverfahren statt Zulassungsverfahren • Anpassung, um Schnittstelle zu KOM-LE-FD vollumfänglich interoperabel auszugestalten
Produkttyp	KOM-LE FD	• Bereitstellung KOM-LE Attached Service (KAS) • Anpassung um Schnittstelle zu KOM-LE-FD vollumfänglich interoperabel auszugestalten. • Anpassungen zu betrieblichen Reporting von Kennzahlen
Anbietertyp	KOM-LE	• Bereitstellung KOM-LE-CM
Produkttyp	VZD	• Anpassung der fachdienstspezifischen Daten für KOM-LE
Produkttyp	Basis-Consumer KTR-Consumer	• Umgang mit großen Nachrichten KOM-LE-Attached-Service beim Versand und Empfang • Weiterleitung der KOM-LE-Nachrichten-Kategorien • Anpassung um Schnittstelle zu KOM-LE-FD vollumfänglich Interoperabel auszugestalten

4.2.31.1.1 Betrieb

Für den KOM-LE Fachdienst in KOM-LE 1.5 werden mit Release 4.0 neue betriebliche Kennzahlen definiert, anhand derer Last- und Performanceverhalten sowie Verfügbarkeit des Fachdienstes präziser gemessen und nachgewiesen werden. Des Weiteren wird der Fachdienst KOM-LE Messdaten erheben, welche die definierten betrieblichen Kenngrößen darstellen und in frei konfigurierbaren Zeitabständen an die Betriebsdatenschnittstelle liefern. Damit entfällt die Pflicht, Daten an die Störungsampel bzw. – an ihrer Stelle – an das TI Service Monitoring zu senden sowie die Lieferung eines monatlichen Performance-Reports. Weiterhin muss kein monatlicher Service Level Report mehr gesendet werden. Dieser wird im übergreifenden TI ITSM bereitgestellt, wobei der Anbieter KOM-LE seine Pflichten zur Messung, Übermittlung und Bewertung der Service Level Messergebnisse gemäß [gemRL_Betr_TI#Kapitel 9.2] zu erfüllen hat.

4.3 ePA

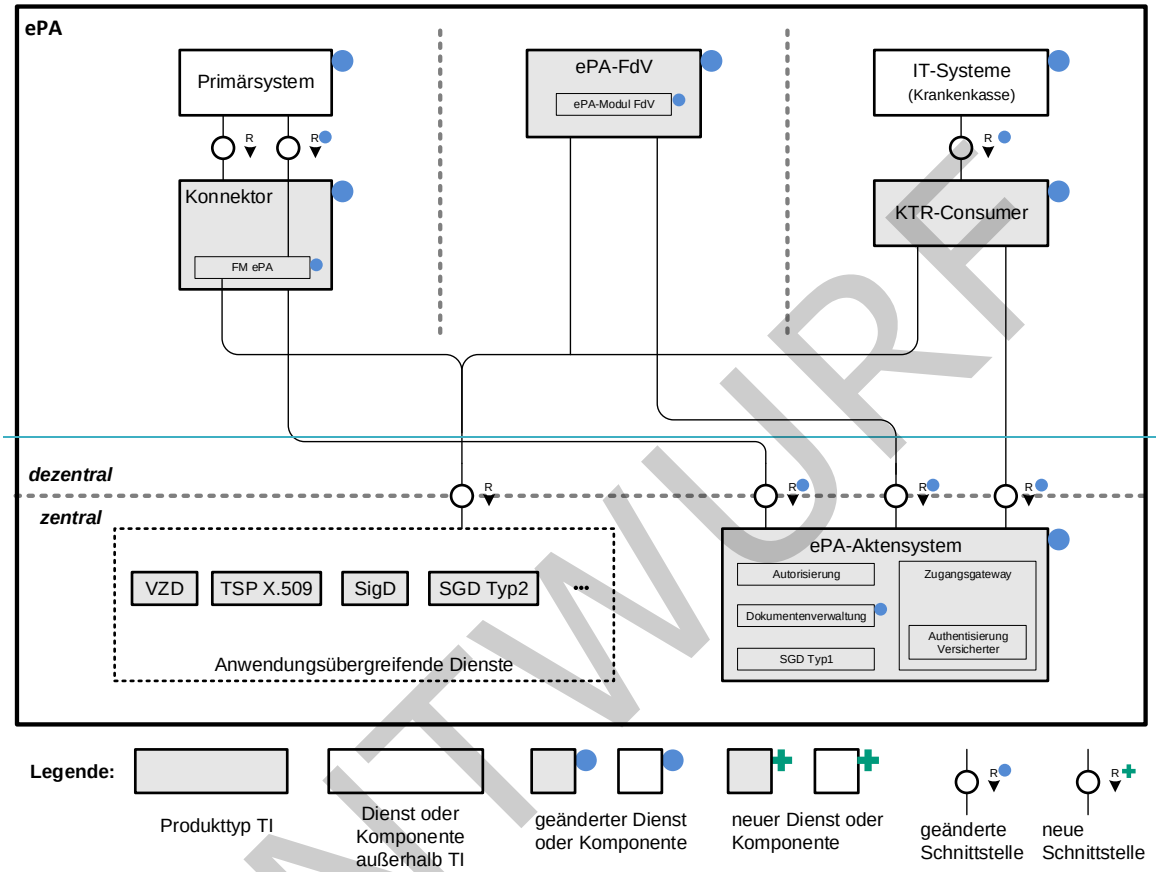
4.3.1.11.1.1.1 Übersicht der Änderungen

Mit ePA 2.0 wird im Release 4.0 der in Kapitel 2.1 definierte fachliche Umfang zusätzlich zu ePA 1.1 (Release 3.1) umgesetzt:

- Rollenprofile für Berufsgruppen
- verfeinertes Berechtigungskonzept
- Erweiterung des Datenmodells
- Elektronische Impfdokumentation
- Elektronisches Zahnbonusheft
- Elektronisches Untersuchungsheft für Kinder
- Elektronischer Mutterpass
- Releaseunabhängiges Einbringen neuer strukturierter Dokumentenformate
- Schemakonformität für strukturierte Dokumente

- ~~Rendering-Vorschriften für strukturierte Dokumente~~
- ~~Verfahren zur gezielten Umschlüsselung (Akten-/Kontextschlüssel)~~
- ~~AdV-/TI-Terminal~~

~~Abbildung 8 zeigt die von den Änderungen betroffenen Produkttypen der TI und der angrenzenden IT-Systeme.~~



~~Abbildung 8: Übersicht über von Änderungen betroffene Produkttypen der TI inkl. angrenzender IT-Systeme für ePA 2.0~~

~~4.3.1.21.1.1 Erweiterung der zugriffsberechtigten Berufsgruppen und Rollenprofile für Berufsgruppen~~

~~Die Einführung neuer zugriffberechtigter Berufsgruppen und die damit verbundene Erweiterung des Nutzerkreises der ePA muss in der Berechtigungsverwaltung des Aktensystems berücksichtigt werden. Entsprechende Policies müssen eingeführt und die Rollen der Nutzer (OIDs) ausgewertet werden.~~

~~Die Zuordnung von Berufsgruppen zu einer Leistungserbringerorganisation im Rahmen der Berechtigungsvergabe kann durch Auswertung der im VZD hinterlegten Zertifikate im Client erfolgen. Die Darstellung von erlaubten Berechtigungen für die jeweilige Berufsgruppe erfolgt im Client auf Basis des geltenden Berechtigungskonzeptes. Eine detaillierte Analyse erfolgt im Rahmen der Ausgestaltung des verfeinerten Berechtigungskonzeptes (s. Kapitel 2.1.2).~~

~~Die Umsetzung erfolgt in den gemäß Kapitel 2.1.1 beschriebenen Komponenten.~~

4.3.1.3 Verfeinertes Berechtigungskonzept

Die Abstimmungen zum verfeinerten Rechtekonzept der ePA sind auf gesetzlicher Ebene noch nicht soweit abgeschlossen, als dass eine belastbare Grundlage für eine tiefergehende fachliche und technische Analyse gegeben ist. Es bestehen zu hohe Umsetzungsrisiken.
Spätestens auf Basis des Kabinettsentwurfs des PDSG werden die entsprechenden Punkte ergänzt.

4.3.1.41.1.1.1 Passdokumente

Der Umgang mit elektronischen Passdokumenten unterliegt besonderen Rahmenbedingungen. Passdokumente sollen für den jeweiligen Zweck zu jedem Zeitpunkt in genau einer aktuell gültigen Version vorliegen (Eindeutigkeit). Es erfolgt zwar eine Versionierung, jedoch wird dem zugreifenden Nutzer zunächst nur die aktuellste Version des Dokumentes angezeigt. Es besteht aber für den Versicherten auch die Möglichkeit, Einsicht in Vorversionen zu nehmen. Infolgedessen stellt das Aktensystem die Eindeutigkeit und die Versionierung eines Passdokumentes sicher.

Um die verschiedenen Passarten im ePA-Aktensystem unterstützen zu können, werden weitere von IHE nativ unterstützte Document Associations für die Verwendung in der Fachanwendung ePA eingeführt. Die aktuell vorzusehenden Passdokumente Impfausweis, Mutterpass, Untersuchungsheft für Kinder sowie Zahnbonusheft werden inhaltlich von der KBV über FHIR-Ressourcen als XML-Dokumente definiert. Über die Metadaten sind diese Pässe im Aktensystem eindeutig auffindbar.

Darüber hinaus müssen Passeinträge aufgrund ihrer medizinischen Bedeutung authentisch und integer sein. Dies wird durch das Signieren beim Einstellen von Passeinträgen durch den Leistungserbringer und dem Prüfen der Signaturen beim Verarbeiten bzw. Anzeigen eines Passdokumentes durch das Primärsystem erreicht. Die Signaturprüfung an einem vom Versicherten genutztem Client ist nicht vorgesehen.

Die Umsetzung der Passdokumente erfolgt in den folgenden Komponenten:

Primärsystem

- Anzeige von Passdokumenten inkl. (Auslösen einer) Signaturprüfung und Transformation in ein lesbares Format
- Aktualisierung von Passdokumenten inkl. (Auslösen einer) Signatur der Einträge
- Löschen von einzelnen Einträgen

ePA-Frontend des Versicherten

- Anzeige oder Löschen von Passdokumenten
- Export von Passdokumenten

Aktensystem

- Unterstützung aller neuen Assoziationen
- Anpassung der erlaubten Value Sets
- Unterstützung von Versionierung oder Fortschreibung der Pässe

4.3.1.5 Erweiterung des Datenmodells und Migration

Um neue (z.B. durch die KBV definierte) Dokumentformate (bzw. medizinische Informationsobjekte) in der ePA verarbeiten zu können, müssen die XDS-Metadaten, d.h. die Value Sets, dynamisch erweitert werden. Die zulässigen Value Sets werden für die Hersteller an zentraler Stelle durch die gematik bereitgestellt.

Die Umsetzung strukturierter Dokumentenformate erfolgt in den folgenden Komponenten:

- Primärsysteme
- ePA-Frontend des Versicherten
- ePA-AdV-App (s. Kapitel 4.3.1.7)
- ePA-Aktensystem

Bestehende Dokumente werden inkl. Metadaten in das neue Berechtigungskonzept migriert bzw. überführt.

4.3.1.61.1.1.1 Schemakonformität und Rendering-Vorschriften für strukturierte Dokumente

Ein systemübergreifender Datenaustausch erfordert, dass alle beteiligten Systeme die prozessrelevanten Daten miteinander in geeigneter Form austauschen und verarbeiten können und insbesondere bezüglich der Daten ein gleiches Verständnis haben. Dieses einheitliche Verständnis wird durch die Vorgabe und Nutzung einheitlicher Schemata und Vorschriften erreicht.

Die Erstellung eines schemakonformen Dokumentes erfolgt, wie auch das Rendering von Dokumenten, üblicherweise in der Fachlogik des Clients, wohingegen die Prüfung eines Dokumentes auf Konformität durch den Server erfolgt. Jedoch ist die serverseitige Konformitätsprüfung durch das Aktensystem aufgrund der Ende-zu-Ende Verschlüsselung der Dokumente nicht möglich. Aus diesem Grund muss auf eine Prüfung verzichtet werden. Der Verzicht auf diese Prüfung wiederum zieht eine stärkere Fokussierung bzw. Durchsetzung der Nutzung von Schemata in den Clients nach sich, um die Verarbeitbarkeit der Dokumente von verschiedensten Clients zu gewährleisten.

Die Funktionalität *Rendering* ermöglicht es, dass allen Akteuren strukturierte Inhalte, die sie zwar aus der ePA herunterladen können, deren Format ihnen aber unbekannt ist, immer auch in mindestens einem menschenlesbaren Standardformat angezeigt werden. Das clientseitige Rendering erlaubt überdies eine endgerätespezifische Darstellung der Daten.

In diesem Zusammenhang definiert die Kassenärztliche Bundesvereinigung (KBV) medizinische Informationsobjekte (MIOs) und stellt Schemata und Rendering-Vorschriften dafür bereit. Diese werden durch die gematik für Hersteller von Clients der ePA an zentraler Stelle bereitgestellt, damit diese in die entsprechenden Produkte integriert werden können.

Desweitern können Hersteller weitere Schemata und Rendering-Vorschriften vorschlagen, die von der gematik geprüft und bereitgestellt werden.

Die Nutzung der Schemata zur Erstellung konformer strukturierter Dokumente sowie das Rendering dieser werden durch folgende Clients durchgeführt:

Primärsysteme

- ePA-Frontend des Versicherten (nur Rendering, eigenverantwortliche Schemavalidierung des Dokumentes)

- ePA-AdV-App (nur Rendering, eigenverantwortliche Schemavalidierung des Dokumentes)

Inwiefern ein Nachweis zur Einhaltung der Schemata durch den Hersteller zu erbringen ist, wird im Rahmen der Spezifikationserstellung eruiert.

4.3.1.7 1.1.1.1 Verfahren zur gezielten Umschlüsselung

Die Umschlüsselung umfasst den Wechsel folgender kryptographischer Schlüssel:

- den betreiberspezifischen Schlüssel
- den Akten- und Kontextschlüssel des Versicherten
- Dokumentenschlüssel
- die Schlüsselgenerierungsdienste SGD1- und SGD2-Schlüssel aller berechtigten Nutzer

und kann nur durch den Versicherten durchgeführt werden.

Prinzipiell kann die Umschlüsselung serverseitig oder clientseitig erfolgen. Da jedoch das Sicherheitskonzept der ePA auf einer Ende-zu-Ende-Verschlüsselung der Dokumente basiert, dürfen Dokumente nur bei berechtigten Akteuren im Klartext vorliegen. Demzufolge kann die Umschlüsselung nur durch einen Client (ePA-FdV, ePA-AdV-App und teilweise dem Fachmodul ePA des Konnektors) durchgeführt werden. Da insbesondere bei mobilen Clients (ePA-FdV) besondere Randbedingungen gegeben sind – bspw. Performance, Bandbreite des Übertragungskanals und eine begrenzte Kapazität der Stromversorgung – kann immer nur eine begrenzte Anzahl von kryptographischen Operationen auf einmal durchgeführt werden. Dies betrifft insbesondere die Umschlüsselung von Dokumenten. Infolgedessen wird die Umschlüsselung nur für aufgerufene Dokumente und somit schrittweise durchgeführt – es besteht jedoch auch die Möglichkeit, alle Dokumente auf einmal umzuschlüsseln. Die schrittweise Umschlüsselung von Dokumenten erfordert ein Versionsmanagement bzw. Vorhalten der alten und des neuen Aktenschlüssels bis alle Dokumentenschlüssel mit dem neuen Aktenschlüssel verschlüsselt wurden. Das Generieren der neuen Schlüssel erfolgt im Client (Dokumentenschlüssel, Akten- und Kontextschlüssel) oder mittels Aufruf des Schlüsselgenerierungsdienstes (SGD) für die SGD1- und SGD2-Schlüssel.

Das Initiieren der Umschlüsselung (Wechsel von Akten- und Kontextschlüssel sowie die SGD1- und SGD2-Schlüssel aller berechtigten Nutzer) erfordert immer die erfolgreiche Anmeldung des Versicherten am Aktensystem. Die regelmäßige oder anlassbezogene Umschlüsselung wird durch das Aktensystem dermaßen angestoßen, dass das Aktensystem eine Aufforderung zur Umschlüsselung (z. B. nach einer Zeitspanne von 2 Jahren) an das ePA-FdV, die ePA-AdV-App (s. auch Kapitel 4.3.1.7) oder in Folge einer Ad-hoc-Berechtigung eines Leistungserbringers dem Fachmodul ePA des Konnektors sendet. Anschließend kann der Versicherte die Umschlüsselung initiieren. Darüber hinaus kann der Versicherte zu jeder Zeit im Rahmen der Anmeldung am Aktensystem den Umschlüsselungsprozess initiieren. Die eigentliche Umschlüsselung der Dokumente erfolgt nach erfolgter Initiierung pro abgerufenem Dokument (vom Versicherten, dessen Vertreter oder Leistungserbringer) oder auf Wunsch auch durch Abruf aller Dokumente einer Akte.

Für den Wechsel des betreiberspezifischen Schlüssels ist der Versicherte nicht notwendig. Die Umschlüsselung kann vom Betreiber durchgeführt werden. Sie muss jedoch innerhalb einer vertrauenswürdigen Ausführungsumgebung (VAU) erfolgen, um den Zugriff des Betreibers auf die Daten technisch auszuschließen.

Die Umsetzung der Umschlüsselung wird durch folgende Produkttypen durchgeführt:

ePA-FdV und AdV-App

4.3.1.81.1.1.1 Abruf der ID aller berechtigten Akteure

- Abruf aller Akten- und Kontextschlüssel von der Komponente Autorisierung
- Anfordern neuer SGD1- und SGD2-Schlüssel von den Schlüsselgenerierungsdiensten für alle berechtigten Akteure
- Erzeugen neuer Akten- und Kontextschlüssel und Umschlüsseln dieser für alle Berechtigten mit den neuen SGD-Schlüsseln
- Umschlüsseln der Dokumentenschlüssel
- Einstellen der neuen Akten- und Kontextschlüssel und der alten Aktenschlüssel für alle Berechtigten
- Anzeige des Umschlüsselungsstatus der ePA-Dokumente (z. B. Anzahl noch nicht mit dem aktuellen Aktenschlüssel verschlüsselter Dokumentenschlüssel)
- Ausführen der Aufforderung zur Umschlüsselung vom Aktensystem (regelmäßige oder anlassbezogene Umschlüsselung)

Fachmodul ePA des Konnektors

- Umschlüsseln der Dokumentenschlüssel mit dem aktuellen Aktenschlüssel
- Ausführen der Aufforderung zur Umschlüsselung vom Aktensystem (regelmäßige oder anlassbezogene Umschlüsselung)

Aktensystem

- Übermitteln der ID aller auf die Akte berechtigten Nutzer an den Client
- Umschlüsseln der Meta-Daten mit dem neuen Kontextschlüssel
- Verwaltung des aktuellen und der alten Aktenschlüssel

Schlüsselgenerierungsdienst

- Bereitstellen aller nutzerindividuellen SGD-Schlüssel für den Versicherten und die berechtigten Akteure

Die Umsetzung der Umschlüsselung betrifft folgende Anbietertypen:

Anbieter Aktensystem

- Der Betreiber des ePA-Aktensystems wird verpflichtet, den betreiberspezifischen Schlüssel regelmäßig oder bei Bedarf anlassbezogen zu wechseln, damit die beim Betreiber gespeicherten, mit dem Kontext- und Aktenschlüssel der Versicherten verschlüsselten Daten immer zusätzlich mit einem sicheren, dem aktuellen Stand der Technik entsprechenden Schlüssel gesichert sind.

4.3.1.9 ePA-AdV-App

Einem Versicherten ohne eigene technische Geräte muss die Möglichkeit geboten werden die Berechtigungen seiner ePA zu verwalten und Dokumente seiner Akte einsehen und

löschen zu können. Dafür wird im KTR-AdV-Terminal eine ePA-AdV-App zur Verfügung gestellt.

Die ePA-AdV-App entspricht in vielen Vorgaben dem ePA-FdV. Unterschiede ergeben sich daraus, dass diese App nicht auf einem Gerät des Versicherten läuft. Daher wird hier nur die Anmeldung mit der eGK im lokalen Kartenterminal des KTR-AdV-Terminals unterstützt. Es können keine Anwendungsfälle als Vertreter ausgeführt werden oder ein Vertreter eingerichtet werden. Dafür wird ein FdV benötigt.

Die ePA-AdV-App verbindet sich über das Internet mit dem Zugangsgateway des Aktensystems. Die Verbindung der ebenfalls im KTR-AdV-Terminal vorhandenen KTR-AdV-App (zur eigenständigen Verwaltung der Anwendungen des Versicherten auf der elektronischen Gesundheitskarte) zum KTR-AdV-Server und darüber an das zentrale Netz der TI wird nicht nachgenutzt, da dies eine Abhängigkeit zwischen den zwei Produkttypen geschaffen hätte, die besonders im Bereich der Sicherheitsnachweise weitgehende Folgen gehabt hätte.

Aus Sicherheitsgründen bietet das KTR-AdV-Terminal nicht die Möglichkeit des Datenaustauschs mit lokalen Speichermedien. Daher können keine Dokumente in die ePA eingestellt oder aus der ePA gespeichert werden. Es darf auch keine Persistierung von Daten eines Versicherten erfolgen, die Spuren eines Nutzers in der Nutzungs-Session eines folgenden Nutzers hinterlassen könnte. Die ePA-AdV-App muss vor jeder neuen Nutzungs-Session aus einem sicheren Image frisch gestartet werden. Während der Verarbeitung von Daten eines Versicherten in der ePA-AdV-App müssen diese Daten – insbesondere der Kontext- und Aktenschlüssel – durch eine vertrauenswürdige Ausführungsumgebung gegen den Zugriff durch Nutzer oder lokale Administratoren geschützt werden.

In der Anwendung ePA müssen die Geräte, auf denen FdVs ausgeführt werden, durch den Versicherten am Aktensystem registriert werden. Dieser Mechanismus ist so nicht auf die KTR-AdV-Terminals in einer Kostenträgergeschäftsstelle anwendbar. Dennoch muss sichergestellt werden, dass durch die Nutzung der ePA-AdV-App nicht das Sicherheitsniveau für den Versicherten sinkt. Daher wird ein Prozess eingeführt, in dem der Versicherte durch einen Mitarbeiter der Kasse alle KTR-AdV-Terminals einer Geschäftsstelle als genutzte Geräte für seine Akte registrieren lässt. Dabei ist sicherzustellen, dass die DeviceID eines KTR-AdV-Terminals niemals außerhalb des Aktensystems bekannt werden kann.

Die Umsetzung der ePA-AdV-App führt zu Anpassungen an den folgenden Komponenten:

- **ePA-AdV-App**

  Die ePA-AdV-App ist ein neuer Produkttyp mit einer Produktzulassung. Die sicherheitstechnische Eignung wird über ein Produktgutachten und ein Sicherheitsgutachten für den Hersteller nachgewiesen. In seinen Vorgaben orientiert sich dieser Produkttyp am Produkttyp ePA-FdV.

KTR-AdV-Terminal

  Mit der Aufnahme der ePA-AdV-App in das KTR-AdV-Terminal ergeben sich hier ggf. Anpassung am Produkt. Der Produktgutachter des KTR-AdV-Terminals muss prüfen ob alle durch die ePA-AdV-App formulierten Voraussetzungen an dessen Ausführungsumgebung im Produkt gegeben sind.

- **Aktensystem**

  Das Aktensystem muss in Abstimmung mit dem Hersteller der ePA-AdV-App und ggf. des KTR-AdV-Terminals eine Methode der Registration am Aktensystem bereitstellen. Im nächsten Schritte muss im Aktensystem bekannt sein, welche

Geräte in welcher Geschäftsstelle verortet sind, ohne dass außerhalb des Aktensystems DeviceIDs bekannt werden.

4.3.2 Geänderte Komponenten, Dienste und Schnittstellen

Tabelle 2: Übersicht geänderte Komponenten und Dienste

Art	Bezeichnung	Änderung
Produkttyp	KTR-AdV-Terminal	• ePA-AdV-App
Produkttyp	KTR-AdV-Terminal: ePA-AdV-App	• Passdokumente • Schemakonformität und Rendering-Vorschriften für strukturierte Dokumente • Verfahren zur gezielten Umschlüsselung
Produkttyp	Konnektor: ePA-Fachmodul	• Verfahren zur gezielten Umschlüsselung
Produkttyp	ePA-Frontend des Versicherten	• Passdokumente • Schemakonformität und Rendering-Vorschriften für strukturierte Dokumente • Verfahren zur gezielten Umschlüsselung
Produkttyp	Aktensystem	• Passdokumente • Verfahren zur gezielten Umschlüsselung • ePA-AdV-App
Produkttyp	Schlüsselgenerierungsdienst	• Verfahren zur gezielten Umschlüsselung
Clientsystem	Primärsystem	• Passdokumente • Schemakonformität und Rendering-Vorschriften für strukturierte Dokumente
Anbietertyp	Aktensystem	• Verfahren zur gezielten Umschlüsselung

4.4 Anwendungsübergreifende Dienste und dezentrale Komponenten

In den folgenden Abschnitten erfolgt eine detailliertere Darstellung der Änderungen im Rahmen des Systemdesigns im Bereich der anwendungsübergreifenden Dienste und dezentralen Komponenten.

4.4.14.1.1 Identity Provider

Im Rahmen des Systemdesigns wird ein Identity Provider (kurz: IdP) als neuer anwendungsübergreifender Dienst eingeführt. Das E-Rezept wird die erste nutzende Anwendung sein, weitere sollen folgen.

Der IdP stellt nutzenden Anwendungen digitale Identitäten (ID) von Nutzern der TI bereit. Die Bereitstellung erfolgt in Form von Token (ID-Token), die Attribute der Identität enthalten. Der IdP stellt ein Token aus, nachdem der entsprechende Nutzer durch den IdP sicher authentifiziert wurde, d.h., das Token stellt einen Nachweis der erfolgten Authentifizierung dar. Der Nutzer muss sich dazu mit einem geeigneten Mittel authentisieren. Im Rahmen des Release 4.0 werden nur Smart Cards der TI unterstützt.

4.4.1.14.1.1.1 Aufbau und Funktionsweise

Für das Release 4.0 ist ein Identity Provider basierend auf dem Standard `OpenID connect` vorgesehen. Dieser nutzt zunächst nur die Smart Cards der TI und die vorhandene Public Key Infrastructure (PKI). Zweck dieser Lösung ist es, die Smart Cards als

Authentisierungsmittel beim IdP nutzbar zu machen und den nutzenden Anwendungen den Zugriff auf die in den Nutzer-Zertifikaten enthaltenen Identitätsattribute zu ermöglichen – daher wird diese erste Ausbaustufe *Smart Card Identity Provider* genannt. Der Smart Card IdP verfügt somit über keine eigene Datenbasis für Identitäten, sondern stellt nur die kartenbasierten Identitäten in Form von ID-Token bereit.

Abbildung 9 zeigt den Aufbau des Smart Card IdP. Als nutzende Komponente ist im Bild links unten ein Anwendungsfrontend einer Anwendung gezeigt – dies könnte z.B. das E-Rezept-Frontend sein. Das Frontend greift auf Dienste im zentralen Bereich der TI zu – im Bild angedeutet mit „Anwendungsdienst A/B".

Die Dienste im zentralen Bereich setzen im Wesentlichen Fachlogik um, während der IdP die Authentifizierung und weitere IdP-Funktionen als Plattformleistung bereitstellt. Diese Aufteilung findet sich auch im dezentralen Bereich. Das Frontend ist weitgehend auf Fachlogik beschränkt, während das beigestellte Authentisierungsmodul die Authentisierung des Nutzers ermöglicht, seine Einwilligung in die Nutzung seiner Identitätsattribute einholt und frontendseitig die Session-ID verwaltet. Die IdP-seitige Session-Verwaltung ermöglicht einen anwendungsübergreifenden Single Sign-On, d.h., der IdP speichert eine bereits erfolgte Authentifizierung des Nutzers und ermöglicht es, erneut und für verschiedene Anwendungen ID-Token auszustellen, ohne jedes Mal eine erneute Authentisierung vom Nutzer anzufordern.

Für die Nutzung eines Dienstes wird ein ID-Token als Nachweis der Authentifizierung benötigt und um Identitätsattribute verarbeiten zu können. Dieses wird wie folgt bereitgestellt (siehe auch die nummerierten Datenflüsse im Bild):

1) Das Frontend erstellt eine Anfrage nach der Nutzer-Identität und delegiert diese an das Authentisierungsmodul.

2) Das Authentisierungsmodul reicht diese Anfrage an den IdP weiter, zusammen mit der ggf. vorhandenen Session-ID.

   Der IdP prüft, ob es zu dieser Session-ID eine gültige Session gibt (Session Data). Falls ja, kann mit Schritt 4 fortgefahren werden (Authentifizierung bereits erfolgt) – sonst mit Schritt 3.

3) Der IdP fordert vom Authentisierungsmodul die Authentisierung des Nutzers und das Einholen der Einwilligung des Nutzers an. Die Authentifizierung erfolgt per Challenge/Response mit der Smart Card, für die Gültigkeitsprüfung nutzt der IdP die vorhandene PKI (OCSP-Abfrage).

4) Bei erfolgreicher Authentifizierung erstellt der IdP intern ein ID-Token und gibt einen Code (Authorization Code) an das Authentisierungsmodul zurück.

5) Der Code wird vom Authentisierungsmodul an das Frontend übergeben.

6) Das Frontend übergibt den Code an den IdP.

7) Der IdP stellt dem Frontend das zum Code gehörende ID-Token bereit.

Der beschriebene Ablauf entspricht dem Standard `OpenID connect` (Authorization Code Flow). Dieser lässt das eigentliche technische Authentifizierungsverfahren offen, weshalb für jedes genutzte Verfahren sowohl beim IdP als auch beim Authentisierungsmodul entsprechende Anteile ergänzt werden müssen (hellblau im Bild).

Im Bild ist auch dargestellt, dass alle nutzenden Anwendungen beim IdP registriert sein müssen (Registrierte Clients), nur Anwendungen mit einer Client-ID können den IdP nutzen. Bei der Registrierung werden u.a. Sicherheitsmechanismen für die Anwendung

konfiguriert, dabei wird auch festgelegt, welche ID-Attribute der IdP einer Anwendung höchstens zur Verfügung stellen darf.

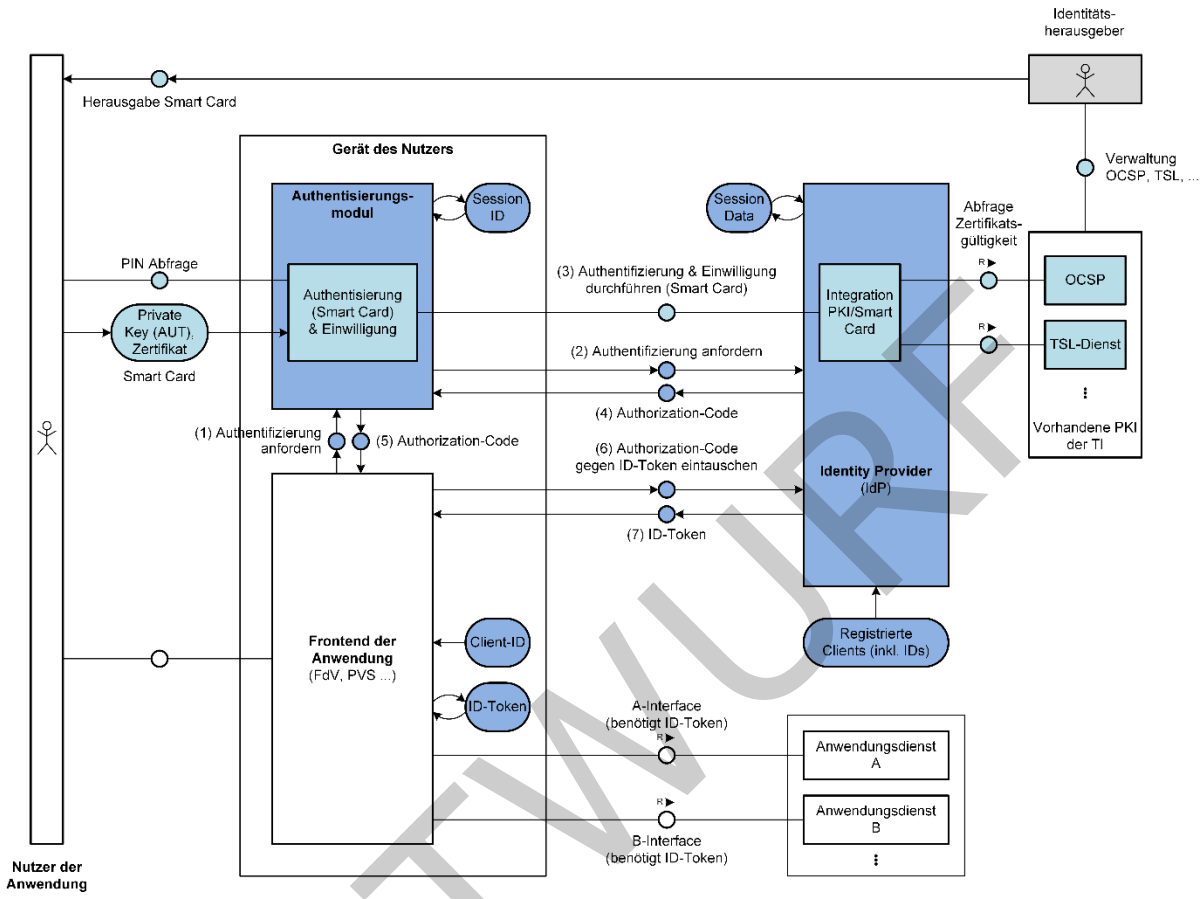


Abbildung 9: Smart Card Identity Provider

~~4.4.1.2~~4.1.1.2 Hintergrund der Lösung und Ausblick

Die vorgestellte Lösung zielt zunächst auf die Einführung eines IdP als neuen Dienst der TI und ermöglicht die Entwicklung von Anwendungen basierend auf `OpenID connect`. Der Smart Card IdP wird von der gematik zunächst für alle Nutzer der Fachanwendung E-Rezept zur Verfügung gestellt und bietet bereits einige Vorteile:

- Komfortgewinn für den Nutzer durch Single Sign-On
- Integration/Nutzung der vorhandenen PKI (geringere Migrationsaufwände)
- Vereinfachung der Anwendungsentwicklung durch Auslagerung von Funktionen auf den IdP
- Reduktion des Umfangs sicherheitsrelevanter Anwendungsbestandteile
- reduzierte Entwicklungs-, Test- und Zulassungsaufwände für Anwendungen
- etablierte, bewährte und für den mobilen Zugang geeignete Standards
- bedarfsgerechte Bereitstellung von Identitäts-Attributen (Privacy By Design)

Der Smart Card IdP ist als eine erste Ausbaustufe des IdP hin zu einer Lösung mit verteilten Identity Providern anzusehen!

Für kommende Releases ist daher vorgesehen, den IdP um zusätzliche Merkmale zu erweitern und ein flexibleres Identity Management zu ermöglichen.

- ~~Identitätsherausgeber (z.B. Vereinfachung der Anwendungsentwicklung durch Auslagerung von Funktionen auf den IdP~~
- ~~Reduktion des Umfangs sicherheitsrelevanter Anwendungsbestandteile~~
- ~~reduzierte Entwicklungs-, Test- und Zulassungsaufwände für Anwendungen~~
- ~~etablierte, bewährte und für den mobilen Zugang geeignete Standards~~
- ~~bedarfsgerechte Bereitstellung von Identitäts-Attributen (Privacy By Design)~~

~~*Der Smart Card IdP ist als eine erste Ausbaustufe des IdP hin zu einer Lösung mit verteilten Identity Providern anzusehen!*~~

~~Für kommende Releases ist daher vorgesehen, den IdP um zusätzliche Merkmale zu erweitern und ein flexibleres Identity Management zu ermöglichen.~~

- ~~Identitätsherausgeber (z.B.~~ Krankenkassen, LEO, …) sollen als Anbieter eigene IdPs mit flexibler Identitätenverwaltung in die TI einbringen können, die den Smart Card IdP für die von ihnen verwalteten Identitäten ersetzen.
- Die Anbieter sollen alternative Authentisierungslösungen anbieten können, sofern diese sicher genug sind.
- Ziel soll es sein, dass der Versicherte seine digitalen Gesundheitsanwendungen mit einer einzigen Identität nutzen kann.

Die Erweiterung der TI um neue Nutzergruppen und die Entwicklung neuer, speziell mobiler Zugangslösungen soll erleichtert werden.

Der Standard `OpenID connect` und darauf beruhende Produkte im Markt bieten zusätzliche Funktionen an, die perspektivisch interessant sind. Dies betrifft z.B. die Integration SAML2-basierter Anwendungen und den Austausch von Identitäten mit externen (föderierten) IdPs für ein sektorenübergreifendes oder EU-weites Identity Management.

4.1.1.3 Sicherheit und Datenschutz

Da die ID-Token den Zugriff auf personenbezogene medizinische Daten ermöglichen, sind sie in den Schutzzielen Vertraulichkeit und Integrität mit einem Schutzbedarf von sehr hoch bewertet. Die Gültigkeit von Token ist zeitlich zu begrenzen und muss sich durch Abmeldung oder Sperrung des Nutzers aufheben lassen.

Die Identitäts-Informationen im IdP sind Grundlage für die Erstellung der ID-Token, die den Zugriff auf personenbezogene medizinische Daten ermöglichen. Der Schutzbedarf für Integrität wird daher mit sehr hoch bewertet, die Prozesse zur Verwaltung dieser Identitäts-Informationen müssen dieses Schutzniveau gewährleisten. Der Schutzbedarf der Informationen bzgl. Vertraulichkeit wird mit hoch bewertet, da es sich um personenbezogene Daten handelt. Beim Smart Card IdP im Release 4.0 sichern die vorhandene PKI, die TSP und Kartenherausgeber die Schutzziele bereits teilweise ab.

Zur Einhaltung der Vorschriften des Datenschutzes ist sicherzustellen, dass beim IdP keine Profilbildung erfolgen kann.

Der IdP muss Authentifizierungsverfahren mit geeignet hohem Sicherheitsniveau anbieten.

Der Schutzbedarf für die Verfügbarkeit des IdP leitet sich aus den Verfügbarkeitsanforderungen der nutzenden Anwendungen ab.

4.1.1.4 Betrieb

Der IdP wird als Smart-Card IdP von der gematik zunächst für alle Nutzer der Fachanwendung E-Rezept zur Verfügung gestellt. In einem späteren Release wird vorgesehen, den Dienst auch für weitere Identitätsherausgeber zu öffnen und als eigenständiges Produkt am Markt anbieten zu lassen (z.B. kartenlose Authentisierung).

Die Erbringung der operativen Betriebsleistungen des IdP-Dienstes erfolgt anhand eines IdP-Anbietertypsteckbriefs, die operativen Betriebsleistungen und sonstigen Leistungen (Herstellen und Anbieten eines Authentisierungsmoduls) des Smart-Card IdP werden von der gematik beauftragt. Der IdP-Anbieter muss ein lokales ITSM unterhalten und am übergreifenden TI-ITSM teilnehmen. Er bedient dort alle relevanten Prozesse mit hohen SLA-Anforderungen. Der Smart-Card IdP-Anbieter muss keinen eigenen Endnutzersupport bereitstellen. Leistungserbringer können sich im Störungsfall weiterhin an den UHD des sie betreuenden VPN-Zugangsdienstes wenden. Versicherte, die im Rahmen des E-Rezeptes den IdP nutzen, wenden sich im Supportfall der an den Anbieter des E-Rezepts-FdV.

4.1.1.5 Zulassung

Der Hersteller des Produkttyps IdP bedarf einer Produktzulassung (Authentisierungsmodul und IdP-Dienst bilden zusammen einen Produkttyp).

Mit Release 4.0 stellt die gematik einen Smart-Card IdP zur Verfügung. Die operativen Betriebsleistungen werden durch einen von der gematik beauftragten Dienstleister erbracht. Eine formale Anbieterzulassung nach Anbietertypsteckbrief ist für den Smart-Card IdP nicht vorgesehen.

Für die Bereitstellung von IdP und Authentisierungsmodul durch die Identitätsherausgeber nach Release 4.0 sind weitere Produkt- und Anbieterzulassungen zulässig.

4.1.2 Anbindung neuer Berufsgruppen an die TI

4.1.2.1 Übersicht der Änderungen

Konzepte und Spezifikationen der gematik enthalten anwendungsübergreifend alle notwendigen funktionalen und technischen Vorgaben für Herausgeber und Anbieter von Heilberufs- und Berufsausweise und/oder Komponenten zur Authentifizierung von Leistungserbringerinstitutionen (SMC-B) als Grundlage entsprechender Herausgabeverfahren, inklusive Zertifikatsprofile, OIDs und angepasste Zulassungs- und Bestätigungsverfahren der betroffenen Produkt- und Anbietertypen.

- ~~IdPs mit flexibler Identitätenverwaltung in die TI einbringen können, die den Smart Card IdP für die von ihnen verwalteten Identitäten ersetzen.~~
- ~~Die Anbieter sollen alternative Authentisierungslösungen anbieten können, sofern diese sicher genug sind.~~

~~Die Erweiterung der TI um neue Nutzergruppen und die Entwicklung neuer, speziell mobiler Zugangslösungen soll erleichtert werden.~~

Der Standard OpenID connect und darauf beruhende Produkte im Markt bieten zusätzliche Funktionen an, die perspektivisch interessant sind. Dies betrifft z.B. die Integration SAML2-basierter Anwendungen und den Austausch von Identitäten mit externen (föderierten) IdPs für ein sektorenübergreifendes oder EU-weites Identity Management.

4.4.1.31.1.1.1 Sicherheit und Datenschutz

Da die ID-Token den Zugriff auf personenbezogene medizinische Daten ermöglichen, sind sie in den Schutzzielen Vertraulichkeit und Integrität mit einem Schutzbedarf von sehr hoch bewertet. Die Gültigkeit von Token ist zeitlich zu begrenzen und muss sich durch Abmeldung oder Sperrung des Nutzers aufheben lassen.

Die Identitäts-Informationen im IdP sind Grundlage für die Erstellung der ID-Token, die den Zugriff auf personenbezogene medizinische Daten ermöglichen. Der Schutzbedarf für Integrität wird daher mit sehr hoch bewertet, die Prozesse zur Verwaltung dieser Identitäts-Informationen müssen dieses Schutzniveau gewährleisten. Der Schutzbedarf der Informationen bzgl. Vertraulichkeit wird mit hoch bewertet, da es sich um personenbezogene Daten handelt. Beim Smart-Card IdP im Release 4.0 sichern die vorhandene PKI, die TSP und Kartenherausgeber die Schutzziele bereits teilweise ab.

Zur Einhaltung der Vorschriften des Datenschutzes ist sicherzustellen, dass beim IdP keine Profilbildung erfolgen kann.

Der IdP muss Authentifizierungsverfahren mit geeignet hohem Sicherheitsniveau anbieten.

Der Schutzbedarf für die Verfügbarkeit des IdP leitet sich aus den Verfügbarkeitsanforderungen der nutzenden Anwendungen ab.

4.4.1.41.1.1.1 Betrieb

Der IdP wird als Smart-Card IdP von der gematik zunächst für alle Nutzer der Fachanwendung E-Rezept zur Verfügung gestellt. In einem späteren Release wird vorgesehen, den Dienst auch für weitere Identitätsherausgeber zu öffnen und als eigenständiges Produkt am Markt anbieten zu lassen (z.B. kartenlose Authentisierung).

Die Erbringung der operativen Betriebsleistungen des IdP-Dienstes erfolgt anhand eines IdP-Anbietertypsteckbriefs, die operativen Betriebsleistungen und sonstigen Leistungen (Herstellen und Anbieten eines Authentisierungsmoduls) des Smart-Card IdP werden von der gematik beauftragt. Der IdP-Anbieter muss ein lokales ITSM unterhalten und am übergreifenden TI ITSM teilnehmen. Er bedient dort alle relevanten Prozesse mit hohen SLA-Anforderungen. Der Smart-Card IdP-Anbieter muss keinen eigenen Endnutzersupport bereitstellen. Leistungserbringer können sich im Störungsfall weiterhin an den UHD des sie betreuenden VPN-Zugangsdienstes wenden. Versicherte, die im Rahmen des E-Rezeptes den IdP nutzen, wenden sich im Supportfall der an den Anbieter des E-Rezepts-FdV.

4.4.1.51.1.1.1 Zulassung

Der Hersteller des Produkttyps IdP bedarf einer Produktzulassung (Authentisierungsmodul und IdP-Dienst).

Mit Release 4.0 stellt die gematik einen Smart-Card IdP zur Verfügung. Die operativen Betriebsleistungen werden durch einen von der gematik beauftragten Dienstleister erbracht. Eine formale Anbieterzulassung nach Anbietertypsteckbrief ist für den Smart-Card IdP nicht vorgesehen.

~~Für die Bereitstellung von IdP und Authentisierungsmodul durch die Identitätsherausgeber nach Release 4.0 sind weitere Produkt- und Anbieterzulassungen zulässig.~~

Die Herausgabe von Komponenten zur Authentifizierung von Leistungserbringerinstitutionen (SMC-B) und elektronischen Heilberufs- und Berufsausweise durch die gematik kann erfolgen, indem mindestens ein Anbieter vertraglich gebunden ist und alle erforderlichen Antrags-, Freigabe und Sperrprozesse definiert sind.

~~4.4.2~~4.1.3 Verzeichnisdienst

~~4.4.3~~1.1.1 ~~Übersicht der Änderungen~~

4.1.3.1 ~~Für die Nutzung des Verzeichnisdienstes durch die~~ Übersicht der Änderungen

Der Verzeichnisdienst (VZD) wird nun auch für die Fachanwendung E-Rezept von Versicherten zur Suche von Apotheken zur Abgabe der auf der Verordnung ausgestellten Arzneimittel genutzt (siehe auch 4.4~~) sind einige~~). Daraus ergeben sich folgende Anpassungen ~~vorgesehen~~:

- Es wird ermöglicht, dass der aufrufende Nutzer sich mit einer vom Identity Provider (siehe 4.1.1) bereitgestellten Identitätsbestätigung authentisiert.
- Der Verzeichnisdienst wird für den Zugriff durch die Versicherten im Internet erreichbar sein.
- Der Verzeichnisdienst wird die über die Suche durch Versicherte abrufbaren Informationen auf diejenigen Informationen beschränken, die für die Suche und Adressierung von abgebenden Leistungserbringern benötigt werden.
- ~~Der Verzeichnisdienst wird für den Zugriff durch die Versicherten im Internet erreichbar sein.~~
- ~~Der Verzeichnisdienst wird die über die Suche durch Versicherte abrufbaren Informationen auf diejenigen Informationen beschränken, die für die Suche und Adressierung von abgebenden Leistungserbringern benötigt werden.~~

~~Für weitere Erläuterungen zu Motivation, fachlichen und betrieblichen Anforderungen wird auf Kapitel 2 verwiesen.~~ Weitere Informationen zur Umsetzung der Anforderungen finden sich in [gemSysL_eRp].

~~4.4.3.1 Zulassungsverfahren~~

~~4.4.4 VPN-Zugangsdienst~~

~~4.4.4.1 Betriebliche Änderungen~~

~~Der VPN-Zugangsdienst (VPN-ZugD) wird mit Release 4.0 Messdaten erheben, welche die bisher definierten technischen Performance-Kenngrößen darstellen, und in frei konfigurierbaren Zeitabständen an die Betriebsdatenschnittstelle liefern. Damit entfällt die Pflicht, Messdaten an die Störungsampel bzw. – an ihrer Stelle – an das TI-Service Monitoring zu senden sowie die Lieferung eines monatlichen Performance-Reports. Weiterhin muss kein monatlicher SL-Report mehr gesendet werden. Dieser wird im~~

~~übergreifenden TI-ITSM bereitgestellt, wobei der Anbieter VPN-ZugD weiterhin seine Pflichten zur Messung der Service Level sowie zur Übermittlung und Bewertung der Service Level Messergebnisse gemäß [gemRL_Betr_TI#Kapitel 9.2] zu erfüllen hat.~~

~~4.4.5~~4.1.4 KTR-AdV-Terminal

~~4.4.5.1~~4.1.4.1 Übersicht der Änderungen

Der Produkttyp KTR-AdV-Terminal bietet dem Versicherten eine Umgebung in der er in einer Kostenträgergeschäftsstelle die KTR-AdV-App nutzen, und so seine datenschutzrechtlichen Betroffenenrechte wahrnehmen kann. Darüber hinaus kann der Versicherte nun am KTR-AdV-Terminal eine ePA-FdV AdV ~~App~~ nutzen und so Dokumente aus seiner ePA ansehen und feingranular Berechtigungen verwalten kann. Die Aspekte der ePA-FdV AdV werden nachfolgend im Zusammenhang mit der Anwendung ePA dargestellt.

Bisher war das KTR-AdV-Terminal zwar spezifiziert, aber da noch kein Verfahren der Prüfung der Sicherheitstechnischen Eignung definiert war, konnte bisher kein Produkt zugelassen werden. Diese Lücke wird nun geschlossen.

4.1.4.2 Sicherheit und Datenschutz

Die sicherheitstechnische Eignung des KTR-AdV-Terminals wird durch ein Produktgutachten nachgewiesen. Darüber hinaus werden die Entwicklungsprozesse und deren Umgebung im Rahmen eines Sicherheitsgutachtens geprüft.

Auf einem KTR-AdV-Terminal dürfen nur zugelassene – und damit sicherheitsgeprüfte – Apps ausgeführt werden. Deren Sicherheit wird entweder über eine Prüfung gegen eine technische Richtlinie (KTR-AdV-App) oder ein ~~App werden nachfolgend im Zusammenhang mit der Anwendung ePA dargestellt.~~

~~Bisher war das KTR-AdV-Terminal zwar spezifiziert, aber da noch kein Verfahren der Prüfung der Sicherheitstechnischen Eignung definiert war, konnte bisher kein Produkt zugelassen werden. Diese Lücke wird nun geschlossen.~~

~~4.4.5.2 Geänderte Komponenten, Dienste und Schnittstellen~~

Sicherheits- und ~~Nicht anwendbar.~~

~~4.4.5.3~~1.1.1.1 ~~Sicherheit und Datenschutz~~

~~Die sicherheitstechnische Eignung des KTR-AdV-Terminals wird durch ein Produktgutachten nachgewiesen. Darüber hinaus werden die Entwicklungsprozesse und deren Umgebung im Rahmen eines Sicherheitsgutachtens geprüft.~~

~~Auf einem KTR-AdV-Terminal dürfen nur zugelassene – und damit sicherheitsgeprüfte – Apps ausgeführt werden. Deren Sicherheit wird entweder über eine Prüfung gegen eine technische Richtlinie (KTR-AdV-App) oder ein~~ Produktgutachten (ePA-FdV AdV ~~App~~) nachgewiesen.

Die Erfüllung von Voraussetzungen, die eine App ggü. ihrer Ausführungsumgebung formuliert, werden im Produktgutachten des KTR-AdV-Terminals berücksichtigt.

Bei der Unterstützung des Versicherten in der Bedienung des KTR-AdV-Terminals durch Mitarbeiter des Kostenträgers müssen geltende Datenschutzbestimmungen eingehalten

werden, da der Mitarbeiter unter Umständen Einsicht in personenbezogene medizinischen Daten erhält. Daher ist der Versicherte hierüber aufzuklären und muss dem zustimmen.

4.1.4.3 Betrieb

Der Betrieb eines KTR-AdV-Terminals obliegt der Geschäftsstelle und ist nicht in die Betriebsprozesse der TI integriert.

4.1.4.4 Zulassungsverfahren

Der Hersteller des KTR-AdV-Terminals muss sein Produkt einer Produktzulassung unterziehen. Eine Anbieterzulassung erfolgt nicht.

~~Die Erfüllung von Voraussetzungen, die eine App ggü. ihrer Ausführungsumgebung formuliert, werden im Produktgutachten des KTR-AdV-Terminals berücksichtigt.~~

~~**4.4.5.41.1.1.1 Betrieb**~~

~~Der Betrieb eines KTR-AdV-Terminals obliegt der Geschäftsstelle und ist nicht in die Betriebsprozesse der TI integriert.~~

~~**4.4.5.51.1.1.1 Zulassungsverfahren**~~

~~Der Hersteller des KTR-AdV-Terminals muss sein Produkt einer Produktzulassung unterziehen. Eine Anbieterzulassung erfolgt nicht.~~

4.1.4.5 Geänderte Komponenten und Dienste

Nicht anwendbar.

4.1.5 SMC-B Dual-Interface

4.1.5.1 Übersicht der Änderungen

Der Produkttyp SMC-B Dual-Interface ist eine Erweiterung der bisher vorhandenen SMC-B mit rein kontaktbehafteter Schnittstelle um die kontaktlose Schnittstelle. SMC-B Dual-Interface können sowohl in kontaktbehafteten Kartenterminals als auch mit kontaktlosen (NFC-) Kartenlesern betrieben werden.

Die Erweiterung der SMC-B um die kontaktlose Schnittstelle erfolgt in Hinblick auf den zukünftig erweiterten Nutzerkreis der TI (siehe 2.1.2) und erlaubt perspektivisch den Zugang zur TI und zur Freischaltung von eGK auch über zulässige Geräte, die lediglich kontaktlose Kartenleser vorsehen, beispielsweise derzeitige mobile Endgeräte. Speziell Zugänge zur TI, die nicht mittels stationärer Konnektoren erfolgen, könnten dadurch in Folgereleases ermöglicht werden.

4.1.5.2 Produkttypausprägungen

Ein Kartenhersteller kann eine SMC-B Dual-Interface nach Erbringung der notwendigen Nachweise durch die gematik zulassen. Auf Basis dieser Zulassung können sowohl SMC-B Dual-Interface mit Nutzung der kontaktlosen Schnittstelle (ID-1, bzw. Scheckkarten-format), als auch SMC-B ohne die kontaktlose Nutzung (ID-000, bzw. SIM-Format ohne Antenne) hergestellt werden.

Die bisher vorhandene, rein kontaktbehaftete SMC-B ist auch weiterhin zulassungsfähig.

4.1.5.3 Sicherheit und Datenschutz

Der Nachweis der sicherheitstechnischen Eignung der SMC-B Dual-Interface erfolgt analog zu den Nachweisen der sicherheitstechnischen Eignung aller vorhandenen Karten der TI.

Das gemeinsame Betriebssystem der Karten (COS) benötigt eine CC-Evaluierung gemäß BSI-CC-PP-0082 durch das BSI. Für das Objektsystem ist das Sicherheitsgutachten einer Prüfstelle gemäß technischer Richtlinie BSI-TR-03110 erforderlich.

4.1.5.4 Kartenausgabe und Betrieb

Die Kartenausgabe erfolgt zunächst durch die Herausgeber bisheriger kontaktbehafteter SMC-B an berechtigte Institutionen. Der Betrieb erfolgt durch die nutzende Institution und entspricht vollumfänglich den Anwendungsmöglichkeiten einer kontaktbehafteten SMC-B. Die kontaktlosen Eigenschaften erweitern ggf. die Nutzung lediglich um den kontaktlosen Gerätezugang, beispielsweise durch mobile Endgeräte.

4.1.5.5 Zulassungsverfahren

Der Hersteller einer SMC-B Dual-Interface muss sein Produkt durch die gematik für den Betrieb in der TI zulassen. Die Zulassungsvoraussetzung (funktionaler Test, Sicherheitsnachweise und Nachweis der mechanisch/physikalischen Prüfung) entspricht dem etablierten Verfahren einer rein kontaktbehafteten SMC-B.

4.1.6 Übergreifende Betriebliche Regelungen

4.1.6.1 Erfassung und Lieferung technischer Performance-Rohdaten

Mit Release 4.0 werden neue betriebliche Kennzahlen definiert, anhand derer Last- und Performanceverhalten sowie Verfügbarkeit der Fachdienste präziser gemessen und nachgewiesen werden. Des Weiteren werden die Fachdienste weiterhin Messdaten erheben, welche die bisher definierten technischen Performance-Kenngrößen darstellen, und in frei konfigurierbaren Zeitabständen an die Betriebsdatenschnittstelle liefern. Damit entfällt die Pflicht, Messdaten an die Störungsampel bzw. – an ihrer Stelle – an das TI Service Monitoring zu senden sowie die Lieferung eines monatlichen Performance-Reports. Weiterhin muss kein monatlicher SL-Report mehr gesendet werden. Dieser wird im übergreifenden TI-ITSM bereitgestellt, wobei der Anbieter seine Pflichten zur Messung der Service Level sowie zur Übermittlung und Bewertung der Service Level Messergebnisse zu erfüllen hat.

4.1.6.2 Geänderte Komponenten und Dienste

Tabelle 5: Übersicht geänderte Komponenten und Dienste

Art	Bezeichnung	Änderung
Produkttyp	KOM-LE Fachdienst	• Erfassen technischer Performance-Rohdaten
Produkttyp	VPN-Zugangsdienst	• Erfassen technischer Performance-Rohdaten
Produkttyp	E-Rezept-Fachdienst	• Erfassen technischer Performance-Rohdaten
Produkttyp	Identity Provider Fachdienst	• Erfassen technischer Performance-Rohdaten

Anbietertyp	Fachdienst KOM-LE	• Lieferung technischer Performance-Rohdaten
Anbietertyp	VPN-Zugangsdienst	• Lieferung technischer Performance-Rohdaten
Anbietertyp	E-Rezept-Fachdienst	• Lieferung technischer Performance-Rohdaten
Anbietertyp	Identity Provider Fachdienst	• Lieferung technischer Performance-Rohdaten

4.1.7 Übergreifende Datenschutz- und Sicherheitsregelungen

4.1.7.1 Übersicht der Änderungen

Bisher sind Dienste der Telematikinfrastruktur (TI) entweder durch den VPN-Zugangsdienst (bei Zugang zur TI mittels Konnektor) oder bei der Anwendung „elektronische Patientenakte" durch ein Gateway (bei durch den Versicherten initiierten Zugang) geschützt. Mit Einführung der Fachanwendungen E-Rezept, eines Identity Providers und der Weiterentwicklung der Fachanwendung KOM-LE wird die Nutzung von Anwendungen der Telematikinfrastruktur über eine Internetschnittstelle an den beteiligten Fachdiensten möglich. Dies erfordert ggf. andere als bisher etablierte Sicherheitsmechanismen auf Netzwerk- Protokoll- und Anwendungsebene, die in den jeweiligen Spezifikationen zu berücksichtigen sind. Beispielsweise müssen nun bei HTTP basierten (RESTful) Schnittstellen eines jeden Fachdienstes entsprechende Sicherheitsvorkehrungen, wie bspw. in dem OWASP cheat sheet zur REST Security beschrieben, definiert werden.

Insbesondere wird mit dem IdP ein Dienst etabliert, der eine elementare und zentrale Rolle in der gesamten TI einnimmt. Daher sind entsprechende Sicherheitsmaßnahmen für den Dienst und zugehörigem Client unablässlig.

Ebenso sind Datenschutzaspekte wie bspw. bei der Abfrage des Status eines Zertifikates (OCSP-Stapling), Profilbildung oder der Protokollierung von sicherheitsrelevanten Daten zu berücksichtigen.

Die Vorgaben an den sicheren Betrieb bzw. an den Anbieter/Betreiber gerichtet, bleiben wie bisher bestehen und sind zu berücksichtigen.

4.1.7.2 Geänderte Komponenten und Dienste

Art	Bezeichnung	Änderung
Produkttyp	E-Rezept-Fachdienst	• Datenschutz- und Sicherheitsvorgaben
Produkttyp	Identity Provider Fachdienst	• Datenschutz- und Sicherheitsvorgaben
Produkttyp	Verzeichnisdienst	• Datenschutz- und Sicherheitsvorgaben

4.2 ePA

4.2.1 Übersicht der Änderungen

Mit ePA 2.0 wird im Release 4.0 der in Kapitel 2.2 definierte fachliche Umfang zusätzlich zu ePA 1.1 (Release 3.1) umgesetzt:

- Rollenprofile für Berufsgruppen

- Verfeinertes Berechtigungskonzept
- Erweiterung des Datenmodells
- Durch die KBV standardisierte Dokumentenformate der ePA
- Verfahren zur gezielten Umschlüsselung
- ePA-FdV AdV

Abbildung 10 zeigt die von den Änderungen betroffenen Produkttypen der TI und der angrenzenden IT-Systeme.

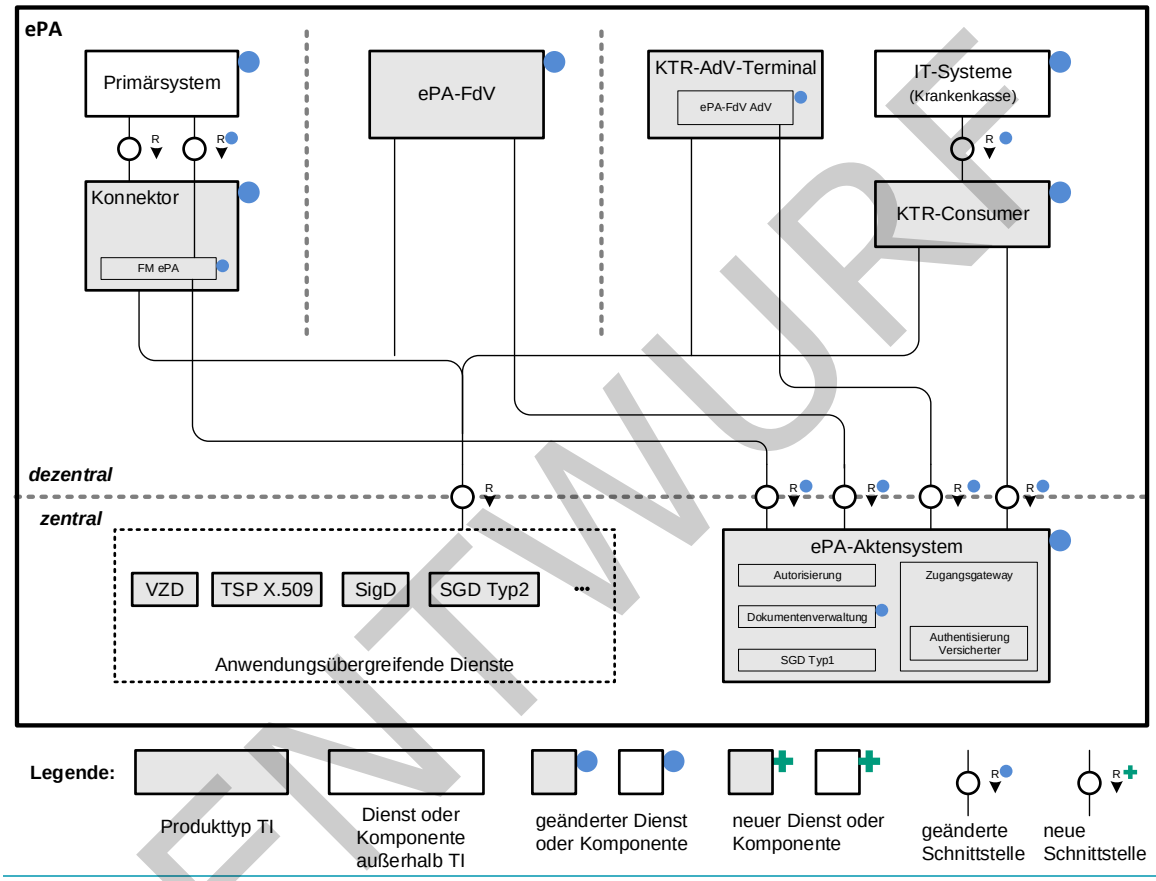


Abbildung 10: Übersicht über von Änderungen betroffene Produkttypen der TI inkl. angrenzender IT-Systeme für ePA 2.0

4.2.1.1 Rollenprofile für Berufsgruppen

Die Einführung neuer zugriffberechtigter Berufsgruppen und die damit verbundene Erweiterung des Nutzerkreises der ePA muss in der Berechtigungsverwaltung des Aktensystems berücksichtigt werden. Entsprechende Policies müssen eingeführt und die Rollen der Nutzer (OIDs) ausgewertet werden.

Die Zuordnung von Berufsgruppen zu einer Leistungserbringerorganisation im Rahmen der Berechtigungsvergabe kann durch Auswertung der Rolle des im VZD hinterlegten Zertifikates der Leistungserbringerorganisation des zu berechtigenden Leistungserbringer im Frontend des Versicherten (ePA-FdV, ePA-FdV AdV) erfolgen. Primärsysteme erhalten die Rolleninformation von der SMC-B bzw. dem Konnektor. Die Darstellung von erlaubten Berechtigungen für die jeweilige Berufsgruppe erfolgt im Client auf Basis des geltenden

Berechtigungskonzeptes. Eine detaillierte Analyse erfolgt im Rahmen der Ausgestaltung des verfeinerten Berechtigungskonzeptes.

Primärsysteme, ePA-FdV und ePA-FdV AdV

- Verarbeitung neuer Rollenprofile

ePA-Fachmodul im Konnektor

- Verarbeitung neuer Rollenprofile

Aktensystem

- Aktualisierung der Berechtigungsverwaltung zur Verarbeitung neuer Rollenprofile

4.2.1.2 Verfeinertes Berechtigungskonzept

Das verfeinerte Berechtigungskonzept wird durch die Frontends des Versicherten (ePA-FdV und ePA-FdV AdV) und Primärsystem (bzw. auch dem Fachmodul ePA des Konnektors) dem Versicherten zur Verfügung gestellt und in Form einer gesetzeskonformen Auswahl zu erteilender Berechtigungen in Abhängigkeit der Rolle bzw. Berufsgruppe des Berechtigungsempfängers durchgesetzt. Darüber hinaus prüft in letzter Instanz das Aktensystem die von den Clients übermittelten Berechtigungen auf Korrektheit und Einhaltung der gesetzlichen Grundlagen und verhindert somit eine Übersteuerung gesetzlich verankerter Rechte durch den Nutzer. Demzufolge müssen sowohl das Aktensystem als auch teilweise die Clients die mit ePA Stufe 2 spezifizierte Berechtigungsrichtlinie umsetzen. Dies setzt voraus, das der Berechtigungsempfänger den gemäß PDSG beschriebenen Berufsgruppen zugeordnet werden kann (siehe auch Kapitel 4.2.1.1). Weiterhin müssen die Voraussetzungen zur Kennzeichnung von Dokumenten entsprechend den vorgegeben Dokumentenkategorien, Fachgebieten, Vertraulichkeitsstufen und einer dokumentenindividuellen Zuordnung zu einer LEI (und somit entsprechende Metadaten und Value-Sets) geschaffen werden. Letztendlich wird die Berechtigungssystematik auf unterster Ebene mittels CRUD-Rechten[1] (siehe Anhang A1) - in Abhängigkeit von Dokumentenkategorien und Berufsgruppe - realisiert.

Die Kennzeichnung von Dokumenten erfolgt durch den Leistungserbringer, durch den Kostenträger oder dem Versicherten beim Einstellen eines Dokumentes in die ePA des Patienten/Versicherten, kann aber in Fällen der eindeutigen Zuordnung von Kennzeichnungen zu dem Dokument unterstützend bis automatisiert durch den Client erfolgen (bspw. ist beim Anlegen eines Impfdokumentes eine Eindeutige Zuordnung zur Dokumentenkategorie gegeben).

Bestehende Berechtigungen (Policies) und Dokumente werden inkl. Metadaten in das neue Berechtigungskonzept migriert bzw. überführt (siehe auch Kapitel 4.2.1.8).

Die Umsetzung der verfeinerten Berechtigungsvergabe erfolgt in den folgenden Komponenten:

ePA-Fachmodul KTR-Consumer

- Kennzeichnung der einzustellenden Dokumente bezüglich der zu verwendenden Vertraulichkeitsstufe und Dokumentenkategorien

ePA-FdV und ePA-FdV AdV

[1] Kurzform von allgemeinen Zugriffsrechten: **C**reate, **R**ead, **U**pdate, **D**elete

- Kennzeichnung der einzustellenden Dokumente bezüglich der zu verwendenden Vertraulichkeitsstufe und Dokumentenkategorien
- Rechtevergabe an den gemäß § 352 PDSG berechtigten Nutzerkreis
- Grob-, mittel- und feingranulare Berechtigungsvergabe
- Ändern von Vertraulichkeitsstufen
- Suche nach einer bestimmten Dokumentenkategorie, Fachgebiet oder Vertraulichkeitsstufe
- Löschen von Dokumenten

Primärsystem

- Kennzeichnung der einzustellenden Dokumente bezüglich Vertraulichkeitsstufen, Dokumentenkategorien und Fachgebieten
- Grob- und mittelgranulare Berechtigungsvergabe im Zuge der ad-hoc Berechtigung
- Auf Wunsch des Versicherten: Ändern der Vertraulichkeitsstufe im Zuge der Wiedereinstellung eines Dokumentes in die ePA
- Suche nach einer bestimmten Dokumentenkategorie oder Fachgebiet
- Auf Wunsch des Versicherten: Löschen eines Dokumentes (auf das die Leistungserbringerinstitution berechtigt ist)

ePA-Fachmodul des Konnektors

- Steuerung der Anzeige und der Bestätigung der am Primärsystem erstellten Berechtigung am Kartenterminal
- Erstellung einer Berechtigung (Policy) gemäß ePA Stufe 2

Aktensystem

- Definition geeigneter Policies und Rules entsprechend den gesetzlichen Vorgaben
- Aktualisierung von Metadaten und Value Sets
- Unterstützung individueller Policies der Versicherten für die feingranulare Steuerung von Berechtigungen auf einzelne Dokumente
- Prüfung der Verträglichkeit individueller Policies des Versicherten mit den gesetzlichen Vorgaben

4.2.1.3 Erweiterung des Datenmodells und Release unabhängiges Einbringen neuer strukturierter Dokumentenformate

Die Erweiterung des bestehenden Datenmodells der ePA wird durch § 341(2) und § 354(2)2 PDSG motiviert. Jedoch werden zukünftig weitere strukturierte Datenformate und ggf. Dokumentenarten definiert werden (z. B. wietere durch die KBV festgelegte MIOs). In Folge dessen müssen einerseits für die ePA gültige Dokumentenformate freigegeben und bereitgestellt werden und andererseits die technischen Voraussetzungen zum Einbringen und Verarbeiten dieser in den Clients und dem Aktensystem geschaffen werden.

Ersteller von Dokumentenformaten können bspw. Institutionen des Gesundheitswesens wie die KBV (für medizinische Informationsobjekte) oder Hersteller sein, die diese der gematik zur Bereitstellung übermitteln können. Gültige und vom Aktensystem zu unterstützende Dokumentenformate werden von der gematik zentral zur Verfügung gestellt. Für die Bereitstellung wird kein neuer Dienst der Telematikinfrastruktur bzw. Produkttyp definiert, sondern bestehende Bereitstellungspunkte für Hersteller wie bspw. VESTA oder das Fachportal genutzt. Hersteller können diese Formate von dort beziehen und ihre Produkte um diese erweitern.

Um neue Dokumentformate (bzw. medizinische Informationsobjekte) in der ePA verarbeiten zu können, müssen die XDS-Metadaten, d.h. die Value Sets, dynamisch erweitert werden. Die zulässigen Value Sets werden von der gematik verwaltet und für die Hersteller ebenfalls an zentraler Stelle durch die gematik bereitgestellt. Für das Einbringen neuer Dokumentenformate und Value-Sets in die entsprechenden Produkte wird ein Mechanismus spezifiziert, der ein zulassungsunabhängiges Einbringen neuer Dokumentenformate erlaubt.

Die Umsetzung strukturierter Dokumentenformate erfolgt in den folgenden Komponenten:

Primärsysteme, ePA-FdV und ePA-FdV AdV

- Unterstützung neuer strukturierter Dokumentenformate
- Unterstützung neuer bzw. erlaubter XDS-Metadaten bzw. Value Sets
- Umsetzung des zulassungsunabhängigen Mechanismus zum Einbringen neuer strukturierter Dokumentenformate

ePA-Aktensystem

- Unterstützung neuer bzw. erlaubter XDS-Metadaten bzw. Value Sets
- Umsetzung des zulassungsunabhängigen Mechanismus zum Einbringen neuer XDS-Metadaten bzw. Value Sets

4.2.1.4 Schemakonformität und Rendering-Vorschriften für strukturierte Dokumente

Ein systemübergreifender Datenaustausch erfordert, dass alle beteiligten Systeme die prozessrelevanten Daten miteinander in geeigneter Form austauschen und verarbeiten können und insbesondere bezüglich der Daten ein gleiches Verständnis haben. Dieses einheitliche Verständnis wird durch die Vorgabe und Nutzung einheitlicher Schemata und Vorschriften erreicht.

Die Erstellung eines schemakonformen Dokumentes erfolgt, wie auch das Rendering von Dokumenten, üblicherweise in der Fachlogik des Clients, wohingegen die Prüfung eines Dokumentes auf Konformität durch den Server erfolgt. Jedoch ist die serverseitige Konformitätsprüfung durch das Aktensystem aufgrund der Ende-zu-Ende Verschlüsselung der Dokumente nicht möglich. Aus diesem Grund muss auf eine Prüfung zur Laufzeit verzichtet werden. Der Verzicht auf diese Prüfung wiederum zieht eine stärkere Fokussierung bzw. Durchsetzung der Nutzung von Schemata in den Clients nach sich, um die Verarbeitbarkeit der Dokumente von verschiedensten Clients zu gewährleisten.

Die Funktionalität *Rendering* ermöglicht es, dass allen Akteuren strukturierte Inhalte, die sie zwar aus der ePA herunterladen können, deren Format ihnen aber unbekannt ist, immer auch in mindestens einem menschenlesbaren Standardformat angezeigt werden. Das clientseitige Rendering erlaubt überdies eine endgerätespezifische Darstellung der Daten.

In diesem Zusammenhang definiert die Kassenärztliche Bundesvereinigung (KBV) medizinische Informationsobjekte (MIOs). Diese MIOs bilden die Grundlage für eine einheitliche Strukturierung der Dokumente und können somit auch als Schema verwendet werden, um eine Konformität zu prüfen. Eine Aussage ob und wie eine Konformitätsprüfung erfolgt, kann aktuell noch nicht getroffen werden.

Um die von der KBV festgelegten MIOs in geeigneter Form dem Nutzer darstellen zu können, wird die KBV den Herstellern einen sogenannten MIO-Viewer zur Verfügung stellen, der in die entsprechenden Produkte integriert werden kann. Es ist aber auch möglich, dass Hersteller eigenen Rendering-Mechanismus verwenden.

Die Umsetzung konformer, strukturierten Dokumentenformate sowie das Rendering dieser werden durch folgende Clients durchgeführt:

Primärsysteme

- Konforme Unterstützung neuer strukturierter Dokumentenformate
- Fachlich korrekte Darstellung der Dokumentenformate (Rendering)

ePA-FdV und ePA-FdV AdV

- Fachlich korrekte Darstellung der Dokumentenformate (Rendering)

Das konkrete Verfahren zur Bestätigung der Konformität für das jeweilige strukturierte Dokumentenformat wird im Rahmen der Spezifikationserstellung eruiert.

4.2.1.5 Passdokumente

Der Umgang mit elektronischen Passdokumenten unterliegt besonderen Rahmenbedingungen. Passdokumente sollen für den jeweiligen Zweck zu jedem Zeitpunkt in genau einer aktuell gültigen Version vorliegen (Eindeutigkeit). Es erfolgt zwar eine Versionierung, jedoch wird dem zugreifenden Nutzer zunächst nur die aktuellste Version des Dokumentes angezeigt. Es besteht aber für den Versicherten auch die Möglichkeit, Einsicht in Vorversionen zu nehmen. Infolgedessen stellt das Aktensystem die Eindeutigkeit und die Versionierung eines Passdokumentes sicher. Darüber hinaus ist es bei bestimmten Passdokumenten (bspw. den Mutterpass) notwendig, dass es mehrere Instanzen eines Passdokumentes geben muss (z. B. pro Kind einen eigenen Mutterpass).

Um die verschiedenen Passarten im ePA-Aktensystem unterstützen zu können, werden weitere von IHE nativ unterstützte Document Associations für die Verwendung in der Fachanwendung ePA eingeführt. Die aktuell vorzusehenden Passdokumente Impfausweis, Mutterpass, Untersuchungsheft für Kinder sowie Zahnbonusheft werden inhaltlich von der KBV über FHIR-Ressourcen als XML-Dokumente definiert. Über die Metadaten sind diese Pässe im Aktensystem eindeutig auffindbar.

Darüber hinaus müssen bestimmte, durch die KBV festgelegte, Passeinträge aufgrund ihrer medizinischen Bedeutung authentisch und integer sein. Dies wird durch das Signieren beim Einstellen von Passeinträgen durch den Leistungserbringer und dem Prüfen der Signaturen beim Verarbeiten bzw. Anzeigen eines Passdokumentes durch das Primärsystem erreicht. Die Signaturprüfung an einem vom Versicherten genutztem Client ist nicht vorgesehen.

Die Umsetzung der Passdokumente erfolgt in den folgenden Komponenten:

Primärsystem

- Anzeige von Passdokumenten

- Je nach Festlegung für einen Passeintrag: Auslösen einer Signaturprüfung
- Transformation in ein lesbares Format
- Aktualisierung von Passdokumenten
- Je nach Festlegung für einen Passeintrag: Auslösen einer Signatur des Eintrags
- Abhängig von der Festlegung im Rahmen der MIO-Erstellung: entweder Löschen des Passes in Gänze oder auch Löschen einzelner Einträge

ePA-FdV

- Vergabe von Berechtigungen auf Passdokumente gemäß verfeinertem Berechtigungskonzept
- Anzeige von Passdokumenten
- Abhängig von der Festlegung im Rahmen der MIO-Erstellung: entweder Löschen des Passes in Gänze oder auch Löschen einzelner Einträge
- Export von Passdokumenten

ePA-FdV AdV

- Vergabe von Berechtigungen auf Passdokumente gemäß verfeinertem Berechtigungskonzept
- Anzeige von Passdokumenten
- Abhängig von der Festlegung im Rahmen der MIO-Erstellung: entweder Löschen des Passes in Gänze oder auch Löschen einzelner Einträge

Aktensystem

- Unterstützung aller neuen Assoziationen
- Unterstützung von Versionierung oder Fortschreibung der Pässe

4.2.1.6 Verfahren zur gezielten Umschlüsselung

Die Umschlüsselung umfasst den Wechsel folgender kryptographischer Schlüssel:

- den betreiberspezifischen Schlüssel
- den Akten- und Kontextschlüssel des Versicherten
- die Dokumentenschlüssel
- die Schlüsselgenerierungsdienste SGD1- und SGD2-Schlüssel aller berechtigten Nutzer

und kann nur durch den Versicherten durchgeführt werden.

Prinzipiell kann die Umschlüsselung serverseitig oder clientseitig erfolgen. Da jedoch das Sicherheitskonzept der ePA auf einer Ende-zu-Ende-Verschlüsselung der Dokumente basiert, dürfen Dokumente nur bei berechtigten Akteuren im Klartext vorliegen. Demzufolge kann die Umschlüsselung nur durch einen Client (ePA-FdV, ePA-FdV AdV und dem ePA-Fachmodul des Konnektors) durchgeführt werden. Da insbesondere bei mobilen Clients (ePA-FdV) besondere Randbedingungen gegeben sind – bspw. Performance, Bandbreite des Übertragungskanals und eine begrenzte Kapazität der Stromversorgung –

muss es auch die Möglichkeit geben, nur eine begrenzte Anzahl von kryptographischen Operationen auf einmal auszuführen. Dies betrifft insbesondere die Umschlüsselung von Dokumenten. Infolgedessen kann die Umschlüsselung nur für aufgerufene Dokumente und somit schrittweise durchgeführt werden – es besteht jedoch auch die Möglichkeit, alle Dokumente auf einmal umzuschlüsseln. Die schrittweise Umschlüsselung von Dokumenten erfordert ein Versionsmanagement bzw. Vorhalten von alten und des neuen Aktenschlüssels, bis alle Dokumentenschlüssel mit dem neuen Aktenschlüssel verschlüsselt wurden. Das Generieren der neuen Schlüssel erfolgt im Client (Dokumentenschlüssel, Akten- und Kontextschlüssel) oder mittels Aufruf des Schlüsselgenerierungsdienstes (SGD) für die SGD1- und SGD2-Schlüssel.

Dem Versicherten ist es zu jeder Zeit möglich den Umschlüsselungsprozess mittels ePA-FdV oder ePA-FdV AdV zu initiieren. Für Versicherte, die kein FdV oder kein KTR-AdV-Terminal nutzen wollen und somit hierüber keinen Schlüsselwechsel explizit auslösen können, bestünde die Möglichkeit, einen expliziten Schlüsselwechsel über organisatorische Prozesse bei ihrem Kostenträger auslösen zu lassen. Darüber hinaus kann die Umschlüsselung in regelmäßigen Zeitabständen (z. B. nach einer Zeitspanne von 5 Jahren) vom Aktensystem initiiert werden: Das Aktensystem sendet nach erfolgter Anmeldung des Versicherten am Aktensystem eine Aufforderung zur Umschlüsselung an das ePA-FdV, ePA-FdV AdV oder in Folge einer Ad-hoc-Berechtigung eines Leistungserbringers dem ePA-Fachmodul des Konnektors.

Nach erfolgter Initiierung generiert der jeweilige Client nun transparent für den Nutzer neues Schlüsselmaterial und hinterlegt dieses – neben dem bisher vorhandenem Schlüsselmaterial - für alle Berechtigten in der Komponente Autorisierung. Das Aktensystem verschlüsselt nun die im Zuge der Anmeldung in der VAU vorliegenden Metadaten mit dem neuen Kontextschlüssel und schließ die VAU anschließend.

Die eigentliche Umschlüsselung der Dokumente kann mittels ePA-FdV oder ePA-FdV AdV durch Abruf aller Dokumente einer Akte erfolgen oder schrittweise pro abgerufenem Dokument innerhalb einer Aktensitzung (ePA-FdV, ePA-FdV AdV und dem ePA-Fachmodul des Konnektors). Somit ist bspw. der gesamte Prozess der Umschlüsselung völlig transparent für den Leistungserbringer, erfordert keine Interaktion durch diesen und es werden keine spürbaren Zusatzressourcen im Konnektor gebunden.

Für den Wechsel des betreiberspezifischen Schlüssels ist der Versicherte nicht notwendig. Die Umschlüsselung kann vom Betreiber durchgeführt werden. Sie muss jedoch innerhalb einer vertrauenswürdigen Ausführungsumgebung (VAU) erfolgen, um den Zugriff des Betreibers auf die Metadaten technisch auszuschließen.

Generell gilt, dass Fehler in den Umschlüsselungsprozessen nicht zu inkonsistenten Zuständen der elektronischen Patientenakte führen dürfen. Daher Bedarf es nun auch eines Schlüsselversionsmanagements, um jederzeit eine eindeutige Beziehung zwischen Akten- und Dokumentenschlüssel herstellen und nicht mehr benötigte Schlüssel löschen zu können.Die Umsetzung der Umschlüsselung wird durch folgende Produkttypen durchgeführt:

ePA-FdV und ePA-FdV AdV

- Schlüsselmaterial erneuern
- Ausführen der Umschlüsselung für alle zu einer Akte gehörenden Dokumente nach Aufforderung durch den Versicherten
- Ausführen der Umschlüsselung für Dokumente einer Aktensession
- Anzeige des Umschlüsselungsstatus der ePA-Dokumente (z. B. Anzahl noch nicht mit dem aktuellen Aktenschlüssel verschlüsselter Dokumentenschlüssel)

ePA-Fachmodul des Konnektors

- Schlüsselmaterial erneuern (regelmäßige oder anlassbezogene Umschlüsselung)
- Ausführen der Umschlüsselung für Dokumente einer Aktensession

Aktensystem

- Umschlüsselung der Meta-Daten mit dem neuen Kontextschlüssel
- Verwalten der Zugehörigkeit von Akten- und Dokumentenschlüssel
- Verwaltung des aktuellen und der alten Aktenschlüssel
- Verwaltung der Schlüsselwechselintervalle

Die Umsetzung der Umschlüsselung betrifft folgende Anbietertypen:

Anbieter Aktensystem

- Der Betreiber des ePA-Aktensystems wird verpflichtet, den betreiberspezifischen Schlüssel regelmäßig oder bei Bedarf anlassbezogen zu wechseln, damit die beim Betreiber gespeicherten, mit dem Kontext- und Aktenschlüssel der Versicherten verschlüsselten Daten immer zusätzlich mit einem sicheren, dem aktuellen Stand der Technik entsprechenden Schlüssel gesichert sind.

4.2.1.7 ePA-FdV AdV

Die ePA-FdV AdV entspricht in vielen Vorgaben dem ePA-FdV. Unterschiede ergeben sich daraus, dass diese App nicht auf einem Gerät des Versicherten läuft. Daher wird hier nur die Anmeldung mit der eGK im lokalen Kartenterminal des KTR-AdV-Terminals (kontaktbehaftet und/oder kontaktlos) unterstützt.

Die ePA-FdV AdV verbindet sich über das Internet mit dem Zugangsgateway des Aktensystems. Die Verbindung der ebenfalls im KTR-AdV-Terminal vorhandenen KTR-AdV-App (zur eigenständigen Verwaltung der Anwendungen des Versicherten auf der elektronischen Gesundheitskarte) zum KTR-AdV-Server und darüber an das zentrale Netz der TI wird nicht nachgenutzt, da dies eine Abhängigkeit zwischen den zwei Produkttypen geschaffen hätte, die besonders im Bereich der Sicherheitsnachweise weitgehende Folgen gehabt hätte.

Aus Sicherheitsgründen bietet das KTR-AdV-Terminal nicht die Möglichkeit des Datenaustauschs mit lokalen Speichermedien. Daher können keine Dokumente in die ePA eingestellt oder aus der ePA gespeichert werden. Es darf auch keine Persistierung von Daten eines Nutzers derart erfolgen, dass ein nachfolgender Nutzer Rückschlüsse auf die vorherige Nutzungs-Session ziehen oder durch Manipulationen die Nutzungs-Session eines nachfolgenden Nutzers beeinflussen kann. Während der Verarbeitung von Daten eines Versicherten in der ePA-FdV AdV müssen diese Daten – insbesondere der Kontext- und Aktenschlüssel – durch eine vertrauenswürdige Ausführungsumgebung gegen den Zugriff durch Nutzer oder lokale Administratoren geschützt werden.

In der Anwendung ePA müssen die Geräte, auf denen FdVs ausgeführt werden, durch den Versicherten am Aktensystem registriert werden. Dieser Mechanismus ist so nicht auf die KTR-AdV-Terminals in einer Kostenträgergeschäftsstelle anwendbar. Dennoch muss sichergestellt werden, dass durch die Nutzung der ePA-FdV AdV nicht das Sicherheitsniveau für den Versicherten sinkt. Daher wird ein Prozess eingeführt, in dem der Versicherte durch einen Mitarbeiter der Kasse alle KTR-AdV-Terminals einer Geschäftsstelle als genutzte

Geräte für seine Akte registrieren lässt. Dabei ist sicherzustellen, dass die DeviceID eines KTR-AdV-Terminals niemals außerhalb des Aktensystems bekannt werden kann.

Die Umsetzung der ePA-FdV AdV führt zu Anpassungen an den folgenden Komponenten:

ePA-FdV AdV

- neuer Produkttyp mit einer Produktzulassung
- Nachweis der sicherheitstechnischen Eignung durch den Hersteller mittels Produkt- und Sicherheitsgutachten
- dieser Produkttyp orientiert sich am Produkttyp ePA-FdV

KTR-AdV-Terminal

- Der Produktgutachter des KTR-AdV-Terminals muss prüfen ob alle durch die ePA-FdV AdV formulierten Voraussetzungen an dessen Ausführungsumgebung im Terminal gegeben sind.

Aktensystem

- Das Aktensystem muss in Abstimmung mit dem Hersteller der ePA-FdV AdV und ggf. des KTR-AdV-Terminals eine Methode der Registration am Aktensystem bereitstellen.
- Im Aktensystem muss bekannt sein, welche Geräte in welcher Geschäftsstelle verortet sind, ohne dass außerhalb des Aktensystems DeviceIDs bekannt werden.

4.2.1.8 Migration von ePA Stufe 1 zu ePA Stufe 2

Migrationsaspekte sind sowohl für die Erweiterung des Datenmodells als auch für das mit ePA 2.0 eingeführte Berechtigungskonzept zu betrachten.

Für den Übergang der Berechtigungsvergabe von Stufe 1 zu Stufe 2 werden 2 Annahmen getroffen:

- Da Aktensystem, ePA-FdV und ePA-FdV AdV von den Kostenträgern angeboten werden, wird davon ausgegangen, dass für diese Produkttypen eine synchrone Umstellung auf das neue Berechtigungskonzept erfolgt, da die gematik hierfür die Voraussetzungen sowohl für die Client- als auch Aktensysteme geschaffen hat. Somit wird auch gewährleistet, dass der Versicherte ohne Verzögerungen die gesetzlich Verankerten Berechtigungen anwenden kann.
- Annahme 1 ist bei Primärsystemen und den von diesen genutzten Konnektoren nicht gegeben, da beide Komponenten nicht von einer einzigen Instanz verantwortet werden und die gematik auch über keine Regelungshoheit bezüglich einer terminierten Umsetzung von Funktionalitäten für Primärsystem verfügt.

Daraus folgt, dass die Migration für Frontends des Versicherten aus einem Update der Produkttypen besteht, wohingegen für Primärsystem und Konnektoren weiterhin die Berechtigungsvergabe gemäß ePA Stufe 1 solange durchgeführt wird, bis beide Komponenten Stufe 2 unterstützen. In dieser Übergangsphase wird der Konnektor auch weiterhin in der Lage sein, Policies gemäß Berechtigungskonzept der ePA Stufe 1 zu erstellen und an das Aktensystem zu übermitteln. Das Aktensystem transformiert dann die Stufe 1 Policy – wie auch bereits vorhandene Policies der Stufe 1 - in eine Stufe 2 Policy, um zumindest auf Seite des Aktensystems einheitlich mit der Berechtigungsrichtlinie gemäß ePA Stufe 2 zu arbeiten. Der Versicherte kann erst bei Umstellung von

Primärsystem und Konnektor auf ePA Stufe 2 seine vollen Rechte in Bezug auf die Berechtigungsvergabe beim Leistungserbringer wahrnehmen.

Im Zuge der Einführung neuer Metadaten und Value Sets in der ePA Stufe 2 und zukünftigen Änderungen am Datenmodel (durch bspw. neue strukturierte Datenformate) und der damit einhergehenden Einführung neuer oder Abkündigung bestehender Metadaten und Value Sets, müssen die Metadaten bestehender Dokumente migriert werden. Darüber hinaus müssen Festlegungen getroffen werden, unter welchen Bedingungen weiterhin alte Metadaten/Value Sets unterstützt werden. Prinzipiell kann eine technische Umsetzung im Zuge einer Anmeldung bzw. dem Öffnen einer Akte und demzufolge dem Vorliegen der Metadaten im Klartext und/oder auf Dokumentenebene bei Abruf und neu Einstellen eines bestehenden Dokumentes erfolgen.

Details zu Migrationsanforderungen sind in den entsprechenden Spezifikationen dokumentiert.

4.2.2 Geänderte Komponenten und Dienste

Tabelle 6: Übersicht geänderte Komponenten und Dienste

Art	Bezeichnung	Änderung
Produkttyp	ePA-FdV AdV	• Rollenprofile für Berufsgruppen • Verfeinertes Berechtigungskonzept • Erweiterung des Datenmodells und Release unabhängiges Einbringen neuer strukturierter Dokumentenformate • Passdokumente • Schemakonformität und Rendering-Vorschriften für strukturierte Dokumente • Verfahren zur gezielten Umschlüsselung
Produkttyp	ePA-Fachmodul KTR-Consumer	• Verfeinertes Berechtigungskonzept
Produkttyp	Konnektor: ePA-Fachmodul	• Verfeinertes Berechtigungskonzept • Verfahren zur gezielten Umschlüsselung
Produkttyp	ePA-FdV	• Rollenprofile für Berufsgruppen • Verfeinertes Berechtigungskonzept • Erweiterung des Datenmodells und Release unabhängiges Einbringen neuer strukturierter Dokumentenformate • Passdokumente • Schemakonformität und Rendering-Vorschriften für strukturierte Dokumente • Verfahren zur gezielten Umschlüsselung
Produkttyp	Aktensystem	• Rollenprofile für Berufsgruppen • Verfeinertes Berechtigungskonzept • Erweiterung des Datenmodells und Release unabhängiges Einbringen neuer strukturierter Dokumentenformate • Passdokumente • Verfahren zur gezielten Umschlüsselung • ePA-FdV AdV
Clientsystem	Primärsystem	• Rollenprofile für Berufsgruppen • Verfeinertes Berechtigungskonzept • Erweiterung des Datenmodells und Release unabhängiges Einbringen neuer strukturierter Dokumentenformate • Passdokumente • Schemakonformität und Rendering-Vorschriften für strukturierte Dokumente
Anbietertyp	Aktensystem	• Verfahren zur gezielten Umschlüsselung

4.3 KOM-LE

4.3.1 Übersicht der Änderungen

Mit KOM-LE 1.5 wird im Release 4.0 der in Kapitel 2.3 definierte fachliche Umfang zusätzlich zu KOM-LE 1.0 (Release 2.1) umgesetzt:

- Flexibilisierung der Integration in Primärsysteme
- Übermittlung von großen Dokumenten bis zu 500 MB
- Unterstützung von Nachrichten-Kategorien

Abbildung 11 zeigt die von den Änderungen betroffenen Produkttypen der TI und der angrenzenden IT-Systeme.

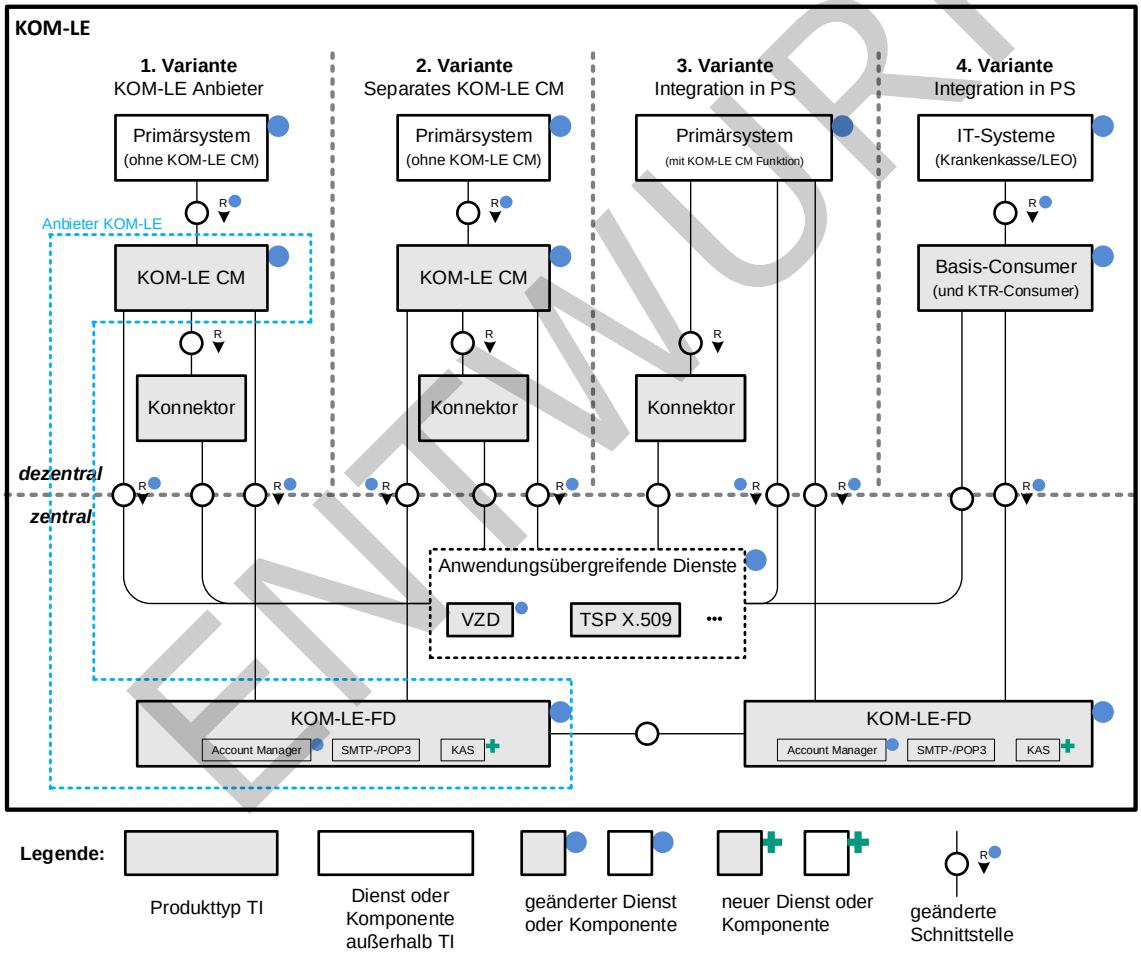


Abbildung 11: Übersicht über Neuerungen für KOM-LE 1.5 inklusive Produkttypen

4.3.1.1 Flexibilisierung der Integration in Primärsysteme

Um es Herstellern von Primärsystemen zu ermöglichen, die Funktionen des KOM-LE-Clientmoduls eigenständig zu entwickeln und in ihr PS zu integrieren, werden folgende Änderungen für KOM-LE 1.5 durchgeführt:

1. Für den Produkttyp KOM-LE-Clientmodul kann eine eigenständige Produktzulassung – unabhängig von KOM-LE-Anbieter – durch eigenständige Hersteller erworben werden. Hierbei wird eine Interoperabilität zu allen KOM-LE 1.5 Fachdiensten sichergestellt.

2. Ein KOM-LE-Anbieter (entsprechend [gemZUL Anbieter] muss weiterhin, neben dem KOM-LE-Fachdienst, ein eigenständiges KOM-LE-Clientmodul umsetzen, zulassen und für seine KOM-LE-Kunden bereitstellen.

3. Für PS-Hersteller besteht als Option die Möglichkeit die KOM-LE-Clientsystem-Funktionalität direkt in ihr PS zu integrieren. Der Einsatz eines KOM-LE-Clientmoduls entfällt bei dieser Option. Falls von PS-Herstellern diese Option gewählt wird, ist eine Zulassung der relevanten KOM-LE-TI-Anteile des PS notwendig. Hierfür wird ein neues Zulassungsverfahren eingeführt. Der Fokus liegt hierbei bei der Prüfung gegen die entsprechenden genutzten TI-Schnittstelle (u.a. Konnektor, VZD, KOM-LE-Fachdienst) unter funktionalen und sicherheitstechnischen Aspekten.

Für die KOM-LE Integration in die Clientseitige-Umgebung ergeben sich insgesamt die drei in Abbildung 11 dargestellten Varianten:

- Variante 1: Das PS nutzt das vom KOM-LE Anbieter bereitgestellte und durch die gematik bestätigte KOM-LE-Clientmodul.
- Variante 2: Das PS nutzt ein unabhängig vom KOM-LE-Anbieter entwickeltes KOM-LE-Clientmodul.
- Variante 3: Das PS integriert im Rahmen einer Eigenentwicklung durch den PS-Hersteller die KOM-LE-Clientmodul-Funktionalität. Relevant sind hierbei lediglich die Funktionalitäten bzw. Schnittstellen des KOM-LE-Moduls Richtung TI (d.h. Richtung KOM-LE FD, Konnektor und VZD).
- Variante 4: KOM-LE-Anbindung für Kassen und Leistungserbringerorganisationen mittels KTR-Consumer bzw. Basis-Consumer.

Die technische Schnittstelle zwischen KOM-LE-Clientmodul und KOM-LE-Fachdienst bzw. Konnektor sind bereits weitgehend in KOM-LE 1.0 interoperabel spezifiziert. Lediglich die Übermittlung des Schlüssels und des TLS-Zertifikats für die beidseitig authentisierte TLS-Verbindung zwischen KOM-LE-Clientmodul und KOM-LE-Fachdienst mittels einer passwortgeschützten PKCS#12 Datei und die Übermittlung des Passworts hierfür sind nicht interoperabel spezifiziert. Dies wird in KOM-LE 1.5 soweit wie notwendig nachgeholt.

Im Rahmen der Zulassung von KOM-LE Clientmodulen und KOM-LE-Fachdiensten sowie dem erwarteten übergangswiesen Parallelbetrieb von KOM-LE 1.0 und KOM-LE 1.5 stellt die gematik im Rahmen der nachzuweisenden eigenverantwortlichen Tests der Hersteller und der Zulassungstests der gematik eine ausreichende Interoperabilität von KOM-LE sicher.

4.3.1.2 Übermittlung von großen Dokumenten bis zu 500 MB

Aufgrund einer Limitierung im Konnektor können derzeit nur Dokumente mit einer maximalen Größe von 25 MB signiert und verschlüsselt werden. Da KOM-LE bei der Übermittlung sowohl eine Nachrichtensignatur durch den Konnektor (unter Verwendung von ID.HCI.OSIG der SMC-B des Senders) als auch eine Verschlüsselung durch den Konnektor (unter Verwendung von ID.HCI.ENC der SMC-B bzw. ID.HP.ENC des HBA der Empfänger) durchführt, ergibt sich für KOM-LE 1.0 eine übertragbare maximale Dokumenten- bzw. Nachrichtengröße von 25 MB je Nachricht (E-Mail).

Mit KOM-LE 1.5 wird der Versand von Nachrichten bis zu einer Größe von 500 MB unterstützt. Die maximale Nachrichtengröße soll hierbei im KOM-LE-FD konfigurierbar und damit leicht anpassbar sein.

Bei Nachrichten bis zu einer Größe von 25 MB wird eine vollständige Rückwärtskompatibilität zu KOM-LE 1.0 sichergestellt. Ebenfalls ist mit KOM-LE 1.5 weiterhin der Einsatz von Standard-E-Mail-Client (analog zu KOM-LE 1.0) möglich.

Große Dokumente werden hierzu nicht mehr über E-Mail (SMTP/POP3) übertragen, sondern zur Übermittlung sicher auf einem Speichersystem des KOM-LE-FD abgelegt. Hierzu werden bei großen Nachrichten über 25 MB, die vom PS an das KOM-LE-CM übertragen werden, alle Anhänge der E-Mail symmetrisch verschlüsselt, beim KOM-LE-FD in einer neuen Komponente KOM-LE-Attached-Service (KAS) abgelegt, und anschließend aus der E-Mail entfernt. Die Verschlüsselung der Anhänge findet über das KOM-LE-CM statt. Die Lokalisierung der Dokumente am KAS ist über eine vergebene URL möglich. In der KOM-LE E-Mail selbst wird die URL und der symmetrische Schlüssel übertragen und hierbei analog zu KOM-LE 1.0 mit den Funktionen des Konnektors mittels SMC-B signiert und mittels SMC-B bzw. HBA für den Empfänger verschlüsselt. Beim Empfang einer derartigen E-Mail durch ein KOM-LE-1.5-Modul werden die über die URL verfügbaren Anhänge vom KAS geladen, entschlüsselt und als Anhang der E-Mail angehängt.

Falls die Funktionalitäten eines KOM-LE-1.5-CM direkt in das PS integriert werden (siehe Variante 3 in Kapitel 4.3.1.1) übernimmt das PS selbst die im vorhergehenden Absatz dargestellt Übermittlung der großen Nachrichten.

Im VZD wird durch den KOM-LE-Anbieter ab KOM-LE 1.5 für jeden KOM-LE-Teilnehmer die unterstützte KOM-LE-Version in den fachdienstspezifischen Daten abgelegt. Anhand dieser Information kann ein PS und ein KOM-LE-CM beim bzw. vor dem Versand von großen Nachrichten erkennen, ob die Empfänger diese Nachricht auch empfangen können und eine Rückmeldung hierzu an den Nutzer geben. Das KOM-LE-CM verhindert den Versand von großen Nachrichten, falls der Empfänger nicht mindestens KOM-LE 1.5 einsetzt.

Damit auch Organisationen des Gesundheitswesens, die KOM-LE einsetzen und hierbei über den Basis-Consumer bzw. KTR-Consumer an die TI gebunden sind, die Funktionen von KOM-LE 1.5 nutzen können, werden ebenfalls Basis-Consumer und KTR-Consumer für KOM-LE 1.5 angepasst. Ein einer Übergangszeit bleiben ebenfalls Basis-Consumer und KTR-Consumer mit dem KOM-LE 1.0 Funktionsumfang gültige Zulassungsobjekte.

4.3.1.3 Unterstützung von Nachrichten-Kategorien

Zur Unterstützung von Nachrichten-Kategorien wird ab KOM-LE 1.5 ein weiteres KOM-LE-spezifisches Attribut im E-Mail-Header als Pflichtfeld aufgenommen. Die Nachrichten-Kategorie soll bereits im PS bzw. Basis-/KTR-Consumer gesetzt werden. Das Attribut wird ebenfalls transparent in der äußeren KOM-LE E-Mail Nachricht übertragen, die vom KOM-LE-CM erzeugt wird. Hierdurch ist sichergestellt, dass beim Empfänger der Nachricht bereits vor dem Entschlüsseln der Nachricht eine automatische Vorverarbeitung der Nachricht möglich ist. Falls ein Clientsystem (bspw. ein Standard-E-Mail-Client) das Attribut nicht setzten kann, setzt das KOM-LE-1.5-CM ein Default-Wert.

Aufgrund der notwendigen Rückwärtskompatibilität zu KOM-LE 1.0 müssen für KOM-LE 1.5 weiterhin auch KOM-LE Nachrichten ohne vorhandenes Attribut zur Nachrichten-Kategorie verarbeitet werden. KOM-LE-Fachdienste und KOM-LE-Clientmodule aus KOM-LE 1.0 leiten dieses Attribut transparent weiter. Empfänger wie z.B. Primärsysteme mit KOM-LE 1.0 Unterstützung und Standard-E-Mail-Clients ignorieren dieses Attribut beim Empfang.

Die gematik pflegt eine Liste mit aktuell gültigen Kategorien und veröffentlicht diese. Zusätzlich wird mit der Veröffentlichung einer Kategorie auf weiterführende Regelungen

der jeweiligen Gesellschafter der gematik bzw. der gematik zu den Kategorien referenziert (beispielsweise Vorgaben zum Nachrichtenformat für die Kategorie). Änderungen zu den gültigen Kategorieneinträgen können durch die gematik und deren Gesellschafter veranlasst werden. Komponenten und Dienste der TI dürfen keine inhaltliche Prüfung der Nachrichten-Kategorien vornehmen. Für Primärsysteme können Regelungen über die PS-Implementierungsleitfäden der gematik aufgenommen werden, falls in einzelnen Anwendungsfällen spezifische Kategorien zu verwenden sind.

4.3.2 Betrieb

Die neuen betriebliche Kenngrößen und Schwellwerte, anhand derer das Last- und Performanceverhalten sowie die Verfügbarkeit des Fachdienstes präziser gemessen und nachgewiesen werden sollen, werden in den nachfolgenden Spezifikationen festgelegt. Dort werden auch die Schnittstellen, Operationen, Messpunkte u.a. definiert, an denen die Kenngrößen ermittelt und gemessen werden können.

Der Fachdienst KOM-LE erhebt zukünftig Performance-Messdaten, welche die definierten betrieblichen Kenngrößen darstellen.

4.3.3 Geänderte Komponenten und Dienste

Tabelle 7 gibt eine Übersicht der vom KOM-LE 1.5 betroffen Produkttypen, Anbietertypen und IT-Systemen.

Tabelle 7: Übersicht geänderte Komponenten und Dienste

Art	Bezeichnung	Änderung
Clientsystem	PS	• Möglichkeit zur Integration der KOM-LE-CM Funktionalität, einschl. Zulassungsverfahren hierzu. • Bei großen (> 25 MB) KOM-LE-Nachrichten, Prüfung ob Empfänger hierzu in der Lage ist (über VZD-Eintrag) • Unterstützung von KOM-LE-Nachrichten-Kategorien
Produkttyp	KOM-LE-CM	• Umgang mit großen (> 25 MB) Nachrichten beim Versand und Empfang • Weiterleitung der KOM-LE-Nachrichten-Kategorien • Eigenständiges Zulassungsverfahren für KOM-LE-CM • Anpassung, um Schnittstelle zu KOM-LE-FD vollumfänglich interoperabel auszugestalten
Produkttyp	KOM-LE FD	• Bereitstellung KOM-LE-Attached-Service (KAS) • Anpassung um Schnittstelle zu KOM-LE-FD vollumfänglich interoperabel auszugestalten. • Anpassungen zu betrieblichen Reporting von Kennzahlen
Anbietertyp	Fachdienst KOM-LE	• Bereitstellung KOM-LE-CM
Produkttyp	VZD	• Anpassung der fachdienstspezifischen Daten für KOM-LE
Produkttyp	Basis-Consumer KTR-Consumer	• Umgang mit großen Nachrichten KOM-LE-Attached-Service beim Versand und Empfang • Weiterleitung der KOM-LE-Nachrichten-Kategorien • Anpassung um Schnittstelle zu KOM-LE-FD vollumfänglich Interoperabel auszugestalten

4.4 E-Rezept

4.4.1 Aufbau und Funktionsweise

Der technische Aufbau der Fachanwendung E-Rezept und die dazu gehörigen Abläufe werden im Dokument [gemSysL_eRp] beschrieben. Daher wird im Folgenden auf eine detailliertere technische Beschreibung der Fachanwendung bzw. des E-Rezept-Fachdienst verzichtet. Eine Übersicht über den logischen Aufbau der zusammenwirkenden Komponenten gibt Abbildung 12.

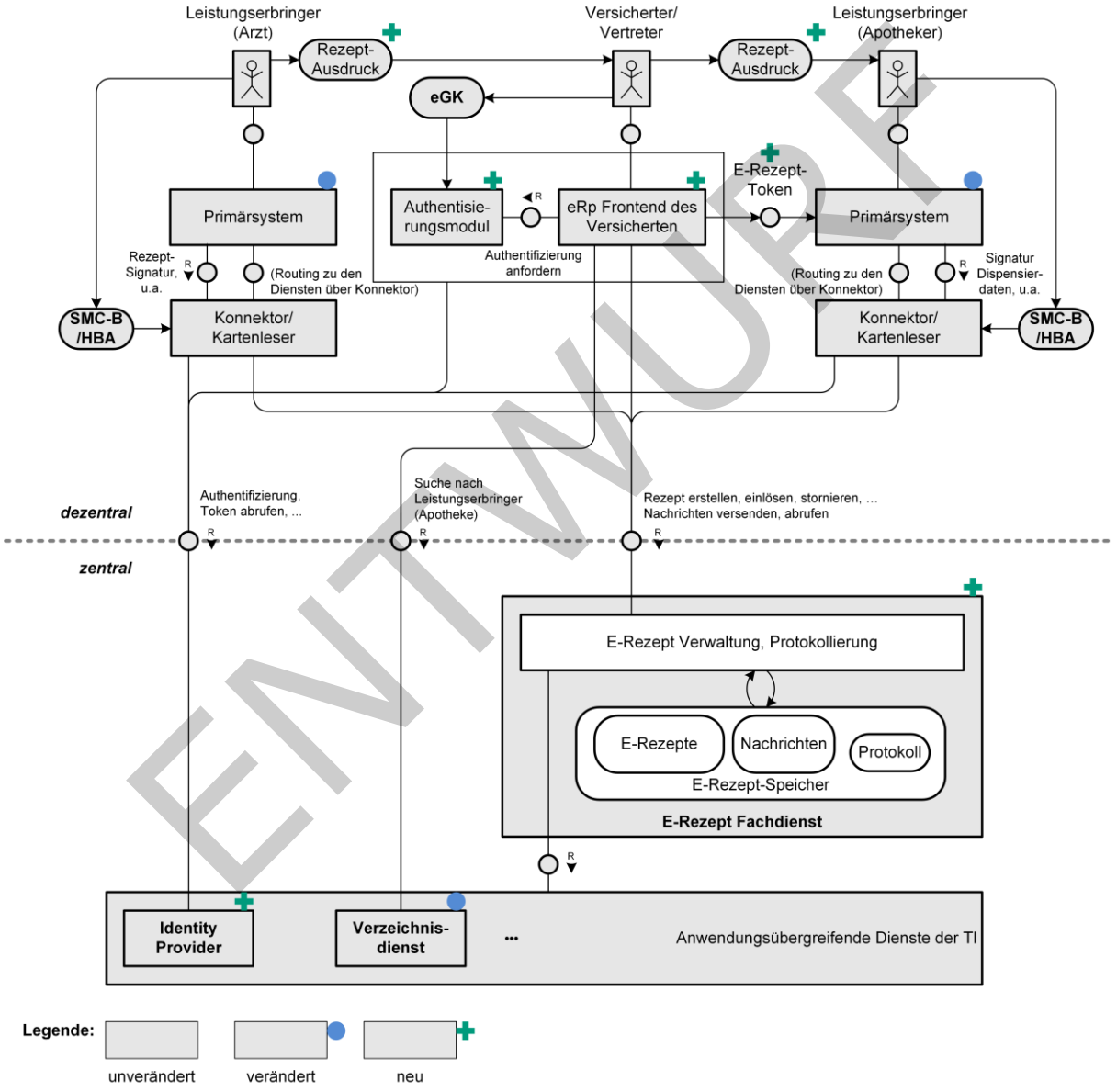


Abbildung 12: Funktionaler Aufbau der fachanwendungsspezifischen Funktion E-Rezept

Zur Umsetzung der Anwendungsfälle wird neben dem neuen E-Rezept-Fachdienst auch ein weiterer neuer Dienst Identity Provider (IdP) benötigt. Dieser wird in Kapitel 4.1.1 dieses Dokumentes beschrieben.

Vom Ablauf her erstellt der verordnende Leistungserbringer für einen Versicherten ein E-Rezept, welches auf dem zentralen E-Rezept-Fachdienst abgelegt wird. Der Standardfall sieht vor, dass der Versicherte seine E-Rezepte mit dem E-Rezept-FdV auf seinem technischen Endgerät verwaltet. Zur Authentisierung nutzen Versicherte bzw. deren Vertreter in der ersten Ausbaustufe NFC-fähige eGKs und NFC-fähige Endgeräte. Der Versicherte kann über sein Frontend im Verzeichnisdienst die Apotheke seiner Wahl aussuchen und sie für die Abgabe der ausgestellten Arzneimittel berechtigen. Die Zugriffs-Berechtigung auf das E-Rezept erfolgt mittels einer elektronischen Übertragung eines für das E-Rezept ausgestellten E-Rezept-Tokens durch den Versicherten an die Apotheke. Für Versicherte ohne eigenes Endgerät bzw. ohne NFC-fähige eGK wird vom verordnenden Leistungserbringer der E-Rezept-Token als 2D-Code sowie beschreibende Rezept-Daten ausgedruckt, mit denen sich der Versicherte an eine Apotheke seiner Wahl wenden kann.

In der E-Rezept-Version 1.0 (Release 4.0) ist eine direkte Kommunikation zwischen dem Versicherten und Apotheken über das E-Rezept vorgesehen (eine im E-Rezept-Fachdienst integrierte Kommunikationsfunktion). Rückfragen zwischen dem abgebenden und dem verordnenden Leistungserbringer können unabhängig davon über KOM-LE erfolgen.

In der Apotheke wird die Abgabe der Arzneimittel auch elektronisch auf dem E-Rezept-Fachdienst vollzogen und quittiert.

Die Umsetzung von Komfort-QES-Signatur-Funktionen wird für ein Maintenance-Release, rechtzeitig zur Verfügbarkeit des Fachdienstes E-Rezept angestrebt..

Versicherte haben jederzeit die Hoheit über auf sie ausgestellte E-Rezepte, da jeglicher Zugriff auf ein konkretes Rezept im E-Rezept-Fachdienst entweder nur den Versicherten selbst, ihren Vertreter oder Apotheken möglich ist, die den entsprechenden E-Rezept-Token erhalten haben.

4.4.2 Sicherheit und Datenschutz

Da der E-Rezept-Fachdienst den Zugriff auf personenbezogene medizinische Daten ermöglicht, ist er bei den Schutzzielen Vertraulichkeit und Integrität mit einem Schutzbedarf von sehr hoch bewertet. Insbesondere dürfen die im E-Rezept-Fachdienst verarbeiteten personenbezogenen Daten nicht zu unzulässigen Verarbeitungszwecken verwendet werden.

Zur Einhaltung der Vorschriften des Datenschutzes ist technisch sicherzustellen, dass beim E-Rezept-Fachdienst keine Profilbildung durch den Anbieter des E-Rezept-Fachdienstes erfolgen kann.

Der Schutzbedarf für die Verfügbarkeit des E-Rezept Fachdienstes ist hoch.

Der E-Rezept-Fachdienst erkennt die von dem E-Rezept-FdV mitgeteilte Versionsnummer und kann festgelegte Versionsnummern abweisen (bspw. abgekündigte Versionen oder Versionen mit erheblichen Sicherheitslücken).

4.4.3 Betrieb

Der E-Rezept-Fachdienst ist nur einmalig in der TI vorhanden und wird als neue Servicekomponente in das übergreifende TI-ITSM integriert. Für den Dienst ist aus Akzeptanz- und Versorgungsgründen eine sehr hohe Verfügbarkeit erforderlich, unterteilt nach Haupt- und Nebenzeit.

Operative Betriebsleistungen werden anhand eines entsprechenden Anbietertypsteckbriefs durch einen von der gematik beauftragten Dienstleister erbracht. Bei Bedarf koordiniert

der Anbieter des E-Rezept-Fachdienstes im Rahmen des TI-ITSM alle E-Rezept-fachanwendungsspezifischen Incidents.

Leistungserbringer können sich im Störungsfall an den User Help Desk des sie betreuenden VPN-Zugangsdienstes wenden. Versicherte wenden sich an einen von der gematik beauftragten Dienstleister, der den User Help Desk für das E-Rezept für Versicherte 24/7 bereitstellt.

Zur betrieblichen Steuerung hat der E-Rezept-Fachdienst Performance-Rohdaten zu erheben und in konfigurierbarer Frequenz an die Betriebsdatenschnittstelle zu liefern.

4.4.4 Zulassungsverfahren der Anwendung

Der Hersteller des Produkttyps E-Rezept-Fachdienst bedarf einer Produktzulassung. Die operativen Betriebsleistungen des Fachdienstes E-Rezept werden von einem durch die gematik beauftragten Dienstleister erbracht. Eine formale Anbieterzulassung nach Anbietertypsteckbrief ist daher nicht vorgesehen.

5 Übersicht Produkt- und Anbietertypen

Die folgenden beiden Tabellen liefern eine Übersicht über die Produkttypen bzw. Anbietertypen, die im Systemdesign enthalten sind. Die Tabellen zeigen außerdem, welche Produkt-/Anbietertypen

- unverändert sind („ - “),
- von Änderungen betroffen sind („Änd.“),
- neu eingeführt werden („neu“) oder
- ggf. entfallen („entf.“).

Die jeweilige Tabelle weist zusätzlich aus, ob ein Produkttyp zu einer bestimmten Anwendung oder zu den anwendungsübergreifenden Produkttypen (anw.übergr.) gehört („definiert“). Falls ein Produkttyp nicht zu einer Anwendung gehört, aber funktional dazu beiträgt, wird dies ebenfalls gezeigt („nutzt“).

Tabelle 8: Übersicht Produkttypen

Produkttyp	Änderung	anw.über.	AdV	VSDM	NFDM	eMP/AMTS	ePA	eRp	KOM-LE
~~Authentisierungsmodul~~	~~neu~~	~~definiert~~	~~-~~	~~-~~	~~-~~	~~-~~	~~-~~	~~nutzt~~	~~-~~
Basis-Consumer	Änd.	definiert	-	-	-	-	-	-	nutzt
CVC-Root – ECC	-	definiert	-	-	-	-	-	-	-
E-Rezept-Fachdienst	neu	-	-	-	-	-	-	definiert	-
E-Rezept FdV	neu	-	-	-	-	-	-	definiert	-
ePA-Aktensystem	Änd.	-	-	-	-	-	definiert	-	-
Fachdienst KOM-LE	Änd.	-	-	-	-	-	-	-	definiert
Fachdienst VSDM	-	-	-	definiert	-	-	-	-	-
gematik-Root-CA	-	definiert	-	-	-	-	-	-	-
HBA	-	definiert	-	nutzt	nutzt	nutzt	-	nutzt	nutzt
Identity Provider (inkl. Authentisierungsmodul)	neu	definiert	-	-	-	-	-	nutzt	-
Intermediär VSDM	-	-	-	definiert	-	-	-	-	-
Kartenterminal	-	definiert	-	nutzt	nutzt	nutzt	nutzt	nutzt	nutzt
KOM-LE-Clientmodul	Änd.	-	-	-	-	-	-	-	definiert
Konfigurationsdienst	-	definiert	-	-	-	-	-	-	-
Konnektor	Änd.	definiert	-	nutzt	nutzt	nutzt	nutzt	nutzt	nutzt
KTR-AdV	Änd.	definiert	nutzt	nutzt	nutzt	nutzt	nutzt	-	-
KTR-AdV-Terminal	Änd.	definiert	nutzt	nutzt	nutzt	nutzt	nutzt	-	-
KTR-Consumer	Änd.	definiert	-	-	-	-	nutzt	-	nutzt
Mobiles Kartenterminal	-	definiert	-	nutzt	-	-	-	-	-
Namensdienst	-	definiert	nutzt	nutzt	-	-	nutzt	nutzt	nutzt
OCSP-Responder-Proxy	-	definiert	nutzt	nutzt	nutzt	nutzt	nutzt	nutzt	nutzt
Schlüsselgenerierungsdienst ePA	Änd.	definiert	-	-	-	-	nutzt	-	-

Produkttyp	Änderung	anw.über.	AdV	VSDM	NFDM	eMP/AMTS	ePA	eRp	KOM-LE
Service Monitoring	Änd.	~~stellt bereit~~definiert	-	nutzt	-	-	nutzt	nutzt	nutzt
Sicherheitsgateway für Bestandsnetze	-	definiert	-	-	-	-	-	-	-
Signaturdienst	-	definiert	-	-	-	-	nutzt	-	-
SMC-B	Änd.	definiert	nutzt	nutzt	nutzt	nutzt	nutzt	nutzt	nutzt
Störungsampel	entf.								
TSP CVC	-	definiert	-	-	-	-	-	-	-
TSP X.509 nonQES - eGK	-	definiert	nutzt	nutzt	nutzt	nutzt	nutzt	nutzt	-
TSP X.509 nonQES - HBA	-	definiert	-	-	nutzt	nutzt	-	-	nutzt
TSP X.509 nonQES – Komp.	-	definiert	nutzt	nutzt	nutzt	nutzt	nutzt	nutzt	nutzt
TSP X.509 nonQES - SMC-B	-	definiert	nutzt	nutzt	nutzt	nutzt	nutzt	nutzt	nutzt
TSP X.509 QES	-	definiert	-	-	nutzt	-	-	nutzt	-
TSL-Dienst	-	definiert	nutzt	nutzt	-	-	nutzt	nutzt	nutzt
Verzeichnisdienst	Änd.	definiert	-	-	-	-	nutzt	nutzt	nutzt
VPN-Zugangsdienst	-	definiert	nutzt	nutzt	nutzt	nutzt	nutzt	nutzt	nutzt
Zeitdienst	-	definiert	nutzt	nutzt	nutzt	nutzt	nutzt	nutzt	nutzt
Zentrales Netz der TI	-	definiert	nutzt	nutzt	nutzt	nutzt	nutzt	nutzt	nutzt

Tabelle 9: Übersicht Anbietertypen

Anbietertyp	Änderung
Anbieter Basis-Consumer	-
Anbieter CVC TSPs für eGK	-
Anbieter ePA-Aktensystem	Änd.
Anbieter E-Rezept-Fachdienst	neu
Anbieter Fachdienst KOM-LE	Änd.
Anbieter HBA	-
Anbieter Identity Provider	neu
Anbieter KTR-AdV	Änd.
Anbieter Schlüsselgenerierungsdienst ePA	-
Anbieter Signaturerstellungsdienst	-
Anbieter SMC-B	-
Anbieter VPN-Zugangsdienst	-
Anbieter X.509 TSPs für eGK	-

Anhang A~~1~~ – Fachliche Übersichten

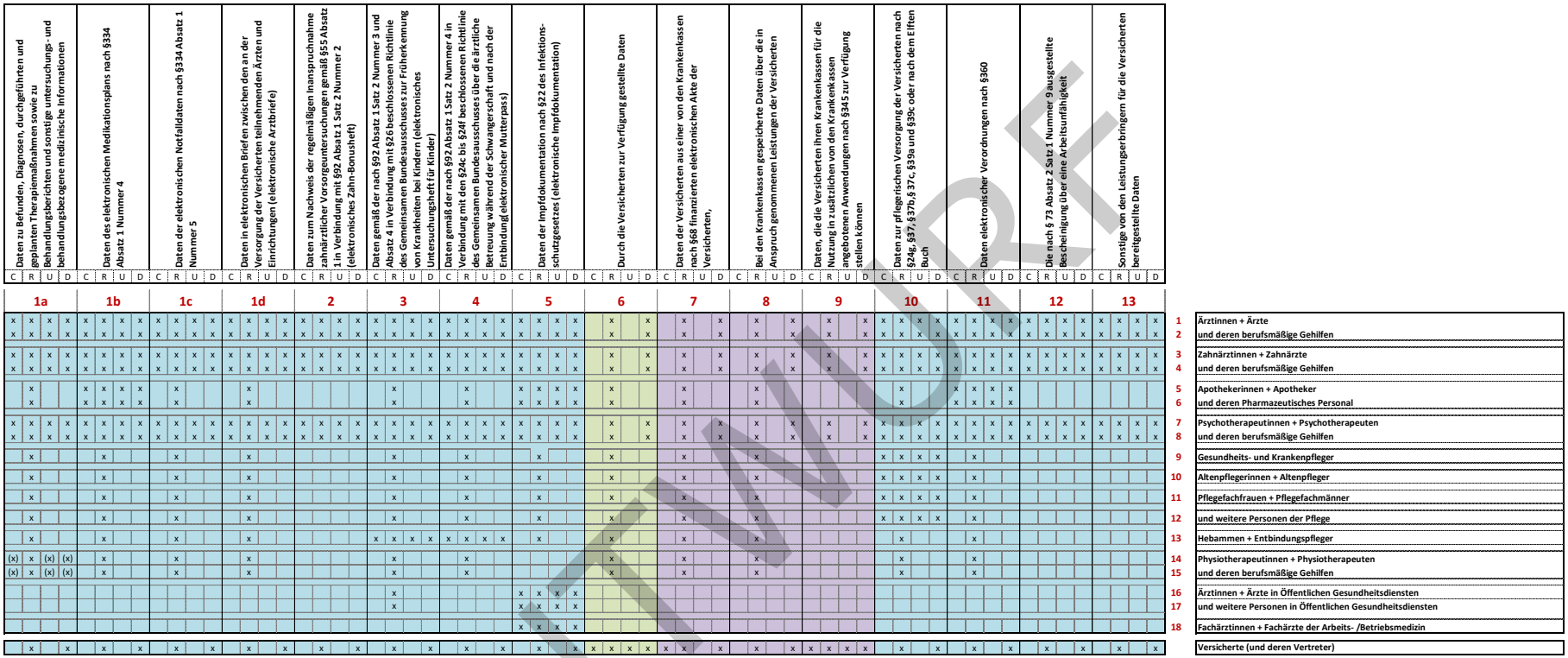
A1 – Berechtigte Berufsgruppen für den Zugriff auf die ePA entsprechend § 352 PDSG

	1a	1b	1c	1d	2	3	4	5	6	7	8	9	10	11	12	13	
	Daten zu Befunden, Diagnosen, durchgeführten und geplanten Therapiemaßnahmen sowie zu Behandlungsberichten und sonstige untersuchungs- und behandlungsbezogene medizinische Informationen	Daten des elektronischen Medikationsplans nach §334 Absatz 1 Nummer 4	Daten der elektronischen Notfalldaten nach §334 Absatz 1 Nummer 5	Daten in elektronischen Briefen zwischen den an der Versorgung der Versicherten teilnehmenden Ärzten und Einrichtungen (elektronische Arztbriefe)	Daten zum Nachweis der regelmäßigen Inanspruchnahme zahnärztlicher Vorsorgeuntersuchungen gemäß §55 Absatz 1 in Verbindung mit §92 Absatz 1 Satz 2 Nummer 2 (elektronisches Zahn-Bonusheft)	Daten gemäß der nach §92 Absatz 1 Satz 2 Nummer 3 und Absatz 4 in Verbindung mit §26 beschlossenen Richtlinie des Gemeinsamen Bundesausschusses zur Früherkennung von Krankheiten bei Kindern (elektronisches Untersuchungsheft für Kinder)	Daten gemäß der nach §92 Absatz 1 Satz 2 Nummer 4 in Verbindung mit den §24c bis §24f beschlossenen Richtlinie des Gemeinsamen Bundesausschusses über die ärztliche Betreuung während der Schwangerschaft und nach der Entbindung(elektronischer Mutterpass)	Daten der Impfdokumentation nach §22 des Infektionsschutzgesetzes (elektronische Impfdokumentation)	Durch die Versicherten zur Verfügung gestellte Daten	Daten der Versicherten aus einer von den Krankenkassen nach §68 finanzierten elektronischen Akte der Versicherten,	Bei den Krankenkassen gespeicherte Daten über die in Anspruch genommenen Leistungen der Versicherten	Daten, die die Versicherten ihren Krankenkassen für die Nutzung in zusätzlichen von den Krankenkassen angebotenen Anwendungen nach §345 zur Verfügung stellen können	Daten zur pflegerischen Versorgung der Versicherten nach §24g, §37, §37b,§ 37c, §39a und §39c oder nach dem Elften Buch	Daten elektronischer Verordnungen nach §360	Die nach § 73 Absatz 2 Satz 1 Nummer 9 ausgestellte Bescheinigung über eine Arbeitsunfähigkeit	Sonstige von den Leistungserbringern für die Versicherten bereitgestellte Daten	
	C R U D	C R U D	C R U D	C R U D	C R U D	C R U D	C R U D	C R U D	C R U D	C R U D	C R U D	C R U D	C R U D	C R U D	C R U D	C R U D	
1	x x x x	x x x x	x x x x	x x x x	x x x x	x x x x	x x x x	x x x x	x	x	x	x	x x	x x x x	x x x x	x x x x	Ärztinnen + Ärzte
2	x x x x	x x x x	x x x x	x x x x	x x x x	x x x x	x x x x	x x x x	x	x	x	x	x x	x x x x	x x x x	x x x x	und deren berufsmäßige Gehilfen
3	x x x x	x x x x	x x x x	x x x x	x x x x	x x x x	x x x x	x x x x	x	x	x	x	x x	x x x x	x x x x	x x x x	Zahnärztinnen + Zahnärzte
4	x x x x	x x x x	x x x x	x x x x	x x x x	x x x x	x x x x	x x x x	x	x	x	x	x x	x x x x	x x x x	x x x x	und deren berufsmäßige Gehilfen
5	x	x x	x x	x		x	x	x	x	x	x		x	x	x	x	Apothekerinnen + Apotheker
6	x	x x	x x	x		x	x	x	x	x	x		x	x	x	x	und deren Pharmazeutisches Personal
7	x x x x	x x x x	x x x x	x x x x	x x x x	x x x x	x x x x	x x x x	x	x	x	x	x x	x x x x	x x x x	x x x x	Psychotherapeutinnen + Psychotherapeuten
8	x x x x	x x x x	x x x x	x x x x	x x x x	x x x x	x x x x	x x x x	x	x	x	x	x x	x x x x	x x x x	x x x x	und deren berufsmäßige Gehilfen
9	x	x	x	x		x	x		x	x	x		x x x x	x		x	Gesundheits- und Krankenpfleger
10	x	x	x	x		x	x		x	x	x		x x x x	x			Altenpflegerinnen + Altenpfleger
11	x	x	x	x		x	x		x	x	x		x x x x	x			Pflegefachkräfte
12	x	x	x	x		x	x		x	x	x		x x x x	x			und weit. Personen der Pflege in oder abgeschl. Ausbildung
13	x	x	x	x		x x x x	x x x x		x	x	x		x	x			Hebammen + Entbindungspfleger
14	x	x	x	x		x	x		x	x	x		x	x			Physiotherapeutinnen + Physiotherapeuten
15						x		x									Ärztinnen + Ärzte in Öffentlichen Gesundheitsdiensten
16						x		x									und weitere Personen in Öffent. Gesund.
17								x									Fachärztinnen + Fachärzte der Arbeits- /Betriebsmedizin
	x x	x x	x x	x x	x x	x x	x x	x x	x x x x	x x x	x x x	x x	x x	x x	x x	x x	Versicherte (und deren Vertreter)
	01.01.2021	01.01.2021	01.01.2021	01.01.2021	01.01.2022	01.01.2022	01.01.2022	01.01.2022	01.01.2021	01.01.2022	01.01.2022	01.01.2023	01.01.2023	01.01.2023	01.01.2023	01.01.2023	Bereitstellung gemäß §342 Absatz 2 Nummer 1, 2 und 3

Legende:

Daten des Versicherten | Daten der Krankenkasse | Daten von Leistungserbringern

C = Create = Anlegen, Hochladen oder Import | R = Read = Lesen, Runterladen oder Export | U = Update = Schreiben, Aktualisieren | D = Delete = Löschen



Legende:

Daten des Versicherten | Daten der Krankenkasse | Daten von Leistungserbringern

C = Create = Anlegen, Hochladen oder Import R = Read = Lesen, Runterladen oder Export U = Update = Schreiben, Aktualisieren D = Delete = Löschen

(x) Recht gilt nur für Untermengen von Dokumenten wie bspw. Dokumente einer bestimmten Fachgruppe (bspw. physiotherapeutische Dokumente)

Anhang B – Verzeichnisse

B1 – Abkürzungen

Kürzel	Erläuterung
AdV	tbd. Endversion
AdV	
AMTS	
CA	
CVC	
CVC	
eGK	
eGK	
eMP	
ePA	
FdV	
g-SMC-K	
g-SMC-KT	
HBA	
KAS	
KOM-LE	
KTR-AdV	
MobKT	
OCSP	
PDSG	
PKI	
SGD	

Kürzel	Erläuterung
SM-B	
SM-B KTR	
SM-B Org	
SMC-B	
SMC-B	
SMC-B KTR	
SMC-B Org	
TI	
TI-ITSM	
TSL	
TSP	
VAU	
VPN-ZugD	
VSDM	
VZD	

B2 – Glossar

Das Glossar der gematik findet sich online unter https://fachportal.gematik.de/glossar/.

Fachwort	Definition
E-Rezept-Token	
Identity Provider (IdP)	
Komfort-QES-Signatur-Funktionen	

B3 – Abbildungsverzeichnis

B4 – Tabellenverzeichnis

B5 – Referenzierte Dokumente

B5.1 – Dokumente der gematik

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

Quelle	Herausgeber: Titel

~~B5.2 – Weitere Dokumente~~

~~Quelle~~	~~Herausgeber (Erscheinungsdatum): Titel~~