

Telematikinfrastuktur

Feature:

ePrescription/eDispensation Land B

Version: 1.0.0_CC
Revision: 1582983
Stand: 27.04.2026
Status: zur Abstimmung freigegeben
Klassifizierung: öffentlich_Entwurf
Referenzierung: gemF_ePeD-B

Dokumenteninformation

Gender-Hinweis

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

Änderungen zur Vorversion

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

Dokumentenhistorie

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
1.0.0_CC	27.04.2026		initiale Erstellung	gematik

Inhaltsverzeichnis

1 Einordnung des Dokuments	7
1.1 Zielsetzung.....	7
1.2 Zielgruppe.....	7
1.3 Abgrenzungen.....	7
1.4 Methodik	8
2 Allgemeine Rahmenbedingungen.....	10
2.1 Gesetzliche Regelungen in Deutschland.....	10
2.2 Rechtliche Rahmenbedingungen in der Europäischen Union	11
2.2.1 Vorgaben an ärztliche Verordnungen gemäß Durchführungsrichtlinie	
2012/52/EU.....	11
2.2.2 Vorgaben zu ePrescription und eDispensation gemäß eHN Guideline	11
2.3 Vorbedingungen zum Abruf von Verordnungsdaten aus dem EU-Ausland	11
2.4 Netzanbindung an das europäische Netzwerk	12
2.5 Validierung und Qualitätskontrolle der eingesetzten Terminologien.....	12
3 Anwendungsumfeld	14
3.1 Anwendungsszenario: ePrescription/eDispensation Land B.....	14
3.2 Akteure und Rollen	15
3.2.1 Selbstverwaltung.....	15
3.2.2 EU-Bürger.....	16
3.2.3 Leistungserbringer.....	16
3.2.4 Technische Betreiber.....	16
3.3 In Scope.....	17
3.4 Out of Scope.....	17
4 Motivation	20
4.1 Kontinuierliche Arzneimittelversorgung für chronisch erkrankte EU-Bürger	20
4.2 Arzneimittelversorgung für EU-Bürger mit kurzfristigem Bedarf	20
5 Features	21
5.1 Authentisierung und Autorisierung des Leistungserbringers in	
Deutschland	21
5.1.1 Beschreibung der Anwenderdomäne	21
5.1.2 User Stories	22
5.2 Information der Betroffenen über ihre Rechte und Pflichten zum Schutz	
ihrer personenbezogenen und gesundheitlichen Daten	24
5.2.1 Beschreibung der Anwenderdomäne	25
5.2.2 User Stories	26

79	5.3 Identifikation des EU-Bürgers in der Apotheke vor Ort	28
80	5.3.1 Beschreibung der Anwenderdomäne	29
81	5.3.2 User Stories	30
82	5.4 Bestätigung des Behandlungsverhältnisses zum EU-Bürger.....	33
83	5.4.1 Beschreibung der Anwenderdomäne	33
84	5.4.2 User Stories	34
85	5.5 Auflistung und Abruf der einlösbaren Rezepte des EU-Bürgers.....	37
86	5.5.1 Beschreibung der Anwenderdomäne	37
87	5.5.2 User Stories	38
88	5.6 Schreiben der Dispensierinformation und Abgabe des oder der	
89	Medikamente an den EU-Bürger	44
90	5.6.1 Beschreibung der Anwenderdomäne	44
91	5.6.2 User Stories	45
92	5.7 Nachvollziehbarkeit und Auskunftsansprüche der Datenverarbeitung	49
93	5.7.1 User Stories	50
94	5.8 Performance und Betrieb.....	51
95	5.8.1 User Stories	51
96	6 Einordnung in die Telematikinfrastruktur	56
97	6.1 Entscheidung für die Integration von ePeD-B in die Telematikinfrastruktur	
98	1.0	58
99	6.2 Ausblick.....	59
100	7 Fachliches Konzept	60
101	7.1 Authentifizierung und Autorisierung des LE-DE	62
102	7.2 Information der Betroffenen über ihre Rechte und Pflichten zum Schutz	
103	ihrer personenbezogenen und gesundheitlichen Daten	63
104	7.3 Identifikation des EU-Bürgers in der Apotheke vor Ort	63
105	7.4 Übersicht über die einlösbaren E-Rezepte eines EU-Bürgers.....	64
106	7.5 Abruf von einlösbaren E-Rezepten eines E-Bürgers.....	65
107	7.6 Einlösung von E-Rezepten eines EU-Bürgers.....	66
108	8 Technisches Konzept.....	67
109	8.1 EU-Webportal.....	67
110	8.1.1 Zugang zum EU-Webportal.....	68
111	8.1.2 Schnittstellen.....	69
112	8.1.2.1 I_Provide_WebApp.....	70
113	8.1.2.2 I_WebApp_Deployment	70
114	8.1.2.3 I_Comm_ASL	70
115	8.1.2.4 I_User_Interaction	71
116	8.1.3 Sichere Auslieferung der WebApp-Bestandteile durch den Webserver.....	71
117	8.1.4 Ausblick	72
118	8.2 NCPeH-Proxy.....	72
119	8.2.1 Zugang zum NCPeH-Proxy	72
120	8.2.2 Schnittstellen.....	73
121	8.2.2.1 I_Comm_ASL	73

122	8.2.2.2 I_Authorization.....	73
123	8.2.2.3 I_Identification.....	73
124	8.2.2.4 I_ISM_Service.....	73
125	8.2.3 API-Gateway Funktion.....	73
126	8.2.4 Client Registrierung.....	74
127	8.2.5 Authentifizierung und Autorisierung.....	75
128	8.2.5.1 Weitergabe von Identitätsattributen.....	75
129	8.2.6 Qualitätsanforderungen an Betrieb und Infrastruktur.....	76
130	8.2.6.1 Erweiterte Anforderungen an Confidential Computing.....	80
131	8.3 NCPeH-FD.....	81
132	8.3.1 Zugang zum NCPeH-FD.....	81
133	8.3.2 Schnittstellen.....	81
134	8.3.2.1 I_Comm_ASL.....	82
135	8.3.2.2 I_ISM_Service.....	82
136	8.3.2.3 I_Patient_Identification_Service.....	83
137	8.3.2.4 I_eHealth_Service.....	83
138	8.3.2.5 I_PZN_Service.....	84
139	8.3.2.6 I_Provide_DocumentSet_Service.....	85
140	8.4 Informationsmodell.....	86
141	8.4.1 Domänenmodell für Land-B-Szenarien.....	86
142	8.4.2 Externe Informationsmodelle.....	87
143	8.4.2.1 International Search Mask (Domain Identifier: list_ism_international)	87
144	8.4.2.2 Patient Demographics Query Request (Domain Identifier:	
145	patient_identification_query).....	88
146	8.4.2.3 Patient Demographics Response (Domain Identifier:	
147	patient_demographics_data).....	88
148	8.4.2.4 Query Request.....	88
149	8.4.2.5 Query Response (Domain Identifier: list_available_prescription).....	89
150	8.4.2.6 Retrieve Request (Domain Identifier: list_selected_prescription_retrieval).....	89
151	8.4.2.7 Retrieve Response (Domain Identifier: list_prescription_retrieved).....	89
152	8.4.2.8 Dispensierdokumente (Domain Identifier: list_dispensation_documents).....	90
153	8.5 Use Cases.....	90
154	8.5.1 Use Case zur Initialisierung der Webapp.....	90
155	8.5.2 Use Cases im Rahmen der Authentifizierung, Autorisierung.....	93
156	8.5.2.1 Authentifizierung und Autorisierung des LE-DE.....	93
157	8.5.2.2 Etablierung eines ASL-Kanals in die VAU-Umgebung des NCPeH-FD.....	96
158	8.5.2.3 Nutzung einer autorisierten Verbindung zum NCPeH-FD.....	98
159	8.5.3 Use Cases im Rahmen der Identifizierung eines EU-Bürgers.....	101
160	8.5.3.1 International Search Masks abrufen.....	101
161	8.5.3.2 Demographische Daten eines EU-Bürgers abrufen.....	103
162	8.5.4 Use Cases im Rahmen der Belieferung durch eine Apotheke in Deutschland.....	106
163	8.5.4.1 Liste der einlösbaren E-Rezepte eines EU-Bürgers abrufen.....	106
164	8.5.4.2 Ausgewählte E-Rezepte eines EU-Bürgers abrufen.....	109
165	8.5.4.3 Dispensierinformationen an Land A übermitteln.....	112
166	9 Datenschutz und Informationssicherheit.....	116
167	9.1 Benötigte Komponenten und Dienste zur Umsetzung des Szenarios.....	116
168	9.2 Anwendungsprozesse und deren Schutzbedarf.....	117
169	9.3 Maßgebliche Informationsobjekte und deren Schutzbedarf.....	117
170	9.4 Maßnahmen zum Schutz der Informationsobjekte.....	129

171	9.5 Erweiterung der Protokollierung	130
172	9.6 Grenze der Sicherheitsleistung.....	130
173	10 Anhang A – Verzeichnisse	131
174	10.1 Abbildungsverzeichnis	131
175	10.2 Tabellenverzeichnis	132
176	10.3 Abkürzungen.....	132
177	10.4 Inkludierte Dokumente.....	134
178	10.5 Referenzierte Dokumente	134
179	10.5.1 Dokumente der gematik.....	134
180	10.5.2 Weitere Dokumente	134
181		
182		

1 Einordnung des Dokuments

Dieses Dokument beschreibt das Anwendungsszenario zum Abruf von Verordnungsdaten und zum Schreiben von Dispensierdaten von elektronischen Rezepten (E-Rezepten) für eine Person aus einem europäischen Mitgliedstaat (Land A), die ihr E-Rezept aus dem EU-Ausland in einer Apotheke in Deutschland (Land B) einlösen möchte.

In diesem Dokument wird für diesen Anwendungsfall auch die Bezeichnung ePrescription/eDispensation-B verwendet, kurz ePeD-B.

Dieses Dokument dient dazu, die fachliche Sicht auf den Anwendungsfall ePeD-B zusammenzufassen. Die Ergebnisse der fachlichen Analyse fließen in ein technisches Konzept für das Land-B-System ein, welches auch Teil dieses Dokuments ist. Das technische Konzept wiederum bildet die Grundlage für die Konzeption und die Spezifikation des National Contact Point foreHealth-Fachdienstes (NCPeH-FD) sowie des gesamten Land-B-Systems.

1.1 Zielsetzung

Dieses Dokument beschreibt den Funktionsumfang aus der Sicht der Nutzer und dient dazu, die Bedürfnisse der Nutzer besser zu verstehen. Mit dem ermittelten Funktionsumfang sollen die gematik und die Deutsche Verbindungsstelle Krankenversicherung-Ausland (DVKA) in die Lage versetzt werden, den zusätzlichen Funktionsumfang des National Contact Point for eHealth (NCPeH) zu bewerten und umsetzen zu können. Außerdem sollen Anbieter und Betreiber der weiteren Komponenten des Land-B-Systems in die Lage versetzt werden, den Funktionsumfang der Komponenten bewerten und umsetzen zu können.

1.2 Zielgruppe

Dieses Featuredokument richtet sich an die gematik und ihre Gesellschafter, die DVKA, das Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM) sowie Hersteller von Apothekenverwaltungssystemen (AVS) als Grundlage für den gemeinsamen Austausch und zur Umsetzung der einzelnen Features.

1.3 Abgrenzungen

In diesem Dokument wird ausschließlich Use Case 1 (UC 1) betrachtet. Die weiteren Use Cases (UC 0, 2, 3, 4) dienen lediglich der Einordnung in den Gesamtkontext.

- UC 0 beschreibt den nationalen E-Rezept Use Case, also eine Verordnung, die in Land A sowohl verordnet als auch dispensiert wird.
- UC 1 beschreibt eine Verordnung in Land A, die in Land B dispensiert wird.
- UC 2 beschreibt eine Verordnung, die in Land B sowohl erstellt als auch dispensiert wird.
- UC 3 beschreibt eine Verordnung in Land B, die in Land A dispensiert wird.
- UC 4 beschreibt eine Verordnung in Land B, die in einem dritten Land C dispensiert wird.

UC	Home	Prescribing	Dispensing	Comment
0	A	A	A	Regular situation, no special MyHealth@EU actions upfront
1	A	A	B	"Medication already prescribed in Country A" use case
2	A	B	B	"Medication newly prescribed in Country B" use case
3	A	B	A	Medication prescribed in Country B and dispensed in home country
4	A	B	C	Two foreign countries involved

Abbildung 1: Abgrenzungen ePeD-B

1.4 Methodik

Use Case

Ein Use Case beschreibt einen Anwendungsfall. Damit wird unter der Berücksichtigung von Rollen beschrieben, welche Aktivitäten durchgeführt werden sollen, die in einer Funktion zusammengefasst werden können.

Feature

Ein Feature beschreibt eine abgrenzbare Sammlung von funktionalen Anforderungen, die in Gänze einen eigenständigen Mehrwert und damit eine Funktionalität für das Produkt bereitstellen.

Ein Feature wird mit einer oder mehreren User Stories konkretisiert.

User Story

Eine User Story beschreibt in natürlicher Sprache eine Anforderung aus Nutzersicht. Sie wird anhand einer Satzschablone formuliert und umfasst, was der erwartete Nutzen bzw. die verfolgte Intention hinter der Aktivität ist. Folgendes Schema wird bei der Formulierung der User Stories verwendet:

„Als [Nutzer in der Rolle XYZ] möchte ich [XYZ], [um | damit] ...“

Akzeptanzkriterien ergänzen die User Story. Damit wird beschrieben, wie die korrekte Umsetzung der User Story getestet werden würde. Dies ist für das Verständnis und für den Test der User Story hilfreich.

Hinweise auf offene Punkte

- 248 Themen, die noch intern geklärt werden müssen oder eine Entscheidung seitens der
249 Gesellschafter erfordern, sind wie folgt im Dokument gekennzeichnet:
250 *Beispiel für einen offenen Punkt.*

2 Allgemeine Rahmenbedingungen

Die allgemeinen Rahmenbedingungen ergeben sich aus dem gesetzlichen Rahmen der Verordnung über den europäischen Gesundheitsdatenraum (EHDS VO) (EU 2025/327), den Guidelines des eHealth Network (eHN) und den Vorgaben der MyHealth@EU - eHealth Digital Service Infrastructure (eHDSI).

Die Anforderungen an das Anwendungsszenario ePrescription/eDispensation-B basieren maßgeblich auf den Vorgaben der eHDSI (v.a. [eHDSI_Requirements_Catalogue]). Diese sind bezüglich der Inhalte der ePrescription allerdings teilweise nicht konsistent mit den Vorgaben der Arzneimittelverschreibungsverordnung (AMVV, § 2) sowie mit den Vorgaben gemäß Durchführungsrichtlinie 2012/52/EU (Anhang). Diese Inkonsistenzen sind mit dem BMG bzw. mit Angehörigen der DG Sante der Europäischen Kommission sowie der eHealth Member States Expert Group (eHMSEG) besprochen worden. Zum Zeitpunkt der Kommentierung des Featuredokuments liegt noch keine Information über die konkreten weiteren Schritte des BMG und der Europäischen Kommission vor. Bis zum Abschluss der weiteren Verfahren sind Anpassungen der Anwendungsfälle daher nicht auszuschließen. Die in diesem Dokument genannten Paragraphen werden unter Vorbehalt der finalen Änderungsverordnung(en) gekennzeichnet und aktualisiert, sobald die neue Version der Verordnung(en) in Kraft tritt.

2.1 Gesetzliche Regelungen in Deutschland

Grundlage für die Inhalte einer Verordnung von Arzneimitteln nach §31 SGB V ist in Deutschland die „Verordnung über die Verschreibungspflicht von Arzneimitteln“ (Arzneimittelverschreibungsverordnung - AMVV). In der [Arzneimittelverschreibungsverordnung §2] ist ebenfalls festgehalten, dass

*„Den aus Deutschland stammenden ärztlichen oder zahnärztlichen Verschreibungen sind entsprechende Verschreibungen aus den Mitgliedstaaten der Europäischen Union, aus den Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum und aus der Schweiz gleichgestellt, sofern diese die Angaben nach Absatz 1 aufweisen und dadurch ihre Authentizität und ihre Ausstellung durch eine dazu berechnigte ärztliche oder zahnärztliche Person nachweisen.“
(§ 2 Abs. 1a AMVV)*

Somit besteht in Deutschland eine rechtliche Grundlage für die Anerkennung von Rezepten aus dem EU-Ausland, dem Europäischen Wirtschaftsraum sowie der Schweiz. Die Anerkennung deutscher Rezepte in anderen Mitgliedstaaten der Europäischen Union erfolgt entsprechend der jeweiligen nationalen Umsetzung der einschlägigen EU-rechtlichen Vorgaben.

2.2 Rechtliche Rahmenbedingungen in der Europäischen Union

Gemäß Artikel 11 Absatz 2 der Richtlinie 2011/24/EU ist die Kommission verpflichtet, Maßnahmen zur Erleichterung der Anerkennung von Verschreibungen zu erlassen, die in einem anderen Mitgliedstaat ausgestellt wurden als in dem, in dem das verschriebene Produkt abgegeben werden soll. Diese Maßnahmen wurden in der Durchführungsrichtlinie 2012/52/EU festgelegt.

2.2.1 Vorgaben an ärztliche Verordnungen gemäß Durchführungsrichtlinie 2012/52/EU

Die [Durchführungsrichtlinie 2012/52/EU] beschreibt Maßnahmen zur Erleichterung der Anerkennung von in einem anderen Mitgliedstaat ausgestellten ärztlichen Verschreibungen. Im Rahmen dieser Richtlinie ist festgelegt, welche Informationen eine Verschreibung enthalten muss, damit diese in einem Mitgliedstaat der Europäischen Union (EU) akzeptiert wird.

Im Rahmen der Richtlinie wird ebenfalls darauf hingewiesen, dass die Bereitstellung der Informationen nur für jene Verschreibungen gelten soll, die in einem anderen Mitgliedstaat eingelöst werden sollen.

Die Vorgaben zum Inhalt einer Verschreibung zur Einlösung in einem EU-Mitgliedstaat kann der Durchführungsrichtlinie entnommen werden.

2.2.2 Vorgaben zu ePrescription und eDispensation gemäß eHN Guideline

Mit der [eHealth Network Guideline on the electronic exchange of health data under Cross-Border Directive 2011/24/EU ePrescription and eDispensation of Authorised Medicinal Products] werden juristische, organisatorische, semantische und technische Anforderungen festgehalten, die sich auf den Abruf von Verordnungsdaten und das Schreiben von Dispensierdaten über den NCPeH beziehen. Darauf aufbauend gelten detaillierte technische Festlegungen, die das Produktverhalten des NCPeH definieren. Diese sind zusammengefasst im [eHDSI_Requirements_Catalogue] (aktuell in der Version 10.0.0 vom 06.03.2026).

2.3 Vorbedingungen zum Abruf von Verordnungsdaten aus dem EU-Ausland

Voraussetzung für die Nutzung von E-Rezepten eines anderen EU-Mitgliedstaats in Deutschland ist die vorherige Anlage und Befüllung von E-Rezepten unter Beachtung der eHDSI-Vorgaben durch autorisierte Leistungserbringer im europäischen Mitgliedstaat des EU-Bürgers. Ferner wird vorausgesetzt, dass eine Netzanbindung an die TI existiert und korrekt freigeschaltet ist, um dadurch den Datenaustausch zu ermöglichen.

2.4 Netzanbindung an das europäische Netzwerk

Die Europäische Kommission hat mit der eHealth Digital Service Infrastructure (eHDSI), oder auch MyHealth@EU Infrastruktur, eine elektronische Infrastruktur geschaffen, durch die bestehende nationale Infrastrukturen grenzüberschreitend vernetzt werden und damit zusätzliche grenzüberschreitende Gesundheitsdienste angeboten werden können. Mit der eHDSI wurde ein Rahmen geschaffen, mit dem die Gesundheitsdaten der Versicherten sicher und interoperabel grenzüberschreitend ausgetauscht werden können. Der Datenaustausch zwischen den einzelnen nationalen Infrastrukturen und der eHDSI erfolgt über die NCPeHs, die unter der Hoheit der einzelnen europäischen Mitgliedstaaten stehen.

Weitere Voraussetzung für den europäischen Datenaustausch ist der Zugang und die Kommunikation mit dem europäischen Netzwerk Trans European Services for Telematics between Administrations - new generation (TESTA-ng). Das Netz TESTA-ng wurde für den steigenden Bedarf an sicherer grenzüberschreitender Zusammenarbeit zwischen den einzelnen Verwaltungen der EU-Mitgliedstaaten aufgebaut und sorgt auf der Netzwerkebene für verschlüsselte und zuverlässige Übertragung von sensiblen Daten. Die eHDSI baut auf TESTA-ng auf. Auf diese Weise wird mittels TESTA-ng ein sicherer Austausch von Gesundheitsdaten zwischen den nationalen Gesundheitsinfrastrukturen der EU-Mitgliedstaaten gewährleistet.

In der aktuellen Konstellation wird in Deutschland die Verbindung zum europäischen Netzwerk über die Anbindung an die Netze des Bundes (NdB) realisiert, welche eine eigene Anbindung an das TESTA-ng unterhalten. Die entsprechende Netzanbindung, Freischaltung und Sicherheitsabnahme muss erfolgreich durchgeführt werden, bevor NCPeHs anderer EU-Mitgliedstaaten eine Abfrage beim deutschen NCPeH-Fachdienst stellen können. Zusätzlich müssen Kommunikationsverbindungen zu den zentralen Diensten der eHDSI möglich sein.

Die eHDSI-Vorgaben fordern im Rahmen der formalen Zulassung zum operativen Betrieb des NCPeH-Fachdienstes eine Konformitätsprüfung [eHDSI_Audit_Framework]. Die Konformitätsprüfung wird durch einen von DG SANTE beauftragten Prüfer durchgeführt, der die Prüfung der Umsetzung des NCPeH gegenüber dem Betreiber durchführt. Damit soll die Konformität des NCPeH des jeweiligen europäischen Mitgliedstaats gemäß Kriterien und Anforderungen der eHDSI auf allen Ebenen eingehalten werden. Die gewonnenen Erkenntnisse sollen die eHDSI und relevanten europäischen Gremien (z.B. eHealth Network) bei der Entscheidung unterstützen, ob der geprüfte NCPeH in den Produktivbetrieb des grenzüberschreitenden eHealth-Informationssystems Cross-Border eHealth Services (CBeHIS) aufgenommen werden kann.

Die Bereitstellung der Ergebnisse der Konformitätsprüfung ist Aufgabe aller an der Entwicklung und dem Betrieb des NCPeH-Fachdienstes beteiligten Partner. Die Verantwortung über die korrekte Abarbeitung der Checkliste obliegt der DVKA, die hierbei von der gematik und dem BfArM unterstützt wird.

2.5 Validierung und Qualitätskontrolle der eingesetzten Terminologien

Im eHDSI-E-Rezept (ePrescription) sind einige Angaben in codierter Form zu erfassen und zu übermitteln. Damit dem Apotheker im Ausland die Bezeichnungen (auch) in seiner Landessprache angezeigt werden können, sieht die eHDSI eine Transkodierung der

nationalen Codes in von der eHDSI vorgegebene Codesysteme und Codes vor. Formale Regeln wurden dafür zwischen den Mitgliedstaaten vereinbart. Die Transkodierung erfolgt mit Hilfe eines Master Value Set Catalogues (MVC) und eines länderspezifischen Master Translation Catalogues (MTC). Die Pflege und Qualitätskontrolle des MVC erfolgt gemeinsam durch die EU-Mitgliedstaaten. Den EU-Mitgliedstaaten obliegt die Validierung und Qualitätskontrolle der national eingesetzten Codesysteme und des jeweiligen MTC. In Deutschland obliegt die Festlegung der semantischen Interoperabilität dem Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM) entsprechend § 219d Abs. 6 SGB V.

HL7 CDA wurde von der eHDSI als das eHDSI-Dokumentenformat für die grenzüberschreitende Übermittlung und Verarbeitung von E-Rezepten vordefiniert. Innerhalb der TI wird eine FHIR-Profilierung für deutsche E-Rezepte verwendet. Für die grenzüberschreitende Datenübermittlung bedeutet dies, dass eine Transformation der Nutzdaten (ePrescription- und eDispensation-Dokument) zwischen den Dokumentformaten HL7 CDA und FHIR notwendig wäre. Erfolgt die Verarbeitung nicht direkt innerhalb des AVS, ist jedoch keine Transformation notwendig.

3 Anwendungsumfeld

3.1 Anwendungsszenario: ePrescription/eDispensation Land B

Elektronische Rezepte (E-Rezepte) sollen von Bürgern aus einem EU-Mitgliedstaat vor Ort in einer Apotheke in Deutschland eingelöst werden. Voraussetzung für die Einlösung von E-Rezepten aus einem anderen EU-Mitgliedstaat ist, dass diese von einem berechtigten Leistungserbringer ausgestellt wurden (siehe Abbildung 2).

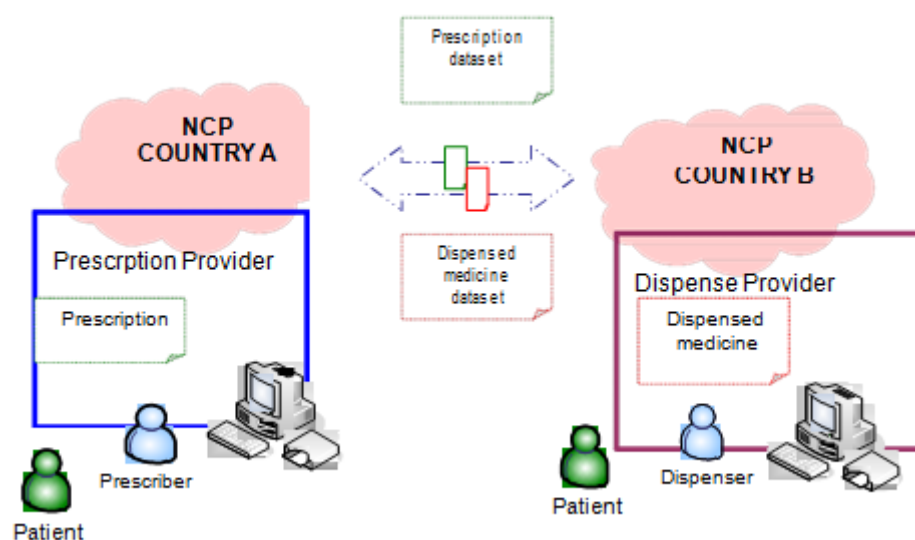


Abbildung 2: Systemischer Blick auf das Anwendungsszenario

Die Durchführung des Anwendungsszenarios umfasst:

1. die Authentisierung und Autorisierung des Leistungserbringers in Deutschland (LE-DE) (über den NCPeH-A),
2. die Aufklärung des EU-Bürgers in der Apotheke (mithilfe der Patient Information Notice (PIN-Dokument)),
3. die Identifikation des EU-Bürgers in der Apotheke vor Ort (mithilfe von NCPeH-A und NCPeH-B),
4. die Bestätigung des Behandlungsverhältnisses zum EU-Bürger (mithilfe von NCPeH-B),
5. die Auflistung und der Abruf der einlösbaren Rezepte des EU-Bürgers (vom NCPeH-A an den NCPeH-B),
6. das Schreiben der Dispensierinformation (vom NCPeH-B an den NCPeH-A) sowie
7. die Abgabe des oder der Medikamente an den EU-Bürger.



Abbildung 3: Flussdiagramm Anwendungsszenario ePeD-B

3.2 Akteure und Rollen

Für das Anwendungsszenario ePrescription/eDispensation Land B werden unterschiedliche Akteure und Rollen berücksichtigt.

Akteure, die an der Realisierung des Service ePrescription/eDispensation-B indirekt oder direkt beteiligt sind:

- Anbieter und Betreiber des NCPeH und der Fachanwendung im Land A
- Betreiber der TESTA-ng
- eHDSI Solution Provider (Betreiber und Anbieter der zentralen Dienste der eHDSI)
- DVKA (Anbieter und Betreiber des NCPeH-Fachdienstes)
- Anbieter und Betreiber des NCPeH-Proxy und des EU-Webportals
- gematik (Test und Bestätigung des NCPeH-Fachdienstes der DVKA)
- eHealth Network (Entscheider zur Inbetriebnahme nach Europa an das TESTA-ng, auf Empfehlung durch die eHealth Member States Expert Group (eHMSEG))
- BfArM (Pflege und Bereitstellung von Terminologien und zugehörigen Transcodier- und Transformationsregeln)
- Beteiligte für die Bereitstellung der Telematikinfrastruktur (Zentrale Dienste etc.)

Zum Zeitpunkt der Kommentierung des Featuredokuments ist noch offen, wer Anbieter bzw. Betreiber des NCPeH-Proxy und des EU-Webportals sein wird.

Rollen, in denen sich Personen als Nutzer an dem Anwendungsszenario beteiligen:

- Bürger aus einem EU-Mitgliedstaat oder einem Mitgliedstaat des Europäischen Wirtschaftsraums (EU-Bürger)
- Leistungserbringer aus einem EU-Mitgliedstaat sowie aus Deutschland (LE-EU und LE-DE)

3.2.1 Selbstverwaltung

Akteure der Selbstverwaltung und des Gesundheitswesens tragen zu den rechtlichen und fachlichen Voraussetzungen für die grenzüberschreitende Nutzung eines E-Rezepts bei. Sie koordinieren die beteiligten Systeme, sichern Qualitätsstandards und unterstützen die Umsetzung auf nationaler Ebene.

- 445 • gematik: Verantwortlich für Konzeption, Spezifikation und Produktbestätigung des
446 NCPeH und weiterer Komponenten des Land-B-Systems sowie Spezifikation der
447 User Experience für LE-DE
- 448 • DVKA: Anbieter und Betreiber des deutschen NCPeH-Fachdienstes
- 449 • DAV/ABDA: Interessensvertretung der Leistungserbringer in der Apotheke in
450 Deutschland und Kommunikation zur Nutzung des EU-E-Rezepts
- 451 • BfArM: Terminologieverantwortliche

452 3.2.2 EU-Bürger

453 Bürger aus einem europäischen Mitgliedstaat initiieren das Anwendungsszenario, indem
454 sie eine Apotheke in Deutschland aufsuchen, um ein in ihrem Zugehörigkeitsland
455 ausgestelltes E-Rezept einzulösen. Dies bedingt technische und administrative
456 Voraussetzungen und datenschutzrechtliche Anforderungen:

- 457 • Es muss ein gültiges E-Rezept im Zugehörigkeitsland (Land A) vorliegen.
- 458 • Es soll das gültige E-Rezept in Deutschland (Land B) eingelöst werden.
- 459 • Die Person muss vom LE-DE identifiziert werden können (bspw. mithilfe eines
460 gültigen Ausweisdokuments).
- 461 • Der Person müssen mithilfe der Patient Information Notice (PIN-Dokument)
462 Informationen über ihre Rechte und Pflichten zum Schutz ihrer persönlichen und
463 gesundheitlichen Daten zur Verfügung gestellt werden.

464 3.2.3 Leistungserbringer

465 Im Rahmen der grenzüberschreitenden E-Rezept-Nutzung übernehmen verschiedene
466 Leistungserbringer konkrete Aufgaben entlang des Versorgungsprozesses, von der
467 Verordnung im Land A bis zum Einlösen des E-Rezepts in der Apotheke in Deutschland.

468 **Verordnende Leistungserbringer im Heimatland (Land A)** stellen elektronische
469 Rezepte nach den nationalen Vorgaben des Herkunftslandes aus.

470 Apotheken in Deutschland (Land B) müssen fachlich und technisch in der Lage sein, E-
471 Rezepte aus dem EU-Ausland zu verarbeiten, was voraussetzt, dass sie an die
472 Telematikinfrastruktur (TI) angebunden sind und auf die Anwendung von MyHealth@EU
473 zugreifen können.

474 **Abgebende Leistungserbringer in Deutschland (Land B)** tragen die fachliche
475 Verantwortung für die Prüfung des E-Rezepts und die Abgabe des Arzneimittels. Sie
476 stehen in direkter Kommunikation mit dem EU-Bürger, müssen Verwaltungsdaten
477 klinisch prüfen (z. B. Plausibilität, Dosierung, Kontraindikationen) und über
478 Besonderheiten des oder der abzugebenden Medikamente informieren (Sprache,
479 Einnahmehinweise etc.).

480 *Hinweis: Eine vollumfängliche pharmazeutische Versorgung und Beratung im Land B*
481 *kann nicht gewährleistet werden, da dem dispensierenden LE-DE nicht alle relevanten*
482 *Informationen für eine vollständige Risikoabschätzung vorliegen werden.*

483 3.2.4 Technische Betreiber

484 Die technische Umsetzung des grenzüberschreitenden E-Rezepts setzt ein
485 Zusammenspiel mehrerer technischer Betreiber von Diensten und Komponenten im

europäischen Mitgliedstaat (Land A), in der MyHealth@EU-Infrastruktur und national in Deutschland (Land B) voraus.

Land A

- Anbieter und Betreiber des NCPeH und der Fachanwendung im Land A

MyHealth@EU Infrastruktur

- Betreiber der TESTA-ng
- eHDSI Solution Provider (Betreiber und Anbieter der zentralen Dienste der eHDSI)

Land B

- DVKA als Anbieter und Betreiber des NCPeH-Fachdienstes
- Anbieter und Betreiber des NCPeH-Proxy und des EU-Webportals
- Anbieter und Betreiber von Diensten und Komponenten in der TI (z.B. zentrale Dienste)

Das Supportkonzept mit beteiligten Akteuren für das Anwendungsszenario ePeD-B wird festgelegt, sobald Anbieter und Betreiber des NCPeH-Proxy und des EU-Webportals feststehen.

3.3 In Scope

Folgende Aspekte werden durch die Umsetzung des Anwendungsszenarios ePeD-B in Apotheken in Deutschland ermöglicht:

- Dispensierung von innerhalb der EU zugelassenen Arzneimitteln auf Basis einer elektronischen Verschreibung eines EU-Bürgers aus einem europäischen Mitgliedstaat unter Berücksichtigung der inhaltlichen Vorgaben gemäß der Durchführungsrichtlinie 2012/52/EU bzw. des [eHDSI_Requirements_Catalogue]
- Einsicht in die vollständigen, aktuellen und im EU-Ausland einlösbaren Verschreibungen eines EU-Bürgers aus einem europäischen Mitgliedstaat
- Einsicht in die vollständigen, aktuellen und nur im europäischen Mitgliedstaat der EU-Bürger einlösbaren E-Rezepte, falls dies durch den europäischen Mitgliedstaat den EU-Bürgern ermöglicht wird
- Substitution auf Basis der deutschen gesetzlichen Vorgaben gemäß §17 ApBetrO

3.4 Out of Scope

Folgende Aspekte werden im vorliegenden Dokument nicht betrachtet:

- **Akteure und Rollen**
 - Versandapotheken:
 - Zum Zeitpunkt der Verfassung dieses Dokuments sehen die eHDSI-Vorgaben vor, dass das Anwendungsszenario ePeD auf Apotheken vor Ort beschränkt ist. Die Anforderungen der eHDSI erfordern eine Identitätsprüfung, die derzeit nur mit einem Lichtbildausweis nachgewiesen

werden kann. Für die Inklusion von Versandapotheken in Deutschland ist es notwendig, auch die EUDI Wallet zu berücksichtigen. Diese Anforderungen werden stufenweise nachträglich analysiert und eingearbeitet.

- Apotheke vor Ort:

- Apotheker, Pharmazieingenieure und Apothekerassistenten:

- Die eHDSI-Vorgaben erfordern eine personenbezogene Multi-Faktor-Authentisierung zum Zwecke der Identifikation, Authentisierung und Autorisierung am NCPeH-B. Für die Einbindung von Apothekern, Pharmazieingenieuren und Apothekerassistenten in Deutschland im Anwendungsszenario ePeD-B ist es notwendig, dass in der TI personenbezogene Leistungserbringer-Identifikationsmittel für sie existieren. Da diese zum aktuellen Zeitpunkt noch nicht flächendeckend existieren, können zunächst nur die Apotheker, Pharmazieingenieure und Apothekerassistenten berücksichtigt werden, die ein personenbezogenes Leistungserbringer-Identifikationsmittel besitzen.

- Pharmazeutisch-technische Assistenten (PTA):

- Im Versorgungsalltag unterstützen PTAs unter Aufsicht der Apotheker bei der Dispensierung und bei der Durchführung technischer Abläufe (Rezeptabruf, Scan etc.). Die Vorgaben der eHDSI erfordern, dass eine personenbezogene Multi-Faktor-Authentisierung zum Zwecke der Identifikation, Authentisierung und Autorisierung am NCPeH-B durchgeführt wird. Für die Einbindung von PTAs in Deutschland im Anwendungsszenario ePeD-B ist es notwendig, dass in der TI personenbezogene Leistungserbringer-Identifikationsmittel für PTAs existieren. Da diese zum aktuellen Zeitpunkt noch nicht existieren, können PTAs zunächst keine eigenständige Dispensierung durchführen.

- Pharmazeutisch-kaufmännische Angestellte (PKA):

- Im Versorgungsalltag unterstützen PKAs vorrangig bei administrativen Tätigkeiten (z. B. bei Abrechnung oder Bestellwesen), nehmen jedoch in manchen Apotheken eine aktivere Rolle in der Medikamentenausgabeein. Für das Anwendungsszenario ePeD-B wird diese Rolle nicht berücksichtigt.

- Krankenhausapotheke:

- Eine Krankenhausapotheke kann einen öffentlichen Anteil haben und damit für Bürger zur Verfügung stehen, die ein E-Rezept einlösen möchten. Im Zuge der Einführung des Anwendungsszenarios ePeD-B in Deutschland kann eine Krankenhausapotheke diesen Dienst grundsätzlich anbieten. Es wird in diesem Dokument jedoch nicht näher auf die Besonderheiten von Krankenhausapotheken eingegangen. Die Krankenhaus-internen Abläufe und die Rolle der Krankenhausapotheke für Anordnungen ist vom Anwendungsszenario ePeD-B unberührt.

- **Funktionale und technische Aspekte**

- EUDI Wallet:

- Die Anforderungen der eHDSI erfordern eine Identitätsprüfung für EU-Bürger, die derzeit nur mit einem Lichtbildausweis nachgewiesen werden kann bzw. eine personenbezogene Multi-Faktor-Authentisierung für Leistungserbringer in Deutschland, die aktuell nur kartenbasiert umgesetzt

572 werden kann. Die Anforderungen der EUDI Wallet werden stufenweise
573 nachträglich analysiert und eingearbeitet.

574 • **Fachliche Aspekte:**

- 575 • Es wird in diesem Dokument und über den NCPeH-B nicht abgebildet, wenn:
- 576 • E-Rezepte im Land B verordnet wurden und dort eingelöst werden sollen;
- 577 • Fälle auftreten, in denen Bürger oder Patienten im Herkunftsland (Land A)
- 578 bestimmte Informationen (z. B. Verschreibungen, Diagnosen) verbergen,
- 579 aber im Behandlungsland (Land B) Einsicht in diese Informationen
- 580 gewähren möchten;
- 581 • es sich um Verordnungen von Betäubungsmitteln gemäß Artikel 71(2) der
- 582 Richtlinie 2001/83/EG handelt;
- 583 • es sich um Verordnungen von Medizinprodukten handelt;
- 584 • es sich um Verordnungen von nicht-pharmazeutischen Maßnahmen oder
- 585 Produkten handelt;
- 586 • Arzneimittel verordnet wurden, die individuell für Patienten in Apotheken
- 587 zubereitet werden (Formula magistralis), oder die nach Vorschriften eines
- 588 Arzneibuchs oder der Apothekenliste in der Apotheke hergestellt werden
- 589 (Formula officinalis).

590

591

4 Motivation

592 Ausländische Rezepte sind insbesondere bei Apotheken in Grenzregionen ein Regelfall in
593 der Versorgung. Eine Verifizierung ausländischer Rezepte erfolgt aktuell behelfsmäßig
594 über Internetrecherche des Apothekers und Vorlegen des Personalausweises des EU-
595 Bürgers. Eine standardisierte Verifizierung existiert bisher nicht und insbesondere auch
596 eine wiederholte Einlösung kann nicht ausgeschlossen werden.
597 Das Ziel ist es, EU-Bürgern eine einfache und rechtssichere Möglichkeit zu bieten, ihre E-
598 Rezepte auch während eines Aufenthalts in Deutschland einzulösen, unter
599 Berücksichtigung der europäischen Interoperabilitätsvorgaben sowie nationaler
600 Regularien.

601 **4.1 Kontinuierliche Arzneimittelversorgung für chronisch** 602 **erkrankte EU-Bürger**

603 1. Ich als EU-Bürger mit einer chronischen Erkrankung und laufender medikamentöser
604 Langzeitbehandlung möchte mein Rezept aus dem Land A in einer deutschen Apotheke
605 einlösen können, um meine Therapie während eines Aufenthalts im EU-Ausland lückenlos
606 fortsetzen zu können – bspw. auch dann, wenn ich meine aktuelle Medikamentenpackung
607 bereits aufgebraucht habe und laut den Abgaberegeln meines Heimatlandes (z. B. nur
608 eine Packung pro Abgabe erlaubt) keine weitere Packung vorab mitnehmen konnte.

609

610 2. Ich als EU-Bürger mit einer chronischen Erkrankung und laufender medikamentöser
611 Langzeitbehandlung möchte mein elektronisches Rezept aus meinem Heimatland in einer
612 Apotheke in Deutschland einlösen können, um meine Therapie auch dann fortsetzen zu
613 können, wenn ich meine Medikamente während eines Aufenthalts im EU-Ausland verloren
614 habe oder sie zu Hause vergessen habe.

615 **4.2 Arzneimittelversorgung für EU-Bürger mit kurzfristigem Bedarf**

616 1. Ich als EU-Bürger mit einem gültigen E-Rezept aus dem EU-Ausland, jedoch ohne
617 laufende Langzeitbehandlung, möchte mein E-Rezept während eines Aufenthalts in
618 Deutschland einlösen können, wenn ich das Medikament vor meiner Abreise im Land A
619 nicht mehr abholen konnte, um dennoch eine notwendige Versorgung sicherzustellen.

620

621 2. Ich als EU-Bürger mit einem gültigen E-Rezept aus dem EU-Ausland, jedoch ohne
622 laufende Langzeitbehandlung, möchte mein E-Rezept während meines Aufenthalts in
623 Deutschland einlösen können, wenn ich das verordnete Medikament vergessen oder
624 verloren habe, um die begonnene Therapie fortführen oder abschließen zu können.

625

5 Features

Im Folgenden werden das Anwendungsszenario und die zugehörigen fachlichen Informationen im Rahmen von aufeinander aufbauenden Features detaillierter betrachtet. Ein Feature umfasst dabei jeweils eine Beschreibung der Anwenderdomäne zur Übersicht über den Workflow des jeweiligen Features sowie die User Stories mit Akzeptanzkriterien.

Legende der Diagramme in der Beschreibung der Anwenderdomäne:

- Grün: Aus vorherigem Feature weiterverwendete fachliche Informationen
- Blau: In diesem Feature neu erzeugte fachliche Informationen

5.1 Authentisierung und Autorisierung des Leistungserbringers in Deutschland

Um eine sichere Gesundheitsversorgung von EU-Bürgern in Deutschland zu gewährleisten, benötigt der Leistungserbringer in Deutschland (LE-DE) Zugriff auf die Gesundheitsdaten des EU-Bürgers. Durch eine eindeutige und sichere Authentisierung sowie Autorisierung des LE wird sichergestellt, dass nur berechtigte und autorisierte LE Zugriff auf grenzüberschreitende Gesundheitsdienste erhalten.

Alle an MyHealth@EU beteiligten Länder sind Teil eines gemeinsamen Vertrauensraums. Eine wesentliche Grundlage für dieses Vertrauen ist die sichere und eindeutige Authentifizierung und Autorisierung jedes LE im lokalen System.

5.1.1 Beschreibung der Anwenderdomäne

Ein LE-DE benötigt persönliche Identifikationsmerkmale und Identifikationsmerkmale der Leistungserbringerinstitution (LEI) (1), um die weiteren Schritte des Anwendungsszenarios durchführen zu können. Diese Identitätsmerkmale werden durch die Smartcards HBA und SMC-B zur Verfügung gestellt. Anhand dieser Smartcards meldet sich der LE-DE am ePeD-B System(detaillierte Beschreibung der beteiligten Komponenten siehe Kapitel 6 ff.) an.

Das ePeD-B System holt einerseits beim zentralen IDP der TI eine Bestätigung der TI-Identität des LE-DE ein (2) und erstellt andererseits eine neue (zeitlich begrenzt gültige) elektronische Identität für diesen (3), die im EU-Kontext funktioniert und Rechte für den Zugriff auf ebendiesen EU-Kontext definiert (4).

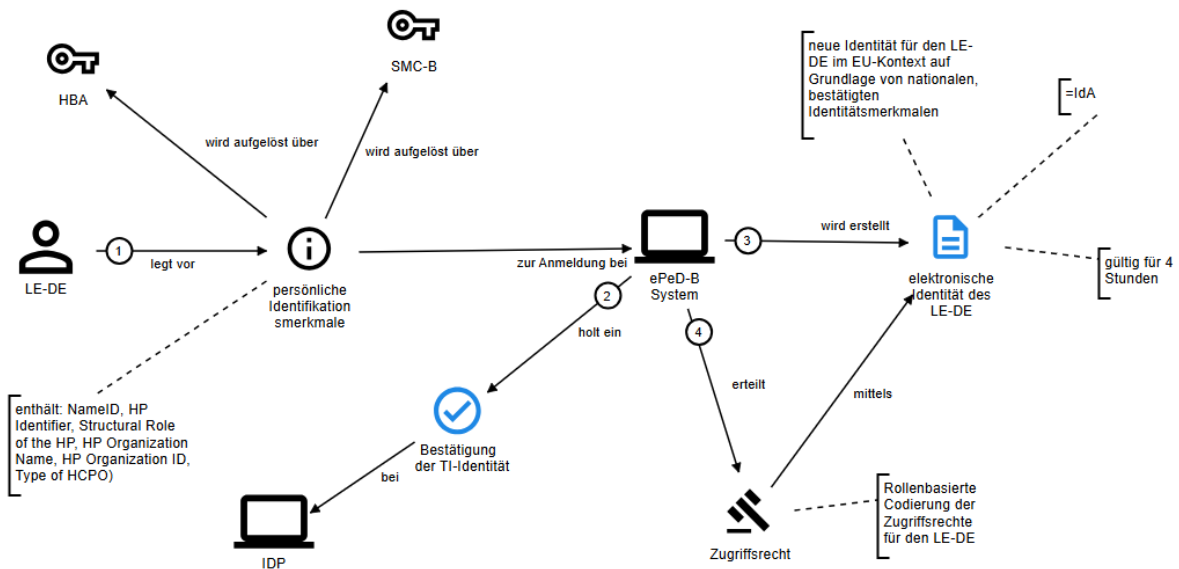


Abbildung 4: Authentisierung und Autorisierung des Leistungserbringers in Deutschland

5.1.2 User Stories

1. Als nationale Verbindungsstelle muss ich sicherstellen, dass der LE-DE seine Identität eindeutig und sicher authentisiert, damit ich den LE-DE berechtigen kann, die Daten eines EU-Bürgers gemäß seiner Rolle und seines Profils abrufen zu können.

ID	Akzeptanzkriterium
1.1	Der LE-DE MUSS sich mit einer 2-Faktor-Methode authentisieren.
1.2	Bei der Authentisierung des LE-DE MUSS ein für lange Zeit gültiger Identifier des LE-DE (Telematik-ID des HBA-Inhabers) übergeben werden.
1.3	Bei der Authentisierung des LE-DE MUSS der personenbezogene Name des LE-DE (menschlich lesbar) übergeben werden.
1.4	Bei der Authentisierung des LE-DE MUSS die Telematik-ID der Apotheke, in der sich der LE-DE befindet, übergeben werden.
1.5	Bei der Authentisierung des LE-DE MUSS der Name des Apothekenstandortes übergeben werden, in dem die Abgabe stattfinden soll.
1.6	Bei der Authentisierung des LE-DE MUSS die Art der LEI übergeben werden, in der die Bedienung bzw. Behandlung des EU-Bürgers stattfindet. (Einzig möglicher Wert für Apotheken: "Pharmacy")
1.7	Nach der Authentisierung des LE-DE in der Rolle Apotheker/Pharmazieingenieur/Apothekerassistent MUSS dieser die Zugriffsrechte zur Einsicht in aktuell einlösbare Rezepte des EU-Bürgers, zur Einsicht in die aktuelle Medikation des EU-Bürgers und zur Aufzeichnung der Dispensierinformation

	für den EU-Bürger bekommen.
1.8	Im Rahmen der Authentisierung des LE-DE MUSS der Behandlungsmodus "TREATMENT" angegeben werden, der besagt, dass der EU-Bürger einwilligungsfähig ist und Informationen zu seiner Gesundheitsversorgung aufnehmen kann (keine Notfall-Behandlung bei bewusstlosem oder nicht einwilligungsfähigem EU-Bürger).

663

664 2. Als nationale Verbindungsstelle muss ich sicherstellen, dass eine Authentisierung des
 665 LE-DE nach Ablauf von vier Stunden ungültig wird, damit nur berechnete LE-DE die
 666 Daten von EU-Bürgern abrufen können. (Vorgabe des [eHDSI_SAML_Profile] #2.1)

ID	Akzeptanzkriterium
2.1	Nach einer erfolgreichen Authentisierung des LE-DE MUSS dieser für einen Zeitraum von vier Stunden Daten von EU-Bürgern abrufen können, ohne sich erneut authentisieren zu müssen.
2.2	Ab vier Stunden nach einer erfolgreichen Authentisierung des LE-DE DARF dieser NICHT mehr Daten von EU-Bürgern abrufen, ohne sich erneut authentisiert zu haben.

667

668 3. Als LE-DE möchte ich eine klare Anleitung und Unterstützung für meine
 669 Authentisierung sowie die anschließende Autorisierung erhalten, damit ich sicherstellen
 670 kann, dass ich die korrekten Schritte durchführe.

ID	Akzeptanzkriterium
3.1	Der LE-DE MUSS eine allgemeine Beschreibung des Gesamt-Ablaufs einsehen können, um besser zu verstehen, wie sich der Prozess der Authentisierung sowie die anschließende Autorisierung des LE-DE in den Vorgang ePrescription/eDispensation einordnet.
3.2	Der LE-DE MUSS eine allgemeine Beschreibung für den Prozess Authentisierung sowie die anschließende Autorisierung des LE-DE einsehen können, um besser zu verstehen, welche Aktivitäten der Vorgang umfasst.
3.3	Der LE-DE MUSS einen eindeutigen Handlungshinweis im Workflow bekommen, dass er eine Authentisierung durchführen muss, um das Anwendungsszenario durchzuführen.

671

672 4. Ich als LE-DE möchte bei aufgetretenen Fehlern und Warnungen darüber informiert
 673 werden und leicht verständlich mögliche Handlungsoptionen angeboten bekommen, um
 674 passend auf Fehlersituationen reagieren zu können.

ID	Akzeptanzkriterium
----	--------------------

4.1	Dem LE-DE MUSS primär eine menschlich verständliche Fehlermeldung angezeigt werden. Dazu MUSS auch eine Information enthalten sein, ob die initiale Fehlermeldung aus dem Land A oder Deutschland stammt.
4.2	Dem LE-DE MÜSSEN als weiterführende Information technische Details angeboten werden, die er auch dem Support als Detailinformation mitgeben kann.
4.3	Dem LE-DE MUSS immer der Kontakt zu Support angeboten werden, um Unterstützung bei der Lösung seines Problems mit dem EU-Szenario erhalten zu können.
4.4	Dem LE-DE MÜSSEN zur Fehlermeldung passende Handlungsmöglichkeiten zum Umgang mit dem Fehler angezeigt werden.
4.5	Bei Anzeige einer Warnung MUSS es für den LE-DE möglich sein, den Workflow dennoch weiterzuführen.
4.6	Bei Auftreten einer Fehlersituation DARF es dem LE-DE NICHT möglich sein, den Workflow weiterzuführen.
4.7	Fehlersituationen, die in Deutschland erkannt werden, MÜSSEN mit einem deutschen Fehlertext gemeldet werden.

675

676 5. Ich als LE-DE möchte meine Authentisierung einfach abbrechen können, um bei
677 Wegfall des Authentisierungsbedarfes unkompliziert reagieren zu können.

ID	Akzeptanzkriterium
5.1	Der LE-DE MUSS den Authentifizierungsvorgang jederzeit abbrechen können.
5.2	Dem LE-DE MUSS bei zeitlichem Ablauf eines Authentisierungsvorgangs (timeout) eine Fehlermeldung angezeigt werden. Desweiteren ist dies wie ein Abbruch des Authentisierungsvorgangs zu behandeln.
5.3	Für den LE-DE MUSS klar erkennbar sein, wo er den Vorgang abbrechen kann.
5.4	Bei Abbruch des Vorgangs durch den LE-DE MÜSSEN (abgesehen von den verpflichtenden Audit-Trails) die Daten des LE-DE in den beteiligten Systemen der nationalen Verbindungsstelle in Deutschland sicher gelöscht werden.

678

679 5.2 Information der Betroffenen über ihre Rechte und Pflichten 680 zum Schutz ihrer personenbezogenen und gesundheitlichen Daten

681 Das Feature ermöglicht die Bereitstellung von Informationen für EU-Bürger (Patient
682 Information Notice (PIN-Dokument)) und LE-DE (Health Professional Information Notice,
683 HPIN-Dokument) über ihre Rechte und Pflichten im Zusammenhang mit der Verarbeitung
684 ihrer personenbezogenen medizinischen Daten. Ziel ist es, Transparenz zu schaffen und

die gesetzlichen Informationspflichten zu erfüllen. Die Informationen sollen leicht verständlich, mehrsprachig verfügbar und bezogen auf die Nutzung des grenzüberschreitenden Gesundheitsdienstes ePrescription/eDispensation in Deutschland abrufbar sein.

5.2.1 Beschreibung der Anwenderdomäne

Damit die weiteren Schritte des Anwendungsszenarios durchgeführt werden können, muss derjenige EU-Bürger, welcher das Medikament erhalten möchte, zunächst vor Ort in der Apotheke in Deutschland (2) über die Verarbeitung seiner personenbezogenen und gesundheitlichen Daten informiert werden. Dies erfolgt über ein vereinheitlichtes PIN-Dokument. Dieses PIN-Dokument wird dem EU-Bürger in seiner Landessprache in der Apotheke vor Ort durch den LE-DE zur Verfügung gestellt (3).

Der Anbieter des NCPeH trägt dafür Sorge, dass dem LE-DE das PIN-Dokument in den Sprachen der Mitgliedsländer zur Verfügung gestellt wird (1).

Der LE-DE bestätigt, dass der EU-Bürger das PIN-Dokument zur Kenntnis genommen hat (4). Dafür nutzt er die bereits zuvor ausgestellte elektronische Identität des LE-DE.

Außerdem trägt der Anbieter des NCPeH dafür Sorge, dass dem LE-DE ebenfalls ein HPIN-Dokument zur Verfügung steht (1), welches über das ePeD-B System angezeigt werden kann (5) und den LE-DE seinerseits informiert, welche seiner Daten verarbeitet werden.

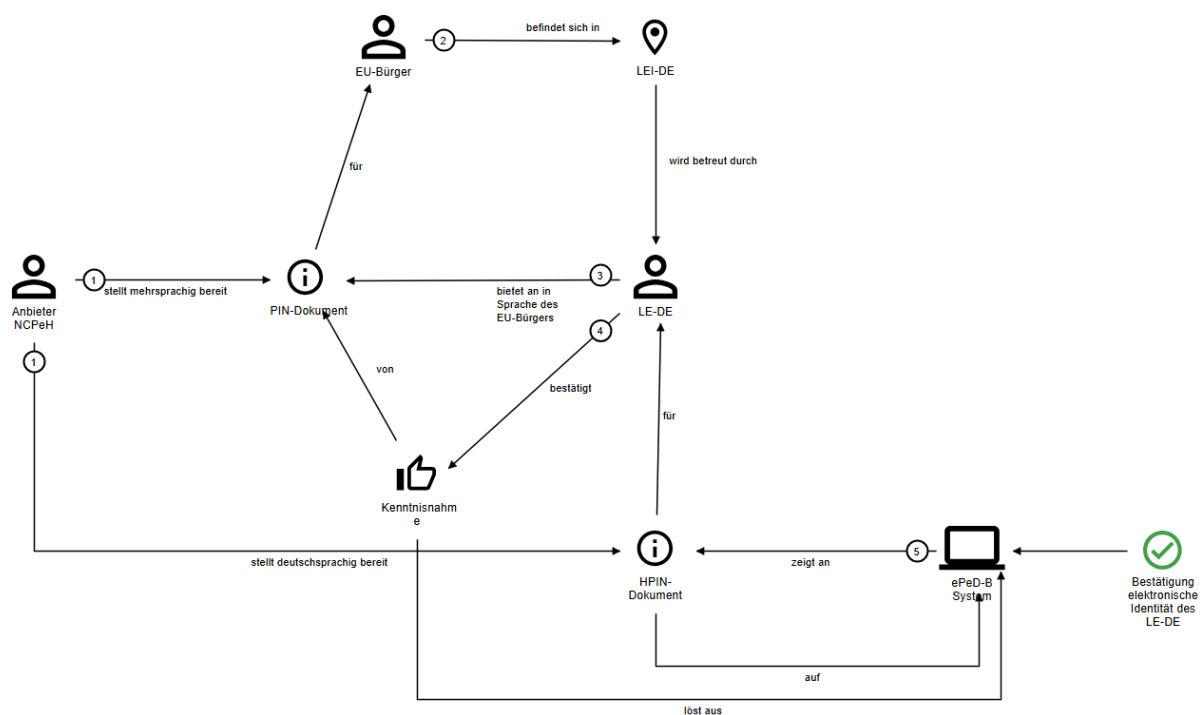


Abbildung 5: Information der Betroffenen über ihre Rechte und Pflichten zum Schutz ihrer personenbezogenen und gesundheitlichen Daten

5.2.2 User Stories

1. Als EU-Bürger möchte ich in einer deutschen Apotheke die Information zu meinen Rechten, Pflichten und Verarbeitung meiner Daten bei der Einlösung meiner Rezepte einsehen können, damit ich über die Nutzung meiner Daten informiert bin, bevor der LE-DE auf meine Rezepte zugreift.

ID	Akzeptanzkriterium
1.1	Die Informationen MÜSSEN dem EU-Bürger in der Sprache seines Zugehörigkeitslandes (Land A) bereitgestellt werden können.
1.2	Die aktuelle Patient Information Notice MUSS dem EU-Bürger durch den LE-DE digital (z.B. Weblink/QR-Code) bereitgestellt werden können.
1.3	Das aktuelle PIN-Dokument MUSS dem EU-Bürger durch den LE-DE in Papierform bereitgestellt werden können.
1.4	Der LE-DE MUSS die personenbezogenen oder Gesundheitsdaten des EU-Bürgers erst dann abrufen können, nachdem die Bereitstellung des PIN-Dokuments an den EU-Bürger dokumentiert wurde.
1.5	Das aktuelle PIN-Dokument MUSS auch in Sprachen anderer EU-Mitgliedstaaten bereitgestellt werden können.
1.6	Der EU-Bürger MUSS entscheiden können, in welcher Sprache und in welchem Format er das PIN-Dokument erhalten möchte.

2. Als LE-DE möchte ich das PIN-Dokument auch auf Deutsch einsehen können, damit ich den Inhalt verstehen und Fragen des EU-Bürgers beantworten kann.

ID	Akzeptanzkriterium
2.1	Der LE-DE MUSS das PIN-Dokument in deutscher Sprache anzeigen können.

3. Als LE-DE möchte ich wissen, welche Informationen genau bzgl. meiner Eigenschaft als LE an das Land des EU-Bürgers gesendet werden und welche Rechte und Pflichten ich bei der Verarbeitung meiner persönlichen Daten habe.

ID	Akzeptanzkriterium
3.1	Der LE-DE MUSS eine vollständige und verständliche Übersicht inklusive personenbezogener Daten des LE und der LEI erhalten können, die im Rahmen der grenzüberschreitenden Transaktion an das andere EU-Land (Land A) übermittelt werden.
3.2	Der LE-DE MUSS sich über seine Rechte und Pflichten nach DSGVO, über die Verantwortlichkeiten der beteiligten Stellen und über die Verarbeitung seiner Daten informieren können. Dabei MÜSSEN die Informationen auf Deutsch

verfügbar sein.

721

722 4. Als LE-DE möchte ich eine klare und unübersehbare GUI-Führung erhalten, die mich
723 zur PIN-Dokument-Bereitstellung veranlasst, damit ich diese nicht vergessen kann und
724 somit eine Verarbeitung der Daten des EU-Bürgers ohne Bereitstellung des PIN-
725 Dokuments vermeide.

ID	Akzeptanzkriterium
4.1	Der LE-DE MUSS aktiv die Bereitstellung des PIN-Dokumentes an den EU-Bürger bestätigen, bevor die Verarbeitung der Daten des EU-Bürgers ermöglicht wird.
4.2	Der LE-DE DARF die Identifizierungsmerkmale des Versicherten erst zum Suchen des EU-Bürgers über die ISM verwenden können, nachdem er bestätigt hat, dass die Bereitstellung des PIN-Dokuments an den EU-Bürger erfolgt ist.

726

727 5. Als LE-DE möchte ich eine klare Anleitung und Unterstützung für den Prozess der PIN-
728 Dokument-Bereitstellung und Einsicht in das HPIN-Dokument erhalten, damit ich
729 sicherstellen kann, dass ich die korrekten Schritte zur PIN-Dokument-Bereitstellung und
730 Einsicht in das HPIN-Dokument durchführe.

ID	Akzeptanzkriterium
5.1	Der LE-DE MUSS eine allgemeine Beschreibung des Gesamt-Ablaufs einsehen können, um besser zu verstehen, wie sich der Prozess der PIN-Dokument-Bereitstellung und Einsicht in das HPIN-Dokument in den Vorgang ePrescription/eDispensation einordnet.
5.2	Der LE-DE MUSS eine allgemeine Beschreibung für den Prozess der PIN-Dokument-Bereitstellung bekommen und Einsicht in das HPIN-Dokument nehmen können, um besser zu verstehen, welche Aktivitäten der Vorgang umfasst.
5.3	Der LE-DE MUSS einen eindeutigen Handlungshinweis im Workflow bekommen, dass er dem EU-Bürger das PIN-Dokument bereitstellen muss und dass er das HPIN-Dokument zur eigenen Information einsehen kann.

731

732 6. Als Anbieter des NCPeH möchte ich den LE-DE das PIN-Dokument bereitstellen
733 können, damit diese sie bei Bedarf einem EU-Bürger bereitstellen können.

ID	Akzeptanzkriterium
6.1	Das PIN-Dokument MUSS nach Bedarf aktualisiert werden können und entspricht dem aktuellen Stand der eHDSI-Vorgaben zur Übermittlung und Verarbeitung von personenbezogenen medizinischen Daten des EU-Bürgers.
6.2	Die angezeigten Informationen des HPIN-Dokuments MÜSSEN regelmäßig aktualisiert werden und entsprechen dem aktuellen Stand der eHDSI-Vorgaben zur Übermittlung und Verarbeitung von personenbezogenen Daten des LE-DE.

6.3	Das PIN-Dokument und das HPIN-Dokument MÜSSEN vom Anbieter des NCPeH digital so bereitgestellt werden, dass sie ohne Informationsverluste durch den LE-DE ausgedruckt werden können.
-----	--

7. Ich als LE-DE möchte bei aufgetretenen Fehlern darüber informiert werden und leicht verständlich mögliche Handlungsoptionen angeboten bekommen, um passend auf Fehlersituationen reagieren zu können.

ID	Akzeptanzkriterium
7.1	Dem LE-DE MUSS primär eine menschlich verständliche Fehlermeldung angezeigt werden.
7.2	Dem LE-DE MÜSSEN als weiterführende Information technische Details angeboten werden, die er auch dem Support als Detailinformation mitgeben kann.
7.3	Dem LE-DE MUSS immer der Kontakt zu Support angeboten werden, um Unterstützung bei der Lösung seines Problems mit dem EU-Szenario erhalten zu können.
7.4	Dem LE-DE MÜSSEN zur Fehlermeldung passende Handlungsmöglichkeiten zum Umgang mit dem Fehler angezeigt werden.
7.5	Bei Auftreten einer Fehlersituation DARF es dem LE-DE NICHT möglich sein, den Workflow weiterzuführen.
7.6	Fehlersituationen, die in Deutschland erkannt werden, MÜSSEN mit einem deutschen Fehlertext gemeldet werden.

5.3 Identifikation des EU-Bürgers in der Apotheke vor Ort

Jeder EU-Bürger muss technisch korrekt identifiziert werden, wenn er grenzüberschreitend eine Gesundheitsdienstleistung im Zusammenhang mit MyHealth@EU in Anspruch nimmt und einen LE-DE aufsucht, damit der Zugriff auf die korrekten Daten des EU-Bürgers im Land A sichergestellt wird.

Um jedoch einen EU-Bürger zu identifizieren, benötigt der LE-DE Unterstützung vom Zugehörigkeitsland (Land A): Das Land A stellt eine Suchmaske bereit und definiert, welche Daten vom EU-Bürger für die Suche erforderlich sind und welche national ausgestellten Dokumente als gültig für die Identifizierung seiner Bürger vor Ort in der LEI-DE gelten.

Das Ergebnis der Patientensuche besteht aus einer möglichst umfassenden Teilmenge der demographischen Daten des EU-Bürgers (persönliche Daten). Der Umfang der bereitgestellten Informationen hängt von den gesetzlichen Bestimmungen des Land A sowie von den verfügbaren Daten des EU-Bürgers ab.

Die vom Land A ermittelten persönlichen Daten inkl. der Identifier des EU-Bürgers werden schließlich an den anfragenden LE-DE gegeben. Der LE-DE ist verpflichtet, die

755 Identität des EU-Bürgers mit den elektronisch ermittelten persönlichen Daten des EU-
756 Bürgers zu überprüfen. Er verwendet dafür die vom Zugehörigkeitsland angegebenen
757 Dokumente, um den EU-Bürger zu identifizieren.

758

759 **5.3.1 Beschreibung der Anwenderdomäne**

760 Die Identifikation findet vor Ort in der LEI-DE statt, indem der EU-Bürger zunächst ein
761 vertrauenswürdige Ausweisdokument vorlegt (1). Begleitend dazu kann der LE-DE bei
762 Bedarf die Vorgangsbeschreibung der Identifikation einsehen (2).

763 Für die Suche werden die Identifier des EU-Bürgers genutzt, die der EU-Bürger
764 bereitstellt (3). Zur Suche des EU-Bürgers im System benutzt der LE-DE unter
765 Verwendung seiner eigenen elektronischen Identität die International Search Mask des
766 Landes des EU-Bürgers und sendet eine Anfrage an das ePeD-B System (4).

767 Anschließend liefert das ePeD-B System die persönlichen Daten des EU-Bürgers (5). Um
768 die Identität zweifelsfrei zu verifizieren, führt der LE-DE einen manuellen Vergleich durch
769 (6). Hierbei wird das physische vertrauenswürdige Ausweisdokument mit den im System
770 vorliegenden persönlichen Daten abgeglichen.

771 Nach erfolgreichem Abgleich stellt der LE-DE die ermittelten und bestätigten Patient
772 Identifier fest (7), welche durch eine Systemanfrage verknüpft werden.

773 Abschließend erzeugt das ePeD-B System automatisch eine Identifikationsdokumentation
774 (8), die das ePeD-B System bereitstellt und die final im Dokumentationsarchiv abgelegt
775 wird.

776

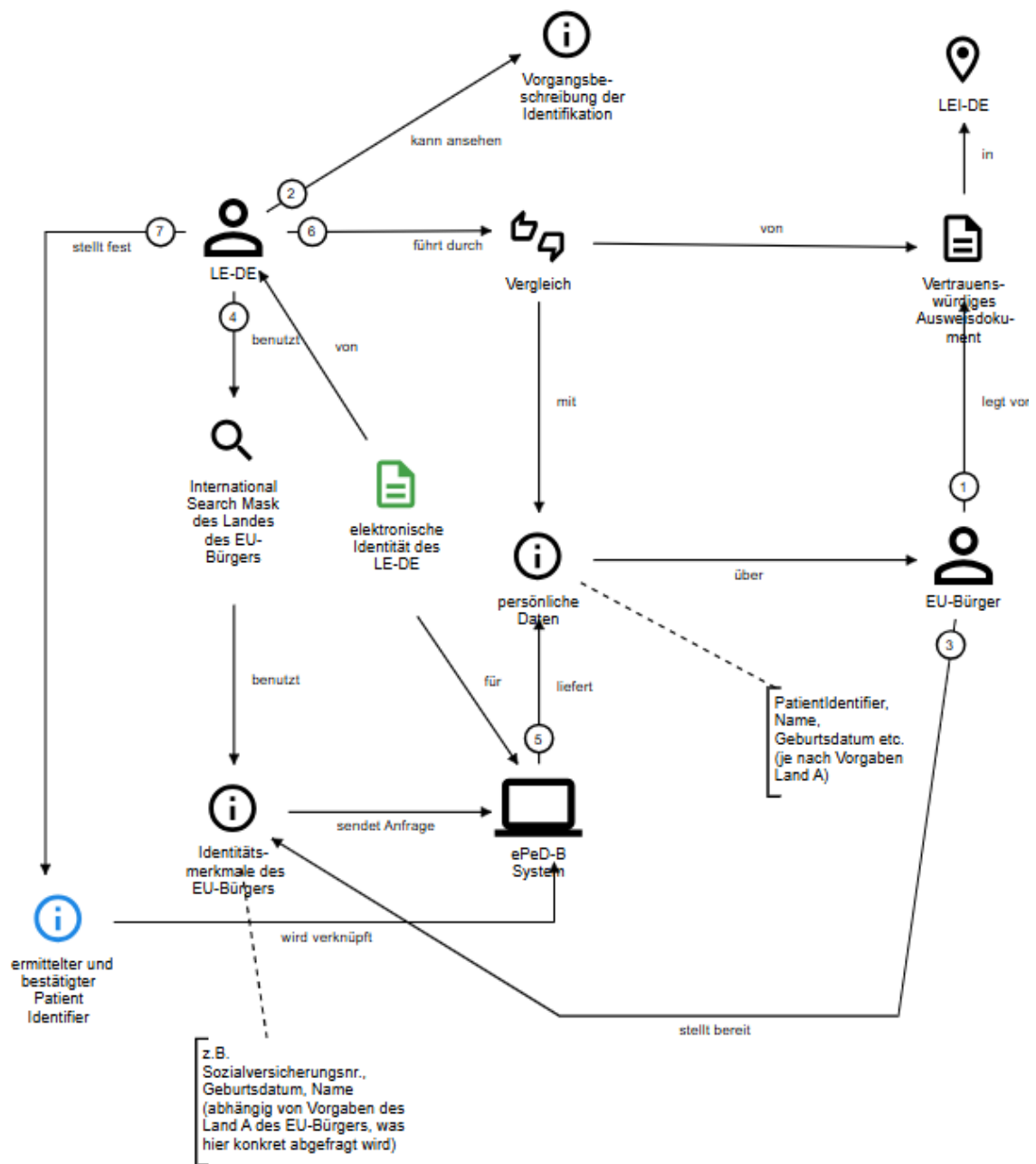


Abbildung 6: Identifikation des EU-Bürgers in der Apotheke vor Ort

5.3.2 User Stories

1. Als LE-DE möchte ich persönliche Daten des EU-Bürgers von der nationalen Infrastruktur des Land A abrufen können, damit ich anhand dieser Daten die Identität des EU-Bürgers abgleichen kann.

ID	Akzeptanzkriterium
1.1	Vor der Identifizierung des EU-Bürgers MUSS der LE-DE authentifiziert und für die

	weiteren Schritte autorisiert sein.
1.2	Der LE-DE MUSS genau die Suchmaske aufrufen, die gemäß den Vorgaben des Land A definiert ist, um persönliche Daten des EU-Bürgers abzurufen.
1.3	Die Suchmaske und die Begleitinformationen (Hilfetexte oder Bilder) aus Land A MÜSSEN korrekt und lesbar angezeigt werden, damit der LE-DE die erforderlichen Suchparameter eingeben kann.

784

785 2. Als LE-DE möchte ich persönliche Daten des EU-Bürgers von der nationalen
 786 Infrastruktur des Land A empfangen können, damit ich die Identität des EU-Bürgers mit
 787 diesen Daten abgleichen kann.

ID	Akzeptanzkriterium
2.1	Die empfangenen Daten MÜSSEN mindestens die zur Identitätsprüfung erforderlichen Attribute enthalten: Patient Identifier, Name und Geburtsdatum.
2.4	Der LE-DE MUSS persönliche Daten genau einer Person finden, um eine erfolgreiche Identifizierung des EU-Bürgers durchführen zu können.

788

789 3. Als LE-DE möchte ich sicher sein, dass die persönlichen Daten, die ich vom
 790 Zugehörigkeitsland erhalte, unverändert und vertrauenswürdig sind, damit ich mich auf
 791 die Korrektheit der Informationen verlassen kann.

ID	Akzeptanzkriterium
3.1	Die Übertragung der persönlichen Daten des EU-Bürgers MUSS verschlüsselt erfolgen, damit die übertragenen Daten nicht eingesehen oder manipuliert werden können.
3.2	Die Anbieter und Betreiber des ePeD-B-Systems DÜRFEN KEINEN Zugriff auf die persönlichen Daten des EU-Bürgers erhalten, damit die Daten nicht von diesen gelesen oder manipuliert werden können.

792

793 4. Als LE-DE möchte ich eine klare Anleitung und Unterstützung für den Prozess der
 794 Identitätsprüfung erhalten, damit ich sicherstellen kann, dass ich die korrekten Schritte
 795 zur Identifizierung des EU-Bürgers durchführe.

ID	Akzeptanzkriterium
4.1	Der LE-DE MUSS eine allgemeine Beschreibung des Gesamtablaufs einsehen können, um besser zu verstehen, wie sich die Identifizierung des EU-Bürgers in den Vorgang ePrescription/eDispensation einordnet.
4.2	Der LE-DE MUSS eine allgemeine Beschreibung zur Identifizierung eines EU-Bürgers einsehen können, um besser zu verstehen, welche Aktivitäten der Vorgang der Identifizierung umfasst.

4.3	Der LE-DE MUSS einen eindeutigen Handlungshinweis im Workflow bekommen, dass er den EU-Bürger identifizieren muss und wie er die Identitätsprüfung durchführen muss.
-----	--

796

797

798

799

5. Ich als LE-DE möchte bei aufgetretenen Fehlern und Warnungen darüber informiert werden und leicht verständlich mögliche Handlungsoptionen angeboten bekommen, um passend auf Fehlersituationen reagieren zu können.

ID	Akzeptanzkriterium
5.1	Dem LE-DE MUSS primär eine menschlich verständliche Fehlermeldung angezeigt werden. Dazu MUSS auch eine Information enthalten sein, ob die initiale Fehlermeldung aus dem Land A oder Deutschland stammt.
5.2	Dem LE-DE MUSS immer der Kontakt zu Support angeboten werden, um Unterstützung bei der Lösung seines Problems mit dem EU-Szenario erhalten zu können.
5.3	Bei Anzeige einer Warnung MUSS es für den LE-DE möglich sein, den Workflow dennoch weiterzuführen.
5.4	Bei Auftreten einer Fehlersituation DARF es dem LE-DE NICHT möglich sein, den Workflow weiterzuführen.
5.5	Dem LE-DE MÜSSEN als weiterführende Information technische Details angeboten werden, die er auch dem Support als Detailinformation mitgeben kann.
5.6	Dem LE-DE MÜSSEN zur Fehlermeldung passende Handlungsmöglichkeiten zum Umgang mit dem Fehler angezeigt werden.
5.7	Fehlersituationen, die in Deutschland erkannt werden, MÜSSEN mit einem deutschen Fehlertext gemeldet werden.
5.8	Fehlertexte aus dem Land A MÜSSEN unverändert oder um weitere Informationen ergänzt an den LE-DE weitergereicht werden.
5.9	Dem LE-DE MUSS bei einem unzureichenden Suchergebnis (kein Fund, mehr als ein Fund) eine Fehlermeldung angezeigt werden, da eine Fortführung der Bedienung des EU-Bürgers ohne eindeutige Identifikation nicht möglich ist.
5.10	Dem LE-DE MUSS bei einem unzureichenden Suchergebnis (falsches Datenformat, fehlende Eingabefelder) eine Fehlermeldung mit Handlungsmöglichkeiten angezeigt werden, da er dann zur Identifizierung eingegebene Daten ändern oder weitere Daten eingeben muss.

800

801

802

803

6. Als LE-DE möchte ich die Suche nach persönlichen Daten eines EU-Bürgers wiederholen können, damit ich durch Korrektur oder Erweiterung der Suchparameter ein eindeutiges Suchergebnis erreichen kann.

ID	Akzeptanzkriterium
6.1	Der LE MUSS nach fehlgeschlagener Suche oder unzureichendem Suchergebnis die Suchmaske des Land A zur Wiederholung der Identifikation eines EU-Bürgers erneut öffnen können.
6.2	Wenn der LE-DE die Suchmaske zur Wiederholung der Suche desselben EU-Bürgers erneut öffnet, dann MUSS diese mit den zuletzt eingegebenen Daten dieses EU-Bürgers vorausgefüllt sein.
6.3	Wenn der LE-DE die Suchmaske zur Suche eines anderen EU-Bürgers öffnet, dann DARF die Suchmaske NICHT mit den zuletzt eingegebenen Daten eines anderen EU-Bürgers vorausgefüllt sein.

804

805 7. Ich als LE-DE möchte die Identifikation des EU-Bürgers abbrechen können, um auf
806 Wunsch des EU-Bürgers oder meinen Wunsch den Vorgang beenden zu können.

ID	Akzeptanzkriterium
7.1	Der LE-DE MUSS den Vorgang der Identifikation des EU-Bürgers jederzeit abbrechen können.
7.2	Für den LE-DE MUSS klar erkennbar sein, wo er den Vorgang abbrechen kann.
7.3	Bei Abbruch des Vorgangs durch den LE-DE MÜSSEN (abgesehen von den verpflichtenden Audit-Trails) die Daten des EU-Bürgers in den beteiligten Systemen der nationalen Verbindungsstelle in Deutschland sicher gelöscht werden.

807

808 5.4 Bestätigung des Behandlungsverhältnisses zum EU-Bürger

809 Dieses Feature belegt die Existenz eines Behandlungsverhältnisses zwischen dem EU-
810 Bürger und dem LE-DE in seiner LEI im Kontext der grenzüberschreitenden Versorgung.
811 Dieses Behandlungsverhältnis kann erst existieren, wenn sich der LE-DE erfolgreich
812 authentisiert und autorisiert hat und der EU-Bürger erfolgreich identifiziert wurde. Die
813 Bestätigung des Behandlungsverhältnisses erfolgt durch die nationale Verbindungsstelle
814 in Deutschland und ist nach Vorgaben in [eHDSI_SAML_Profile] #4.1 maximal 2
815 Stunden gültig.

816

817 5.4.1 Beschreibung der Anwenderdomäne

818 Aufbauend auf der erfolgreichen Identifikation des EU-Bürgers initiiert der LE-DE den
819 nächsten Prozessschritt. Er führt die Bestätigung des Behandlungsverhältnisses im ePeD-
820 B System durch (1). Dabei wird der zuvor im System hinterlegte ermittelte und
821 bestätigte Patient Identifier als Basis für die Zuordnung verwendet.

Im Rahmen dieses Vorgangs überprüft das ePeD-B System die elektronische Identität des LE-DE (2). Die Prüfung ist essenziell, da die Identität spezifische Zugriffsrechte enthält, die für den LE-DE gelten und die Legitimität des Zugriffs sicherstellen.

Nach erfolgreicher Prüfung erzeugt das ePeD-B System die elektronische Bestätigung des Behandlungsverhältnisses (3). Dieses digitale Objekt, auch als TRC-Assertion bezeichnet, weist eine zeitliche Begrenzung auf und enthält eine digitale Signatur im EU-Kontext, um die grenzüberschreitende Anerkennung der Informationsweitergabe und die Sicherheit zu gewährleisten.

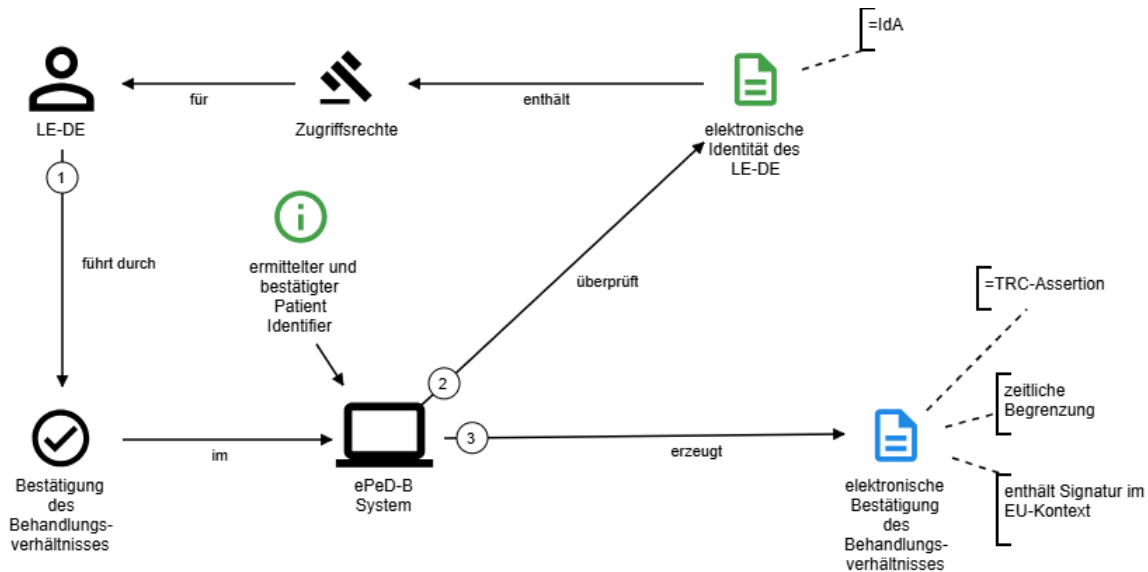


Abbildung 7: Bestätigung des Behandlungsverhältnisses zum EU-Bürger

5.4.2 User Stories

1. Als nationale Verbindungsstelle möchte ich die Bestätigung des Behandlungsverhältnisses für LE-DE und die ermittelte EU-Bürger-ID nach EU-Vorgaben erstellen und signieren, um sie authentisch und für EU-Mitgliedstaaten nachprüfbar bereitzustellen.

ID	Akzeptanzkriterium
1.1	Für die Bestätigung des Behandlungsverhältnisses MÜSSEN die gleichen LE-DE-Identifizierer (als Verknüpfung zur Identität des LE-DE) wie für die Authentisierung/Autorisierung des LE-DE genutzt werden.
1.2	Die Bestätigung des Behandlungsverhältnisses MUSS auf eine Authentisierung und Autorisierung des LE-DE verweisen, die zeitlich noch mindestens 30 Minuten gültig ist.
1.3	Die Bestätigung des Behandlungsverhältnisses DARF NICHT erstellt werden, wenn der LE-DE nicht für den ePrescription und den eDispensation-Dienst autorisiert ist.

1.4	Für die Bestätigung des Behandlungsverhältnisses MÜSSEN die gleichen Patient Identifier des EU-Bürgers genutzt werden, wie sie bei der Identifikation des EU-Bürgers ermittelt wurden.
1.5	Bei Angabe von Zugriffsinformationen auf Dokumente des EU-Bürgers MÜSSEN diese in der Behandlungsbestätigung enthalten sein.
1.6	Die Bestätigung des Behandlungsverhältnisses MUSS vor dem Abruf von medizinischen Daten des EU-Bürgers erstellt werden.
1.7	Alle weiteren Daten MÜSSEN entsprechend eHDSI-Vorgaben in der Bestätigung des Behandlungsverhältnisses enthalten sein.

839

840 2. Als LE-DE möchte ich eine klare und unübersehbare GUI-Führung erhalten, damit ich
 841 eine Bestätigung des Behandlungsverhältnisses nicht ohne vorhergehende erfolgreiche
 842 Identifizierung des EU-Bürgers durchführen kann.

ID	Akzeptanzkriterium
2.1	Der LE-DE DARF das Behandlungsverhältnis zum EU-Bürger erst bestätigen können, nachdem der LE-DE den EU-Bürger erfolgreich identifiziert hat.

843

844 3. Als EU-Bürger möchte ich, dass eine Anfrage zur Bestätigung des
 845 Behandlungsverhältnisses zeitlich begrenzt gültig ist, damit meine medizinischen Daten
 846 nicht zeitlich uneingeschränkt einsehbar sind.

ID	Akzeptanzkriterium
3.1	Die erfolgte Bestätigung des Behandlungsverhältnisses DARF entsprechend Vorgaben der eHDSI NUR maximal 2 Stunden gültig sein.
3.2	Wenn die Bestätigung des Behandlungsverhältnisses nach Ablauf der Zeit nicht erneuert wird, MÜSSEN die personenbezogenen Daten des EU-Bürgers (abgesehen von verpflichtenden Audit Trail Logs und Protokollierungsdaten) gelöscht werden.

847

848 4. Als LE-DE möchte ich eine klare Anleitung und Unterstützung für den Prozess der
 849 Bestätigung des Behandlungsverhältnisses erhalten, damit ich sicherstellen kann, dass
 850 ich die korrekten Schritte zur Bestätigung des Behandlungsverhältnisses durchführe.

ID	Akzeptanzkriterium
4.1	Der LE-DE MUSS eine allgemeine Beschreibung des Gesamt-Ablaufs einsehen können, um besser zu verstehen, wie sich die Bestätigung des Behandlungsverhältnisses in den Vorgang ePrescription/eDispensation einordnet.
4.2	Der LE-DE MUSS eine allgemeine Beschreibung zur Bestätigung des Behandlungsverhältnisses einsehen können, um besser zu verstehen, welche Aktivitäten der Vorgang umfasst.

851

852 5. Ich als LE-DE möchte bei aufgetretenen Fehlern darüber informiert werden und leicht
 853 verständlich mögliche Handlungsoptionen angeboten bekommen, um passend auf
 854 Fehlersituationen reagieren zu können.

ID	Akzeptanzkriterium
5.1	Dem LE MUSS primär eine menschlich verständliche Fehlermeldung angezeigt werden.
5.2	Dem LE MUSS immer der Kontakt zu Support angeboten werden, um Unterstützung bei der Lösung seines Problems mit dem EU-Szenario erhalten zu können.
5.3	Dem LE MÜSSEN als weiterführende Information technische Details angeboten werden, die er auch dem Support als Detailinformation mitgeben kann.
5.4	Dem LE MÜSSEN zur Fehlermeldung passende Handlungsmöglichkeiten angezeigt werden, um mit dem Fehler umgehen zu können.
5.5	Bei Auftreten einer Fehlersituation DARF es dem LE-DE NICHT möglich sein, den Workflow weiterzuführen.
5.6	Fehlersituationen, die in Deutschland erkannt werden, MÜSSEN mit einem deutschen Fehlertext gemeldet werden.

855

856 6. Ich als LE-DE möchte die Bestätigung des Behandlungsverhältnisses abbrechen
 857 können, um auf Wunsch des EU-Bürgers oder meinen Wunsch den Vorgang beenden zu
 858 können.

ID	Akzeptanzkriterium
6.1	Der LE-DE MUSS den Vorgang der Bestätigung des Behandlungsverhältnisses jederzeit abbrechen können.
6.2	Für den LE-DE MUSS klar erkennbar sein, wo er den Vorgang abbrechen kann.
6.3	Bei Abbruch des Vorgangs durch den LE-DE MÜSSEN (abgesehen von den verpflichtenden Audit-Trails) die Daten des EU-Bürgers in den beteiligten nationalen Systemen sicher gelöscht werden.
6.4	Ein Abbruch der Bestätigung des Behandlungsverhältnisses MUSS wie ein Abbruch des Gesamtvorgangs behandelt werden.

859

5.5 Auflistung und Abruf der einlösbaren Rezepte des EU-Bürgers

Damit der LE-DE die Rezepte auswählen kann, die der EU-Bürger einlösen möchte, muss für den LE-DE eine Liste der einlösbaren Rezepte des EU-Bürgers einsehbar sein. Falls das Land A informativ auch im EU-Ausland nicht einlösbare Rezepte bereitstellt, die aber im Land A einlösbar wären, so werden diese auch informativ mit angezeigt.

Die einlösbaren Rezepte können in einem weiteren Schritt abgerufen werden, um mehr inhaltliche Details des Rezepts einsehen zu können und das Rezept im nächsten Schritt dispensieren zu können, falls der EU-Bürger dies möchte.

Die Datenelemente der Rezepte sollen wenn möglich auf deutsch übersetzt dargestellt werden, um die Verständlichkeit der Inhalte für den LE-DE zu erleichtern. Die Möglichkeit zur Übersetzung in die deutsche Sprache ist abhängig von der Verfügbarkeit strukturierter und codierter Daten.

5.5.1 Beschreibung der Anwenderdomäne

Sobald die elektronische Bestätigung des Behandlungsverhältnisses zwischen dem EU-Bürger und dem LE-DE vorliegt, stellt das ePeD-B System dem LE-DE die verfügbaren Rezepte bereit (1). Dabei nutzt es erneut die elektronische Identität des LE-DE.

Um die Verständlichkeit und Weiterverarbeitung zu gewährleisten, übersetzt das ePeD-B System die codierten Daten und erzeugt codierte Rezeptinformationen auf deutsch (2). Diese Struktur enthält essenzielle pharmazeutische Details wie den ATC-Code, den Wirkstoff, die Wirkstärke, die Darreichungsform, den Namen des verordnenden LE-EU sowie die Angabe, ob eine Substitution erlaubt ist.

Das ePeD-B System zeigt in der Auflistung den aktuellen Status der Rezepte an (3) und differenziert dabei nach nicht einlösbaren Rezepten und einlösbaren Rezepten des EU-Bürgers. Die Übersicht enthält dabei bereits eine Beschreibung des Rezepts.

Aus den einlösbaren Rezepten ruft der LE-DE einzelne oder mehrere Rezepte ab (4). Die resultierende Menge der abgerufenen, einlösbaren Rezepte enthält mindestens die verpflichtenden Rezeptdaten eines jeden Rezepts aus dieser Menge. Hierbei wird unterschieden in Rezeptdaten, die vorhanden sein müssen und Rezeptdaten, die vorhanden sein sollten (bei Fehlen ist eine Begründung erforderlich). Zudem werden - sofern vorhanden - die Kennzeichnung des Substitutionsverbots sowie optionale Rezeptdaten angezeigt.

Ergänzend bietet der Ablauf eine optionale Validierungsmöglichkeit: Der LE-DE kann das Originalrezept einsehen (5), welches im Datensatz des einlösbaren Rezepts enthalten ist. Für eine bessere Lesbarkeit kann der LE-DE die Spracheinstellung der angezeigten Rezeptdaten ändern (5), beispielsweise um zwischen der Originalsprache (Land A), Englisch oder Deutsch zu wechseln.

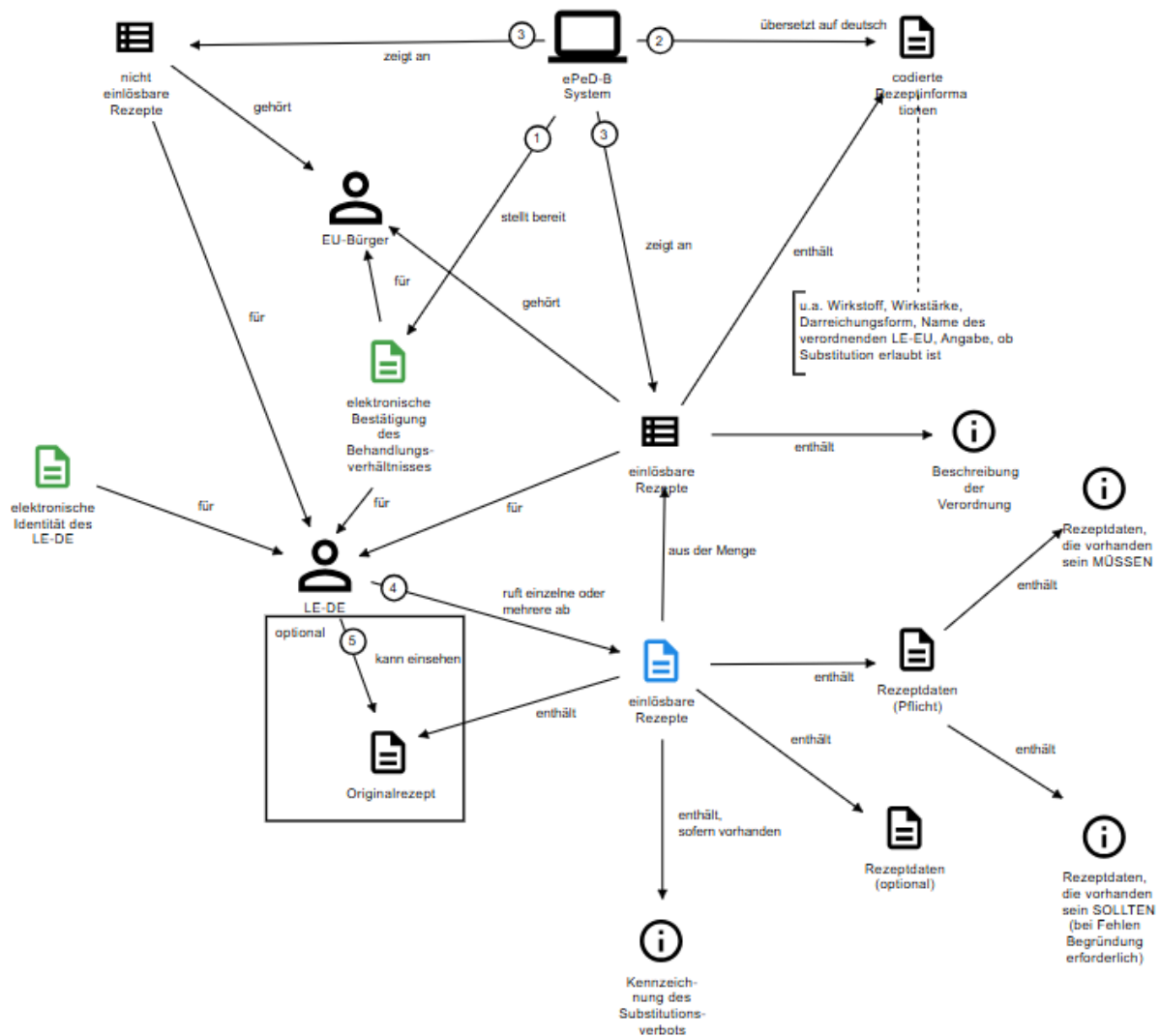


Abbildung 8: Auflistung und Abruf der einlösbaren Rezepte des EU-Bürgers

5.5.2 User Stories

1. Als LE-DE möchte ich die einlösbaren Rezepte eines EU-Bürgers mit den wichtigsten Daten auflisten können, um mit dem EU-Bürger eine erste Auswahl der einzulösenden Rezepte treffen zu können.

ID	Akzeptanzkriterium
1.1	Die folgenden Daten MÜSSEN bei der Anzeige der Rezepte in der Liste enthalten sein: <ul style="list-style-type: none"> • Beschreibung der Verordnung (Freitext) • Einlösbarkeit (ja/nein)

	<ul style="list-style-type: none"> Datum der Verordnung
1.2	<p>Wenn die folgenden codierten, optionalen Daten von Land A geliefert werden, MÜSSEN diese bei der Anzeige der Rezepte in der Liste mit angezeigt werden:</p> <ul style="list-style-type: none"> ATC-Code und ATC-Text Wirkstärke Darreichungsform Name des verordnenden LE-EU Angabe, ob Substitution erlaubt ist
1.3	Wenn keine offenen Rezepte des EU-Bürgers verfügbar sind, MUSS dem LE-DE eine eindeutige Meldung angezeigt werden und eine Wiederholung der Rezeptsuche oder ein Abbruch des Gesamtvorgangs ermöglicht werden.
1.4	Bei codierten Informationen des Rezeptes MUSS ein deutscher Text angegeben werden, wenn ein Mapping auf einen deutschen Text möglich ist.
1.5	Fremdsprachige Daten von Rezepten MÜSSEN korrekt angezeigt werden.
1.6	Fehlerinformationen zu Rezepten MÜSSEN klar erkennbar sein und diese Rezepte dürfen dann nicht abrufbar sein.

906

907

908

909

2. Als LE-DE möchte ich außerhalb des Land A nicht einlösbare Rezepte des EU-Bürgers anzeigen können, sofern diese vom Land A mit ausgegeben werden, um die aktuelle Abgabe von Medikamenten besser bewerten zu können.

ID	Akzeptanzkriterium
2.1	Alle im Moment der Auflistung verfügbaren, im Land A aktiven Rezepte des EU-Bürgers MÜSSEN dem LE-DE angezeigt werden.
2.2	Die aufgelisteten nicht einlösbaren E-Rezepte MÜSSEN die gleichen Datenkategorien beinhalten wie die einlösbaren Rezepte.
2.3	Durch den LE-DE nicht einlösbare Rezepte MÜSSEN klar als solche erkennbar sein.
2.4	Durch den LE-DE nicht einlösbare Rezepte DÜRFEN NICHT abrufbar sein.

910

911

912

913

914

3. Als LE-DE möchte ich nach dem Auflisten der Rezepte verstehen können, dass ich in einem weiteren Schritt die vollständigen Rezepte des EU-Bürgers abrufen muss, um den Inhalt der Rezepte bestmöglich verstehen zu können und um das Medikament im Anschluss dispensieren zu können.

ID	Akzeptanzkriterium
3.1	Es MUSS eine eindeutig erkennbare Handlungsvorgabe für den LE-DE geben, dass

die vollständigen einlösbaren Rezepte des EU-Bürgers abgerufen werden müssen.

915

916

917

918

4. Als LE-DE möchte ich die vollständigen fachlichen Inhalte eines oder mehrerer Rezepte des EU-Bürgers abrufen und anzeigen können, um Verordnungen aus dem Land A sicher verstehen und korrekt dispensieren zu können.

ID	Akzeptanzkriterium	Offener Punkt
4.1	<p>Folgende Daten MUSS jedes abgerufene Rezept des EU-Bürgers beinhalten und angezeigt werden:</p> <ul style="list-style-type: none"> EU-Bürger: Vollständiger Name, Geburtsdatum EU-LE: Berufsbezeichnung, Land der Ausstellung des Rezepts Rezept: Rezept-ID, Wirkstoff, Darreichungsform, Packungsmenge Verschreibungsdaten: Datum der Verschreibung, verantwortliche LE/LEI im Land A 	<p><i>Welche genauen Daten das abgerufene Rezept beinhalten muss, ist noch vorbehaltlich der in Kapitel 2 genannten Klärung der rechtlichen Rahmenbedingungen mit BMG bzw. mit Angehörigen der DG Sante der Europäischen Kommission.</i></p>
4.2	<p>Folgende Daten SOLL das abgerufene Rezept des EU-Bürgers beinhalten und angezeigt werden (wenn diese Daten nicht bereitgestellt werden, muss eine Begründung aus Land A vorliegen und angezeigt werden.):</p> <ul style="list-style-type: none"> EU-Bürger: Patient Identifier EU-LE: Identifier, vollständiger Name Rezept: Wirkstärke, Packungsart und -größe 	
4.3	Im abgerufenen Rezept MUSS klar ersichtlich sein, wenn eine Substitution <u>nicht</u> erlaubt ist.	
4.4	Wenn weitere optionale Daten des Rezepts vom Land A geliefert werden, MÜSSEN diese mit angezeigt werden.	
4.5	Nach erfolgtem Abruf eines Rezepts MUSS es die Möglichkeit der Rückkehr zur Listenansicht geben, wenn das abgerufene Rezept doch nicht eingelöst werden soll.	

919

920

921

922

5. Als LE-DE möchte ich das Originalrezept zu jedem abgerufenen Rezept einsehen und bei Auswahl für die Dispensierung auch speichern können, um ein vollständigeres Verständnis zu den Rezepten eines EU-Bürgers bekommen zu können.

ID	Akzeptanzkriterium
5.1	Im abgerufenen Rezept MUSS für den LE-DE klar ersichtlich sein, dass das Original-Rezept im PDF-Format einsehbar ist.

5.2	Im abgerufenen Rezept MUSS für den LE-DE klar ersichtlich sein, dass er das Original-Rezept zu Dokumentationszwecken lokal abspeichern kann.
-----	--

923

924 6. Als nationale Verbindungsstelle möchte ich Rezepte nur authentisierten und
 925 autorisierten LE-DEs mit gültiger Behandlungsbeziehung zum EU-Bürger zur Verfügung
 926 stellen, um die gesetzlichen Anforderungen an IT-Sicherheit und Datenschutz
 927 einzuhalten.

ID	Akzeptanzkriterium
6.1	Beim Zugriff auf die Rezepte des EU-Bürgers MUSS sichergestellt sein, dass der LE-DE aktuell für diesen Vorgang authentisiert und autorisiert ist.
6.2	Beim Zugriff auf die Rezepte des EU-Bürgers MUSS sichergestellt sein, dass eine gültige Behandlungsbeziehung zum EU-Bürger besteht.
6.3	Wenn der LE-DE im Moment der Auflistung oder des Abrufs der Rezepte nicht mehr authentisiert und autorisiert oder der bestätigte Behandlungskontext nicht mehr gültig ist, MUSS sich der LE-DE erneut authentisieren und autorisieren und der gültige Behandlungskontext MUSS erneuert werden, bevor er auf die Rezepte des EU-Bürgers zugreifen kann.

928

929 7. Als LE-DE möchte ich bei der vollständigen Anzeige der fachlichen Inhalte eines
 930 Rezepts zwischen der Originalsprache des Rezepts und der deutschen Sprache wählen
 931 können, um ein vollständigeres Verständnis zu den Rezepten eines EU-Bürgers
 932 bekommen zu können.

ID	Akzeptanzkriterium
7.1	Die Beschreibung der Attributfelder MUSS immer in deutscher Sprache angegeben werden.
7.2	Bei codierten Informationen des Rezeptes MUSS ein deutscher Text angegeben werden, wenn ein Mapping auf einen deutschen Text möglich ist.
7.3	Im abgerufenen Rezept MUSS in deutscher Sprache eindeutig ersichtlich sein, ob eine Substitution ausgeschlossen ist.
7.4	Wenn kein Mapping von Codes möglich ist, MÜSSEN die textuellen Informationen aus dem Land A falls verfügbar in englischer Sprache angezeigt werden. Falls die englische Sprache nicht verfügbar ist, MUSS die Information in der Originalsprache des Dokuments angezeigt werden.
7.5	Fremdsprachige Daten von Rezepten MÜSSEN korrekt angezeigt werden.

933

934 8. Als LE-DE möchte ich sicher sein, dass die persönlichen Daten, die ich vom
 935 Zugehörigkeitsland erhalte, unverändert und vertrauenswürdig sind, damit ich mich auf
 936 die Korrektheit der Informationen verlassen kann.

ID	Akzeptanzkriterium
8.1	Die Übertragung der persönlichen Daten des EU-Bürgers MUSS verschlüsselt erfolgen, damit die übertragenen Daten nicht eingesehen oder manipuliert werden können.
8.2	Die Anbieter und Betreiber des ePeD-B-Systems DÜRFEN KEINEN Zugriff auf die persönlichen Daten des EU-Bürgers erhalten, damit die Daten nicht von diesen gelesen oder manipuliert werden können.

937

938

939

940

9. Als LE-DE möchte ich eine klare Anleitung und Unterstützung für den Prozess des Auflistens und des Abrufs einlösbarer Rezepte des EU-Bürgers erhalten, damit ich sicherstellen kann, dass ich die korrekten Schritte dieses Vorgangs durchführe.

ID	Akzeptanzkriterium
9.1	Der LE-DE MUSS eine allgemeine Beschreibung des Gesamt-Ablaufs einsehen können, um besser zu verstehen, wie sich die Auflistung und der Abruf der einlösbaren Rezepte des EU-Bürgers in den Vorgang ePrescription/eDispensation einordnet.
9.2	Der LE-DE MUSS eine allgemeine Beschreibung zu Auflistung und Abruf der einlösbaren Rezepte des EU-Bürgers einsehen können, um besser zu verstehen, welche Aktivitäten der Vorgang umfasst.
9.3	Der LE-DE MUSS einen eindeutigen Handlungshinweis im Workflow bekommen, dass er aus der angezeigten Liste die Rezepte, die der EU-Bürger einlösen möchte, zur Einsicht in die Rezeptdetails und zur Dispensierung auswählen muss.
9.4	In der Liste MUSS ein Hinweis angezeigt werden, dass, wenn ein Rezept aus der Liste abgerufen, aber nicht dispensiert wird, es je nach Herkunftsland nicht mehr eingelöst werden kann.

941

942

943

944

10. Ich als LE-DE möchte bei aufgetretenen Fehlern oder Warnungen darüber informiert werden und leicht verständlich mögliche Handlungsoptionen angeboten bekommen, um passend auf Fehlersituationen reagieren zu können.

ID	Akzeptanzkriterium
10.1	Dem LE-DE MUSS primär eine menschlich verständliche Fehlermeldung angezeigt werden. Dazu MUSS auch eine Information enthalten sein, ob die initiale Fehlermeldung aus dem Land des EU-Bürgers oder Deutschland stammt.
10.2	Dem LE-DE MUSS immer der Kontakt zu Support angeboten werden, um Unterstützung bei der Lösung seines Problems mit dem EU-Szenario erhalten zu können.
10.3	Dem LE-DE MÜSSEN als weiterführende Information technische Details angeboten

	werden, die er auch dem Support als Detailinformation mitgeben kann.
10.4	Bei Auftreten einer Fehlersituation DARF es dem LE-DE NICHT möglich sein, den Workflow weiterzuführen.
10.5	Bei Anzeige einer Warnung MUSS es für den LE-DE möglich sein, den Workflow dennoch weiterzuführen.
10.6	Dem LE-DE MÜSSEN zur Fehlermeldung passende Handlungsmöglichkeiten angezeigt werden, um mit dem Fehler umgehen zu können.
10.7	Fehlersituationen, die in Deutschland erkannt werden, MÜSSEN mit einem deutschen Fehlertext gemeldet werden.
10.8	Fehlertexte aus dem Land A MÜSSEN unverändert oder um weitere Informationen ergänzt an den LE-DE weitergereicht werden.
10.9	Wenn bei der Rezeptsuche kein Rezept gefunden wurde, MUSS dem LE-DE wieder die Maske zur Identifikation des EU-Bürgers angezeigt werden. In der Maske MÜSSEN die zuvor eingegebenen Daten des EU-Bürgers vorausgefüllt sein.
10.10	Wenn bei der Rezeptsuche kein Rezept gefunden wurde, MUSS dem LE-DE ein Hinweis angezeigt werden, dass keine Rezepte gefunden wurden.

945

946

947

948

11. Ich als LE-DE möchte die Auflistung und den Abruf der einlösbaren Rezepte des EU-Bürgers jederzeit abbrechen können, um auf Wunsch des EU-Bürgers oder meinen Wunsch den Vorgang beenden zu können.

ID	Akzeptanzkriterium
11.1	Der LE-DE MUSS den Vorgang der Auflistung und des Abrufs einlösbarer Rezepte jederzeit abbrechen können.
11.2	Für den LE-DE MUSS klar erkennbar sein, wo er den Vorgang abbrechen kann.
11.3	Bei Abbruch des Vorgangs durch den LE-DE MÜSSEN (abgesehen von den verpflichtenden Audit-Trails) die Daten des EU-Bürgers in den beteiligten nationalen Systemen sicher gelöscht werden.
11.4	Wenn der LE-DE den Vorgang abbrechen möchte, MUSS ihm angezeigt werden, dass sämtliche Daten verloren gehen.
11.5	Dem LE-DE MUSS bei zeitlichem Ablauf der Bestätigung des Behandlungsverhältnisses (timeout) eine Fehlermeldung angezeigt werden. Des Weiteren ist dies wie ein Abbruch der Bestätigung des Behandlungsverhältnisses zu behandeln und das Behandlungsverhältnis MUSS zur Weiterführung des Workflows erneut bestätigt werden.

949

5.6 Schreiben der Dispensierinformation und Abgabe des oder der Medikamente an den EU-Bürger

In diesem Feature wird das Schreiben der Dispensierinformation und die Abgabe des oder der Medikamente an den EU-Bürger betrachtet.

Falls eine Substitution durch den verschreibenden LE im Land A nicht ausgeschlossen wurde, kann der LE-DE auf Basis der deutschen gesetzlichen Regelungen eine Substitution der Verordnung vornehmen.

Der LE-DE muss dann für alle Rezepte, die der EU-Bürger dispensiert haben möchte, eine Dispensierinformation an das Land A zurückschicken. Im Rahmen des Dispensiervorgangs muss außerdem das Medikament an den EU-Bürger übergeben und der Bezahlvorgang abgewickelt werden. Das Land A muss den LE-DE über den Erhalt der Dispensierinformation informieren. Bevor das Land A den Erhalt der Dispensierinformation nicht bestätigt hat, können die einlösbaren Rezepte des EU-Bürgers nicht erneut eingesehen werden. Der Prozess in der Apotheke endet dann, es sei denn, der EU-Bürger möchte weitere Rezepte einlösen oder hat weitere Fragen, die eine erneute Einsicht in die Informationen des EU-Bürgers erfordern.

Der LE-DE sollte den EU-Bürger über das Verschicken der Dispensierinformation an das Land A informieren.

Die Dispensierinformation sollte möglichst direkt bei Abschluss des Ausgabevorgangs an das Land A verschickt werden, um keine zeitliche Verzögerung der Informationsweitergabe zu haben und damit eingelöste Rezepte nicht erneut dispensiert werden können. Außerdem soll vermieden werden, dass bei einem Versenden der Dispensierinformation nach zeitlichem Ablauf der bestätigten Behandlungsbeziehung der gesamte Ablauf erneut durchgeführt werden muss. Je nach Bedingungen im Land A müsste der EU-Bürger dafür erneut involviert werden, ist aber in der Apotheke nicht mehr verfügbar.

Das Verschicken der Dispensierinformation ist erst möglich, sobald der komplette Dispensiervorgang inklusive Bezahlvorgang abgeschlossen ist, weil das Rezept danach als eingelöst gilt und die Dispensierinformation nicht mehr verändert werden kann.

Bei einer erforderlichen Bestellung des Medikaments muss die Dispensierinformation schon bei ebendieser Bestellung verschickt werden, weil das Rezept bei Abholung je nach Umsetzung im Land A nicht erneut abgerufen werden kann und je nach vergangener Zeitspanne zwischen Bestellung und Abholung das gesamte Anwendungsszenario erneut durchlaufen werden müsste.

5.6.1 Beschreibung der Anwenderdomäne

Nach dem Abruf der Rezeptdaten erfolgt die physische Abgabe der Medikamente sowie die digitale Dokumentation durch den LE-DE. Voraussetzung hierfür ist das Vorliegen der elektronischen Identität des LE-DE sowie die elektronische Bestätigung des Behandlungsverhältnisses.

Der Ablauf beginnt damit, dass der LE-DE ein oder mehrere einlösbare Rezepte festlegt (1). In einem optionalen Zwischenschritt kann der LE-DE das Rezept auf eine Kennzeichnung des Substitutionsverbots prüfen (2). Sofern diese Kennzeichnung nicht vorhanden ist, kann der LE-DE auf gesetzlicher Basis eine Substitution vornehmen. Findet eine Substitution statt, wird diese in der Dispensierinformation dokumentiert.

Anschließend ergänzt der LE-DE für jedes dispensierte Rezept die Dispensierinformation (3). Dieser Vorgang geschieht verkaufsbegleitend. In der Dispensierliste werden die Dispensierinformationen der zu dispensierenden Rezepte gebündelt. Sobald die Liste vollständig ist, übernimmt das ePeD-B System die Dispensierliste für die Weiterverarbeitung (4).

Der Ablauf sieht zudem ein Verfahren bei Fehlern vor: Das ePeD-B System kann einen Dispensierinformationsfehler erzeugen (5). Diesem Fehler werden Handlungsoptionen für das Fehlerbild hinzugefügt. Über diese Optionen wird der LE-DE informiert, um entsprechende Maßnahmen einzuleiten.

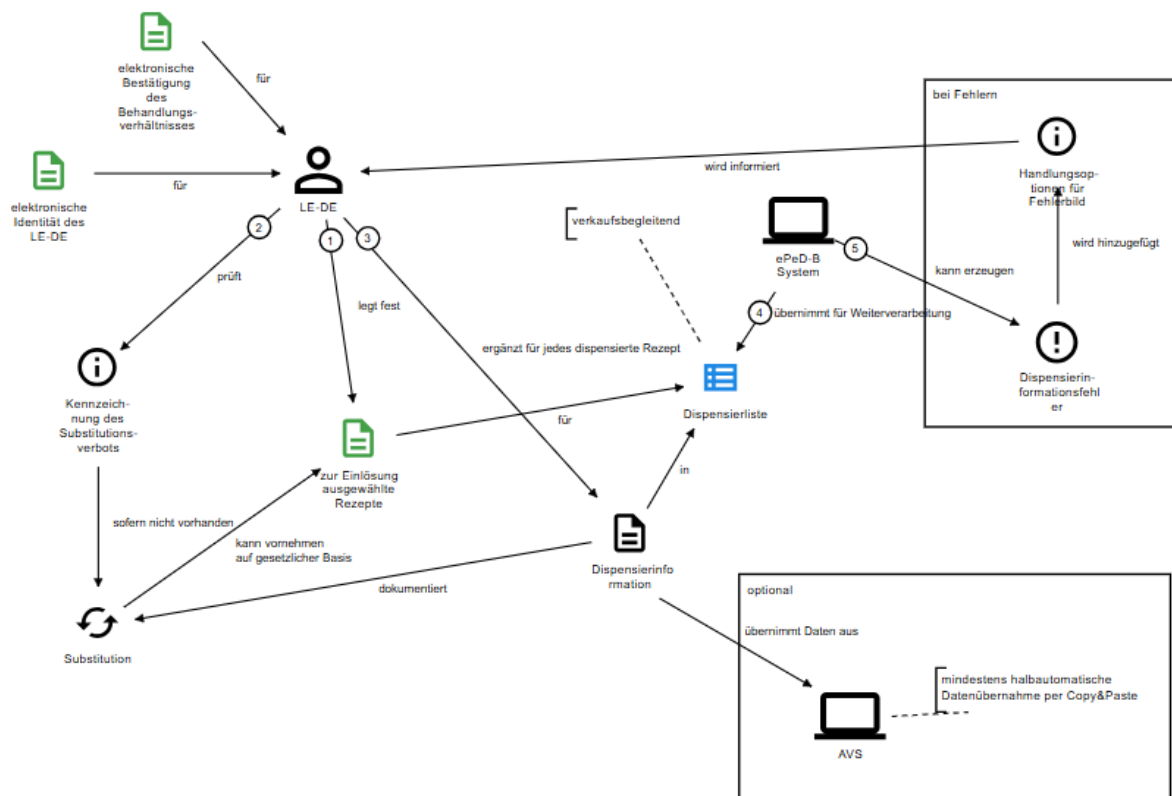


Abbildung 9: Schreiben der Dispensierinformation

5.6.2 User Stories

In den folgenden User Stories werden nur die technischen Vorgänge des Schreibens und Verschickens der Dispensierinformation betrachtet, auch wenn der Vorgang zusätzlich die Ausgabe und die Bezahlung des ausgegebenen Medikaments beinhaltet.

1. Als LE-DE möchte ich die Rezepte, die der EU-Bürger dispensiert haben möchte, auswählen und gebündelt dispensieren können, um effizient arbeiten zu können.

ID	Akzeptanzkriterium
----	--------------------

1.1	Es DÜRFEN NUR Rezepte dispensiert werden können, die vorher abgerufen worden sind.
1.2	Jedes einlösbare Rezept MUSS klar erkennbar zur Dispensierung auswählbar sein.
1.3	Es MUSS möglich sein, mehrere Rezepte gemeinsam (in einem Vorgang) zu dispensieren.
1.4	Der LE-DE MUSS vor Absenden der Dispensierinformation jederzeit entscheiden können, welche Rezepte dispensiert werden sollen.

1014

1015

1016

1017

2. Als LE-DE möchte ich auf Basis eines Rezepts und den in Deutschland gesetzlich erlaubten Substitutionsmöglichkeiten ein verfügbares Produkt dispensieren können, um eine möglichst umfassende Arzneimittelversorgung sicherzustellen.

ID	Akzeptanzkriterium
2.1	Bei Substitution MUSS auf der Dispensierinformation klar erkennbar sein, dass substituiert wurde und mit welchem Produkt substituiert wurde.

1018

1019

1020

1021

3. Als LE-DE möchte ich nach dem Abruf von Rezepten verstehen können, dass ich in einem weiteren Schritt des EU-Workflows die Dispensierinformation an das Land A verschicken muss, um den EU-Workflow korrekt durchzuführen.

ID	Akzeptanzkriterium
3.1	Der LE-DE MUSS eine allgemeine Beschreibung des Gesamt-Ablaufs einsehen können, um besser zu verstehen, wie sich die Dispensierung ausgewählter Rezepte des EU-Bürgers in den Vorgang ePrescription/eDispensation einordnet.
3.2	Der LE-DE MUSS eine allgemeine Beschreibung zur Dispensierung ausgewählter Rezepte des EU-Bürgers einsehen können, um besser zu verstehen, welche Aktivitäten der Vorgang umfasst.
3.3	Es MUSS eine eindeutig erkennbare Handlungsvorgabe für den LE-DE geben, dass im nächsten Schritt noch eine Dispensierinformation an das Land A gesendet werden muss.
3.4	Der LE-DE MUSS eine Warnung angezeigt bekommen, wenn er den Vorgang ohne Senden der Dispensierinformation beenden will und MUSS im Bedarfsfall zum offenen Vorgang zurückkehren können.
3.5	Dem LE-DE MUSS angezeigt werden, dass bei einer eventuellen Bestellung von Medikamenten trotzdem ein Verschicken der Dispensierinformation an das Land A durchzuführen ist.

1022

1023

1024

4. Als Verarbeiter von Dispensierinformationen im EU-Mitgliedsland möchte ich darüber informiert werden, dass Rezepte eines Bürgers meines Landes eingelöst wurden, um den

1025 Medikationsprozess des Bürgers nach eigenem Landesbedarf korrekt dokumentieren zu
1026 können.

ID	Akzeptanzkriterium
4.1	Die an das Land A zurückgesendete Dispensierinformation MUSS folgende Daten enthalten: <ul style="list-style-type: none"> • EU-Bürger: Patient Identifier, Vor- und Nachname • LE-DE: Identifier, Vor- und Nachname • Dispensiertes Medikament: Dispensierinformations-ID, Rezept-ID, ID des Medikaments auf dem Rezept, Markenname, Wirkstoff, Darreichungsform, Wirkstärke, Packungsmenge, Packungsgröße • Dispensierungsdaten: Datum der Dispensierung, Angabe dass substituiert wurde (im Falle dass substituiert wurde)
4.2	Die an das Land A zurückgesendete Dispensierinformation SOLLTE folgende Daten enthalten (wenn diese Daten nicht angegeben werden können, MUSS eine Begründung angegeben werden) <ul style="list-style-type: none"> • LEI-DE: ID, Name, vollständige Adresse (Straße, Hausnummer, Stadt, PLZ, Bundesland, Land) • Dispensiertes Medikament: Packungstyp
4.3	Die an das Land A zurückgesendete Dispensierinformation KANN außerdem Dosierungsanweisungen enthalten, falls der LE-DE die Angabe dieser für erforderlich hält.
4.3	Die Dispensierdaten, die nicht die konkret abzugebenden Medikamente betreffen (z.B. Rezept-ID, Angaben zu EU-Bürger, LE-DE und LEI-DE) SOLLEN vorausgefüllt angeboten werden.
4.4	Die Dispensierdaten SOLLEN zeitlich direkt bei Abschluss der Dispensierung gesendet werden.
4.5	Der Dispensiervorgang MUSS innerhalb des zeitlich gültigen Behandlungsverhältnisses durchgeführt werden oder das Behandlungsverhältnis MUSS bei ausstehenden Dispensierinformationen erneuert bzw. verlängert werden.
4.6	Bei Notwendigkeit der Bestellung eines Medikaments MUSS die Dispensierinformation schon bei ebendieser übermittelt werden und nicht erst bei Abholung.
4.7	Das Verschicken der Dispensierinformation DARF technisch NUR möglich sein, wenn der Abgabevorgang abgeschlossen wurde oder das Medikament bestellt und bezahlt wurde.

1027

1028 5. Als LE-DE möchte ich erkennen können, dass der Dispensiervorgang abgeschlossen
1029 ist, um sicher zu verstehen, dass ich alle Schritte korrekt befolgt habe.

ID	Akzeptanzkriterium
5.1	Es MUSS eine eindeutig verständliche Information angezeigt werden, die bestätigt, dass der Dispensiervorgang abgeschlossen ist.

1030

1031

1032

6. Als EU-Bürger möchte ich weitere Rezepte einlösen können, um eine umfassende Betreuung in der Apotheke zu erhalten.

ID	Akzeptanzkriterium
6.1	Die Option der weiteren Dispensierung von Rezepten des EU-Bürgers MUSS dem LE-DE eindeutig verständlich angezeigt werden.
6.2	Die Dispensierinformation der schon dispensierten Rezepte MUSS verschickt worden sein, bevor weitere Rezepte eingelöst werden können.
6.3	Wenn die Auswahl für die Einlösung weiterer Rezepte gerufen wurde, MUSS die Rezeptliste auf Basis einer erneuten Suche angezeigt werden.

1033

1034

1035

1036

7. Ich als LE-DE möchte bei aufgetretenen Dispensierfehlern oder Warnungen darüber informiert werden und leicht verständlich mögliche Handlungsoptionen angeboten bekommen, um passend auf Fehlersituationen reagieren zu können.

ID	Akzeptanzkriterium
7.1	Dem LE-DE MUSS primär eine menschlich verständliche Fehlermeldung angezeigt werden. Dazu MUSS auch eine Information enthalten sein, ob die initiale Fehlermeldung aus dem Land des EU-Bürgers oder Deutschland stammt.
7.2	Dem LE-DE MUSS immer der Kontakt zu Support angeboten werden, um Unterstützung bei der Lösung seines Problems mit dem EU-Szenario erhalten zu können.
7.3	Dem LE-DE MÜSSEN als weiterführende Information technische Details angeboten werden, die er auch dem Support als Detailinformation mitgeben kann.
7.4	Bei Anzeige einer Warnung MUSS es für den LE-DE möglich sein, den Workflow dennoch weiterzuführen.
7.5	Dem LE-DE MÜSSEN zur Fehlermeldung passende Handlungsmöglichkeiten angezeigt werden, um mit dem Fehler umgehen zu können.
7.6	Fehlersituationen, die in Deutschland erkannt werden, MÜSSEN mit einem deutschen Fehlertext gemeldet werden.
7.7	Fehlertexte aus dem Land A MÜSSEN unverändert oder um weitere Informationen ergänzt an den LE-DE weitergereicht werden.

7.8	Der LE-DE MUSS bei aufgetretenen Dispensierfehlern umgehend darüber informiert werden.
7.9	Der Dispensiervorgang DARF NICHT abgeschlossen werden können, bevor Dispensierfehler zurückgemeldet werden konnten und korrigiert worden sind.
7.10	Jede auf dem Verarbeitungsweg der Dispensierinformation befindliche Stelle muss die davorliegenden Stellen über aufgefallene Fehlersituationen informieren.

1037

1038 8. Ich als LE-DE möchte die Dispensierung ausgewählter Rezepte des EU-Bürgers
 1039 jederzeit abbrechen können, um auf Wunsch des EU-Bürgers oder meinen Wunsch den
 1040 Vorgang beenden zu können.

ID	Akzeptanzkriterium
8.1	Der LE-DE MUSS den Vorgang der Dispensierung ausgewählter Rezepte jederzeit abbrechen können.
8.2	Für den LE-DE MUSS klar erkennbar sein, wo er den Vorgang abbrechen kann.
8.3	Bei Abbruch des Vorgangs durch den LE-DE MÜSSEN (abgesehen von den verpflichtenden Audit-Trails) die Daten des EU-Bürgers in den beteiligten nationalen Systemen sicher gelöscht werden.
8.4	Wenn der LE-DE den Vorgang abbrechen möchte, muss ihm angezeigt werden, dass sämtliche Daten verloren gehen.
8.5	Dem LE-DE MUSS bei zeitlichem Ablauf der Bestätigung des Behandlungsverhältnisses (timeout) eine Fehlermeldung angezeigt werden. Des Weiteren ist dies wie ein Abbruch der Bestätigung des Behandlungsverhältnisses zu behandeln und das Behandlungsverhältnis MUSS zur Weiterführung des Workflows erneut bestätigt werden.

1041

1042 5.7 Nachvollziehbarkeit und Auskunftsansprüche der 1043 Datenverarbeitung

1044 Authentisierte und autorisierte Leistungserbringer in Deutschland (LE-DE) können
 1045 jederzeit eine Anfrage zur Bereitstellung von E-Rezepten eines EU-Bürgers stellen.

1046 Im Streitfall, z.B. wegen einer möglichen Fehlbehandlung, möchte der LE-DE und der EU-
 1047 Bürger in der Lage sein, die Audit Trails Logs aller Nachrichten anhand eines
 1048 angeforderten Datensatzes zu erhalten. Um dies zu ermöglichen, geht aus den Audit Trail
 1049 Logs hervor, wer wann auf welche Daten zugegriffen hat.

1050 Die Inhalte der Audit Trail Logs sind im [eHDSI_Audit_Trail_Profile] vorgegeben.

5.7.1 User Stories

1. Als LE-DE möchte ich, dass alle von mir durchgeführten Zugriffe und Zugriffsversuche auf Rezepte eines EU-Bürgers protokolliert werden, damit diese nachvollzogen werden können und ich mich ggf. gegen falsche Beschuldigungen verteidigen kann.

ID	Akzeptanzkriterium
1.1	Es MÜSSEN Protokoll- und Audittraileinträge für das Feature "Authentisierung und Autorisierung des LE-DE" geschrieben werden.
1.2	Es MÜSSEN Protokoll- und Audittraileinträge für das Feature "Identifikation des EU-Bürgers" geschrieben werden.
1.3	Es MÜSSEN Protokoll- und Audittraileinträge für das Feature "Bestätigung des Behandlungsverhältnisses zum EU-Bürger" geschrieben werden.
1.4	Es MÜSSEN Protokoll- und Audittraileinträge für das Feature "Einlösbare Rezepte des EU-Bürgers auflisten und abrufen" geschrieben werden.
1.5	Es MÜSSEN Protokoll- und Audittraileinträge für das Feature "Ausgewählte Rezepte dispensieren" geschrieben werden.
1.6	Es MÜSSEN Protokoll- und Audittraileinträge bei Erfolg als auch bei Fehlern von Features geschrieben werden.
1.7	Die Audit Trail Logs MÜSSEN mindestens 3 Jahre nach Zugriff oder Zugriffsversuch abrufbar sein.

2. Als LE-DE möchte ich sicher sein, dass Audit Trail Einträge zu mich betreffenden Vorgängen sicher und unverfälscht gespeichert werden, um eine zuverlässige Auditierung der mich betreffenden Aktivitäten und Daten erhalten zu können.

ID	Akzeptanzkriterium
2.1	Es MUSS sichergestellt werden, dass Audit Trail Logs erst nach Ablauf der Aufbewahrungsfrist gelöscht werden dürfen.
2.2	Es MUSS sichergestellt werden, dass Audit Trail Logs nicht verändert werden können.
2.3	Nur berechnigte Personen DÜRFEN Einsicht in Audit Trail Einträge bekommen.

3. Als nationale Verbindungsstelle möchte ich Daten zur Nachverfolgbarkeit, die entsprechend über eine Schnittstelle abrufbar sein müssen, zur Verfügung stellen können, um berechnigte Auskunftsinteressen bedienen zu können.

ID	Akzeptanzkriterium
----	--------------------

3.1	Der LE-DE MUSS den Datenfluss seiner Daten nachverfolgen können.
-----	--

4. Als nationale Verbindungsstelle möchte ich eine Anfrage auf Einsicht in die Audit Trails auf Legitimität prüfen können, um sicherzustellen, dass nur zugriffsberechtigte Personen Einblick in ihre Audit Trail Einträge erhalten.

ID	Akzeptanzkriterium
4.1	Die nationale Verbindungsstelle MUSS sicherstellen, dass nur zugriffsberechtigte Personen und Institutionen Zugriff auf die jeweiligen Audit Trail Einträge haben.
4.2	Autorisierte Personen MÜSSEN einen berechtigten Grund zur Einsichtnahme haben.

5.8 Performance und Betrieb

Um einen geordneten Betriebsablauf herzustellen, benötigen die Anbieter des Land-B-Systems, die gematik als gesamtverantwortlicher Betreiber der TI sowie die eHDSI Informationen zur Nutzung und Qualität der eingesetzten Komponenten. Diese setzen sich aus zu definierenden Rohdaten und Use-Case-bezogenen Informationen zusammen. Mithilfe dieser Informationen ist es möglich, den aktuellen Stand der Nutzung der Anwendung nachzuvollziehen sowie bei auftretenden Störungen schnell und gezielt reagieren und eine umgehende Fehlerbehebung vorantreiben zu können.

Im Rahmen der Anwendung ePrescription/eDispensation Land B ist außerdem eine aktuelle und korrekt übersetzte International Search Mask (ISM) von entscheidender Bedeutung, um das Land des EU-Bürgers auszuwählen und die relevanten personenbezogenen Daten zur Identifikation eingeben zu können.

5.8.1 User Stories

1a. Als EU-Bürger möchte ich jederzeit (24 Stunden am Tag, 7 Tage die Woche) bedarfsgerecht und zeitnah Rezepte einlösen können, damit eine bestmögliche Versorgungsqualität gewährleistet ist.

1b. Als LE-DE möchte ich jederzeit (24 Stunden am Tag, 7 Tage die Woche) bedarfsgerecht und zeitnah Rezepte eines EU-Bürgers bearbeiten können, damit eine bestmögliche Versorgungsqualität gewährleistet ist.

ID	Akzeptanzkriterium
1.1	Die Gesamtverfügbarkeit der Anwendung ePrescription/eDispensation Land B MUSS innerhalb der Hauptzeit bei 99,90 % liegen.
1.2	Die Gesamtverfügbarkeit der Anwendung ePrescription/eDispensation Land B MUSS innerhalb der Nebenzeit bei 99,70% liegen. Das System MUSS auf

	unterschiedliche Systemlast reagieren.
1.3	Genehmigte Wartungsfenster DÜRFEN NICHT negativ in die Verfügbarkeitsberechnung einzählen.
1.4	Die Haupt- und Nebenzeiten MÜSSEN wie folgt umgesetzt werden: Montag bis Freitag: 6:00 Uhr - 22:00 Uhr Samstag und Sonntag: 6:00 Uhr - 20:00 Uhr Alle übrigen Stunden der Woche sind Nebenzeit Bundeseinheitliche Feiertage werden wie Sonntage behandelt, alle übrigen Feiertage werden wie normale Werktage behandelt.

1089

1090

1091

1092

2. Als EU-Bürger und LE-DE möchte ich, dass bei der Bereitstellung der Rezepte möglichst geringe Wartezeiten entstehen, damit mehr Zeit für die sichere Identifizierung der Arzneimittel und Beratung zur Verfügung steht.

ID	Akzeptanzkriterium
2.1	Die Systemreaktion der Anwendung ePrescription/eDispensation nach der Anfrage in Deutschland SOLL innerhalb von 5 Sekunden und MUSS innerhalb von 15 Sekunden beantwortet werden.
2.2	Bei Antwortzeiten länger als 10 Sekunden von NCPeH Land A MUSS ein automatischer Time-Out generiert werden.
2.3	Timeouts MÜSSEN konfigurierbar sein.

1093

1094

1095

1096

3. Als LE-DE möchte ich, dass ein Service Desk für mich erreichbar ist, damit ich mich bei technischen Problemen während der Behandlung eines EU-Bürgers an einen zentralen Ansprechpartner wenden kann.

ID	Akzeptanzkriterium
3.1	Der LE-DE MUSS Zugriff auf die Kontaktinformationen des Service Desk haben und diesen kontaktieren können.
3.2	Der Service Desk MUSS die Anforderungen an einen „Country Service Desk“ gemäß [eHDSI_Operations_Framework] erfüllen.
3.3	Der Service Desk MUSS Anfragen zur Rolle Land-B abdecken und bedarfsweise mit den Betreibern der verschiedenen beteiligten Komponenten Kontakt aufnehmen können.

1097

1098

1099

1100

1101

4. Als Anbieter des Land-B-Systems möchte ich mir und der gematik ein Monitoring zu Verfügbarkeit, Auslastung und Sicherheitslage anbieten, damit sichergestellt werden kann, dass eine gleichbleibende Servicequalität im operativen Betrieb vorliegt und wir falls notwendig auf Veränderungen reagieren können.

ID	Akzeptanzkriterium
4.1	Die Verfügbarkeit und Auslastung der nationalen Produkte für die Anwendung ePrescription/eDispensation Land B MUSS in 5-minütigen Intervallen nachvollziehbar sein.
4.2	Fehlersituationen und sicherheitsrelevante Zustandsänderungen MÜSSEN basierend auf einem 5-minütigem Reportingintervall zeitnah erkannt werden.
4.3	Fehlersituationen und sicherheitsrelevante Zustandsänderungen DÜRFEN HÖCHSTENS pseudonymisierte Informationen von EU-Bürgern enthalten.

1102

1103

1104

1105

5. Als eHDSI Solution-Provider und gematik möchte ich regelmäßig über definierte Key Performance Indicators (KPI) informiert werden, um den Zustand und die Nutzung des Systems nachvollziehen und die Servicequalität optimieren zu können.

ID	Akzeptanzkriterium
5.1	Die Aufzeichnung und Übermittlung der KPIs MÜSSEN die Anforderungen gemäß [MyHealth@EU_Monitoring_Framework] erfüllen.
5.2	Die an den eHDSI Solution Provider übermittelten Daten MÜSSEN innerhalb von einer Woche mit der gematik geteilt werden.

1106

1107

1108

1109

6. Als Anbieter des Land-B-Systems möchte ich den LE-DE eine stets aktuelle International Search Mask (ISM) zur Länderauswahl bereitstellen, damit der LE-DE seine Aufgaben bestmöglich wahrnehmen kann.

ID	Akzeptanzkriterium
6.1	Der Anbieter des Land-B-Systems MUSS bei Bereitstellung einer neuen ISM durch ein Land A zeitnah den Client-Systemen eine aktualisierte ISM bereitstellen (sowohl bei Live-Gang mit einem Land A als auch bei Aktualisierung einer ISM).

1110

1111

1112

1113

7. Als Anbieter des Land-B-Systems möchte ich den LE-DE eine in die deutsche Sprache übersetzte ISM bereitstellen, damit der LE-DE seine Aufgaben bestmöglich wahrnehmen kann.

ID	Akzeptanzkriterium
7.1	Sämtliche Datenfelderbeschreibungen MÜSSEN auf Deutsch übersetzt bereitgestellt werden.
7.2	Zusätzlich MUSS die Datenfeldbeschreibung auf Englisch angezeigt werden, um die Kommunikation mit dem EU-Bürger zu erleichtern.
7.3	Zusätzlich MUSS ein Hilfetext verfügbar sein, in dem die Datenfeldbeschreibung in Deutsch und in der jeweiligen Landessprache angezeigt wird, um die Kommunikation

mit dem EU-Bürger zu erleichtern.

1114

1115 8. Als Anbieter des Land-B-Systems möchte ich genau die Länder für den
 1116 Datenaustausch konfigurieren und zur Nutzung anbieten, mit denen dieser vereinbart
 1117 wurde, damit der LE-DE nur mit EU-Bürgern von tatsächlich nutzbaren EU-
 1118 Mitgliedsländern den EU-Workflow starten kann.

ID	Akzeptanzkriterium
8.1	Sobald der Service mit einem neuen EU-Land live ist, MUSS der EU-Workflow für dieses Land auswählbar sein.
8.2	Länder, mit denen der Service noch nicht live ist, DÜRFEN NICHT für den EU-Workflow auswählbar sein.
8.3	Länder, zu denen nach offizieller Nicht-Verfügbarkeitsmeldung die Kommunikation über längere Zeit unterbrochen wird, DÜRFEN für diese Zeit NICHT für den EU-Workflow auswählbar sein.
8.4	Falls ein Service eines EU-Landes geplant nicht verfügbar sein wird, MUSS der Administrator rechtzeitig darüber informiert werden und entscheiden, ob der Service für dieses EU-Land zum entsprechenden Zeitpunkt deaktiviert werden soll.

1119

1120 9. Als nationale Verbindungsstelle möchte ich meine relevanten Servicedaten auf dem
 1121 zentralen Dienst der EU bekanntmachen, damit die Anfragen als Land B von anderen
 1122 Ländern akzeptiert und verarbeitet werden.

ID	Akzeptanzkriterium
9.1	Die nationale Verbindungsstelle MUSS sicherstellen, dass die aktuellen Service Metadaten für Deutschland auf dem eHDSI Configuration Service abrufbar sind.
9.2	Jede Aktualisierung der Service Metadaten MUSS im Security Audit Trail protokolliert werden.

1123

1124 10. Als Anbieter des Land-B-Systems möchte ich die Aktualität von Mappingdaten (MVC,
 1125 MTC, PZN-Tabelle) sicherstellen, damit Übersetzungen medizinischer Daten für die
 1126 Versorgung in der Apotheke stets auf dem aktuellsten Stand sind.

ID	Akzeptanzkriterium
10.1	Jede Aktualisierung von Mappingdaten MUSS im Security Audit Trail protokolliert werden.
10.2	Der Anbieter des Land-B-Systems MUSS sicherstellen, dass die aktuellen MVC, MTC und weitere nationale Mappingdaten für die Transformation und Transcodierung von Daten der EU-Bürger und der LE-DE zur Verfügung stehen.

1127

- 1128 11. Als Anbieter des Land-B-Systems möchte ich Fehler im laufenden System erkennen,
 1129 analysieren und nachvollziehen können, um Fehler in funktionalen und nicht-funktionalen
 1130 Aspekten korrigieren und eine hohe Qualität in der Bereitstellung der Funktionalität
 1131 sicherstellen zu können.
 1132 Hinweis: Es handelt sich hierbei nicht um die in Kapitel 5.7 beschriebenen Audit Trails,
 1133 sondern um Protokollierung.

ID	Akzeptanzkriterium
11.1	Es MUSS beim Anbieter eines Produktes ein Fehlerprotokoll verfügbar sein, dass die Analyse aufgetretener funktionaler Fehler ermöglicht.
11.2	Es MUSS beim Anbieter eines Produktes ein Fehlerprotokoll verfügbar sein, dass die Analyse aufgetretener Fehler bzgl. Stabilität und Performanz ermöglicht.
11.3	Die Protokolle zu Fehlern in der Verarbeitung der Daten eines EU-Bürgers MÜSSEN für die nationale Verbindungsstelle einsehbar sein.
11.4	Die Protokolle zu Fehlern in der Verarbeitung der Daten eines EU-Bürgers MÜSSEN für das BfArM einsehbar sein.

- 1134
 1135 12. Als EU-Bürger und LE-DE möchte ich sicher sein, dass meine personenbezogenen
 1136 Daten in den betrieblichen Protokolldaten bestmöglich geschützt sind, damit keine
 1137 unberechtigte Person Rückschlüsse auf meine Person und damit verbundene
 1138 Gesundheitsdaten ziehen kann.

ID	Akzeptanzkriterium
12.1	Personenbezogene Daten in den Protokolldaten MÜSSEN pseudonymisiert sein.

- 1139
 1140 13. Als Anbieter des Land-B-Systems möchte ich die Pflege der Systemkonfiguration
 1141 sicher gestalten, um fehlerhafte oder unzulässige Änderungen der Systemkonfiguration
 1142 vorzubeugen bzw. durchgeführte Änderungen nachvollziehen zu können.

ID	Akzeptanzkriterium
13.1	Änderungen an der Systemkonfiguration MÜSSEN von Administratoren im Vier-Augen-Prinzip durchgeführt werden.
13.2	Sicherheitsrelevante Änderungen an der Systemkonfiguration am NCPeH-FD MÜSSEN im Security Audit Trail des NCPeH-FD protokolliert werden.
13.3	Änderungen an der Systemkonfiguration MÜSSEN in der eigenen Betriebsumgebung protokolliert werden.

6 Einordnung in die Telematikinfrastruktur

1143

1144 Das Anwendungsszenario ePrescription/eDispensation Land B (ePeD-B) ermöglicht es,
1145 dass berechnigte Leistungserbringer in Deutschland (LE-DE) E-Rezepte von EU-Bürgern
1146 aus anderen EU-Mitgliedstaaten abrufen und dispensieren können.

1147 Die Systemübersicht in der folgenden Abbildung gibt für das Anwendungsszenario ePeD-
1148 B einen Überblick über die beteiligten TI-Systeme und externen Systeme sowie über die
1149 sichere Kommunikation zwischen ihnen:

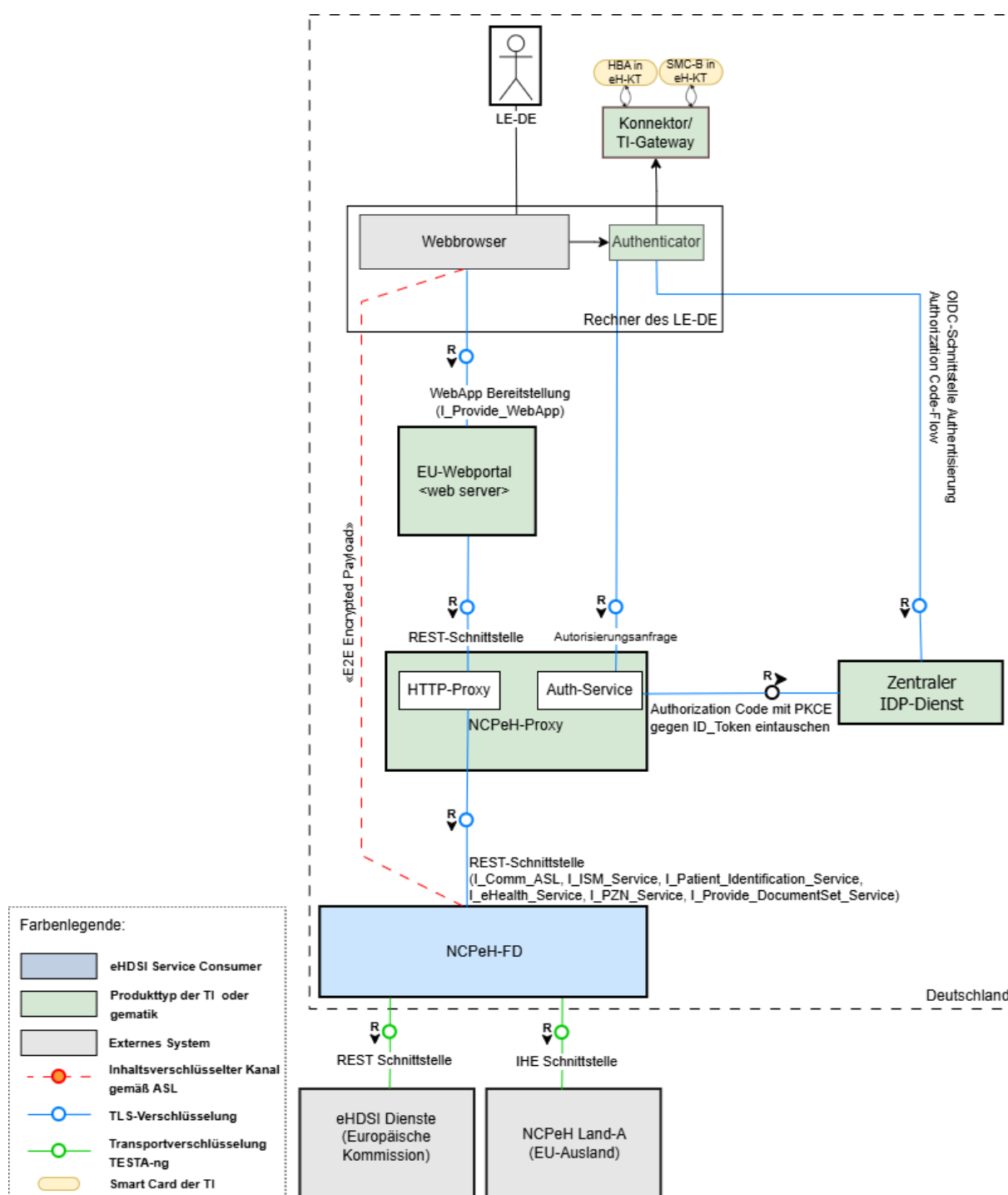


Abbildung 10: Systemübersicht des Anwendungsszenarios ePrescription/eDispensation Land B

Der LE-DE verwendet seinen lokalen Rechner mit installiertem Webbrowser, um das aus dem Internet erreichbare EU-Webportal aufzurufen und die Funktionen des ePeD-B Szenarios zu nutzen. Es bietet eine graphische Oberfläche und ermöglicht die Interaktion mit dem Anwendungsszenario ePeD-B. Perspektivisch kann das ePeD-B Szenario direkt

1159 über das AVS des LE-DE bedienbar sein, wodurch die direkte Integration der
1160 Funktionalitäten in bestehende Systeme ermöglicht wird.

1161 Der gematik-Authenticator ist auf dem Rechner des LE-DE installiert und konfiguriert und
1162 ermöglicht mittels des Konnektors oder TI-Gateway den Zugriff auf Smartcards der TI,
1163 insbesondere HBA und SMC-B, um die Authentisierung und Identitätsprüfung
1164 vorzunehmen. Die Anforderung einer starken Authentisierung und die Verwendung
1165 sowohl persönlicher als auch institutioneller Identitätsinformationen stammen aus den
1166 Vorgaben der eHDSI. Die Authentisierung erfolgt über die OIDC-Schnittstelle des
1167 zentralen IDP-Dienstes der TI und nutzt den Authorization Code Flow.

1168 Der NCPeH-Proxy ist ein neuer Produkttyp der TI und übernimmt die zentrale Rolle als
1169 Authorization Server für den Zugriff auf den grenzüberschreitenden eHealth-Dienst ePeD-
1170 B. Er verarbeitet die vom IDP-Dienst bestätigten TI-Identitäten, prüft und erteilt im
1171 Erfolgsfall eine Zugriffsberechtigung auf den Dienst ePeD-B für den anfragenden LE-DE.

1172 Nach erfolgreicher Authentisierung und damit Anmeldung am EU-Webportal kann der LE-
1173 DE die demographischen Daten und E-Rezepte des EU-Bürgers abrufen. Das EU-
1174 Webportal sendet die fachlichen Anfragen des LE-DE an den NCPeH-Proxy, der die
1175 Anfragen an den NCPeH-FD weiterleitet. Der NCPeH-FD agiert dabei als eHDSI Service
1176 Consumer, baut die Vertrauensbeziehung zum NCPeH Land A auf und transkodiert dabei
1177 die E-Rezepte nach den Vorgaben der BfArM in die deutsche Sprache.

1178 Die E-Rezepte werden auf dem EU-Webportal angezeigt. Im Rahmen der Abgabe von
1179 Arzneimitteln an EU-Bürger erfasst der LE-DE die Dispensierinformationen, die über den
1180 NCPeH-Proxy und NCPeH-FD an den NCPeH Land-A übermittelt werden. Der NCPeH-FD
1181 implementiert die semantischen Anforderungen der eHDSI und transkodiert die
1182 Dispensierinformationen gemäß den Vorgaben des BfArM in das entsprechende eHDSI
1183 eDispensation Pivotformat.

1184

1185 **6.1 Entscheidung für die Integration von ePeD-B in die** 1186 **Telematikinfrastruktur 1.0**

1187 Die Entscheidung, das Anwendungsszenario ePeD-B in die Telematikinfrastruktur 1.0 (TI
1188 1.0) zu integrieren, basiert auf mehreren technischen und regulatorischen
1189 Rahmenbedingungen. Eine Integration in die Telematikinfrastruktur 2.0 (TI 2.0) ist
1190 derzeit nicht umsetzbar, da zentrale Voraussetzungen für die Nutzung der TI 2.0 fehlen
1191 und die termingerechte Bereitstellung des Szenarios ePeD-B gefährden würden.

1192 Die wesentlichen Gründe umfassen das Fehlen klar definierter Anforderungen zur
1193 Integration von ZETA Client in das EU-Webportal sowie die fehlende Absicherung durch
1194 ZETA Guard im NCPeH-Proxy. Diese Lücken machen eine zuverlässige Nutzung dieser TI
1195 2.0 Leistungsmerkmale in diesem Kontext bis auf weiteres unmöglich. Hinzu kommt,
1196 dass derzeit keine hardware-unabhängigen digitalen Identitäten für LE-DE, weder zentral
1197 (z.B. als sektoraler IDP für LE) noch dezentral (z.B. Wallet-Lösungen) zur Verfügung
1198 stehen.

1199 Dies schränkt die Nutzung des Anwendungsszenarios ePeD-B im TI 2.0-Kontext ein und
1200 macht den Einsatz der Smartcard-basierten TI-Identitäten, wie HBA und SMC-B, in
1201 Kombination mit Konnektoren, erforderlich. Das Thema der Nutzung von digitalen
1202 Identitäten für LE-DE befindet sich aktuell in einer strategischen Abstimmung mit den
1203 Gesellschaftern, sodass derzeit keine projizierte Bereitstellung von hardware-
1204 unabhängigen digitalen Identitäten bekannt ist.

Ein weiterer entscheidender Faktor ist die zeitliche Verzögerung, die durch die verspätete Integration der genannten Leistungsmerkmale der TI 2.0 entstehen würde. Diese Verzögerung würde den geplanten Go-Live des Anwendungsszenarios ePeD-B gefährden und damit die Einhaltung der Frist für die Inbetriebnahme der grenzüberschreitenden eHealth-Dienste gemäß EHDS-Verordnung unmöglich machen. Gemäß der EHDS-Verordnung müssen alle EU-Mitgliedstaaten spätestens bis 26.03.2029 mit den relevanten grenzüberschreitenden eHealth-Diensten der ersten prioritären Kategorien einschließlich ePeD-B produktiv verfügbar sein.

Aufgrund dieser Einschränkungen muss das Anwendungsszenario ePeD-B zunächst auf Basis einer Integration in die Telematikinfrastruktur 1.0 umgesetzt werden. Diese Entscheidung stellt sicher, dass die Anforderungen an die sichere Authentisierung und Kommunikation erfüllt werden können und der Go-Live des Szenarios innerhalb der vorgegebenen Frist erfolgt.

6.2 Ausblick

Im Rahmen der zukünftigen Weiterentwicklung des Anwendungsszenarios ePrescription/eDispensation Land B werden Maßnahmen vorgesehen, die eine Erweiterung der Funktionalitäten sowie eine Optimierung der bestehenden Prozesse ermöglichen sollen. Diese Maßnahmen zielen darauf ab, die Integration in die TI 2.0 zu ermöglichen, die User Experience zu steigern und die Sicherheit der Systeme weiter zu erhöhen. Im Folgenden werden zentrale Themen und potenzielle Features beschrieben, die in späteren Ausbaustufen umgesetzt werden könnten:

- Umzug in die TI 2.0 mit Integration des ZETA Clients in das EU-Webportal, Absicherung durch ZETA Guard sowie Nutzung der Zero Trust Architektur: Die Integration von ZETA Client und die Client-Attestierung in Webportalen ist für frühestens 2027 geplant. Die Implementierung dieser Funktion für Land B Anwendungsszenarien soll den Zugriff auf den NCPeH-Proxy durch die Einführung von ZETA Guard sichern. Diese Sicherheitslösung gewährleistet einen robusten und zuverlässigen Schutz der Schnittstellen und schützt sensible Daten vor unbefugtem Zugriff.
- Integration des Anwendungsszenarios ePeD-B in das AVS: Die direkte Integration von ePeD-B in das AVS soll die nahtlose Aufnahme europäischer E-Rezepte und die Erstellung von Dispensierinformationen ermöglichen, sowie die leichtere Nutzung des Warenwirtschaftssystems. Dazu gehört auch die Definition und Verarbeitung von Datenformaten für E-Rezepte und Dispensierinformationen.
- Einsatz der Wallet-Lösung für Identity Management: Um alternative Authentisierungsmöglichkeiten für Leistungserbringer und ihre Gehilfen zu schaffen, wird die Integration von Wallet-Lösungen in Betracht gezogen. Die Einführung der Wallet-Lösung kann die Akzeptanz und Nutzbarkeit der Land-B Anwendungsszenarien erheblich steigern, gleichzeitig die Diversität der Authentisierungsoptionen erweitern und die Abhängigkeit zu Konnektoren lösen.

1247

7 Fachliches Konzept

1248

Der Ablauf des Anwendungsszenarios ist mithilfe des Sequenzdiagramms in folgender Abbildung verbildlicht.

1249



Abbildung 11: Sequenzdiagramm des Anwendungsszenarios ("Main-Flow")

Vollständige Ansicht der hochauflösenden Version des Sequenzdiagramms:

<https://github.com/gematik/api-ncpeh/blob/master/images/feature/eped-b/overview/main-flow-tech-seq.svg>

7.1 Authentifizierung und Autorisierung des LE-DE

Der Zugriff auf das Anwendungsszenario ePrescription/eDispensation Land B (ePeD-B) und damit auf die E-Rezepte von EU-Bürgern über das EU-Webportal ist ausschließlich nach erfolgreicher Authentifizierung des LE-DE und seiner Institution (LEI-DE) möglich. Für die Durchführung der Authentisierung sind sowohl der Heilberufsausweis (HBA) des LE-DE als auch die SMC-B der LEI-DE erforderlich. Beide Smartcards müssen über den konfigurierten Konnektor oder TI-Gateway erreichbar sein, wobei sich die SMC-B-Karte im freigeschalteten Modus befinden muss. Zusätzlich muss auf dem Rechner des LE-DE, neben einem modernen Webbrowser, die Authentisierungssoftware (gematik-Authenticator) installiert und korrekt konfiguriert sein, sodass sie den Konnektor oder TI-Gateway sowie die Smartcards ansprechen kann.

Die Authentisierung wird durch den LE-DE initiiert, indem er sich über seinen Webbrowser am EU-Webportal anmeldet. Die Kommunikation mit dem zentralen IDP-Dienst und die Durchführung der Authentisierung erfolgt durch den gematik-Authenticator. Dabei wird das OIDC-Protokoll mit Authorization Code-Flow verwendet. Für die Bestätigung der TI-Identitäten gemäß den Anforderungen der eHDSI ist es erforderlich, sowohl den HBA des LE-DE (z.B. Name, Rolle, Identifier) als auch die SMC-B der LEI-DE (Bezeichnung, Typ, Identifier) einzubinden. Im Rahmen des Authentisierungsprozesses kann es erforderlich sein, dass der LE-DE die PIN seiner HBA-Karte am angeschlossenen Kartenterminal eingibt.

Nach erfolgreicher Authentifizierung stellt der IDP-Dienst dem gematik-Authenticator für die Identitäten der Smartcards jeweils einen Authorization Code aus. Diese Codes werden an den NCPEH-Proxy, genauer gesagt an dessen Authorization Service, weitergeleitet. Der Authorization Service tritt gegenüber dem zentralen IDP-Dienst als Client für die Durchführung der PKCE-Challenge auf. Dieser tauscht die Codes beim IDP-Dienst gegen ID-Tokens ein. Die ID-Tokens enthalten die relevanten Identitätsattribute (Claims), die im späteren Verlauf insbesondere für den Zugriff auf das Anwendungsszenario ePeD-B vom NCPEH-FD innerhalb der eHDSI benötigt werden.

Anhand der gewonnenen Identitätsinformationen überprüft der NCPEH-Proxy die Rolle des LE-DE und stellt sicher, dass diese gemäß nationalen Vorgaben für den Zugriff auf das Anwendungsszenario ePeD-B berechtigt ist. Nach der abschließenden Überprüfung der Zugriffsberechtigung wird dem EU-Webportal das Ergebnis der Autorisierung als `ncpehprx_access_token` zu Verfügung gestellt, welcher vom EU-Webportal für alle nachfolgenden Anfragen an den NCPEH-Proxy gesendet wird.

Der `ncpehprx_access_token` ist nur kurzzeitig gültig. Eine bedarfsgerechte Verlängerung ist über den Refresh-Token-Mechanismus in Anlehnung an die eHDSI-Vorgaben zur Identity Assertion eines LE-DE (siehe [eHDSI_SAML_Profile]) innerhalb von 4 Stunden möglich.

Der LE-DE hat die Möglichkeit, die Session jederzeit über das EU-Webportal manuell zu beenden, wodurch er sich aus dem EU-Webportal abmeldet.

7.2 Information der Betroffenen über ihre Rechte und Pflichten zum Schutz ihrer personenbezogenen und gesundheitlichen Daten

Im Rahmen des Anwendungsszenarios ePrescription/eDispensation Land B ist es wichtig, dass EU-Bürger eine Möglichkeit haben, sich vor jeglichem Zugriff auf ihre personenbezogenen Daten, der Verarbeitung oder der Dispensierung ihrer E-Rezepte über ihre Rechte und Pflichten zum Schutz ihrer personenbezogenen und gesundheitlichen Daten zu informieren.

Der LE-DE muss dem EU-Bürger Informationen über die relevanten Datenschutzbestimmungen und den Schutz seiner persönlichen und gesundheitlichen Daten zur Verfügung stellen. Hierzu kann der LE-DE im EU-Webportal auf eine zentrale Website (siehe [MyHealth@EU_Cross-Border_Health_Services]) weitergeleitet, die von der Europäischen Kommission bereitgestellt wird.

Auf dieser Website werden für das Anwendungsszenario ePrescription/eDispensation in Deutschland als Land B vom Anbieter des NCPeH-FD Übersetzungen des Dokuments Patient Information Notice (PIN-Dokument) in verschiedenen europäischen Sprachen zur Verfügung gestellt. Das PIN-Dokument enthält detaillierte Informationen über die Rechte und Pflichten des EU-Bürgers sowie über die Art und Ort der Verarbeitung seiner Daten im Rahmen des grenzüberschreitenden Dienstes. Der LE-DE kann das entsprechende PIN-Dokument in der Sprache des Zugehörigkeitslandes des EU-Bürgers auswählen und bei Bedarf ausdrucken. Alternativ kann der LE-DE den Link zur Website oder direkt zum entsprechenden PIN-Dokument vom EU-Webportal aus digital an den EU-Bürger bereitstellen, z. B. in Form eines QR-Codes.

Darüber hinaus kann sich der LE-DE bei eigenem Interesse über seine eigenen Rechte und Pflichten sowie über die Verantwortlichkeiten der beteiligten Stellen informieren. Hierzu kann er im EU-Webportal auf eine andere externe Website oder Ressource zugreifen, die vom Anbieter des NCPeH-FD bereitgestellt wird. Auf der Webseite kann der LE-DE die Informationen in deutscher Sprache finden.

7.3 Identifikation des EU-Bürgers in der Apotheke vor Ort

Der autorisierte LE-EU wählt im EU-Webportal das Zugehörigkeitsland des EU-Bürgers (Land A) und die Anwendung ePrescription aus. Anschließend wird im EU-Webportal die passende internationale Suchmaske (International Search Mask) angezeigt, die vom Land A definiert und bereitgestellt wird.

Die Suchmaske wird vom Land A definiert, um die Identifikation seiner Bürger im Ausland und ggf. den Zugriff auf ihre Dokumente gemäß den jeweiligen nationalen Richtlinien im Land A zu ermöglichen. Die Verantwortung für die Pflege und Aktualisierung der Suchmaske sowie deren Veröffentlichung über den zentralen eHDSI-Configuration Service liegt vollständig bei Land A. Der NCPeH-FD kann die aktuelle Version der Suchmaske für das Land A über die Mechanismen des zentralen eHDSI-Dienstes abrufen und auf Anfrage dem EU-Webportal zur Verfügung stellen.

Die Suchmaske kann ein oder mehrere Eingabefelder enthalten. Die Beschriftungen der Eingabefelder werden im EU-Webportal in deutscher Sprache angezeigt. In die Eingabefelder kann der LE-DE die vom EU-Bürger bereitgestellten Identitätsmerkmale und ggf. Zugriffsinformationen für Dokumentensuche manuell eingeben. Nach Eingabe und Bestätigung durch den LE-DE wird eine Anfrage mit den eingegebenen Identitätsmerkmalen zur Validierung sowie zur Ermittlung weiterer demographischer Daten des EU-Bürgers an den NCPeH-Proxy gestellt.

1343 Die gesendete Anfrage des LE-DE enthält neben den Suchparametern auch den
1344 `ncpehprx_access_token`, der im Rahmen des Kapitel 7.1- Authentifizierung und
1345 Autorisierung des LE-DE erstellt wurde. Der NCPeH-Proxy prüft die Anfrage auf
1346 Vollständigkeit und Gültigkeit, insbesondere die Validität des `ncpehprx_access_tokens`.
1347 Nach erfolgreicher Prüfung ermittelt der NCPeH-Proxy die an die Session gebundenen
1348 und vom IDP-Dienst bestätigten Identitätsattribute des LE-DE und der LEI-DE. Diese
1349 Identitätsattribute werden zusammen mit den relevanten Daten aus der Anfrage des LE-
1350 DE an den NCPeH-FD weitergeleitet.

1351 Der NCPeH-FD übernimmt die Überführung der Identitätsattribute des LE-DE und der
1352 LEI-DE in das SAML2.0-Format gemäß den Vorgaben der eHDSI. Dabei wird eine Identity
1353 Assertion erstellt, die die Echtheit der Identitäten des LE-DE und der LEI-DE
1354 bestätigt. Basierend auf den vom LE-DE über die Suchmaske des Land A eingegebenen
1355 Suchparametern erzeugt und stellt der NCPeH-FD an den NCPeH Land A die Suchanfrage
1356 inklusive der zuvor erstellten Identity Assertion zur Ermittlung von weiteren
1357 demographischen Daten des EU-Bürgers.

1358

1359 Im Erfolgsfall antwortet Land A mit zusätzlichen demographischen Daten und bestätigt
1360 gleichzeitig die eindeutige Identitätskennung des EU-Bürgers. Diese Daten werden dem
1361 LE-DE im EU-Webportal angezeigt. Basierend auf den bereitgestellten demographischen
1362 Daten führt der LE-DE die Identifikation des EU-Bürgers mithilfe eines von diesem
1363 vorgelegten Dokuments (z.B. Reisepass) durch.

1364 Die eindeutige Identitätskennung des EU-Bürgers wird für nachfolgende Transaktionen
1365 benötigt, z.B. für den Abruf und die eindeutige Ermittlung von E-Rezepten des EU-
1366 Bürgers.

1367 Möchte der LE-DE demographischen Daten für denselben EU-Bürger erneut
1368 abrufen, dann ist der Inhalt der Suchmaske mit den zuvor eingegebenen Daten
1369 vorausgefüllt.

1370 Wenn der LE-DE demographische Daten für einen anderen EU-Bürger abrufen möchte,
1371 würden die vom LE-DE in die Suchmaske eingegebenen Identitätsmerkmale und die
1372 bereits abgerufenen demographischen Daten im EU-Webportal verworfen und dem LE-DE
1373 würde je nach seiner Wahl entweder eine leere Suchmaske für Land A oder die
1374 vollständige Übersicht über die EU-Länder angezeigt werden.

1375 Zur Unterstützung des LE-DE bei der Identifikation des EU-Bürgers kann die Suchmaske
1376 ergänzende Begleitinformationen, wie erläuternde Texte oder Abbildungen, enthalten.
1377 Diese Informationen bieten dem LE-DE zusätzliche Hilfestellung und erleichtern die
1378 Identifikation durch visuelle und inhaltliche Veranschaulichungen. Der Zugriff auf diese
1379 Begleitinformationen erfolgt optional und kann bei Bedarf vom LE-DE angefordert
1380 werden.

1381 **7.4 Übersicht über die einlösbaren E-Rezepte eines EU-Bürgers**

1382 Der autorisierte LE-DE kann eine Übersicht über die einlösbaren E-Rezepte eines EU-
1383 Bürgers abrufen, nachdem die demographischen Daten des EU-Bürgers abgerufen
1384 wurden und dessen eindeutige Identitätskennung vom Land A bestätigt wurde. Der LE-
1385 DE bestätigt im EU-Webportal die Behandlungsbeziehung zum EU-Bürger gemäß den
1386 Anforderungen der eHDSI.

1387 Die gesendete Anfrage des LE-DE über das EU-Webportal an den NCPeH-Proxy enthält
1388 die eindeutige Identitätskennung des EU-Bürgers, gegebenenfalls zusätzliche
1389 Zugriffsinformationen für die Dokumentensuche (siehe 7.3- Identifikation des EU-Bürgers)

1390 in der Apotheke vor Ort), die vom Land A für den Zugriff auf die E-Rezepte verlangt
1391 werden, sowie den `ncpehprx_access_token`, der im Rahmen des Kapitel 7.1-
1392 Authentifizierung und Autorisierung des LE-DE erstellt wurde. Nach erfolgreicher
1393 Validierung der Anfrage ermittelt der NCPeH-Proxy die an die Session gebundenen und
1394 vom IDP-Dienst bestätigten Identitätsattribute des LE-DE und der LEI-DE. Diese
1395 Identitätsattribute werden zusammen mit den relevanten Daten der Anfrage an den
1396 NCPeH-FD weitergeleitet.

1397 Der NCPeH-FD erstellt eine SAML2.0 TRC-Assertion gemäß den Vorgaben der eHDSI, die
1398 das Behandlungsverhältnis zwischen LE-DE und dem EU-Bürger bestätigt. Der NCPeH-FD
1399 sendet die Anfrage zur Auflistung von einlösbaren E-Rezepten zusammen mit der TRC-
1400 Assertion und der bereits in 7.3- Identifikation des EU-Bürgers in der Apotheke vor Ort
1401 erstellten Identity Assertion an den NCPeH Land A.

1402 Der NCPeH Land A ermittelt die relevanten Metainformationen zu den einlösbaren E-
1403 Rezepten des EU-Bürgers und übermittelt diese an den NCPeH-FD. Die
1404 Metainformationen enthalten wichtige Angaben zu den einzelnen E-Rezepten, wie z. B.
1405 die E-Rezept-ID, den Wirkstoff, die Dosierung und andere relevante Metainformationen,
1406 enthalten nicht vollständige Angaben zu den E-Rezepten.

1407 Falls die Metainformationen kodiert sind (z. B. Wirkstoffbezeichnungen), transkodiert der
1408 NCPeH-FD diese gemäß den Mappingregeln des BfArM ins Deutsche. Die transkodierten
1409 Metainformationen werden anschließend an den NCPeH-Proxy weitergeleitet, der sie an
1410 das EU-Webportal übermittelt. Dort werden die Metainformationen strukturiert und
1411 übersichtlich dargestellt. Die Übersicht über die E-Rezepte des EU-Bürgers kann auch
1412 nicht einlösbare E-Rezepte enthalten, sofern diese vom Land A mit ausgegeben werden.

1413 Die Auflistung von Metainformationen der E-Rezepte bietet für die einlösbaren E-Rezepte
1414 zusätzlich folgende Optionen für den nachfolgenden Rezeptabruf (Kapitel 7.5- Abruf von
1415 einlösbaren E-Rezepten eines E-Bürgers):

1416

- 1417 • **Kodierte Darstellung auf Deutsch:**
1418 Der LE-DE kann den Inhalt des E-Rezepts in kodierter Form und auf Deutsch
1419 anzeigen lassen.
- 1420 • **Nicht kodierte Darstellung im PDF/A-Format:**
1421 Alternativ kann der LE-DE das E-Rezept im PDF/A-Format anzeigen lassen. In
1422 diesem Fall wird der Inhalt des E-Rezepts in der Sprache des Land A dargestellt
1423 und steht nicht in deutscher Sprache zur Verfügung.

1424 **7.5 Abruf von einlösbaren E-Rezepten eines E-Bürgers**

1425 Der autorisierte LE-DE hat die Möglichkeit, im EU-Webportal mehrere einlösbare E-
1426 Rezepte eines EU-Bürgers auszuwählen, um deren vollständigen Inhalt aus Land A
1427 abzurufen und anzeigen zu lassen. Der Abruf der ausgewählten E-Rezepte erfolgt über
1428 denselben technischen Weg, wie im Kapitel 7.4- Übersicht über die einlösbaren E-
1429 Rezepte eines EU-Bürgers beschrieben. Dabei werden die E-Rezepte durch den NCPeH-FD
1430 vom Land A abgerufen und über den NCPeH-Proxy an das EU-Webportal bereitgestellt.

1431 Nach erfolgreicher Bereitstellung der E-Rezepte im EU-Webportal werden die
1432 vollständigen Inhalte der E-Rezepte dem LE-DE strukturiert und in kodierter Form auf
1433 Deutsch angezeigt.

1434 Zusätzlich hat der LE-DE die Möglichkeit, sich das Originalrezept des abgerufenen E-
1435 Rezepts des EU-Bürgers im EU-Webportal anzeigen zu lassen. Das Originalrezept wird im

1436 PDF/A-Format dargestellt und enthält den Inhalt des E-Rezepts in der Sprache des Land-
1437 A. Eine Übersetzung ins Deutsche ist bei der Anzeige des Originalrezepts nicht
1438 vorgesehen. Der LE-DE kann das Originalrezept bei Bedarf herunterladen und lokal auf
1439 seinem Rechner abspeichern, um es für Dokumentationszwecke zu verwenden.

1440 **7.6 Einlösung von E-Rezepten eines EU-Bürgers**

1441 Nach erfolgreichem Abruf der E-Rezepte eines EU-Bürgers muss der autorisierte LE-DE
1442 für jedes eingelöste E-Rezept eine Dispensierinformation an das Land A übermitteln, um
1443 den EU-Workflow gemäß den Vorgaben korrekt durchzuführen. Dazu wählt der LE-DE im
1444 EU-Webportal jedes einzulösende E-Rezepte aus, um für diese passende
1445 Dispensierinformationen zu erfassen.

1446 Der LE-DE erfasst alle relevanten Angaben inkl. der Pharmazentralnummern (PZN) zur
1447 Abgabe des Medikaments. Falls ein Produkt substituiert wurde, kann der LE-DE in den
1448 Dispensierinformationen die Substitution einschließlich der Angaben zum substituierten
1449 Produkt angeben.

1450 Der LE-DE hat die Möglichkeit, den Vorgang der Dispensierung jederzeit abubrechen,
1451 entweder auf eigenen Wunsch oder auf Wunsch des EU-Bürgers. Falls der Vorgang ohne
1452 Übermittlung der Dispensierinformationen beendet werden soll, zeigt das EU-Webportal
1453 eine Warnung an, um den LE-DE auf die fehlende Übermittlung hinzuweisen. Der LE-DE
1454 kann in diesem Fall den Vorgang wieder aufnehmen und die offenen
1455 Dispensierinformationen vervollständigen.

1456 Nach erfolgreicher Übermittlung der Dispensierinformationen an Land A erhält der LE-DE
1457 eine Erfolgsmeldung im EU-Webportal, die den Abschluss des Dispensiervorgangs
1458 bestätigt. Anschließend kann der LE-DE entscheiden, ob weitere E-Rezepte des EU-
1459 Bürgers dispensiert werden sollen oder ob die Bedienung des EU-Bürgers damit
1460 abgeschlossen ist.

1461 Falls der LE-DE die Einlösung weiterer E-Rezepte des EU-Bürgers vornehmen möchte,
1462 wählt er im EU-Webportal den Vorgang gemäß dem Kapitel 7.4- Übersicht über die
1463 einlösbaren E-Rezepte eines EU-Bürgers aus. Die Rezeptliste wird dann auf Basis einer
1464 erneuten Suche angezeigt und der LE-DE kann weitere E-Rezepte auswählen und
1465 dispensieren.

1466 Wenn der LE-DE E-Rezepte eines anderen EU-Bürgers abrufen möchte, dann wählt er im
1467 EU-Webportal den Vorgang gemäß dem Kapitel 7.3- Identifikation des EU-Bürgers in der
1468 Apotheke vor Ort und beginnt damit den Prozess von Neuem. Die personenbezogenen
1469 und E-Rezept-Daten des nicht mehr bedienten EU-Bürgers sind im EU-Webportal nicht
1470 mehr vorhanden.

1471

8 Technisches Konzept

Dieses Kapitel beschreibt das technische Konzept für das Anwendungsszenario ePeD-B und strukturiert den zugrunde liegenden Lösungsraum in die dafür erforderlichen Systeme. Ziel ist es, einen Überblick über den technischen Aufbau, die Verantwortlichkeiten der beteiligten Komponenten sowie deren Zusammenspiel zu vermitteln.

Hierzu werden die technischen Systeme wie das EU-Webportal, der NCPeH-Proxy und der NCPeH-FD vorgestellt. Das Kapitel beschreibt, wie die Systeme erreicht werden, welche Webschnittstellen sie bereitstellen und wie diese aus technischer und fachlicher Sicht genutzt werden.

Darüber hinaus werden die zugrunde liegenden Informationsmodelle vorgestellt, die als Bestandteil der Nachrichten zwischen den Systemen ausgetauscht werden. Abschließend werden die Abläufe der einzelnen Anwendungsfälle detailliert beschrieben und anhand von Sequenzdiagrammen nachvollziehbar dargestellt, um das Zusammenwirken der Systeme transparent zu machen.

8.1 EU-Webportal

Das EU-Webportal besteht aus folgenden Komponenten:

1. Einer clientseitigen WebApp (client-side WebApp)
2. Einem Webserver, welcher die WebApp ausliefert und Nutzungsregeln für diese definiert.

Definition: clientseitige WebApp

Eine clientseitige WebApp im Sinne dieses Konzepts wird wie folgt definiert:

- Bestandteile (Quellcode, Business-Logik, Libraries, statischer Content usw.) zur Nutzung des ePeD-B Szenarios werden vollständig in den Browser des LE-DE geladen und durch die WebApp selbst verarbeitet.
- Durch den Aufruf per Link bzw. URL-Eingabe im bereits vorinstallierten Standard-Browser beim LE-DE wird die WebApp (als Ganzes (Startseite und Bundles) geladen, dort automatisch aufgerufen und gestartet. Der Start passiert im selben Tab, mit welchem der Link geöffnet wurde (vergleichbar mit dem Aufruf einer Website).
- Das GUI der WebApp wird nicht nur im Browser angezeigt, sondern auch vollständig dort gerendert. Es findet keine Pre-Renderung auf dem Webserver statt.
- Die WebApp setzt sich selbst aus Subkomponenten für die Darstellung des GUI (z.B. Widgets, Boxen, Tabellen, Layouts, Formatanweisungen), dessen Rendering und Navigation zusammen. Weiterhin gibt es zur Ablaufsteuerung Subkomponenten für die Zustandsverwaltung, ASL-Kanal und API-Zugriff.
- Die Session-Verwaltung inkl. User-Identifikation erfolgt über OAuth2 Access-Tokens gemäß RFC 6749.

- Die WebApp muss nicht durch den User konfiguriert werden. Die Konfiguration wird durch den Lade- und Startvorgang automatisch ausgeführt.
- Der Login wird unter Verwendung des Authenticators durchgeführt, der auf demselben Arbeitsplatz-PC des LE-DE installiert ist.
- Persönliche medizinische Daten werden über einen ASL-Kanal Ende-zu-Ende verschlüsselt.
- Es gelten die in Abschnitt 8.1.3- Sichere Auslieferung der WebApp-Bestandteile durch den Webserver beschriebenen Sicherungsmaßnahmen für die WebApp.

Folgende Abbildung fasst den Aufbau und die Nutzung der WebApp des EU-Webportals zusammen:

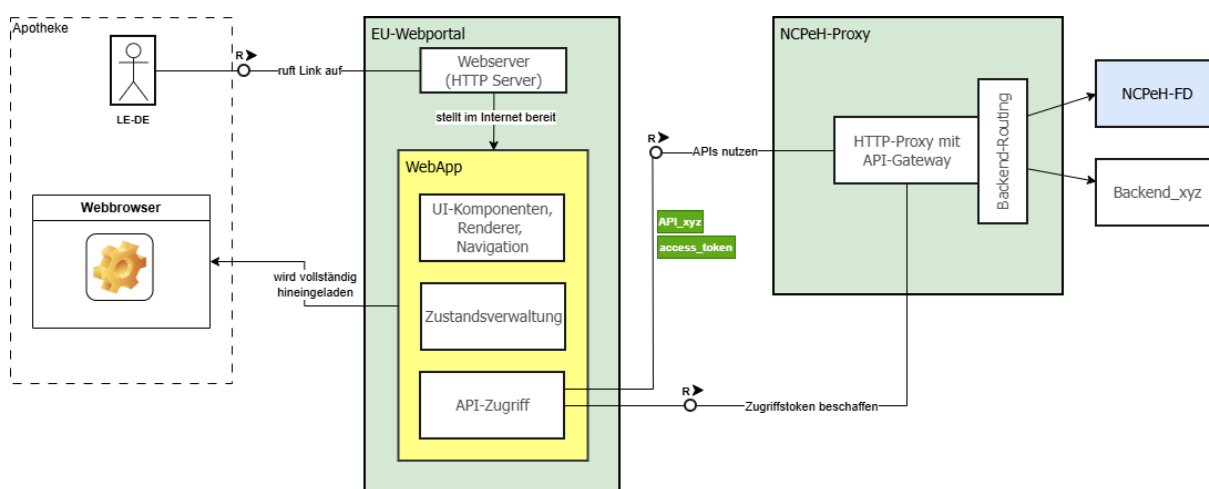


Abbildung 12: Aufbau und Nutzung der WebApp-Komponente

8.1.1 Zugang zum EU-Webportal

Der Zugang zum EU-Webportal erfolgt für die Nutzer über ihren lokal installierten Webbrowser. Die Verbindung zum Webserver des EU-Webportals wird über das Internet hergestellt. Die initiale Verbindung wird zwischen dem Browser und dem EU-Webportal mittels TLS v1.2 oder v1.3 abgesichert.

Nach dem erfolgreichen Verbindungsaufbau lädt der Browser eine WebApp herunter, die direkt im Webbrowser des LE-DE ausgeführt wird. Die WebApp ist eine dynamische Anwendung, über die das Rendering der Webinhalte sowie die Durchführung weiterer Aufrufe und Datenverarbeitungen erfolgt. Die WebApp im Browser stellt die Nutzerschnittstelle zwischen dem LE-DE und den Funktionalitäten des Anwendungsszenarios ePeD-B dar und ermöglicht eine interaktive Nutzung der angebotenen Dienste bzw. Workflows.

Die Authentisierung des LE-DE wird von der WebApp initiiert, sobald der LE-DE eine entsprechende Anfrage stellt. Dabei wird der lokal installierte gematik Authenticator über einen parametrisierten Deeplink aufgerufen. Der gematik Authenticator übernimmt die Authentisierung des LE-DE und seiner Institution (LEI-DE) mittels der HBA und der SMC-B. Zu diesem Zweck muss der gematik Authenticator die zugelassene dezentrale Komponente Konnektor oder TI-Gateway aufrufen können.

8.1.2 Schnittstellen

Tabelle 1: Funktionale Schnittstellen und Operationen des EU-Webportals

Funktionale Schnittstelle	Komponente	Rolle	Operationsbeschreibung
I_Provide_WebApp	Webserver	Producer	Herunterladen der WebApp in den Browser
I_WebApp_Deployment	Webserver	Consumer	Bereitstellung einer neuen Version der WebApp
I_Comm_ASL	WebApp	Consumer	Nutzt verschiedene APIs und Endpunkte für ASL-verschlüsselte Requests/Responses
I_Authorization	WebApp	Consumer	Erstellen von Autorisierungsanfragen durch die WebApp des EU-Webportals und den Authenticator
I_User_Interaction	WebApp	Producer	Grafische Benutzeroberfläche für den LE-DE
I_Patient_Identification_Service	WebApp	Consumer	siehe Abschnitt 8.3.2- <u>Schnittstellen</u> zu Schnittstellen des NCPeH-FD
I_eHealth_Service	WebApp	Consumer	siehe Abschnitt 8.3.2- <u>Schnittstellen</u> zu Schnittstellen des NCPeH-FD
I_Provide_DocumentSet_Service	WebApp	Consumer	siehe Abschnitt 8.3.2- <u>Schnittstellen</u> zu Schnittstellen des NCPeH-FD

Bestimmte API-Calls der WebApp werden nicht durch den einen zusätzlichen ASL-Kanal verschlüsselt und benutzen somit nicht I_Comm_ASL, da hier keine personenbezogenen medizinischen Daten übertragen werden. Stattdessen nutzen sie gewöhnlicher HTTP-Requests/-Responses in einem TLS-Kanal zwischen der WebApp und dem NCPeH-Proxy.

Diese Aufrufe durch die WebApp an folgenden Schnittstellen benutzen nicht I_Comm_ASL:

- 1551 • I_Authorization (alle mit Authentifizierung des LE-DE gemäß 8.5.2.1-
- 1552 Authentifizierung und Autorisierung des LE-DE befassten Endpoints)
- 1553 • I_ISM_Service

1554 **8.1.2.1 I_Provide_WebApp**

1555 Diese Outbound HTTPS-Schnittstelle des Webserver ist read-only und verfügt über einen
1556 öffentliche URL an einer noch festzulegenden und zu registrierenden Domain, die eigens
1557 für das EU-Webportal vorgesehen ist. Bei Aufruf der Schnittstelle werden alle WebApp-
1558 Bestandteile in den Browser geladen, wodurch die WebApp lauffähig in der lokalen
1559 Sandbox des Browsers des LE-DE ist.

1560 **8.1.2.2 I_WebApp_Deployment**

1561 Diese Inbound Schnittstelle des Webserver empfängt neue Versionen der WebApp und
1562 legt sie in einem dafür vorgesehenen lokalen Webserver-Pfad ab. Die Schnittstelle ist als
1563 Ende (Deployment-Target) einer Build/Deployment-Pipeline gedacht, daher wird das
1564 Protokoll für Inbound-Anfragen hier nicht festgelegt.

1565 **8.1.2.3 I_Comm_ASL**

1566 Zwischen der WebApp und dem VAU-Verarbeitungskontext des NCPeH-FD wird ein
1567 logischer Ende-zu-Ende-Kanal für die Inhaltsverschlüsselung aufgebaut, der durch das
1568 ASL-Protokoll realisiert wird. Der NCPeH-FD agiert dabei in der Rolle als ASL-Server und
1569 implementiert den Endpoint/ASL gemäß den Vorgaben aus [gemSpec_Krypt#ZETA/ASL
1570 (VAU-Protokoll)], während die WebApp des EU-Webportals die Rolle des ASL-Clients
1571 einnimmt.

1572 Da die TLS-Verbindungen an den jeweiligen Komponenten enden, wird die Vertraulichkeit
1573 der Inhalte (Payload) mittels des ASL-Protokolls auf der Anwendungsebene durch eine
1574 Ende-zu-Ende Verschlüsselungsschicht zusätzlich abgesichert. Das ASL-Protokoll
1575 ermöglicht diese Ende-zu-Ende-Inhaltsverschlüsselung zwischen der Webapp und dem
1576 VAU-Verarbeitungskontext des NCPeH-FD. Dadurch wird sichergestellt, dass die Inhalte
1577 selbst innerhalb des NCPH-Proxys oder der Webschnittstelle des NCPeH-FD nicht im
1578 Klartext vorliegen.

1579 Zum Aufbau der zusätzlichen Verschlüsselungsschicht ist ein zusätzlicher Handshake auf
1580 Protokollebene notwendig, welcher in 8.5.2.2- Etablierung eines ASL-Kanals in die VAU-
1581 Umgebung des NCPeH-FD beschrieben ist. Während originäres KEM-TLS, auf welchem
1582 das ASL-Protokoll aufbaut, eine Modifikation des TLS-Protokolls auf OSI-Schicht 6/7
1583 darstellt, agiert das ASL-Protokoll gemäß [gemSpec_Krypt#ZETA/ASL (VAU-Protokoll)]
1584 nur auf der OSI-Schicht 7. ASL tunnelt seine Handshake-Nachrichten als HTTP-Payloads
1585 über eine bereits existierende TLS-Verbindung. Die 24h-Löschfrist (und Neuaushandlung)
1586 der im Handshake ausgehandelten symmetrischen Verschlüsselungsschlüssel wird in
1587 dem hier beschriebenen ePeD-B Szenario deutlich unterschritten, da der Aufbau und die
1588 Lebensdauer eines ASL-Kanals an die kurze, personalisierte Session-Dauer eines LE-DE
1589 von 4h gebunden ist.

1590 Diese Inbound-/Outbound-Schnittstelle ist ausschließlich für autorisierte Kommunikation
1591 des authentisierten LE-DE vorgesehen, vgl. dazu 8.5.2.3- Nutzung einer autorisierten
1592 Verbindung zum NCPeH-FD.

8.1.2.4 I_User_Interaction

Der LE-DE sieht das grafische Frontend der WebApp im Browser und interagiert damit (Maus- und Tastatureingaben). Es ist ein separater [Figma-Clickdummy] für diese Schnittstelle vorhanden.

8.1.3 Sichere Auslieferung der WebApp-Bestandteile durch den Webserver

Da die WebApp vollständig im Browser abläuft, findet kein Rendering und keine Vorverarbeitung auf dem Webserver statt. Stattdessen nimmt der Webserver die Rolle eines Content Delivery Edge-Nodes ein, der dafür optimiert ist, die Bestandteile der WebApp zügig an den Anfragenden (den LE-DE) auszuliefern. Daher ist von entscheidender Bedeutung, dass die Bestandteile der WebApp bei der Auslieferung stets authentisch und aktuell sind. Um das zu erreichen, werden folgende Mechanismen und Techniken eingesetzt.

Einsatz von HTTP Strict Transport Security (HSTS)

Der Webserver zwingt den Browser vor dem Laden der WebApp eine ausschließlich verschlüsselte Verbindung zur Domain mit dem Aufruf-Endpoint der WebApp aufzubauen.

Verwendung von CSP-Response-Header

Der Webserver gibt der WebApp eine strikte Content Security Policy (CSP) aus, die verhindert, dass App-fremde Inhalte nach- oder von der Seite geladen werden. In den Directiven der Policy wird festgelegt, dass WebApp-Bestandteile nur vom Webserver selbst geladen werden dürfen (z.B. Direktive `script-src 'self'` für clientseitige Skripte).

SRI-Tags für kritische und aktive WebApp-Bestandteile

Mindestens alle Laufzeit-Bestandteile, Libraries und Links zu anderen Bestandteilen der WebApp werden mit Subresource Integrity Tags (SRI-Tags) ausgestattet. Der Browser als Laufzeitumgebung ist somit gezwungen, die Hashes in den SRI-Tags zu validieren. Die SRI-Tags selbst werden bereits während des Build-Prozesses der WebApp erzeugt. Eine notwendige Aktivierung von Cross Origin Resource Sharing (CORS) für diese WebApp-Bestandteile kann zugunsten der SRI-Tags hingenommen werden.

Komponenten-Hashes für jeden Build

Mit jedem Build und anschließendem Deployment/Bereitstellen der WebApp auf dem Webserver werden explizite Hashes für die Komponenten/Resources der WebApp gebildet und am Aufruf dieser attribuiert. Gleichzeitig erfolgt der Build für die WebApp ausschließlich aus einem eigenen dafür vorgesehenen Repository, dessen Deployment-Ziel der Aufruf-Endpoint der WebApp auf dem Webserver ist. Durch den Build werden einzigartige Deployment-Artefakte erzeugt, als Bundle zusammengefasst und auf dem Webserver hinterlegt (sog. Immutable Deployment).

Clientseitige und serverseitige SBOM mit inkludierten Komponenten-Hashes

Für alle Bestandteile der WebApp wird durch den Build-Prozess der WebApp zwei SBOMs erstellt, von denen eine Fassung gemeinsam mit der WebApp über `I_Provide_WebApp` ausgeliefert wird und die andere Fassung serverseitig (am NCPeH-Proxy) hinterlegt wird. Bei Requests durch die WebApp werden vorab alle Elemente der SBOM anhand ihrer Hashes gegen die serverseitige Fassung anhand einer dort hinterlegten Policy auf Identität geprüft. Nur bei vollständiger Identität werden die Client-Requests folgeverarbeitet. Die zwei SBOM-Fassungen haben unterschiedlichen Umfang:

- Die reduzierte Fassung in der WebApp enthält eindeutige Package-Bezeichner für jedes Package, dessen jeweiliger Hash und einen vollständigen Dependency-Tree.

- Die volle Fassung am NCPeH-Proxy enthält neben den Inhalten des Client-SBOM auch Zusatzinformationen wie Komponentennamen, Version, Lizenz und Lieferquelle.

Durch die beschriebenen Mechanismen wird sichergestellt, dass nur solche Client-Komponenten mit dem Proxy interagieren, die durch den Aussteller der WebApp im Bereitstellungsprozess selbst für gültig und berechtigt erklärt worden sind.

Darüber hinaus sorgt der Webserver durch entsprechende Konfiguration dafür, dass das Caching bestimmter WebApp-Bestandteile unterdrückt wird.

8.1.4 Ausblick

Weitere Anwendungsszenarien nach ePeD-B könnten über separate, Szenario-spezifische clientseitige WebApps über andere Endpoints des Webserver am EU-Webportal ausgeliefert werden. Eine zwingende Notwendigkeit, alle Szenarien in einer gemeinsamen WebApp auszuliefern, besteht nicht. Das ePeD-B Szenario ist auf den sehr speziellen Bedarf von Apothekern zugeschnitten, daher können dedizierte WebApps für andere diffizile Nutzergruppen sinnvoll sein und werden hier nicht ausgeschlossen.

8.2 NCPeH-Proxy

Der NCPeH-Proxy besteht aus folgenden Komponenten:

1. HTTP-Proxy, durch welchen sämtlicher Traffic zwischen der clientseitigen WebApp des EU-Webportals und dem NCPeH-FD vermittelt wird.
2. Authorization-Service (aka. "Auth-Service"), welcher exklusiv für die NCPeH-Land-B Domäne Autorisierungsdienstleistungen erbringt. Zu diesen Autorisierungsdienstleistungen gehören insbesondere
 - Herausgabe signierter ID- und Access-Tokens mit bestimmten Claims auf der Grundlage von definierbaren und definierten Authentisierungsmitteln
 - Umtausch von gültigen Tokens von Upstream-IDPs in eigene Tokens mit lokalem, eigen-definierten Scope

8.2.1 Zugang zum NCPeH-Proxy

Der NCPeH-Proxy ist ausschließlich über TLS-gesicherte RESTful Schnittstellen mittels eines dedizierten FQDN über das Internet zugänglich und wird durch API-Calls der WebApp des EU-Webportals genutzt. Dabei ist die Identität und Validität des FQDN durch ein End-Entity-Zertifikat prüfbar, welches von einer CA ausgestellt wurde, die die [\[Baseline Requirements for the Issuance and Management of Publicly Trusted Certificates\]](#) erfüllt. Während der HTTP-Proxy direkt über Webschnittstellen erreichbar ist, kann der Authorization-Service nur durch vorherige Policy-basierte Erlaubnis (vgl. dazu Abschnitt 8.1.3: Sichere Auslieferung der WebApp-Bestandteile durch den Webserver und die Use Cases im Abschnitt 8.5.2: Use Cases im Rahmen der Authentifizierung, Autorisierung) mittelbar durch die WebApp genutzt werden.

8.2.2 Schnittstellen

Tabelle 2: Funktionale Schnittstellen und Operationen des NCPeH-Proxy

Funktionale Schnittstelle	Komponente	Operationsbeschreibung(en)
I_Comm_ASL	HTTP-Proxy	Vermittelt verschiedene APIs und Endpunkte für ASL-verschlüsselte Requests/Responses anhand von Attributen des äußeren Request (z.B. Headerinformationen, Requestparameter, URL-Pfade)
I_Authorization	Authorization-Service	Bearbeitung von Autorisierungsanfragen durch die WebApp des EU-Webportals und den Authenticator
I_Identification	Authorization-Service	Anfragen an IDP-Dienst als Upstream-IDP
I_ISM_Service	HTTP-Proxy	Suchmasken der zulässigen Länder-A bereitstellen

8.2.2.1 I_Comm_ASL

Zur grundsätzlichen Beschreibung dieser Schnittstellen sei auf den Abschnitt 8.1.2.3- I_Comm_ASL verwiesen.

Die Rolle der HTTP-Proxy Komponente des NCPeH-Proxy an diesen beiden Schnittstellen ist es, einerseits die Gateway-Funktionen gemäß 8.2.3- API-Gateway Funktion bereitzustellen und die Use Cases entsprechend ihrer Vorgaben gemäß 8.5- Use Cases zu verarbeiten andererseits.

8.2.2.2 I_Authorization

Diese Schnittstelle ist Bestandteil der in Abschnitt 8.2.5- Authentifizierung und Autorisierung beschriebenen Funktionalität.

8.2.2.3 I_Identification

Diese Schnittstelle ist Bestandteil der in Abschnitt 8.2.5- Authentifizierung und Autorisierung beschriebenen Funktionalität.

8.2.2.4 I_ISM_Service

Diese Schnittstelle vermittelt Anfragen zu Suchmasken der zulässigen Länder-A an den NCPeH-FD. Die Funktionsbeschreibung ist in Abschnitt 8.3.2.2- I_ISM_Service zu finden.

8.2.3 API-Gateway Funktion

Die HTTP-Proxy Komponente des NCPeH-Proxy ist mit einer Basis-API-Gateway Funktionalität ausgestattet, die folgendes ermöglicht:

- Anwenden und Auswerten von Gateway-Policies zu HTTP-Traffic (vgl. dazu auch Abschnitt 8.5.2.3- Nutzung einer autorisierten Verbindung zum NCPeH-FD, in welchem die Anwendung von solchen Policies skizziert ist) in Bezug auf

- 1701 • Pfad-, Methoden-, Header- oder Host-basiertes Routing von eingehenden
1702 Requests an die korrekten Services bzw. APIs (als Reverse Proxy)
- 1703 • Traffic-Splitting auf Basis von Header-Regeln, um z.B. neue Service-Versionen
1704 sicher ausrollen zu können
- 1705 • Traffic-Modification in Bezug auf Hinzufügen/Entfernen/Anpassen von HTTP-
1706 Headern, Query-Parametern und Pfaden
- 1707 • Load Balancing des Traffics auf ggf. mehrere Instanzen des NCPeH-FD oder
1708 anderer Backend-Services. Der HTTP-Proxy reagiert dabei dynamisch auf
1709 skalierende Instanzen.
- 1710 • Security-Offloading
 - 1711 • Validierung von JWT ID-Tokens gem. [OpenID Connect Core#2] und Access-
1712 Tokens gem. [RFC 9068] sowie [RFC 7519] (vgl. dazu auch Abschnitt 8.5.2.3-
1713 Nutzung einer autorisierten Verbindung zum NCPeH-FD)
 - 1714 • TLS-Terminierung
 - 1715 • Anwendung und Auswertung von Gateway-Policies zu Web Security,
1716 insbesondere
 - 1717 • IP-White-/Blacklisting
 - 1718 • Schutz vor gängigen Angriffsvektoren
 - 1719 • Ermöglichen/Aufrufen von dedizierten Backend-for-Frontend-Services (BFF-
1720 Pattern analog zu [Backends for Frontends]) bzw. Delegationsmöglichkeit an diese
1721 Services, ohne selbst API-Aggregation/API-Composition Funktionalität anbieten zu
1722 müssen
 - 1723 • Ermöglichen und Anwenden von Resilience-Patterns
 - 1724 • Throttling und Rate Limiting von Requests
 - 1725 • Abfangen und Kompensieren von Backend-Ausfällen durch Mechanismen wie
1726 Retries und Circuit Breakern
 - 1727 • Context Propagation zu einem konfigurierbaren OpenTelemetry Collector inkl.
1728 Span-Erzeugung von Erzeugung und Weitergabe von Corellation-IDs.

1729 8.2.4 Client Registrierung

1730 Der Authorization-Service des NCPeH-Proxy tritt gegenüber dem zentralen IDP-Dienst als
1731 Identity Broker für ein Anwendungsfrontend auf. Somit übernimmt der Authorization-
1732 Service die Rolle der OIDC Relying Party bzw. des OAuth2-Clients gegenüber dem IDP-
1733 Dienst. Daher benötigt der Authorization-Service eine zugewiesene `client_id`, um
1734 Tokens vom IDP-Dienst abfragen zu dürfen. Die zugewiesene `client_id` (inkl.
1735 kryptographisches Material/`client_secret`) wird im Authorization-Service dann als
1736 Credentials dem IDP-Dienst als IDP-Upstream-Provider für OIDC zugeordnet.

1737 Die Zuweisung und Erhalt der `client_id` erfolgt einmalig und statisch und ist gemäß
1738 [gemSpec_IDP_Dienst#3.5] und [gemSpec_IDP_Dienst#A_20742] durchzuführen. Da es
1739 keinen Self-Service für die automatisierte Umsetzung des Erhalts der `client_id` gibt,
1740 muss der Onboarding-Prozess der gematik durchlaufen werden, die dann die `client_id`
1741 zuweist.

1742 Der Scope von Tokens, der auf Basis der zugewiesenen `client_id` in einem Token
1743 attribuiert ist und durch den IDP-Dienst herausgegeben wird, ist "openid ncpeh".

8.2.5 Authentifizierung und Autorisierung

Die Authentifizierung und Autorisierung erfolgt mittels OAuth2 und OIDC am Authorization-Service sowie mittels DPOP am HTTP-Proxy über die Schnittstelle I_Authorization. Da die WebApp des EU-Webportals, die Authentifizierungskomponente (gematik Authenticator) und der Authorization-Service des NCPEH-Proxy asynchron ablaufen, müssen die Schnittstellen zum Authorization-Service einen entkoppelten, nicht sequenziellen Login unterstützen. Gleichzeitig muss der Authorization-Service selbst einen asynchronen Authentication-Flow unterstützen und intern mehrere längerlaufende Autorisierungsanfragen parallel handhaben können. Vgl. dazu 8.5.2.1- Authentifizierung und Autorisierung des LE-DE und 8.5.2.3- Nutzung einer autorisierten Verbindung zum NCPEH-FD.

Der Authentication-Flow umfasst eine Einbindung des zentralen IDP-Dienstes und die Herausgabe von Autorisierungs-codes (AUTH_CODE) über die Schnittstelle I_Identification. Um dieses für die WebApp des EU-Webportals abzusichern, unterstützt der Authorization-Service PKCE-Challenges gemäß RFC 7636.

Der Authorization-Service muss in der Lage sein, OAuth2 Authorization-Codes in ID-Tokens umzuwandeln und diese anschließend über eine Exchange-Policy in systemgebundene Access-Tokens und ID-Tokens zu tauschen.

An die WebApp des EU-Webportals herausgegebene Access-Tokens müssen bei Ihrer Benutzung an ein clientseitig generiertes asymmetrisches Schlüsselpaar gebunden sein (DPoP gemäß RFC 9449).

Die API des Authorization-Service muss Konzepte für Multi-Faktor- bzw. Multi-Karten-Logins (HBA + SMC-B über ein eHealth-Kartenterminal) verarbeiten können, wobei diese Smartcards den TI-gebundenen, hardwarebasierten Vertrauensanker bilden.

8.2.5.1 Weitergabe von Identitätsattributen

Der Authorization-Service bezieht die für den in Abschnitt 8.5.2.1- Authentifizierung und Autorisierung des LE-DE beschriebenen Use Case benötigten Identitätsattribute vom IDP-Dienst in Form zweier ID-Tokens, mappt diese und gibt diese in Form von neuen Claims in neu ausgestellten Tokens mit `audience=ncpeh-fd` sowie `audience=eu-webportal` an den NCPEH-FD bzw. die WebApp des EU-Webportals weiter.

Tabelle 3: Verwendete und vom IDP-Dienst bestätigte Identitätsattribute des HBA

fachliches Identitätsattribut	Verwendetes Identitätsattribut des HBA	Verwendeter Claim aus ID Token des IDP-Dienstes
ID-Nummer des LE-DE	Telematik-ID des HBA Inhabers (Admission.registrationNumber)	idNummer
Vollständiger Name	Vor- und Nachname des HBA Inhabers (Subject.commonName)	given_namefamily_name
Rolle	OID der Rolle des HBA Inhabers (Admission.professionOID)	professionOID

1776

Tabelle 4: Verwendete und vom IDP-Dienst bestätigte Identitätsattribute der SMC-B

fachliches Identitätsattribut	Verwendetes Identitätsattribut der SMC-B	Verwendeter Claim aus ID Token des IDP-Dienstes
ID-Nummer der LEI-DE	Telematik-ID der Institution aus SMC-B (Admission.registrationNumber)	idNummer
Typ der Institution	OID der Institution aus SMC-B (Admission.professionOID)	professionOID
Name der Institution	Name der Institution aus SMC-B (Subject.commonName)	organizationName

1777

Die Claims aus diesen beiden Tabellen werden gemappt auf:

1778

- IdA_Claims in ID-Token IdA_raw (audience=ncpeh-fd)

1779

- Disp_Claims in ID-Token euwp_id_token (audience=eu-webportal)

1780

8.2.6 Qualitätsanforderungen an Betrieb und Infrastruktur

1781

Die folgenden systematischen Abbildungen (SysML Requirements Diagramme) fassen die nicht-funktionalen Qualitätsanforderungen (Stereotyp "Requirement") an die Betriebs- und Infrastrukturumgebung des NCPEH-Proxy zusammen und zeigen dabei grobgranulare Lösungsansätze (Stereotyp "Element"), die in der Betriebs- und Infrastrukturumgebung umzusetzen sind.

1786

Bei diesen Lösungsansätze wird zwischen den Typen "Cloud-native OS Feature" und "ermöglicht durch Cloud-native OS" unterschieden. Erstes besagt, dass das Lösungselement idealerweise bereits Feature bzw. Kernbestandteil der Betriebs- und Infrastrukturumgebung sein soll ("out-of-the-box"). Gleichzeitig ist die Betriebs- und Infrastrukturumgebung ein Cloud-natives "Betriebssystem" bzw. eine Cloud-native Laufzeitumgebung. Zweites besagt, dass die Cloud-native Laufzeitumgebung das Lösungselement grundsätzlich ermöglichen muss (z.B. durch einen Plugin-Mechanismus), ohne es selbst direkt bereitstellen zu müssen.

1794

Qualitätsanforderungen an die Ausfallsicherheit der Betriebs- und Infrastrukturumgebung:

1795

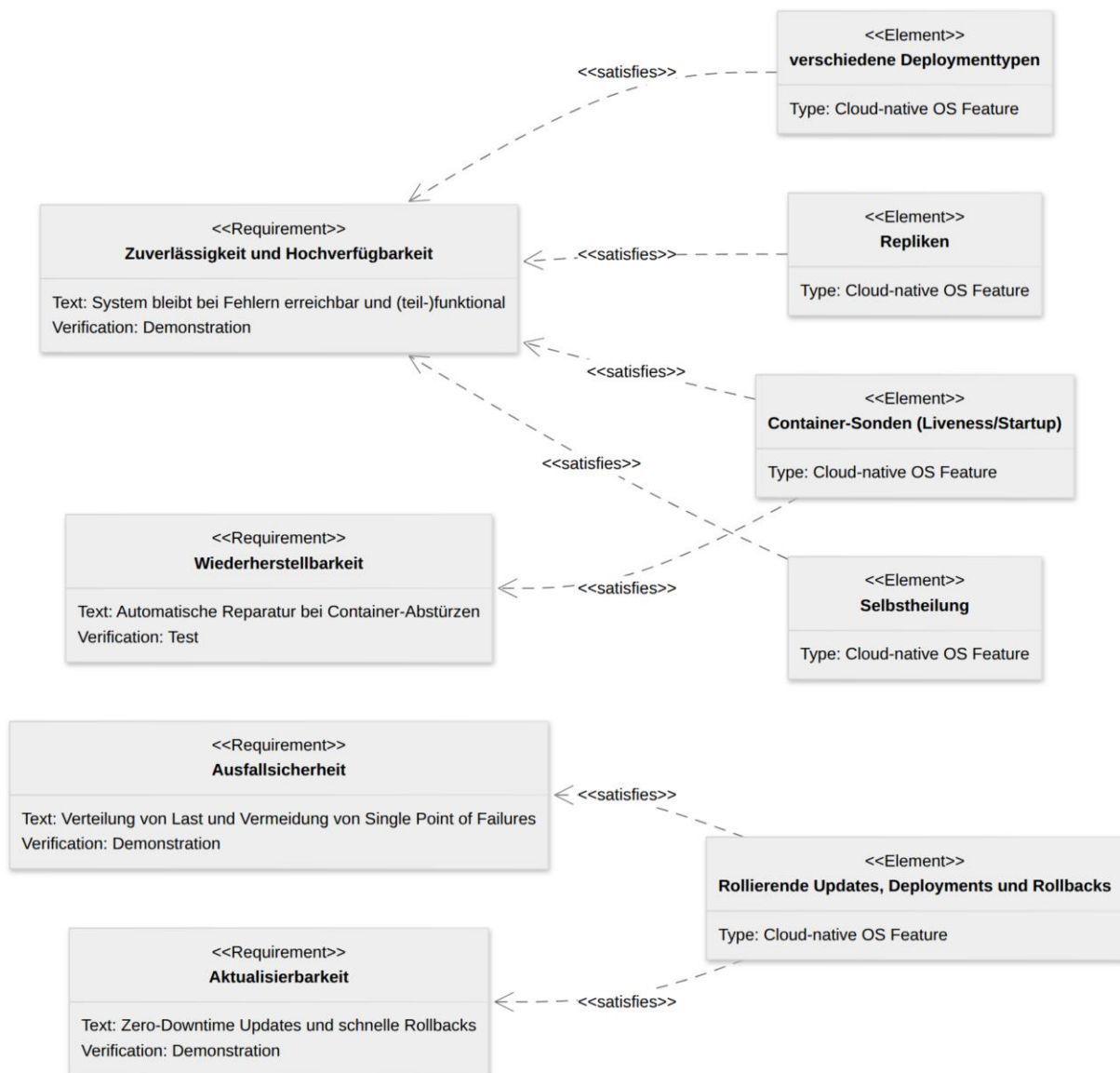


Abbildung 13: Qualitätsanforderungen an die Ausfallsicherheit der Betriebs- und Infrastrukturmgebung des NCPeH-Proxy

Qualitätsanforderungen an die Informationssicherheit der Betriebs- und Infrastrukturmgebung:

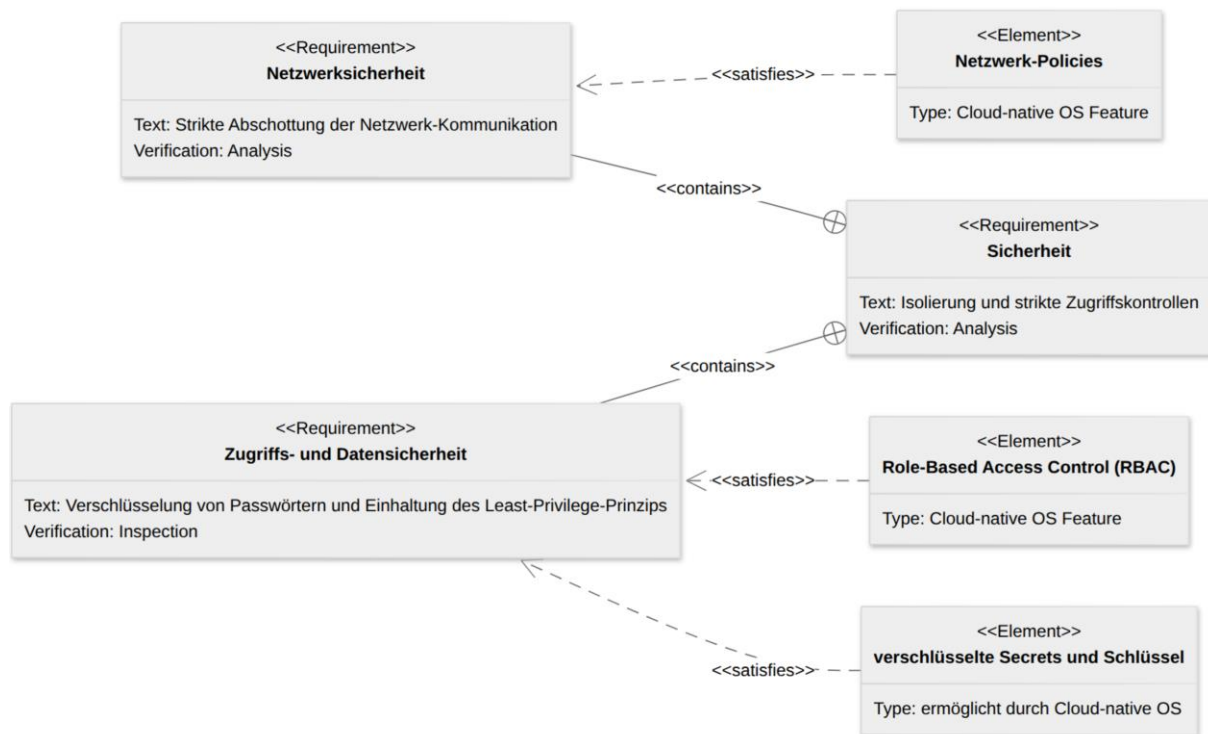


Abbildung 14: Qualitätsanforderungen an die Informationssicherheit der Betriebs- und Infrastrukturmgebung des NCPeH-Proxy

sonstige Qualitätsanforderungen an die Betriebs- und Infrastrukturmgebung:

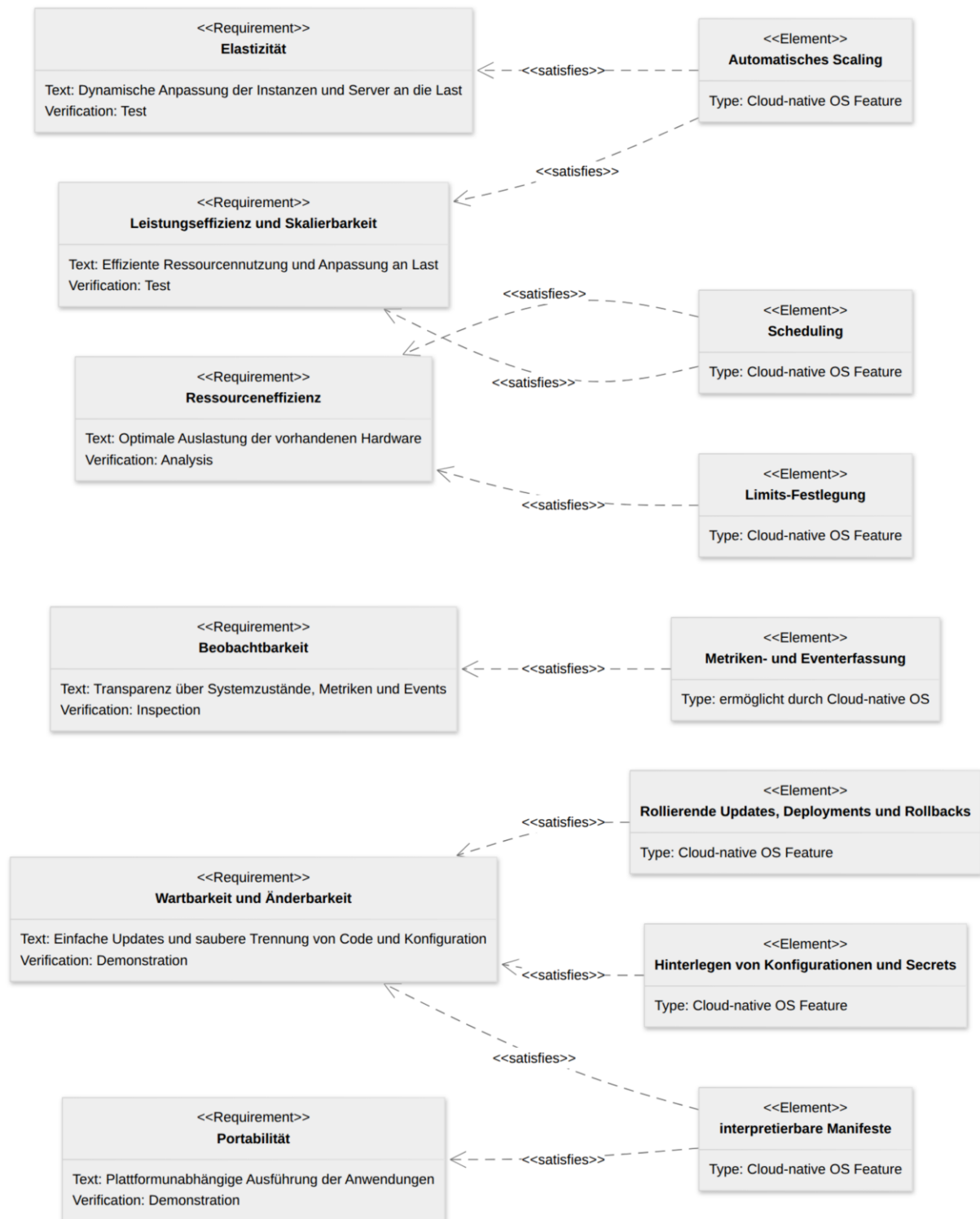


Abbildung 15: sonstige Qualitätsanforderungen an die Betriebs- und Infrastrukturumgebung des NCPeH-Proxy

8.2.6.1 Erweiterte Anforderungen an Confidential Computing

Die im vorherigen Abschnitt beschriebenen Qualitätsanforderungen und Leistungsmerkmale an eine Betriebs- und Infrastrukturmgebung ermöglichen eine spätere Migration der beschriebenen Gesamtlösung in eine ZETA-konforme Infrastruktur, die aus den in Abschnitt 6.1- Entscheidung für die Integration von ePeD-B in die Telematikinfrastruktur 1.0 genannten Gründen zur Zeit nicht konzipiert werden kann. Gleichzeitig muss sichergestellt sein, dass diese Cloud-native Infrastruktur

- über ein zu einer VAU-Umgebung (vgl. [gemSpec_NCPeH_FD#Anforderungen an die Vertrauenswürdige Ausführungsumgebung]) äquivalentes Maß an Sicherheitsleistung hinsichtlich Vertraulichkeit verfügt,
- mit anderen TI-Services bzw. -Produkten in einer Betriebsumgebung konsolidiert werden kann, die einen vergleichbar sehr hohen Sicherheits- und Schutzbedarf aufweisen (Nutzung synergetischer Effekte hinsichtlich Ressourcennutzung/-konsolidierung einerseits und Hochskalierfähigkeit der Betriebsplattform andererseits).

Zu diesen Zwecken ist der gesamte Lösungsansatz von Healthcare Confidential Computing gemäß [gemSpec_HCC] und dessen erreichter, finaler Definitionsstand von Q3/2026 als sichere, vertrauenswürdige und Ausführungsumgebung des NCPeH-Proxy vorzusehen. Eine bereits aufgebaute (und damit verfügbare), sichere, vertrauenswürdige Ausführungsumgebung gemäß [gemSpec_HCC] ist betrieblich und infrastrukturell durch die Komponente NCPeH-Proxy nachzunutzen bzw. mitzubenutzen.

Fallback

Aus folgenden Unwägbarkeiten heraus ist es nicht ausschließbar, dass die in den vorherigen Absätzen beschriebene, favorisierte Lösung für die sichere, vertrauenswürdige Ausführungsumgebung nicht oder noch nicht eingesetzt werden kann:

- projektplanerische Machbarkeit (inkl. Zeit-/Terminzielen, Abhängigkeiten),
- Auswertungsergebnisse von parallel stattfindender Markterkundung,
- Festlegungen zur Betreiberrolle.

Beim Eintreten einer solchen Unwägbarkeit sind zwei Fallback-Alternativen vorgesehen für sichere, vertrauenswürdige Ausführungsumgebungen (aufgelistet in der Reihenfolge der Machbarkeit):

1. Nachnutzung der VAU-Betriebsumgebung des NCPeH-FD, womit ein Wechsel des Anforderungshaushaltes von [gemSpec_HCC] hin zu [gemSpec_NCPeH_FD#Anforderungen an die Vertrauenswürdige Ausführungsumgebung] bzgl. der geforderten Sicherheitsleistung verbunden ist.
2. Aufbau, Betrieb und Nutzung einer neuen, eigens umzusetzenden sicheren, vertrauenswürdigen Ausführungsumgebung gemäß [gemSpec_HCC]. Hiermit ist kein Wechsel des Anforderungshaushaltes verbunden.

Zu betonen ist, dass diese beiden Fallback-Alternativen bzgl. der geforderten Sicherheitsleistung der zu schützenden Informationsobjekte mit dem Lösungsansatz zwar wirkungsgleich sind, jedoch

- Fallback-Alternative 1 nicht die in Abschnitt 8.2.6- Qualitätsanforderungen an Betrieb und Infrastruktur genannten Qualitätserforderungen für eine skalierfähige, hochverfügbare, moderne Cloud-Umgebung erfüllt und wenig nachhaltig ist,
- Fallback-Alternative 2 mit zusätzlichen Aufwänden an Anbieter/Betreiber hinsichtlich Implementierung und Bereitstellung der in [gemSpec_HCC]

1857 beschrieben Sicherheitsarchitektur, Plattformleistung und ggf. der Rolle als
1858 HCC-Provider verbunden ist.

1859 Keine Fallback-Alternative (und damit Out of Scope) ist hingegen eine zusätzliche VAU-
1860 Betriebsumgebung, die zwar den Anforderungen
1861 aus [gemSpec_NCPeH_FD#Anforderungen an die Vertrauenswürdige
1862 Ausführungsumgebung] genügt, aber individuell zu implementieren und zu betreiben
1863 wäre.

1864

1865 8.3 NCPeH-FD

1866 8.3.1 Zugang zum NCPeH-FD

1867 Die NCPeH-FD-Webschnittstellen für das Anwendungsszenario ePeD-B sind über das
1868 Internet zugänglich. Der Zugang zu den Schnittstellen des NCPeH-FD ist ausschließlich
1869 für den NCPeH-Proxy vorgesehen. Die Absicherung der Verbindungen zwischen NCPeH-
1870 FD und NCPeH-Proxy erfolgt mittels mTLS-Authentifizierung. Direkte
1871 Schnittstellenaufrufe von anderen Clients oder Systemen sind nicht zulässig und müssen
1872 vom NCPeH-FD aktiv blockiert werden.

1873 Die NCPeH-FD-Webschnittstellen für das Anwendungsszenario ePeD-B sind grundsätzlich
1874 über das Internet erreichbar. Der Zugriff auf diese Schnittstellen ist jedoch ausschließlich
1875 dem NCPeH-Proxy vorbehalten.

1876 Die Absicherung der Kommunikation zwischen NCPeH-FD und NCPeH-Proxy erfolgt mittels
1877 gegenseitiger TLS-Authentifizierung (mTLS). Direkte Schnittstellenaufrufe durch andere
1878 Clients oder externe Systeme sind nicht zulässig und müssen vom NCPeH-FD technisch
1879 unterbunden werden.

1880

1881 Zusätzlich zur Transportverschlüsselung wird der Austausch von E-Rezepten und
1882 Dispensierinformationen auf Anwendungsebene mittels ASL (Application Security Layer)
1883 verschlüsselt. Die Verschlüsselung erfolgt gemäß den Vorgaben des VAU-Protokolls
1884 ([gemSpec_Krypt#"ZETA/ASL (VAU-Protokoll)"]). Dabei agiert der NCPeH-FD in der Rolle
1885 als ASL-Server. Die verschlüsselte Payload wird in der WebApp des EU-Webportals im
1886 inneren Request des ASL-Kanals erzeugt und über den NCPeH-Proxy an den NCPeH-FD
1887 weitergeleitet. Dieser Payload kann ausschließlich vom NCPeH-FD entschlüsselt werden,
1888 wodurch die Daten vor unbefugtem Zugriff geschützt sind.

1889 8.3.2 Schnittstellen

1890 Der NCPeH-FD umfasst die eigentlichen Funktionen des Anwendungsszenarios ePeD-B
1891 wie in der folgenden Tabelle dargestellt.

1892 **Tabelle 5: Funktionale Webschnittstellen und Operationstypen des NCPeH-FD**

Funktionale Webschnittstellen	Operationstyp
I_Comm_ASL	Der NCPeH-FD stellt den Endpunkt dar, agiert in der Rolle als ASL-Server und tauscht die ASL-Schlüssel für das ASL-Protokoll mit dem EU-Webportal aus.

I_ISM_Service	Suchmasken der zulässigen Länder-A bereitstellen
I_Patient_Identification_Service	Demographischen Daten des EU-Bürgers abrufen
I_eHealth_Service	Verfügbare Gesundheitsdaten des EU-Bürgers auflisten
	Ausgewählte Gesundheitsdaten des EU-Bürgers abrufen
I_PZN_Service	Die Webschnittstelle antwortet auf empfangene und unterstützte Pharmazentralnummern (PZN) mit einer Liste, die detaillierte Informationen zu Wirkstoffen, Packungsgrößen, Darreichungsformen usw. enthält.
I_Provide_DocumentSet_Service	Dispensierinformationen übermitteln

1893

1894 8.3.2.1 I_Comm_ASL

1895 Der NCPeH-FD stellt für das Anwendungsszenario ePeD-B mehrere Webschnittstellen
 1896 bereit, die über das HTTPS-Protokoll erreichbar sind. Diese Schnittstellen dienen als
 1897 Eingangs- und Ausgangspunkte für Anfragen und Antworten, die mittels des NCPeH-
 1898 Proxy zwischen der WebApp des EU-Webportals und dem NCPeH-FD ausgetauscht
 1899 werden. Um die Vertraulichkeit und Integrität der personenbezogenen medizinischen
 1900 Daten zu gewährleisten, wird zusätzlich zur Transportverschlüsselung mittels TLS auf der
 1901 Anwendungsebene eine Ende-zu-Ende-Inhaltsverschlüsselung durch das ASL-Protokoll
 1902 implementiert.

1903 Die Anfragen, die über HTTPS an eine Webschnittstelle des NCPeH-FD gesendet werden,
 1904 werden intern an den VAU-Verarbeitungskontext (Verarbeitungskomponente für
 1905 verschlüsselte Inhalte) weitergeleitet. Dieser VAU-Verarbeitungskontext ist für die
 1906 Entschlüsselung, Verarbeitung und Verschlüsselung der Inhalte verantwortlich. Die
 1907 Antwort des VAU-Verarbeitungskontexts wird wiederum an die Webschnittstelle des
 1908 NCPeH-FD übergeben und über den NCPeH-Proxy zurück an die WebApp gesendet.

1909 Für weiterführende Informationen zur Nutzung der Webschnittstelle wird auf Kapitel
 1910 8.1.2.3- I_Comm_ASL verwiesen.

1911

1912 8.3.2.2 I_ISM_Service

1913 Die Webschnittstelle des NCPeH-FD stellt auf Anfrage des NCPeH-Proxy die aktuellen
 1914 International Search Masks (ISM) der zulässigen Länder-A bereit. Die ISMs definieren,
 1915 welche Identitätsattribute für die Identifizierung von EU-Bürgern in den jeweiligen
 1916 Zugehörigkeitsländern (Länder-A) verwendet werden. Diese Webschnittstelle ist ein
 1917 essentieller Bestandteil des Anwendungsszenarios ePeD-B und gewährleistet die korrekte
 1918 Bereitstellung der ISMs.

1919 Der NCPeH-FD verfügt über die Information der zulässigen europäischen Länder (Länder-
 1920 A), mit denen ein gegenseitiger Betrieb für den grenzüberschreitenden Austausch von
 1921 ePrescription/eDispensation besteht. Diese Liste wird vom Systemadministrator des

1922 NCPeH-FD gepflegt und regelmäßig aktualisiert. Sie dient als Grundlage für die
1923 Ermittlung der relevanten Länder, deren ISM abgerufen und bereitgestellt werden
1924 müssen.

1925 Der NCPeH-FD nutzt die Information über die zulässigen Länder-A, um einmal täglich die
1926 aktuellen ISM dieser Länder vom zentralen eHDSI Configuration Service herunterzuladen.
1927 Dieser Abruf erfolgt automatisiert oder auf Anfrage des Systemadministrators und stellt
1928 sicher, dass die im NCPeH-FD gespeicherten ISM stets auf dem neuesten Stand sind. Die
1929 heruntergeladenen ISM werden verschlüsselt im NCPeH-FD gespeichert.

1930 Auf eine Anfrage des NCPeH-Proxy an die Webschnittstelle des NCPeH-FD liefert der
1931 NCPeH-FD die gesamte Liste der aktuell gespeicherten ISM zurück. Da die ISM keine
1932 personenbezogenen oder schützenswerten Daten enthalten, ist es nicht erforderlich, dass
1933 die Anfrage Identitätsangaben oder Tokens einer WebApp oder LE-DE umfasst.

1934 Die Kommunikation zwischen dem NCPeH-Proxy und der Webschnittstelle des NCPeH-FD
1935 erfolgt über TLS v1.3.

1936 **8.3.2.3 I_Patient_Identification_Service**

1937 Die Webschnittstelle des NCPeH-FD verarbeitet Anfragen zur Bereitstellung von weiteren
1938 demographischen Daten des EU-Bürgers aus Land A. Die Anfrage wird durch den NCPeH-
1939 Proxy an den NCPeH-Fachdienst übermittelt und besteht aus einem äußeren sowie einem
1940 inneren Request.

1941 Der innere Request enthält die fachlichen Suchparameter, die zur eindeutigen Ermittlung
1942 demographischer Daten des EU-Bürgers erforderlich sind. Diese Suchparameter sind
1943 mittels ASL verschlüsselt, um die Vertraulichkeit der sensiblen personenbezogenen Daten
1944 sicherzustellen.

1945 Der äußere Request enthält ein vom NCPeH-Proxy elektronisch signiertes ID-Token.
1946 Dieses ID-Token umfasst relevante Identitätsmerkmale des LE-DE sowie der LE-LEI.
1947 Basierend auf den im ID-Token enthaltenen Informationsmerkmalen erstellt der NCPeH-
1948 FD eine SAML 2.0 Identity Assertion (IdA) für den LE-DE, sofern für den LE-DE im
1949 NCPeH-FD noch keine gültige IdA vorliegt. Die IdA wird durch den NCPeH-FD mit dem
1950 eigenen privaten eHDSI-SEAL-Schlüsselmaterial elektronisch signiert. Diese dient als
1951 Sicherheitsobjekt für diese und nachfolgende Kommunikation mit dem NCPeH Land A,
1952 daher wird sie in der VAU des NCPeH-FD gespeichert.

1953 Die Anfrage wird einschließlich der IdA und der fachlichen Suchparameter gemäß den
1954 Vorgaben der eHDSI sowie HL7 XCPD an den NCPeH Land A übermittelt. Der NCPeH Land
1955 A verarbeitet die Anfrage und liefert als Antwort:

- 1956 • weitere demographische Daten des EU-Bürgers
- 1957 • eine bestätigte, eindeutige Patientenidentifikation (Patient Identifier).

1958 Der NCPeH-FD nimmt diese Antwort entgegen, verarbeitet die enthaltenen Informationen
1959 und sendet sie gemäß der Beschreibung des Informationsmodells 8.4.2.3- Patient
1960 Demographics Response (Domain Identifier: patient_demographics_data) an die WebApp
1961 des LE-DE weiter.

1962 **8.3.2.4 I_eHealth_Service**

1963 Über die Webschnittstelle des NCPeH-FD werden zwei Operationen bereitgestellt:

- 1964 • Verfügbare Gesundheitsdaten des EU-Bürgers auflisten und
- 1965 • Ausgewählte Gesundheitsdaten des EU-Bürgers abrufen.

1966	Diese Operationen sind bewusst anwendungsneutral konzipiert, sodass sie unabhängig
1967	vom konkreten Anwendungsszenario wie beispielsweise ePeD-B genutzt und auch von
1968	zukünftigen Anwendungsszenarien wiederverwendet werden können.
1969	Mit Erhalt der Anfrage werden sowohl Identitätsdaten als auch fachliche Metadaten an die
1970	Webschnittstelle übermittelt. Zur Verarbeitung der Anfrage wertet der NCPeH-FD das im
1971	äußeren Request enthaltene ID-Token aus. Auf dieser Basis ermittelt er die zuvor
1972	erzeugte SAML 2.0 Identity Assertion (IdA) für den LE-DE. Diese Assertion wurde im
1973	Rahmen der Webschnittstelle <u>8.3.2.3- I_Patient_Identification_Service</u> erzeugt.
1974	Zusätzlich generiert der NCPeH-FD eine weitere SAML 2.0 Assertion, (TRC Assertion).
1975	Diese dient gegenüber dem anfragenden NCPeH Land-A als elektronischer Nachweis einer
1976	bestehenden Behandlungsbeziehung zwischen LE-DE und dem EU-Bürger. Die TRC
1977	Assertion wird durch den NCPeH-FD mit dem eigenen privaten eHDSI-SEAL-
1978	Schlüsselmaterialelektronisch signiert, um deren Integrität und Authentizität
1979	sicherzustellen. Der innere Request der gesamten Anfrage enthält darüber hinaus die
1980	fachlichen Nutzdaten, insbesondere:
1981	<ul style="list-style-type: none"> • LOINC-Code zur eindeutigen Identifikation des Anwendungskontexts,
1982	<ul style="list-style-type: none"> • Ländercode des Land A,
1983	<ul style="list-style-type: none"> • Patient Identifier (vom Land A bestätigte eindeutige Kennung des EU-Bürgers),
1984	<ul style="list-style-type: none"> • optionale Zugriffsinformationen zur Dokumentensuche.
1985	Operation: Verfügbare Gesundheitsdaten des EU-Bürgers auflisten (im Kontext
1986	ePeD-B)
1987	Im Rahmen dieser Operation mit Kontext auf das Anwendungsszenario ePeD-B werden
1988	die Daten einschließlich IdA und TRC Assertion gemäß den Vorgaben der eHDSI und dem
1989	IHE XCA.Query Profil an den NCPeH Land A übermittelt. Der NCPeH Land A verarbeitet
1990	die Anfrage und liefert als Antwort die relevanten Metadaten zu den einlösbaren E-
1991	Rezepten des EU-Bürgers zurück. Der NCPeH-FD bereitet diese Metadaten entsprechend
1992	dem Informationsmodell <u>8.4.2.5- Query Response (Domain Identifier:</u>
1993	<u>list_available_prescription)</u> auf und sendet sie an die WebApp des anfragenden LE-DE.
1994	Operation: Ausgewählte Gesundheitsdaten des EU-Bürgers abrufen (im Kontext
1995	ePeD-B)
1996	Für den Abruf ausgewählter E-Rezepte übermittelt der NCPeH-FD eine Anfrage mit den
1997	zuvor erhaltenen und durch den Leistungserbringer ausgewählten Metadaten an das
1998	entsprechende Land A. Auch diese Anfrage enthält die erforderlichen
1999	Sicherheitsartefakte, die IdA sowie die TRC Assertion, und wird gemäß den Vorgaben von
2000	eHDSI und dem IHE XCA.Retrieve Profil an den NCPeH Land A gesendet. Der NCPeH Land
2001	A stellt daraufhin die entsprechenden E-Rezepte bereit. Der NCPeH-FD übernimmt die
2002	Entgegennahme und leitet die E-Rezepte im Nachrichtenformat gemäß dem
2003	Informationsmodell in <u>8.4.2.7- Retrieve Response (Domain Identifier:</u>
2004	<u>list_prescription_retrieved)</u> an die WebApp des LE-DE weiter.
2005	8.3.2.5 I_PZN_Service
2006	Die Webschnittstelle I_PZN_Service dient der technischen Unterstützung des LE-DE bei
2007	der Erfassung von Dispensierinformationen im EU-Webportal. Ziel der Schnittstelle ist es,
2008	dem LE-DE bei der Eingabe von Pharmazentralnummern (PZN) zusätzliche Sicherheit zu
2009	geben, indem zu jeder eingegebenen PZN geprüfte Arzneimittelinformationen angezeigt
2010	werden. Hierdurch wird die korrekte Identifikation des Arzneimittelprodukts unterstützt
2011	und das Risiko von Fehleingaben im grenzüberschreitenden Datenaustausch reduziert.

2012 Die PZN ist ein bundeseinheitlicher, nationaler Identifikationsschlüssel für in deutschen
2013 Apotheken vertriebene Arzneimittel, Medizinprodukte und weitere apothekenübliche
2014 Produkte. Jede Arzneimittelpackung wird durch eine achtstellige numerische Kennung
2015 eindeutig identifiziert, die u. a. Produktbezeichnung, Darreichungsform und
2016 Packungsgröße referenziert. Da die PZN ausschließlich innerhalb Deutschlands verwendet
2017 wird und in anderen europäischen Staaten nicht direkt interpretierbar ist, ist für den
2018 grenzüberschreitenden Datenaustausch eine Validierung und inhaltliche Anreicherung
2019 notwendig.

2020 Das EU-Webportal übermittelt im Rahmen der Dispensierung eine oder mehrere PZN an
2021 die Webschnittstelle I_PZN_Service. Nach Eingang der Anfrage prüft der NCPeH-FD über
2022 den I_PZN_Service, ob die empfangenen PZN fachlich und technisch unterstützt werden
2023 können. Hierzu werden die PZN automatisiert validiert und gegen die relevanten
2024 nationalen Referenzdaten geprüft.

2025 Die für die Prüfung und Anreicherung der PZN erforderlichen Informationen zu
2026 Arzneimittelzulassungen werden aus der LTR (Local Terminology Repository) des NCPeH-
2027 FD herangezogen. Diese enthält die amtlich geprüften und autorisierten Zulassungsdaten
2028 sowie produktbezogene und regulatorische Metadaten zu zugelassenen Arzneimitteln, wie
2029 beispielsweise Handelsname, Zulassungsnummer, Zulassungsstatus und weitere
2030 relevante Metadaten.

2031 Die Validierung der PZN und die fachliche Ableitung der Produktinformationen erfolgen
2032 auf Basis der vom BfArM bereitgestellten Mapping- und Transferregeln. Diese Regeln
2033 stellen sicher, dass die abgeleiteten Informationen den regulatorischen Vorgaben
2034 entsprechen und konsistent im NCPeH-Datenaustausch verwendet werden können.

2035 Bei erfolgreich validierten PZN leitet der NCPeH-FD die erforderlichen nationalen
2036 Arzneimittelinformationen ab. Die angereicherten Produktinformationen werden als
2037 strukturierte Antwort an das EU-Webportal zurückgegeben und dort dem LE-DE
2038 angezeigt.

2039 Hinweis:

2040 Das BfArM prüft derzeit, ob die bestehende Vereinbarung mit der Informationsstelle für
2041 Arzneyspezialitäten (IFA) zur Nutzung von Zuordnungsinformationen zwischen
2042 Pharmazentralnummern (PZN) und den jeweiligen nationalen Zulassungsnummern von
2043 Arzneimitteln auch für den vorgesehenen Einsatz im Rahmen der Webschnittstelle
2044 I_PZN_Service zulässig ist. Sofern die aktuelle Vereinbarung diesen spezifischen
2045 Nutzungszweck nicht hinreichend abdeckt, ist die Notwendigkeit einer gesonderten
2046 vertraglichen Regelung zur rechtssicheren Bereitstellung und Verwendung der
2047 entsprechenden Zuordnungsdaten im Kontext des NCPeH-FD und der Webschnittstelle
2048 I_PZN_Service zu bewerten und gegebenenfalls herbeizuführen.

2049 **8.3.2.6 I_Provide_DocumentSet_Service**

2050 Die vorliegende Webschnittstelle ist anwendungsneutral konzipiert, sodass sie
2051 unabhängig von konkreten Anwendungsszenarien wie ePeD-B genutzt und auch für
2052 zukünftige Anwendungsszenarien wiederverwendet werden kann.

2053 Über diese Schnittstelle werden Gesundheitsdaten entgegengenommen, die durch den
2054 LE-DE innerhalb der WebApp des EU-Webportals erstellt wurden und zur
2055 Weiterverarbeitung an ein Land A übermittelt werden sollen.

2056 Im Rahmen der Nutzung des Dienstes eDispensation erstellt der LE-DE während der
2057 Medikamentenabgabe sogenannte Dispensierinformationen. Diese enthalten relevante
2058 Angaben zur erfolgten Abgabe eines Medikaments an einen EU-Bürger. Die
2059 Dispensierinformationen, bestehend aus PZN-Angaben, werden in der WebApp des LE-DE

2060 erfasst und übermittelt diese in einer Anfrage über den NCPeH-Proxy an die
2061 Webschnittstelle des NCPeH-FD.

2062 Der innere Request der Anfrage enthält die PZN (zur eindeutigen Identifikation von
2063 Dispensierinformationen), demographische Daten des EU-Bürgers sowie einen LOINC-
2064 Code (zur eindeutigen Identifikation des Anwendungskontexts). Auf Basis des LOINC-
2065 Codes erkennt der NCPeH-FD eindeutig, dass es sich um eine Transaktion im Kontext der
2066 Anwendung eDispensation handelt. In der Folge validiert der NCPeH-FD die PZN und
2067 leitet die kodierten Arzneimittelinformationen auf Basis der vom BfArM bereitgestellten
2068 Mappingregeln ab. Um die Dispensierinformationen für den eHDSI-Datenaustausch und
2069 im Land A semantisch nutzbar zu machen, transkodiert der NCPeH-FD die ermittelten
2070 und kodierten Arzneimittelinformationen gemäß BfArM-Mappingregeln.

2071 Anschließend übermittelt der NCPeH-FD die Dispensierinformationen konform zu den
2072 Vorgaben der eHDSI und des IHE XDR Profils an den zuständigen NCPeH Land A.

2073 Der NCPeH Land A verarbeitet die übermittelten Daten und liefert eine Rückmeldung über
2074 den Bearbeitungsstatus der Dispensierinformationen, insbesondere hinsichtlich des
2075 Erfolgs oder möglicher Fehler. Der NCPeH-FD nimmt diese Antwort entgegen, verarbeitet
2076 sie und stellt das Ergebnis über die Webschnittstelle der WebApp des anfragenden LE-DE
2077 zur Verfügung.

2078

2079 8.4 Informationsmodell

2080 8.4.1 Domänenmodell für Land-B-Szenarien

2081 Das Informationsmodell basiert auf dem Domänenkonzept. Die Domäne beschreibt das
2082 gesamte Problemfeld, das es - gestützt durch IT-Systeme - zu lösen gilt. Da diese
2083 Hauptdomäne zu komplex ist, um sie als Ganzes in einem einzigen "Software-Block"
2084 abzubilden, wird sie in kleinere, handhabbare Bausteine zerlegt, die sog. Sub-
2085 Domänen. Diese sind logische, fachliche Teilbereiche der Hauptdomäne. Sie helfen dabei,
2086 die Komplexität zu reduzieren und das Gesamtsystem besser zu verstehen.

2087 Folgende Sub-Domänen unterschiedlichen Typs werden für das Feature unterschieden:

Sub-Domäne	Typ	zugehörige Domänenobjekte
siehe [subdomains.yaml] Die Zuordnung einer Sub-Domäne zu ihrem Typ erfolgt jeweils über das "type"-Attribut.	Core / Supporting / Generic	siehe [domainobj-eped-b.yaml] Die Zuordnung von Domänenobjekten zu Subdomains erfolgt jeweils über das "x-subdomains"-Attribut.

2088 Die Sub-Domänen können nach ihrem strategischen Wert für die Erfüllung des Szenarios
2089 aus dieser Feature-Beschreibung (und folgender Szenarien) nach Typen "Core Domain",
2090 "Supporting Domain" und "Generic Domain" klassifiziert werden.

2091 Daraus ergeben sich folgende Implikationen, unterschieden nach Sub-Domärentyp:

2092 Typ "Core":

- 2093 • Hier sind Alleinstellungsmerkmale und hoher Geschäftswert (Business Value) in
2094 der Umsetzung des Szenarios vorhanden.

- 2095 • Hier entsteht höchster Zugewinn, wenn hier alles fehlerfrei und gemäß der
- 2096 Qualitätsvorgaben umgesetzt wird.
- 2097 • Hier entsteht höchster Schaden, wenn es hier zu Qualitätsproblemen kommt.
- 2098 • Hier ist besonders auf eine hochwertige, saubere Software-Architektur zu achten.

2099 Typ "Supporting":

- 2100 • Hier werden die Grundlagen geschaffen, damit Sub-Domänen vom Typ "Core"
- 2101 funktionieren können, ohne i.d.R. selbst einen eigenen Mehrwert zu liefern.
- 2102 • Wird in der Regel als Eigenentwicklung durchgeführt, jedoch mit dem Fokus auf
- 2103 schlanke bzw. aufwandsarme Umsetzung.

2104 Typ "Generic":

- 2105 • Subdomänen dieses Typs bringen keinen Geschäftswert, sondern sind notwendig,
- 2106 weil sonst das Szenario nicht sinnvoll funktionieren kann.
- 2107 • Es wird versucht, entweder Eigenimplementierungen ganz zu vermeiden oder
- 2108 vollständig die Implementierungen Dritter zu konsumieren und diese
- 2109 entsprechend zu integrieren.

2110 Die Einteilung in Sub-Domänen und die Klassifizierung dieser geben Orientierung beim

2111 Zuschnitt der Zielarchitektur (Umsetzung).

2112 8.4.2 Externe Informationsmodelle

2113 Die in diesem Kapitel beschriebenen Informationsmodelle gelten für den Datenaustausch

2114 zwischen dem EU-Webportal, NCPeH-Proxy und NCPeH-FD. Die beschriebenen

2115 Informationsmodelle basieren auf dem aktuellen fachlichen und technischen Stand.

2116 Zukünftige normative Anforderungen aus der EHDS-Verordnung sowie dem zugehörigen

2117 Implementing Act insbesondere in Bezug auf Schnittstellen und Nachrichtenformate

2118 sowie die verpflichtende Nutzung von FHIR-Profilen können Auswirkungen auf diese

2119 Modelle haben. Eine Angleichung an die entsprechenden EHDSI-Vorgaben ist in einer

2120 späteren Umsetzungsstufe vorgesehen.

2121 Die Zuordnung der externen Informationsmodelle zum 8.4.1.- Domänenmodell für Land-

2122 B-Szenarien erfolgt über das "x-external-reference"-Attribut am jeweiligen

2123 Domänenobjekt in [[domainobj-eped-b.yaml](#)].

2124 8.4.2.1 International Search Mask (Domain Identifier:

2125 list_ism_international)

2126 Das Informationsmodell für die International Search Mask (ISM) ist definiert und bereits

2127 im Wirkbetrieb mehrerer EU-Mitgliedstaaten im Rahmen der eHDSI eingesetzt. Die

2128 Definition der ISM erfolgte in Zusammenarbeit zwischen dem eHDSI Solution Provider

2129 und den beteiligten Mitgliedstaaten.

2130 Das zugehörige XSD-Schema ist unter folgendem Link verfügbar: [eHDSI_ISM_XSD].

2131 Für den Transport mehrerer ISM-Dokumente zwischen NCPeH-FD, NCPeH-Proxy und EU-

2132 Webportal wird eine auf FHIR basierende Transportstruktur verwendet. Hierbei dient die

2133 Ressource `Bundle` mit dem Typ `collection` als technischer Container für mehrere

2134 voneinander unabhängige Ressourcen, ohne dass zwischen ihnen eine transaktionale

2135 oder semantische Abhängigkeit besteht.

2136 Für jede einzelne ISM wird innerhalb des Bundles eine eigene FHIR Ressource `Entry`

2137 erzeugt, die jeweils eine Instanz der FHIR-Ressource `Binary` enthält. Die `Binary`-

2138 Ressource dient dabei als generischer Container für nicht-FHIR-konforme Inhalte und
2139 ermöglicht den Transport beliebiger Datenformate innerhalb einer FHIR-basierten REST-
2140 Schnittstelle.

2141 Das ISM-Dokument im XML-Format wird base64-kodiert in die FHIR Ressource
2142 aufgenommen.

2143 **8.4.2.2 Patient Demographics Query Request (Domain Identifier:** 2144 **patient_identification_query)**

2145 Die Erstellung der Abfragenachricht basiert auf den Vorgaben der ISM des jeweiligen
2146 Land A. Die ISM definiert, welche Identitätsmerkmale eines EU-Bürgers für eine Suche
2147 nach seinen demographischen Daten übermittelt werden müssen. Diese Angaben werden
2148 durch den LE-DE manuell im EU-Webportal erfasst. In diesem Kontext agiert das
2149 EU-Webportal gemäß IHE-Terminologie als Patient Demographics Consumer. Auf
2150 Grundlage dieser Informationen generiert das EU-Webportal die strukturierte
2151 Abfragenachricht. Die Anfrage kann beispielsweise Angaben wie Patientenidentifizier, Vor-
2152 und Nachname, Geburtsdatum, Geburtsort, Wohnadresse oder Geschlecht enthalten.

2153 Die fachliche Struktur der Abfragenachricht basiert auf dem HL7-v3-
2154 Nachrichtenmodell `PRPA_MT201306UV02("Patient Registry Query by Demographics")`
2155 gemäß [ITI-55] und ist ausschließlich konform zum
2156 Element `PRPA_MT201306UV02.ParameterList` entsprechend den Vorgaben des
2157 zugehörigen XSD-Schemas [`PRPA_MT201306UV02.xsd`].

2158 Für den Transport vom EU-Webportal zum NCPeH-FD innerhalb der FHIR-basierten
2159 Kommunikation wird die `ParameterList`-Abfragenachricht base64-kodiert in eine Instanz
2160 der FHIR-Ressource `Binary` aufgenommen.

2161 **8.4.2.3 Patient Demographics Response (Domain Identifier:** 2162 **patient_demographics_data)**

2163 Die vom Land A des EU-Bürgers bereitgestellten demographischen Daten unterstützen
2164 den LE-DE dabei, die übermittelten Angaben mit den Daten des vorgelegten
2165 Ausweisdokuments abzugleichen und den Identifikationsprozess des EU-Bürgers im
2166 Rahmen des eHDSI abzuschließen.

2167 Die fachliche Struktur der Antwortnachricht basiert auf dem HL7-v3-Nachrichtenmodell
2168 `PRPA_MT201310UV02 ("Patient Registry Find Candidates Query Response")` gemäß
2169 [ITI-55] und ist insbesondere konform zur Struktur des
2170 Elementes `PRPA_MT201310UV02.Patient` gemäß dem zugehörigen XSD-Schema
2171 [`PRPA_MT201310UV02.xsd`]. Die Nachricht kann demographische Angaben wie
2172 Patientenidentifizier, Name, Geburtsdatum, Geschlecht oder weitere Identitätsmerkmale
2173 enthalten, die für die abschließende Patientenidentifikation relevant sind.

2174 Für den Transport innerhalb der FHIR-basierten Kommunikation wird die
2175 Antwortnachricht base64-kodiert in einer Instanz der FHIR Ressource `Binary` abgelegt,
2176 die als generischer Container für nicht-FHIR-konforme Inhalte dient.

2177 **8.4.2.4 Query Request**

2178 Die Anfrage zur Auflistung einlösbarer E-Rezepte des EU-Bürgers aus Land A sieht keine
2179 Übermittlung eines Payloads an den NCPeH-FD. Stattdessen werden die notwendigen
2180 Angaben, etwa der Patienten Identifizier, der LOINC-Code für die Anwendung ePrescription
2181 sowie der Ländercode des Land A als Suchparameter in der URL der Anfrage an NCPeH-
2182 FD übergeben.

2183 Aus diesem Grund enthält dieses Unterkapitel kein eigenes Informationsmodell.

2184 **8.4.2.5 Query Response (Domain Identifier: list_available_prescription)**

2185 Als Antwort auf eine Query-Anfrage zur Auflistung einlösbarer elektronischer Rezepte des
2186 EU-Bürgers übermittelt das Land A die relevanten Metadaten zu den verfügbaren E-
2187 Rezepten. Diese Metadaten dienen dem EU-Webportal dazu, die vorhandenen E-Rezepte
2188 darzustellen und dem LE-DE eine Auswahl der einzulösenden E-Rezepte zu ermöglichen.

2189 Die fachliche Struktur der Antwortnachricht basiert auf dem IHE-Profil Cross Gateway
2190 Query Response im Rahmen des Profils Cross-Community Access (XCA). Die Syntax und
2191 Semantik der Nachricht entsprechen dabei den Vorgaben der
2192 [eHDSI_XCA_Profile#"FindDocuments Response Message"] sowie dem [ITI-38]. Kodierte
2193 Inhalte können um entsprechende Transkodierungen ergänzt werden, die vom NCPeH-FD
2194 gemäß den Vorgaben des BfArM erzeugt und in die Antwortnachricht integriert werden.

2195 Für den Transport innerhalb der FHIR-basierten Kommunikation wird die XCA.Query-
2196 Antwortnachricht base64-kodiert in einer Instanz der FHIR Ressource `Binary` abgelegt.

2197 **8.4.2.6 Retrieve Request (Domain Identifier: 2198 list_selected_prescription_retrieval)**

2199 Im Kontext des Abrufs von E-Rezepten des EU-Bürgers wird die Anfragenachricht im EU-
2200 Webportal erzeugt. Grundlage für die Struktur und Semantik der Anfrage bildet das
2201 Informationsmodell für die Operation der IHE XCA.Retrieve. Diese definiert das
2202 Nachrichtenformat.

2203 Im EU-Webportal wählt der LE-DE gezielt diejenigen E-Rezepte aus, die aus dem Land A
2204 abgerufen werden sollen. Für jedes ausgewählte elektronische Rezept werden die
2205 entsprechenden bereits abgerufenen Metainformationen übernommen. Dazu gehören der
2206 eindeutige ePrescriptionId. sowie weitere Identifikatoren, die im Rahmen des IHE XCA
2207 Profils zur eindeutigen Referenzierung des Dokuments im Land A erforderlich sind, wie
2208 beispielsweise RepositoryUniqueId, DocumentUniqueId und HomeCommunityId. Für die
2209 ausgewählten E-Rezepte werden diese Metadaten innerhalb der Anfragenachricht in Form
2210 mehrerer `DocumentRequest`-Elemente abgebildet, wodurch der gleichzeitige Abruf
2211 mehrerer ePrescriptions innerhalb einer einzelnen Retrieve-Anfrage ermöglicht wird.

2212 Zur Integration in eine FHIR-basierte Kommunikation wird die XCA.Retrieve Nachricht
2213 base64-kodiert und als Payload in einer Instanz der FHIR-Ressource `Binary` eingebettet.

2214 **8.4.2.7 Retrieve Response (Domain Identifier: 2215 list_prescription_retrieved)**

2216 Als Antwort auf eine Retrieve-Anfrage zum Abruf ausgewählter E-Rezepten des EU-
2217 Bürgers übermittelt das Land A die E-Rezepte. Die Antwort entspricht
2218 dem Nachrichtentyp `RetrieveDocumentSetResponse` und erfüllt die Vorgaben aus [ITI-
2219 43#3.43.4.2]. Die Antwort kann mehrere E-Rezepte enthalten. Das Informationsmodell
2220 der bereitgestellten E-Rezeptformate ist durch die eHDSI in
2221 [eHDSI_CDA_ePrescription_L1] und [eHDSI_CDA_ePrescription_L3] definiert. Die E-
2222 Rezepte, die dem Dokumentenformat [eHDSI_CDA_ePrescription_L3] entsprechen,
2223 werden im NCPeH-FD gemäß BfArM-Vorgaben transkodiert.

2224 Für den Transport innerhalb der FHIR-basierten Kommunikation wird die komplette IHE
2225 XCA.Retrieve-Antwortnachricht als base64-kodiert in einer Instanz der FHIR Ressource
2226 `Binary` angehängt.

8.4.2.8 Dispensierdokumente (Domain Identifier: list_dispensation_documents)

Das fachliche Informationsmodell der Dispensierdokumente ist durch die eHDSI definiert und normativ in [eHDSI_CDA_eDispensation] beschrieben. Es legt die inhaltliche Struktur und Semantik der CDA-basierten Dispensierdokumente fest, die im Rahmen der grenzüberschreitenden E-Rezept-Abwicklung verwendet werden.

Die CDA-Dispensierdokumente enthalten sowohl administrative als auch medizinische Informationen. Dazu gehören insbesondere Angaben zum Patienten, zum Autor des Dokuments (LE-DE), der eindeutige Prescription Identifier sowie die kodierten Dispensierinformationen als medizinische Angaben zu den tatsächlich abgegebenen Arzneimitteln. Die Dispensierinformationen umfassen unter anderem den Produktnamen, den Wirkstoff, die Darreichungsform sowie die Darreichungsstärke des abgegebenen Arzneimittels.

Die Generierung der CDA-Dispensierdokumente erfolgt im NCPeH-FD gemäß den Vorgaben aus [eHDSI_CDA_eDispensation]. Da die PZN ausschließlich in Deutschland verwendet wird und in anderen europäischen Ländern nicht interpretierbar ist, muss der NCPeH-FD auf Basis der jeweiligen PZN jedes abzugebendes E-Rezeptes eines EU-Bürgers entsprechende nationale sowie eHDSI-konforme Transkodierungen der Dispensierinformationen ableiten. Diese Transkodierungen erfolgen gemäß den Vorgaben des BfArM und werden anschließend in das CDA-Dispensierdokument integriert.

Da die Erstellung der CDA-Dispensierdokumente im NCPeH-FD durch die Vorgaben des BfArM gesteuert wird, erfolgt die detaillierte Abstimmung der zu übertragenden Daten und Datenstrukturen an der jeweiligen Schnittstelle erst im Rahmen der nachfolgenden Spezifikation.

8.5 Use Cases

8.5.1 Use Case zur Initialisierung der Webapp

AF_10436 -Basis-Initialisierung der WebApp und der Kommunikation

Attribute	Bemerkung
Beschreibung	<p>Der Use Case beschreibt</p> <ul style="list-style-type: none"> den grundsätzlichen Aufruf der WebApp des EU-Webportals durch den LE-DE, die Initialisierung der WebApp, die Basis-Basisvalidierungen, die vor Benutzung durch den LE-DE erfolgreich abgeschlossen sein müssen, die Basis-Kommunikationskanäle. <p>Bei den Basis-Kommunikationskanälen (Boxen mit orangefarbenen Header) wird der späteste Zeitpunkt gezeigt, zu welchem der jeweilige Kommunikationskanal verfügbar sein muss, damit die anschließenden Ablaufschritte wie beschrieben stattfinden können.</p>
Vorbedingung	siehe Sequenzdiagramm, obere Partition (inkl. Constraints)

Nachbedingung	<ul style="list-style-type: none">• API-Requests können über bestehende Basis-Kommunikationskanäle gesendet und API-Responses empfangen werden.• Bestehende Kommunikationskanäle werden wiederbenutzt (Connection Pooling, Session Resumption) und werden im Bedarfsfall erneut aufgebaut.
---------------	---

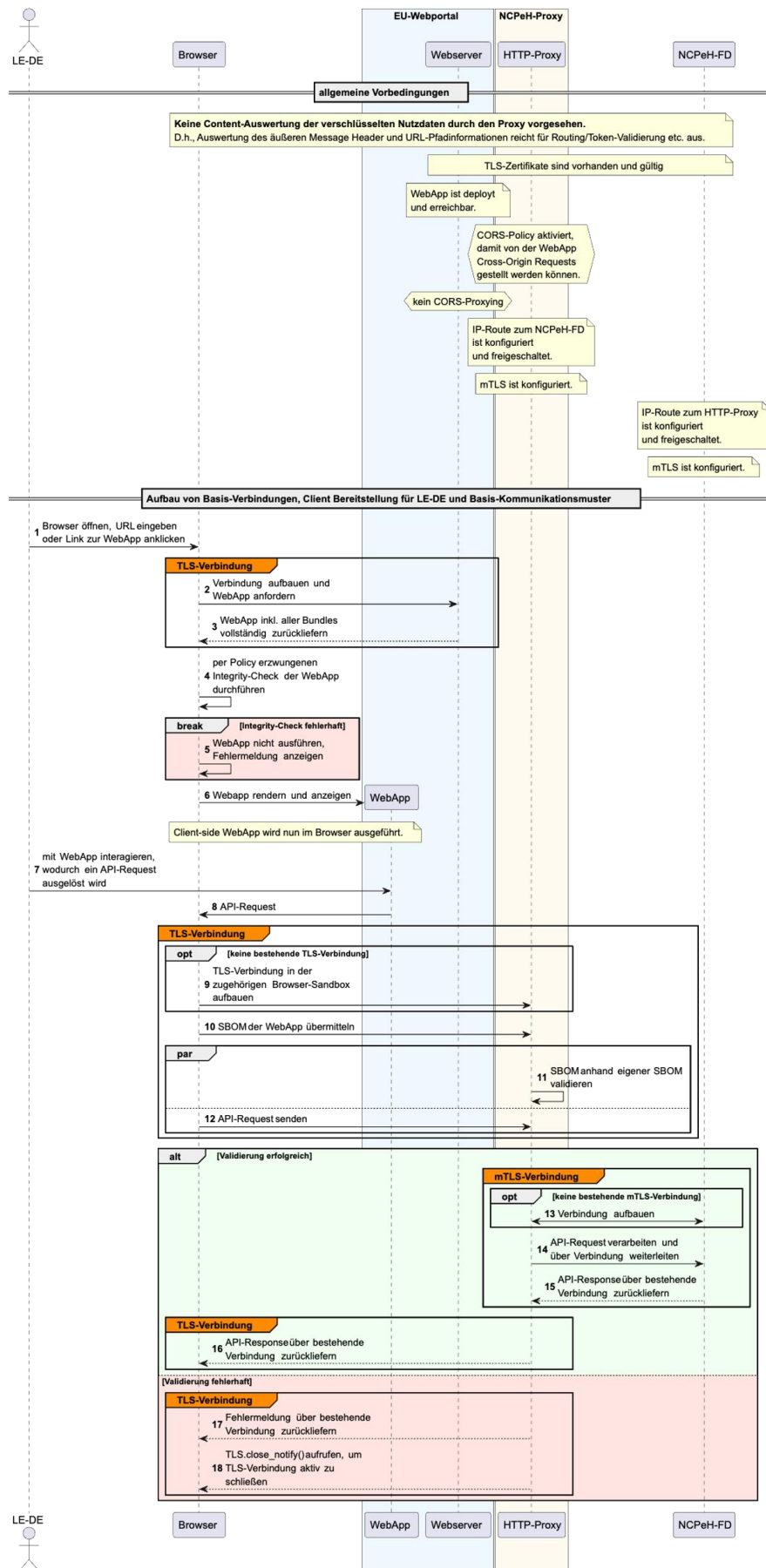


Abbildung 16: Sequenzdiagramm - Basis-Initialisierung der WebApp und der Kommunikation

[<=]

Vollständige Ansicht der hochauflösenden Version des Sequenzdiagramms:

https://github.com/gematik/api-ncpeh/blob/master/images/feature/eped-b/common/basic-init_seq.svg

8.5.2 Use Cases im Rahmen der Authentifizierung, Autorisierung

8.5.2.1 Authentifizierung und Autorisierung des LE-DE

AF_10429 -Authentifizierung und Autorisierung des LE-DE

	Authentifizierung und Autorisierung des LE-DE
Beschreibung	<p>Der Use Case beschreibt, wie sich ein Nutzer (LE-DE) gegenüber dem NCPeH-FD legitimiert, um grenzüberschreitende Gesundheitsdienste dieses Szenarios zu nutzen. Kern des Verfahrens ist ein Decoupled-Auth-Flow, bei dem die Weboberfläche und die eigentliche Identitätsprüfung (via gematik Authenticator) entkoppelt voneinander stattfinden. Die Schutzleistung wird durch DPOP (Demonstrating Proof-of-Possession) und PKCE verbessert.</p> <p>Phase 1: Initiierung und Decoupled Request (Partitionen 1 und 5) Das EU-Webportal generiert ein lokales Schlüsselpaar und sendet einen Decoupled Auth Request an den NCPeH-Proxy. Dieser erzeugt eine <code>auth_req_id</code> sowie PKCE-Parameter und liefert eine <code>poll_uri</code> zurück. Das EU-Webportal verbleibt ab diesem Zeitpunkt in einer Polling-Schleife, um auf den Abschluss der Authentifizierung zu warten. Zum Abschluss der Authentifizierung erhält das EU-Webportal die <code>auth_req_id</code>.</p> <p>Phase 2: Authentifizierung (Partitionen 2-4) Parallel zum Polling öffnet der Nutzer den gematik Authenticator (via Deeplink). In einer Schleife erfolgt die Authentifizierung für beide Smartcards (HBA und SMC-B):</p> <ol style="list-style-type: none"> 1. Consent: Der Nutzer erteilt die Zustimmung zur Identitätsdaten-Übermittlung. 2. Karteninteraktion: Der Konnektor signiert eine Challenge (ggf. nach PIN-Eingabe am Kartenterminal). 3. Token Exchange: Der IDP validiert die Signatur und stellt einen <code>AUTH_CODE</code> aus. Der NCPeH-Auth-Service tauscht diesen Code beim IDP gegen ein ID-Token ein. <p>Phase 3: erneuter Token-Tausch und Policy-Prüfung (Partition 5) Sobald die ID-Tokens für beide Karten vorliegen, führt der Auth-Service interne Prüfungen durch:</p> <ul style="list-style-type: none"> • Access-Token-Generierung: Prüfung der Rollen und Claims aus

	<p>den ID-Tokens. Erstellung eines spezifischen ncpehprx_access_token.</p> <ul style="list-style-type: none"> • Claims-Mapping: Die Claims werden in ein ID-Token als IdA-Vorstufe transformiert, welcher für den Zugriff auf den NCPeH-FD benötigt wird.
Vorbedingung	<ul style="list-style-type: none"> • Browser geöffnet • URL des EU-Webportals aufgerufen
Nachbedingung	<p>Das EU-Webportal erhält im Rahmen des Pollings das fertige Access-Token (gebunden an den DPoP-Schlüssel). Mit dem Vorhandensein dieses Tokens und des ID-Tokens (IdA-Vorstufe) wird ein gesicherter ASL-Kanal (Application Security Layer) zum NCPeH-Fachdienst aufgebaut, über den die eigentlichen Backend-Abrufe erfolgen (Partition 6).</p> <p>Damit nach erfolgreicher Authentisierung der Backend-Zugriff stattfinden kann, muss</p> <ul style="list-style-type: none"> • ein ASL-Kanal gemäß <u>8.5.2.2-1- Etablierung eines ASL-Kanals in die VAU-Umgebung des NCPeH-FD</u> etabliert sein, • jeder Request durch das EU-Webportal gemäß <u>8.5.2.3-1- Nutzung einer autorisierten Verbindung zum NCPeH-FD</u> durchgeführt werden.

2268

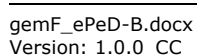


Abbildung 17: Sequenzdiagramm - Authentifizierung und Autorisierung des LE-DE

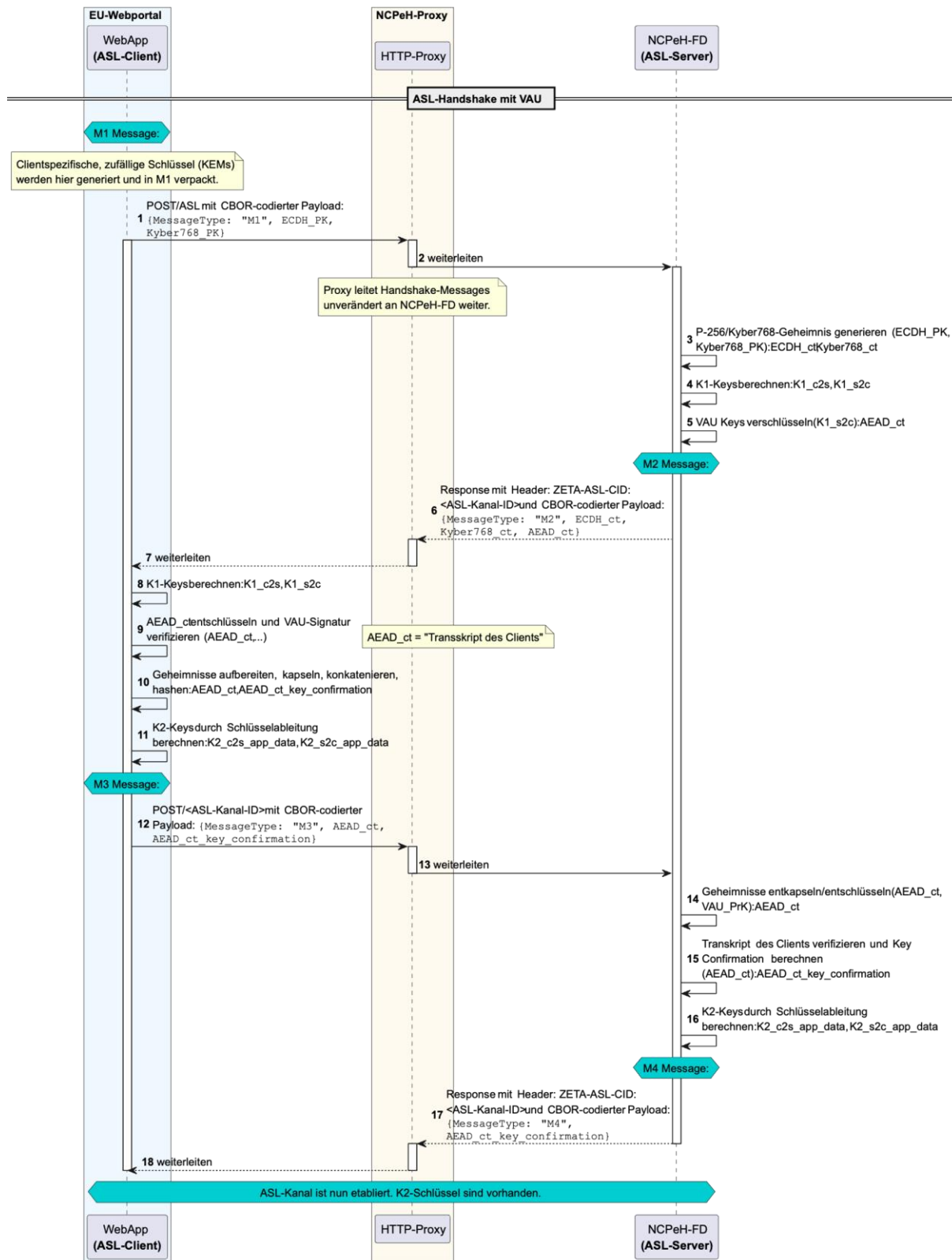
[<=]

Vollständige Ansicht der hochauflösenden Version des Sequenzdiagramms:

https://github.com/gematik/api-ncpeh/blob/master/images/feature/eped-b/auth/auth_seq-alternative2.svg**8.5.2.2 Etablierung eines ASL-Kanals in die VAU-Umgebung des NCPeH-FD****AF_10430 -Etablierung eines ASL-Kanals in die VAU-Umgebung des NCPeH-FD**

	Etablierung eines ASL-Kanals in die VAU-Umgebung des NCPeH-FD
Beschreibung	Bevor das EU-Webportal medizinischen Nutzdaten austauschen kann, wird ein Ende-zu-Ende gesicherter Kanal zum NCPeH-FD hergestellt. Dazu ist ein ASL-Handshake notwendig, der wie beschrieben abläuft.
Vorbedingung	keine (wurde bereits durch den aufrufenden Use Case erfüllt)
Nachbedingung	Es ist symmetrisches K2-Schlüsselmateriale erzeugt für diesen ASL-Kanal, mit jeweils einem Schlüssel für die Kommunikation vom EU-Webportal zum NCPeH-FD und umgekehrt.

2279



2280

2281

2282

Abbildung 18: Etablierung eines ASL-Kanals in die VAU-Umgebung des NCPeH-FD

[<=]

Vollständige Ansicht der hochauflösenden Version des Sequenzdiagramms:

https://github.com/gematik/api-ncpeh/blob/master/images/feature/eped-b/common/asl-channel_seq.svg

8.5.2.3 Nutzung einer autorisierten Verbindung zum NCPeH-FD

AF_10431 -Nutzung einer autorisierten Verbindung zum NCPeH-FD

	Nutzung einer autorisierten Verbindung zum NCPeH-FD
Beschreibung	<p>Dieser Use Case beschreibt den abgesicherten Datenaustausch zwischen einem Leistungserbringer (LE-DE) über ein EU-Webportal und dem NCPeH-FD. Der Fokus liegt auf der Ende-zu-Ende-Verschlüsselung der Nutzdaten sowie der mehrstufigen Autorisierung mittels DPOp (Demonstrating Proof-of-Possession) und Access-Tokens.</p> <p>Zu beachten:</p> <ul style="list-style-type: none"> Die Formate der im Sequenzdiagramm genannten Chiffre sind den annotierten Anforderungen (A_..) definiert. Das Token <code>DPOp-Token-2</code> muss bei jedem Request erneut generiert werden. Die hier erwähnten, zu verschlüsselnden Nutzdaten beziehen sich insbesondere auf Informationsobjekte aus <u>8.4- Informationsmodell</u>, die das Attribut <code>"x-medical-personal-information: true"</code> tragen. <p>Sicherheitslogik der Session-Tupel: Im Diagramm wird ein Session-Tupel-Konzept verwendet, um die Last auf den IDP-Komponenten zu reduzieren und um eine eigene logische Session aufzuspannen. Anhand der grünen Lifelines ist das logische Session-Handling zu erkennen. Diese logische Session wird durch Session-Tupel definiert.</p> <ul style="list-style-type: none"> Proxy-Ebene: Das Paar (<code>ncpehprx_access_token</code>, <code>IdA_raw</code>) erlaubt es dem Proxy, Requests ohne erneute Rücksprache mit dem AuthService durchzureichen, solange die Validität gegeben ist. Fachdienst-Ebene: Das Paar (<code>IdA_raw</code>, <code>IdentityAssertion</code>) dient der Vermeidung redundanter SAML-Validierungen. Der FD wandelt die Claims des <code>IdA_raw</code> ID-Tokens einmalig in eine interne, signierte Identität (<code>IdentityAssertion</code>) um und speichert diese für die Session-Dauer. Die Tokens werden wie beschrieben validiert. Invalide Tokens sorgen für ein ungültiges Session-Tupel und somit für eine ungültige Session.
Vorbedingung	<ul style="list-style-type: none"> Ein ASL-Kanal gemäß <u>8.5.2.2-1- Etablierung eines ASL-Kanals in</u>

	<p><u>die VAU-Umgebung des NCPeH-FD</u> muss etabliert sein.</p> <ul style="list-style-type: none"> • Tokenübergabe: Dem EU-Webportal wurde bereits einen ncpehprx_access_token ausgestellt. • Tokenübergabe: Der HTTP-Proxy-Komponente wurde bereits ein IdA_raw Token ausgestellt.
Nachbedingung	<ul style="list-style-type: none"> • NCPeH-FD enthält eine gültige IdentityAssertion. • Ein Nachweis über die erfolgte Ausstellung der IdentityAssertion ist im NCPeH-FD in Form eines HP Assurance Audit Trail persistiert.

[illegible]

Seite 100 von 137
Stand: 27.04.2026

Abbildung 19: Sequenzdiagramm - Nutzung einer autorisierten Verbindung zum NCPeD-FH

[<=]

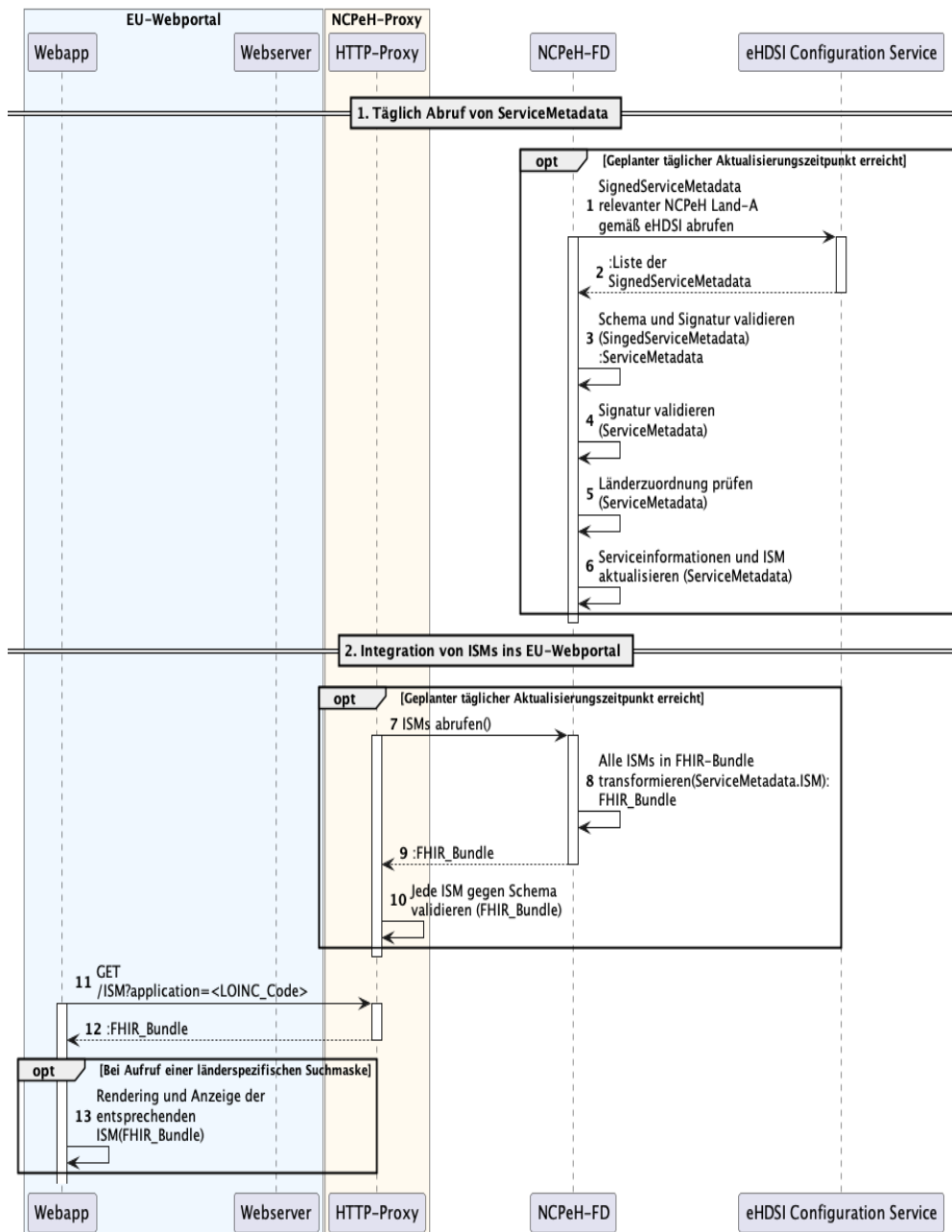
Vollständige Ansicht der hochauflösenden Version des Sequenzdiagramms:

https://github.com/gematik/api-ncpeh/blob/master/images/feature/eped-b/auth/backend-access_seq.svg**8.5.3 Use Cases im Rahmen der Identifizierung eines EU-Bürgers****8.5.3.1 International Search Masks abrufen****AF_10427 -International Search Masks abrufen**

Alle am Anwendungsfall "International Search Masks abrufen" beteiligten Produkttypen und Komponenten MÜSSEN die nachfolgenden Festlegungen umsetzen.

	International Search Masks abrufen
Kurzbeschreibung des Verlaufes	<ul style="list-style-type: none">Auf Anfrage eines Systemadministrators oder zeitgesteuert ruft der NCPeH-FD die ServiceMetadata und ISMs aller relevanten Länder-A vom eHDSI Configuration Service ab und hält diese lokal aktuell vor.Auf Anfrage eines Systemadministrators oder zeitgesteuert bezieht der NCPeH-Proxy alle ISMs vom NCPeH-FD und hält diese für Anfragen von der WebApp bereit.
Vorbedingung	<ul style="list-style-type: none">Der tägliche Abruf von aktuellen ISM hat im NCPeH-Proxy und NCPeH-FD nicht stattgefunden.Die Aktualisierung durch den NCPeH-FD und den NCPeH-Proxy sind so abgestimmt, dass die Aktualisierung durch den NCPeH-Proxy zeitlich ausreichend nach der Aktualisierung durch den NCPeH-FD erfolgt, so dass der NCPeH-Proxy die aktuellen ISM-Versionen abruft.
Nachbedingung	<ul style="list-style-type: none">Die ISM stehen im NCPeH-Proxy zum Abruf durch das EU-Webportal bereit.Die mTLS-Verbindung zwischen NCPeH-Proxy und NCPeH-FD ist aufgebaut.

2309



2310

2311

Abbildung 20: Sequenzdiagramm - International Search Masks abrufen

2312

2313

[<=]

2314

2315

2316

Vollständige Ansicht der hochauflösenden Version des Sequenzdiagramms:

2317

<https://github.com/gematik/api-ncpeh/blob/master/images/feature/eped-b/functional/ISM%20bereiststellen.svg>

2318

2319

8.5.3.2 Demographische Daten eines EU-Bürgers abrufen

AF_10428 -Demographische Daten eines EU-Bürgers abrufen

Alle am Anwendungsfall "Demographische Daten eines EU-Bürgers abrufen" beteiligten Produkttypen und Komponenten MÜSSEN die nachfolgenden Festlegungen umsetzen.

	Demographische Daten eines EU-Bürgers abrufen
Kurzbeschreibung des Verlaufes	<ul style="list-style-type: none"> Der LE-DE kann in der WebApp die jeweils erforderlichen Datenschutzbestimmungen für sich selbst (HPIN-Dokument) oder für den EU-Bürger (PIN-Dokument) aufrufen. Die Anzeige der Datenschutzbestimmungen ist in der Zielsprache des Zugehörigkeitslandes des EU-Bürgers möglich. Darüber hinaus kann der LE-DE die Datenschutzbestimmungen ausdrucken oder in der WebApp einen QR-Code mit einem Link zur entsprechenden Quelle anzeigen lassen. Auf Anfrage eines LE-DE startet die WebApp eine ISM-Abfrage für die Anwendung ePrescription beim NCPeH-Proxy, der daraufhin eine entsprechende Liste der ISMs zurückliefert. Auf Anfrage eines LE-DE zeigt das EU-Webportal im Browser die Suchmaske für das ausgewählte Land A an. Der LE-DE gibt die erforderlichen Daten manuell in die Suchmaske ein und bestätigt die Anfrage zum Abruf weiterer demographischer Daten eines EU-Bürgers. Die eingegebenen Daten werden vom EU-Webportal verschlüsselt an den NCPeH-FD übertragen und sind damit für Dritte nicht einsehbar. Der NCPeH-FD leitet die vom LE-DE eingegebenen Daten an den NCPeH Land A weiter, um weitere demographische Daten abzurufen und einen eindeutigen Patient Identifier zu bestätigen. Die ermittelten demographischen Daten des EU-Bürgers werden anschließend im EU-Webportal im Browser angezeigt.
Vorbedingung	<ul style="list-style-type: none"> Der Anwendungsfall <u>8.5.3.1-1- International Search Masks abrufen</u> wurde von dem LE-DE ausgeführt. Der LE-DE ist autorisiert die Anwendung ePrescription zu nutzen. Zwischen Deutschland und Land A besteht eine Vereinbarung über den grenzüberschreitenden Austausch von personenbezogenen Daten. URL oder Inhalte der Datenschutzbestimmungen (HPIN-Dokument und PIN-Dokument) sind in der WebApp enthalten. Die mTLS-Verbindung zwischen NCPeH-Proxy und NCPeH-FD ist aufgebaut.
Nachbedingung	<ul style="list-style-type: none"> Der Patient Identifier (z.B. zur eindeutigen Ermittlung von einlösbaren E-Rezepten im Land A) ist im EU-Webportal für

	<p>nachfolgende Transaktionen zwischengespeichert.</p> <ul style="list-style-type: none">• Zugriffsinformationen für Dokumentensuche (z.B. für berechtigten Abruf von E-Rezepten aus Land-A) sind im EU-Webportal zwischengespeichert.• Die demographischen Daten des EU-Bürgers sind im EU-Webportal zwischengespeichert.• Die Suchmasken (ISM) sind weiterhin im Webportal vorhanden und können auf Anfrage des LE-DE angezeigt werden.• NCPeH-FD enthält Einträge zu Non-Repudiation Origin und Receipt.• Der LE-DE kann die Suche nach demographischen Daten desselben EU-Bürgers wiederholen. Dabei ist die Suchmaske des Land A mit den zuletzt vom LE-DE eingegebenen Daten dieses EU-Bürgers vorausgefüllt.• Wenn der LE-DE die Suchmaske zur Suche von demographischen Daten eines anderen EU-Bürgers öffnet, dann ist die Suchmaske leer. Die bisher zwischengespeicherten Daten zu vorherigen EU-Bürgern sind nicht mehr im EU-Webportal vorhanden.• Ein HP Assurance Audit Trail Eintrag ist gemäß eHDSI-Vorgaben erstellt und im NCPeH-FD persistiert.
--	---

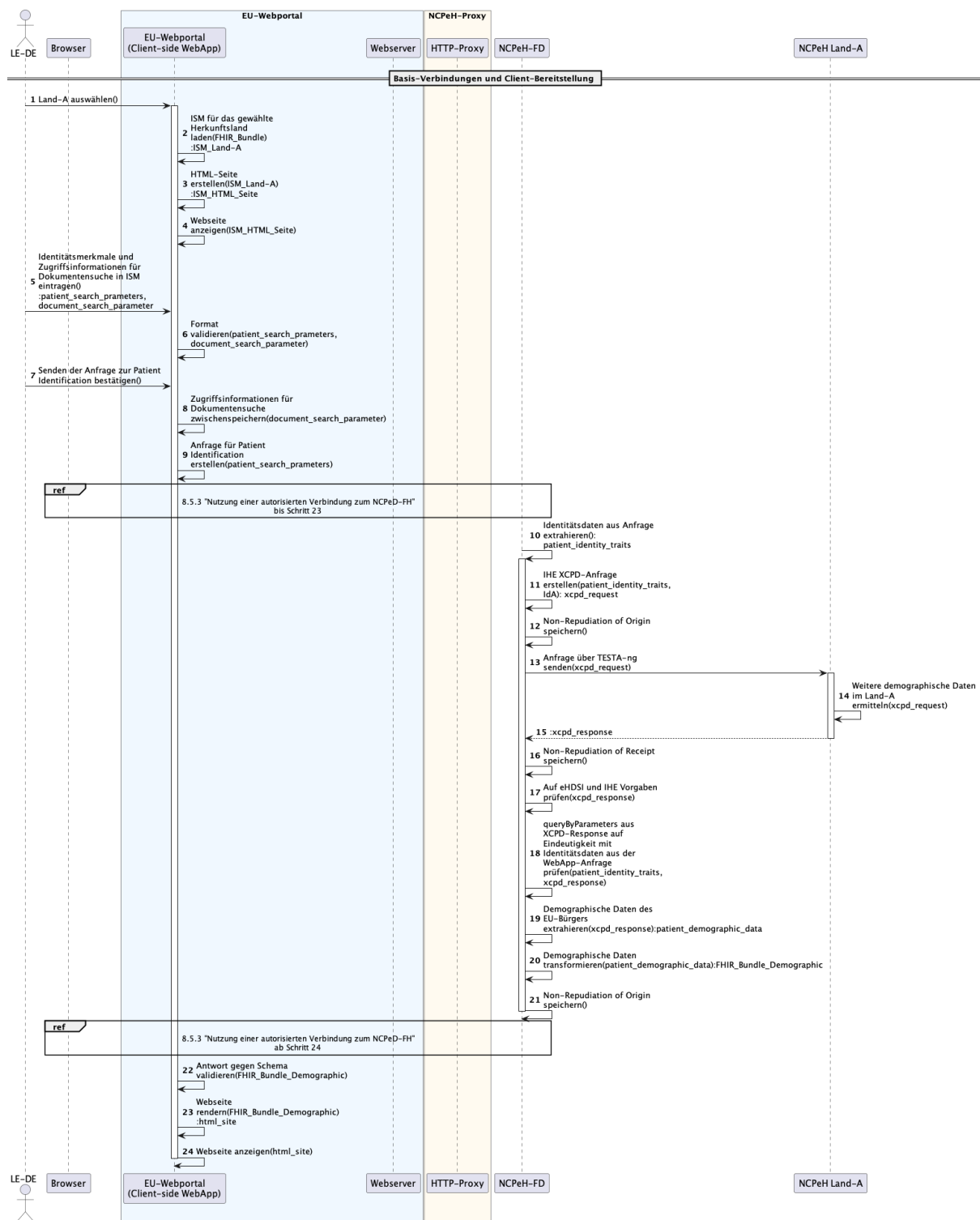


Abbildung 21: Sequenzdiagramm - Demographische Daten eines EU-Bürgers abrufen

[<=]

Vollständige Ansicht der hochauflösenden Version des Sequenzdiagramms:

https://github.com/gematik/api-ncpeh/blob/master/images/feature/eped-b/functional/Demographische_Daten_eines_EU-Buergers_abrufen.svg

8.5.4 Use Cases im Rahmen der Belieferung durch eine Apotheke in Deutschland

8.5.4.1 Liste der einlösbaren E-Rezepte eines EU-Bürgers abrufen

AF_10432 -Liste der einlösbaren E-Rezepte eines EU-Bürgers abrufen

Alle am Anwendungsfall "Liste der einlösbaren E-Rezepte eines EU-Bürgers abrufen" beteiligten Produkttypen und Komponenten MÜSSEN die nachfolgenden Festlegungen umsetzen.

	Liste der einlösbaren E-Rezepte eines EU-Bürgers abrufen
Kurzbeschreibung des Verlaufes	<ul style="list-style-type: none"> Der LE-DE bestätigt im EU-Webportal die Behandlungsbeziehung zum EU-Bürger Der LE-DE stellt im EU-Webportal die Anfrage zur Auflistung der einlösbaren E-Rezepte des EU-Bürgers. Das EU-Webportal übermittelt mit der Anfrage die Zugriffsinformationen für die Suche nach E-Rezepten (siehe Nachbedingung in <u>8.5.3.2-1- Demographische Daten eines EU-Bürgers abrufen</u>) Der NCPeH-FD überprüft die Zulässigkeit des Abrufs von E-Rezepten aus dem Land A des EU-Bürgers. Der NCPeH-FD ermittelt die bereits erstellte und persistierte elektronische Identität des LE-DE (IdA - Identity Assertion) und prüft deren Gültigkeit. Der NCPeH-FD wandelt die Informationen zur Behandlungsbeziehung in eine SAML 2.0 TRC Assertion gemäß eHDSI-Vorgaben. Die TRC Assertion wird mit der IdA verknüpft und für nachfolgende Transaktionen nutzbar gemacht. Der NCPeH-FD sendet eine Anfrage an den NCPeH Land A, inklusive des eindeutigen Patient Identifiers des EU-Bürgers, um Metadaten der einlösbaren E-Rezepte bereitzustellen. Der NCPeH-FD überprüft die erhaltenen Metadaten auf die Einhaltung der eHDSI-Vorgaben. Die Metadaten werden gemäß den Vorgaben des BfArM

	<p>transkodiert.</p> <ul style="list-style-type: none"> Die Metadaten der einlösbaren E-Rezepte werden im EU-Webportal gerendert und dem LE-DE angezeigt.
Vorbedingung	<ul style="list-style-type: none"> Der LE-DE ist autorisiert die Anwendung ePrescription zu nutzen. Zwischen Deutschland und Land A besteht eine Vereinbarung über den grenzüberschreitenden Austausch von E-Rezepten. Der Anwendungsfall <u>8.5.3.2-1- Demographische Daten eines EU-Bürgers abrufen</u> wurde von dem LE-DE ausgeführt. Die mTLS-Verbindung zwischen NCPeH-Proxy und NCPeH-FD ist aufgebaut. Ein ASL-Kanal zwischen EU-Webportal und NCPeH-FD ist aufgebaut und vorhanden.
Nachbedingung	<ul style="list-style-type: none"> Der Patient Identifier des EU-Bürgers (z.B. zur eindeutigen Ermittlung von einlösbaren E-Rezepten im Land A) ist weiterhin im EU-Webportal für nachfolgende Transaktionen zwischengespeichert. Metadaten der einlösbaren E-Rezepte sind für nachfolgende Transaktionen im EU-Webportal zwischengespeichert Der NCPeH-FD hat für die ein- und ausgehenden Nachrichten Einträge zu Non-Repudiation Origin und Receipt persistiert. Informationen über erfolgte Events (z.B. Query, Transcoding, Issuance of a TRC Assertion etc.) sind gemäß eHDSI-Vorgaben im passenden HP Assurance Audit Trail Eintrag enthalten.

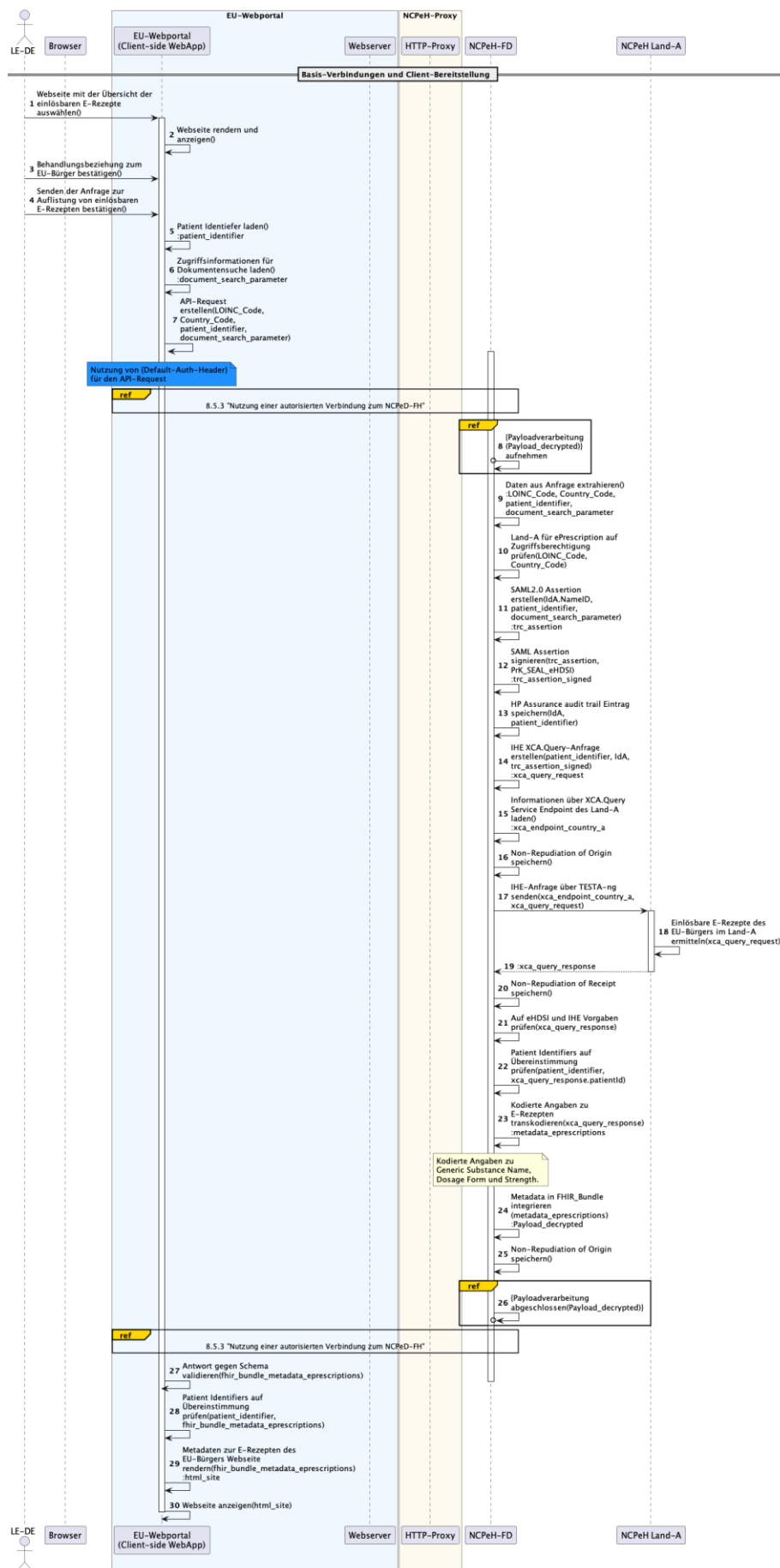


Abbildung 22: Sequenzdiagramm - Liste der einlösbaren E-Rezepte eines EU-Bürgers abrufen

[<=]

Vollständige Ansicht der hochauflösenden Version des Sequenzdiagramms:

https://github.com/gematik/api-ncpeh/blob/master/images/feature/eped-b/functional/Liste_der_einloesbaren_E-Rezepte_eines_EU-Buergers_abrufen.svg

8.5.4.2 Ausgewählte E-Rezepte eines EU-Bürgers abrufen

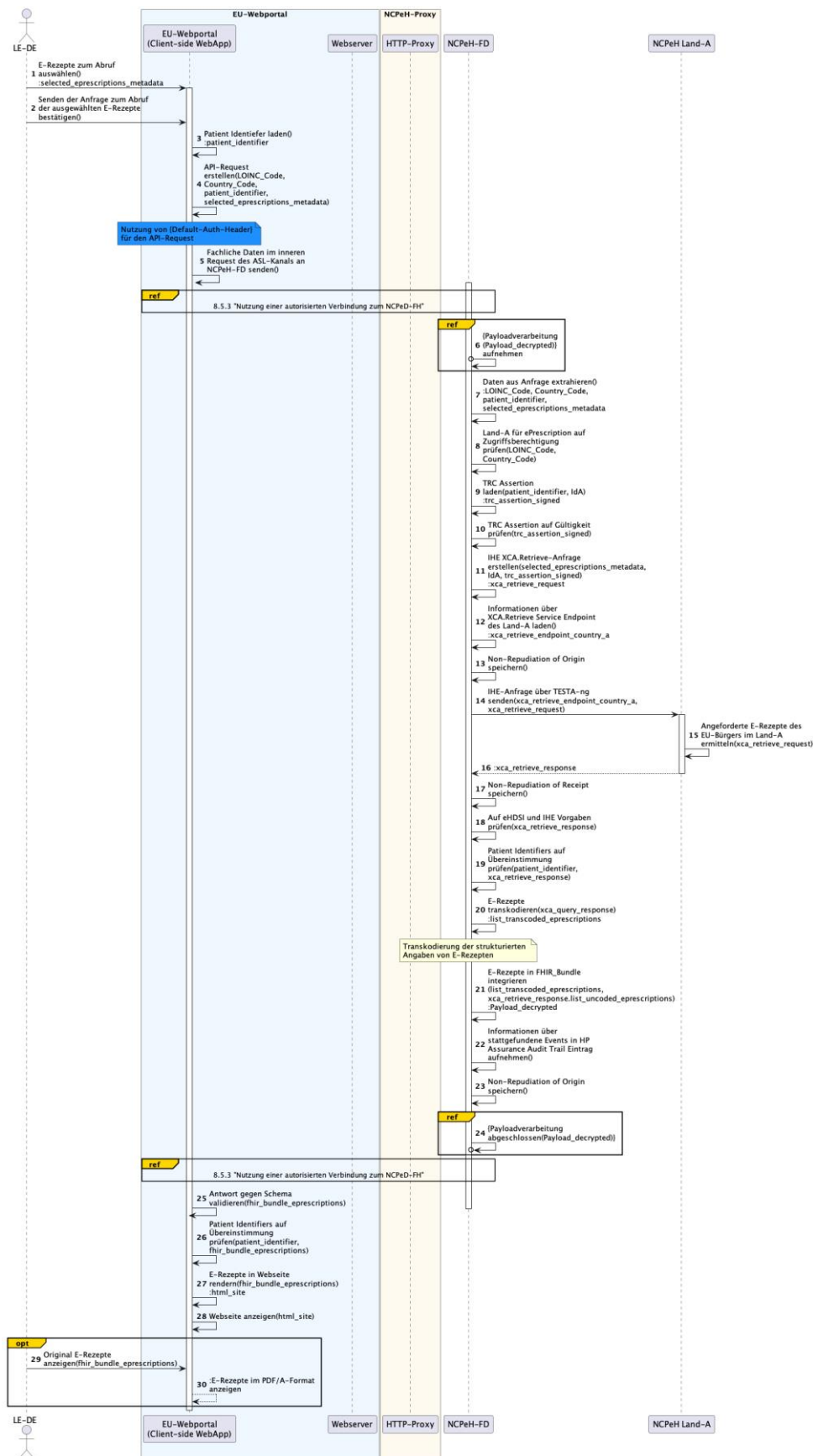
AF_10433 -Ausgewählte E-Rezepte eines EU-Bürgers abrufen

Alle am Anwendungsfall "Ausgewählte E-Rezepte eines EU-Bürgers abrufen" beteiligten Produkttypen und Komponenten MÜSSEN die nachfolgenden Festlegungen umsetzen.

Ausgewählte E-Rezepte eines EU-Bürgers abrufen	
Kurzbeschreibung des Verlaufes	<ul style="list-style-type: none"> Der LE-DE wählt im EU-Webportal E-Rezepte aus, deren vollständigen Inhalt er anzeigen möchte. Der LE-DE stellt im EU-Webportal die Anfrage zum Abruf von ausgewählten E-Rezepten. Das EU-Webportal sendet die Anfrage an den NCPeH-FD. Der NCPeH-FD überprüft die Zulässigkeit des Abrufs von E-Rezepten aus dem Land-A des EU-Bürgers. Der NCPeH-FD ermittelt die bereits erstellte und persistierte elektronische Identität des LE-DE (IdA - Identity Assertion) und Bestätigung der Behandlungsbeziehung zum EU-Bürger (TRC Assertion) und überprüft diese auf ihre zeitliche Gültigkeit. Der NCPeH-FD sendet eine Anfrage an den NCPeH Land-A mit Angaben zu den angeforderten E-Rezepten, um diese in eHDSI CDA ePrescription Level 1 und Level 3 Dokumentformaten abzurufen. Der NCPeH-FD überprüft die erhaltenen E-Rezepte auf die Einhaltung der eHDSI-Vorgaben. Der NCPeH-FD überprüft die Patient Identifiers aus den E-Rezepten auf Übereinstimmung. Der NCPeH-FD transkodiert die E-Rezepte gemäß BfArM-Vorgaben. Der NCPeH-FD sendet die transkodierten E-Rezepte ans EU-Webportal. Die E-Rezepte werden dem LE-DE im EU-Webportal angezeigt. Neben der Darstellung der strukturierten Inhalte der E-Rezepte besteht für den LE-DE im EU-Webportal optional die

	Möglichkeit, sich zusätzlich die Original-E-Rezepte im PDF/A-Format anzeigen zu lassen.
Vorbedingung	<ul style="list-style-type: none"> • Der LE-DE ist autorisiert die Anwendung ePrescription zu nutzen. • Der Anwendungsfall 8.5.4.1-1- Liste der einlösbaren E-Rezepte eines EU-Bürgers abrufen wurde von dem LE-DE ausgeführt. • Die mTLS-Verbindung zwischen NCPeH-Proxy und NCPeH-FD ist aufgebaut. • Ein ASL-Kanal zwischen EU-Webportal und NCPeH-FD ist aufgebaut und vorhanden.
Nachbedingung	<ul style="list-style-type: none"> • Der Patient Identifier des EU-Bürgers (z.B. zur eindeutigen Ermittlung von einlösbaren E-Rezepten im Land-A) ist weiterhin im EU-Webportal für nachfolgende Transaktionen zwischengespeichert. • Metadaten der einlösbaren E-Rezepte sind für den Dispensiervorgang im EU- Webportal zwischengespeichert. • Der NCPeH-FD hat für die ein- und ausgehenden Nachrichten Einträge zu Non-Repudiation Origin und Receipt persistiert. • Informationen über erfolgte Events (z.B. Retrieve, Transcoding, etc.) sind im HP Assurance Audit Trail Eintrag enthalten. • Im EU-Webportal liegen die Inhalte der abgerufenen E-Rezepte und deren Metadaten vor.

2361



2362

Abbildung 23: Sequenzdiagramm - Ausgewählte E-Rezepte eines EU-Bürgers abrufen

[<=]

Vollständige Ansicht der hochauflösenden Version des Sequenzdiagramms:

https://github.com/gematik/api-ncpeh/blob/master/images/feature/eped-b/functional/Ausgewaehlte_E-Rezepte_eines_EU-Buergers_abrufen.svg

8.5.4.3 Dispensierinformationen an Land A übermitteln

AF_10434 -Dispensierinformationen an Land A übermitteln

Alle am Anwendungsfall "Dispensierinformationen an Land A übermitteln" beteiligten Produkttypen und Komponenten MÜSSEN die nachfolgenden Festlegungen umsetzen.

	Dispensierinformationen an Land A übermitteln
Kurzbeschreibung des Verlaufes	<ul style="list-style-type: none"> Der LE-DE wählt im EU-Webportal die zuvor abgerufenen E-Rezepte des EU-Bürgers aus, die im Rahmen des Anwendungsszenarios dispensiert werden sollen. Für die ausgewählten E-Rezepte erfasst der LE-DE die jeweiligen PZN. Die WebApp übermittelt die eingegebenen PZN an den NCPeH-FD zur Validierung sowie zur Ermittlung des zugehörigen Produktnamens des Arzneimittels. Als Antwort liefert das NCPeH-FD den ermittelten Produktnamen zurück, der dem LE-DE im EU-Webportal als Bestätigung der eingegebenen PZN angezeigt wird. Für jedes zur Abgabe vorgesehene E-Rezept erfasst der LE-DE die entsprechende PZN als Bestandteil der Dispensierinformationen. Die WebApp übermittelt die eingegebene PZN an das NCPeH-FD zur Validierung und zur Ermittlung des zugehörigen Produktnamens des Arzneimittels. Das NCPeH-FD liefert als Antwort den validierten Produktnamen, welcher dem LE-DE im EU-Webportal angezeigt wird. Nach erfolgreicher Prüfung bestätigt der LE-DE die offizielle Übermittlung der Dispensierinformationen (insbesondere PZN). Im Rahmen dieser Übermittlung werden zusätzlich die zuvor ermittelten demographischen Daten des EU-Bürgers an den NCPeH-FD übergeben. Das EU-Webportal leitet die Dispensieranfrage an das NCPeH-FD weiter. Das NCPeH-FD prüft die grundsätzliche Zulässigkeit der Dispensierung von E-Rezepten in Bezug auf das Zugehörigkeitsland (Land-A) des EU-Bürgers. Anschließend ermittelt der NCPeH-FD die bereits erstellte und persistierte elektronische Identität des LE-DE (IdA - Identity

	<p>Assertion) sowie die Bestätigung der Behandlungsbeziehung zum EU-Bürger (TRC Assertion). Beide Assertions werden auf ihre zeitliche Gültigkeit überprüft.</p> <ul style="list-style-type: none"> Für jedes abzugebende E-Rezept erstellt das NCPeH-FD jeweils ein CDA eDispensation Dokument. Die Dokumente basieren auf den Informationen zum LE-DE, den demographischen Daten des EU-Bürgers, den Metadaten des jeweiligen E-Rezeptes, den aus der PZN abgeleiteten Arzneimittelinformationen sowie den gemäß den BfArM-Vorgaben transkodierten Werten. Das NCPeH-FD übermittelt die Anfrage einschließlich der erstellten CDA eDispensation Dokumente an den NCPeH Land-A. Der NCPeH Land-A bestätigt mit seiner Antwort die erfolgreiche Verarbeitung der Dispensierinformationen. Der Status der Verarbeitung der Dispensierung wird dem LE-DE im EU-Webportal angezeigt.
Vorbedingung	<ul style="list-style-type: none"> Der LE-DE ist autorisiert die Anwendung eDispensation zu nutzen. Der Anwendungsfall <u>8.5.4.2-1- Ausgewählte E-Rezepte eines EU-Bürgers abrufen</u> wurde von dem LE-DE ausgeführt. Die mTLS-Verbindung zwischen NCPeH-Proxy und NCPeH-FD ist aufgebaut. Ein ASL-Kanal zwischen EU-Webportal und NCPeH-FD ist aufgebaut und vorhanden.
Nachbedingung	<ul style="list-style-type: none"> Im EU-Webportal können dispensierte E-Rezepte nicht erneut dispensiert werden. Der NCPeH-FD hat für die ein- und ausgehenden Nachrichten Einträge zu Non-Repudiation Origin und Receipt persistiert. Informationen über erfolgte Events (z.B. Transcoding, etc.) sind im HP Assurance Audit Trail Eintrag enthalten.

2376
2377



Abbildung 24: Sequenzdiagramm - Dispensierinformationen an Land-A übermitteln

[<=]

Vollständige Ansicht der hochauflösenden Version des Sequenzdiagramms:

https://github.com/gematik/api-ncpeh/blob/master/images/feature/eped-b/functional/Dispensierinformationen_an_Land-A_uebermitteln.svg

9 Datenschutz und Informationssicherheit

Das Anwendungsszenario E-Prescription/ E-Dispensation Land B soll es EU-Bürgern ermöglichen, ihre im EU-Heimatland (Land A) ausgestellten E-Rezepte auch in Deutschland (Land B) einlösen zu können. Nach Abgabe durch deutsche Apotheker werden die Dispensierinformationen ins EU-Heimatland zurückgemeldet. Die rechtlichen Grundlagen hierzu werden insbesondere in Kapitel 2.1. beleuchtet. Dieses Kapitel gibt einen Überblick über den Schutzbedarf der notwendigen Anwendungsprozesse sowie die darin verarbeiteten maßgeblichen Informationsobjekte, deren Schutzbedarf sowie Maßnahmen zum Schutz dieser. Konkret werden als besonders schützenswerte Daten personenbezogene medizinische Daten des EU-Bürgers verarbeitet. Ebenso werden personenbezogene Daten des LE-DE im Zuge der Authentifizierungs- und Autorisierungsprozesses verarbeitet. Diese Daten unterliegen der Datenschutzgrundverordnung der EU. Die Bewertung der Schutzbedarfe erfolgt nach den Methoden der gematik analog der Produkte der TI, da die personenbezogenen medizinischen Daten des EU-Bürgers als gleichwertig schützenswert zu denen deutscher Versicherter angesehen werden. Die Maßnahmen zum Schutz der Daten orientieren sich am Niveau der Schutzmaßnahmen der Telematikinfrastruktur.

9.1 Benötigte Komponenten und Dienste zur Umsetzung des Szenarios

Zur Umsetzung des Anwendungsszenarios werden die bereits weiter oben beschriebenen Dienste und Komponenten benötigt. Die Bestimmung des Schutzbedarfs der Komponente und Dienste erfolgt nach dem Maximumprinzip der verarbeiteten Informationsobjekte.

Tabelle 6: Schutzbedarf der Dienste und Komponenten

Dienst / Komponente	Zweck	Schutzbedarf der Dienste/ Komponenten
EU-Webportal (Dienst)	Stellt als Webserver den Download der WebApp zur Verfügung.	Vertraulichkeit: niedrig Verfügbarkeit: hoch Integrität: hoch
WebApp (Komponente des EU-Webportals)	Frontend und Verarbeitungsfachlogik in der Leistungserbringerumgebung.	Vertraulichkeit: sehr hoch Verfügbarkeit: hoch Integrität: hoch
NCPeH-Proxy (Dienst mit Teildiensten HTTP-Proxy und Auth-Service)	Dienst zur Authentifizierung und Autorisierung der LE-DE sowie zum gezielten Routing von Anfragen an den NCPeH-FD.	Vertraulichkeit: hoch Verfügbarkeit: hoch Integrität: hoch
NCPeH-FD (Dienst)	Dienst der nationalen Kontaktstelle eHealth zur Kommunikation mit	Vertraulichkeit: sehr hoch

	Gesundheitssystemen der EU-Mitgliedsstaaten sowie zur Transkodierung von E-Rezepten.	Verfügbarkeit: hoch Integrität: hoch
--	--	---

2410

2411 9.2 Anwendungsprozesse und deren Schutzbedarf

2412 Für den reibungslosen Ablauf des Anwendungsszenarios sind die im Kapitel 8.5
 2413 beschriebenen Anwendungsprozesse essentiell. Aufgrund dessen wird der Schutzbedarf
 2414 der Verfügbarkeit aller Anwendungsprozesse dieses Anwendungsszenarios mit hoch
 2415 bewertet.

2416 9.3 Maßgebliche Informationsobjekte und deren Schutzbedarf

2417 Die maßgeblichen Informationsobjekte sowie deren Schutzbedarf sind in der
 2418 nachfolgenden Tabelle ersichtlich. Die jeweiligen Domänenobjekte befinden sich, soweit
 2419 vorhanden, zur besseren Nachvollziehbarkeit in Klammern.

2420

2421 **Tabelle 7: Schutzbedarfsfeststellung der maßgeblichen Informationsobjekte**

Informationsobjekt (Domänenobjektname(n))	Beschreibung	Schutzbedarf der Integrität	Schutzbedarf der Vertraulichkeit	Begründung des Schutzbedarfs
International Searchmask Suchparameter aus SignedServiceMetadata (ISMNational)	Die Suchparameter der ISM werden benötigt, um den EU-Bürger zu identifizieren. Hierzu wird die ISM wie bereits in AF_1042 beschrieben, innerhalb der VAU des NCPeH-FD gespeichert und entsprechend über einen TLS-Kanal dem NCPeH-	Mittel	niedrig	Der Schutzbedarf für die Vertraulichkeit wird mit "niedrig" bewertet, da die Parameter bei Nutzung quasi öffentlich verfügbar sind und täglich angewandt werden bei der Identifizierung des Versicherten in der

	Proxy zur Validierung und dem EU-Webportal zur Nutzung bereitgestellt.			Apotheke. Der Schutzbedarf der Integrität wird mit mittel bewertet, da selbst bei Manipulation der Suchparameter die personenbezogenen Daten nur innerhalb der VAU des NCPeH-FD im Klartext verarbeitet werden und sie auf der Strecke zum NCPeH-FD per ASL-Kanal übertragen werden. Durch Manipulation der Suchparameter kann es jedoch weiterhin zu einer Prozessverzögerung kommen.
PKCE Code Verifier (AuthorizationTask.Code_Verifier)	Der Code Verifier wird als Schutzmaßnahme für den Tausch Auth-Code zu ID-Token zwischen IDP-Dienst und Auth-Service im	mittel	hoch	Der Schutzbedarf der Vertraulichkeit wird mit "hoch" bewertet, da die ID-Token als Vorstufe zum NCPeH-Proxy-Access-

	<p>Rahmen des PKCE-Flow eingesetzt. Er garantiert, dass der Auth-Service der legitime Client für den Erhalt des Token ist.</p>			<p>Token notwendig sind, welches den Zugriff auf personenbezogene medizinische Daten ermöglicht. Da die personenbezogenen medizinischen Daten jedoch verschlüsselt übertragen werden, ist ein Erhalt der ID-Token lediglich ein Teilschritt und ermöglicht keinen vollständigen Zugriff. Die Verarbeitung und Vorhaltung des Code Verifier erfolgt innerhalb der VAU auf Seiten des NCPeH-Proxy. Der Schutzbedarf der Integrität wird mit mittel bewertet, da eine Verletzung der Integrität lediglich zu einer Prozessverzögerung führt.</p>
--	--	--	--	---

				gerung führt.
DPoP PrK (DPoPAsymmetricKeyPair.PrK)	Der private Key wird benötigt um die initiale Authentisierung- und Autorisierung-Anfrage zu signieren und später die Response, die das NCPeH-Proxy Accesstoken enthält zu entschlüsseln. DPoP schützt das NCPeH-Proxy Access Token.	mittel	hoch	Der Schutzbedarf der Vertraulichkeit sowie der Integrität wird durch den Schutzbedarf des unverschlüsselten NCPeH-Proxy Access-Token vererbt
DPoP PuK (DPoPAsymmetricKeyPair.PuK)	Mittels des DPoP Public Key wird das NCPeH-Proxy Accesstoken vom Auth-Service verschlüsselt, sodass nur der Client (WebApp) dies entschlüsseln kann.	mittel	niedrig	Der Schutzbedarf der Vertraulichkeit wird mit niedrig bewertet, da es sich um öffentliche Daten handelt. Der Schutzbedarf der Integrität wird mit mittel bewertet, da es durch eine Integritätsverletzung zu Prozessverzögerungen kommt.

NCPeH-Proxy Access Token (AuthorizationTask.ncpehprx_access_token)	Das NCPeH-Proxy Access-Token wird als Nachweis für einen legitimen Zugriff auf personenbezogene medizinische Daten benötigt. Die WebApp erhält dies nach erfolgreicher Authentisierung und Autorisierung verschlüsselt mit dem öffentlichen Schlüssel des DPOP-Token 1. Dieses Accesstoken wird vom Auth-Service des NCPeH-Proxy aus den beiden zuvor erhaltenen ID-Token erzeugt	mittel	mittel	Der Schutzbedarf der Vertraulichkeit wird mit „mittel“ bewertet, da das Token nur gemeinsam mit der Signatur des privaten Schlüssels des DPOP-Token genutzt werden kann und es verschlüsselt an die WebApp übertragen wird. Der Schutzbedarf der Integrität wird mit mittel bewertet, da der LE-DE erneut den Auth-Flow durchlaufen könnte. Es kommt zu keinen weiteren Auswirkungen durch die Integritätsverletzung.
Authorisation Code (AuthorizationTask.code)	Der Autorisierungscodeword wird auf Anfrage des Authenticators vom IDP erzeugt. Der Auth-Code ist alleine nicht	mittel	mittel	Der Schutzbedarf für Vertraulichkeit wird mit "mittel" bewertet, da damit alleine kein ID-Token für

	<p>nutzbar und wird zur Verarbeitung an den Auth-Service im NCPeH-Proxy weitergeleitet . Die beiden Auth-Codes der Autorisierung mittels HBA und SMC-B werden vom Auth-Service anschließend in ID-Token umgewandelt .</p>			<p>den Nutzer am IDP abgerufen werden kann. Es ist zusätzlich der Code Verifier notwendig. Zudem ist ein Abruf des ID-Tokens mit dem Authorization Code und Code Verifier nur für den Fachdienst möglich, für den der Authorization Code ausgestellt wurde. Der Schutzbedarf für Integrität wird mit "mittel" bewertet, da eine Änderung dazu führt, dass die Anmeldung nicht möglich ist.</p>
ID-Token des IDP signiert	<p>Die ID-Token werden vom IDP nach Anfrage vom Auth-Service ausgegeben. Absicherung über PKCE Code Verifier</p>	mittel	hoch	<p>Der Schutzbedarf der Vertraulichkeit wird, durch den zusätzlichen Schutz des Code Verifiers, mit hoch bewertet. Der Schutzbedarf der</p>

				Integrität wird mit mittel bewertet, da die ID-Token signiert sind.
IdA_raw signiert	Die IdA_raw ist ein zweites ID-Token, welches die Berechtigungen der jeweiligen LE-DE enthält und als Vorstufe für die Identity Assertion benötigt wird. Der Auth-Service stellt dies gemeinsam mit dem Access-Token aus und leitet die ida_raw an den HTTP-Proxy weiter. Diese wird dann gemeinsam mit dem NCPeH-Proxy Access-Token benötigt, um zwei Session-Tuple zu erzeugen und die Requests gezielt weiterzuleiten an den NCPeH-FD.	mittel	hoch	Der Schutzbedarf der Vertraulichkeit wird mit hoch bewertet, da die IdA_raw personenbezogene Daten enthält, die notwendig zur Transparenz und Nachvollziehbarkeit von Zugriffen sind. Da die IdA_raw signiert ist, wird der Schutzbedarf der Integrität mit mittel bewertet. Die IdA_raw wird an den NCPeH-FD weitergeleitet und dort zur Identity Assertion verarbeitet. Zudem wird die IdA_raw zum Binden einer Session an ein gültiges NCPeH-Proxy Access-Token vom

				NCPeH-Proxy genutzt.
ASL-Keys	Beim Aufbau des ASL-Kanals zwischen WebApp und NCPeH-FD werden symmetrische Schlüssel ausgehandelt, mit denen die zum NCPeH-FD übermittelten Nachrichten in der folgenden Kommunikation geschützt werden.	mittel	sehr hoch	Der Schutzbedarf der Vertraulichkeit wird mit sehr hoch bewertet, da er die medizinischen Daten des EU-Bürgers vor illegitimen Zugriffen schützt. Der Schutzbedarf der Integrität wird mit "mittel" bewertet, da bei einer Änderung der Keys der Nutzer nicht mehr auf den NCPeH-FD zugreifen kann. Er kann sich jedoch neu verbinden und dann wieder mit den NCPeH-FD kommunizieren.
IdA (IdentityAssertion)	Die IdA ist der Identitätsnachweis des LE-DE sowie der LEI-DE, welcher nach EU-Vorgaben umgesetzt ist. Dieser	hoch	hoch	Da es sich um personenbezogene Daten des LE-DE handelt, wird der Schutzbedarf der Vertraulichkeit

	wird aus der IdA_raw im NCPeH-FD erzeugt.			it mit hoch bewertet. Der Schutzbedarf der Integrität wird ebenfalls mit hoch bewertet, da eine Integritätsverletzung zu einem Mangel an Transparenz führt.
Patient Identifier (PatientIdentifier)	Der Patient Identifier ist ein spezifischer Parameter, welcher vom Land A zur eindeutigen Identifizierung des EU-Bürgers benötigt wird.	hoch	hoch	Der Schutzbedarf der Vertraulichkeit wird mit hoch bewertet, da es sich um ein personenbezogenes Datum handelt. Der Schutzbedarf der Integrität wird ebenfalls mit hoch bewertet, da eine Veränderung sowohl zu Prozessverzögerungen, als auch zu einem Mangel an Transparenz innerhalb der Audit Trails führen würde.
Demographische Versichertendaten	Die	hoch	hoch	Da es sich

(PatientIdentificationData)	demographischen Versichertendaten werden dem LE-DE nach initialer Übermittlung des Patient Identifiers an Land A übermittelt. Der LE-DE überprüft anhand der übermittelten demographischen Versichertendaten sowie eines Identitätsdokuments wie dem Reisepass die Identität.			um personenbezogene Daten des Versicherten handelt, wird der Schutzbedarf der Vertraulichkeit mit hoch bewertet. Der Schutzbedarf der Integrität wird mit hoch bewertet, da eine Manipulation der demographischen Daten zu einem Prozessabbruch führen könnte und der Prozess wiederholt werden müsste.
E-Rezepte des EU-Bürgers (PrescriptionRetrievedList, PrescriptionList, PrescriptionRedeemable, PrescriptionNonRedeemable, Selected PrescriptionRetrievalList)	Die E-Rezepte des EU-Bürgers enthalten unter anderem die E-Rezept ID, den Wirkstoff sowie Dosierung der Arznei und den Patient Identifier.	sehr hoch	sehr hoch	Da es sich um personenbezogene medizinische Daten handelt, wird der Schutzbedarf der Vertraulichkeit sowie der Integrität mit sehr hoch bewertet.
Dispensierinformationen (DispensationInformation)	Die Dispensierinformationen	sehr hoch	sehr hoch	Da es sich um personenbezogene Daten handelt, wird der Schutzbedarf der Vertraulichkeit mit sehr hoch bewertet.

	beinhalten die genauen Angaben darüber, welche Arznei in welcher Größe und welchem Wirkstoff vom LE-DE abgegeben wurde.			ogene medizinische Daten handelt, wird der Schutzbedarf der Vertraulichkeit sowie der Integrität mit sehr hoch bewertet.
Patient Information Notice (PINDocument)	Das PIN-Dokument ist ein Informationsdokument, welches den EU-Bürger über seine Betroffenenrechte im Zusammenhang mit der Verarbeitung seiner Daten aufklären soll.	mittel	niedrig	Da es sich um öffentliche Daten handelt, wird der Schutzbedarf der Vertraulichkeit mit niedrig bewertet. Der Schutzbedarf der Integrität wird mit mittel bewertet, da bei Verletzung der Integrität es zu Prozessverzögerungen bei der Ausübung der Betroffenenrechte kommen kann.
Healthcare Professional Information Notice (HPINDocument)	Das HPIN-Dokument ist ein Informationsdokument, welches den LE-DE über	mittel	niedrig	Da es sich um öffentliche Daten handelt, wird der Schutzbedarf

	seine Betroffenenrechte im Zusammenhang mit der Verarbeitung seiner Daten aufklären soll.			der Vertraulichkeit mit niedrig bewertet. Der Schutzbedarf der Integrität wird mit mittel bewertet, da bei Verletzung der Integrität es zu Prozessverzögerungen bei der Ausübung der Betroffenenrechte kommen kann.
Healthcare Professional Assurance Audit Trail Eintrag signiert (AuditTrailEntry)	Der HP Assurance Audit Trail Eintrag ist ein Protokolleintrag für den LE-DE um in Fällen von Unklarheiten Nachvollziehbarkeit zu gewährleisten.	mittel	hoch	Da es sich um personenbezogene Daten handelt, die keine spezifischen Rückschlüsse auf medizinische Daten zulassen, wird die Vertraulichkeit mit hoch bewertet. Die Integrität wird mit mittel bewertet, da der Audit Trail Eintrag signiert ist.

9.4 Maßnahmen zum Schutz der Informationsobjekte

Nachfolgend sollen die Maßnahmen zum Schutz der Informationsobjekte beschrieben werden. Wie bereits erwähnt, werden die Daten von EU-Bürgern als gleichwertig schützenswert zu denen deutscher Versicherter angesehen, sodass auf bewährte Maßnahmen der Produkte der Telematikinfrastruktur zurückgegriffen wird.

Zur Gewährleistung der Vertraulichkeit und Integrität werden personenbezogene medizinische Daten ausschließlich über einen ASL-Kanal von der WebApp in die VAU des NCPeH-FD übertragen. Dies stellt sicher, dass durch den Endpunkt des ASL-Kanals in die vertrauenswürdige Ausführungsumgebung des NCPeH-Fachdienstes sowie die Inhaltsverschlüsselung keine unberechtigten Dritten auf die Daten zugreifen oder diese lesen können. Die Klartextverarbeitung ist somit nur lokal im Browser sowie in der VAU des NCPeH-FD möglich.

Zum Schutz der im NCPeH-Proxy erzeugten NCPeH-Proxy Access-Token, welche es ermöglichen auf personenbezogene medizinische Daten zuzugreifen, wird eine vertrauenswürdige Ausführungsumgebung gefordert. Diese schließt vor allem unberechtigtem Zugriff durch den Betreiber aus. Die Anforderungen an die VAU werden entweder gleichwertig zum NCPeH-FD umgesetzt oder, falls es zum Zeitpunkt der Umsetzung einen HCC-Provider gibt, durch die Anforderungen der VAU der HCC-Spezifikation. Zusätzlich werden Maßnahmen bereits während der Authentifizierung ergriffen, um das unberechtigte Erhalten und Nutzen der Token zu verhindern. Hier wird auf die Sicherheitsverfahren DPoP und PKCE zurückgegriffen. Während DPoP sicherstellt, dass nur der berechtigte Client das NCPeH-Proxy-Access-Token nutzen kann, ist PKCE als vorgelagerter Sicherheitsmechanismus dafür verantwortlich, dass lediglich der Auth-Service des NCPeH-Proxy die ID-Token erhält, um diese in ein Access-Token umzuwandeln.

Es erfolgt keine Persistierung personenbezogener Daten im NCPeH-Proxy, sondern lediglich die Verarbeitung personenbezogener Daten zu Zwecken der Authentisierung im Auth-Service. Die Absicherung der personenbezogenen Daten erfolgt ebenfalls mittels der Verarbeitung innerhalb der VAU sowie einer Transportverschlüsselung zwischen den Diensten.

Um das Ziel der Nichtverkettung zu wahren, werden die schützenswerten Daten innerhalb einer VAU verarbeitet oder lokal verarbeitet, verschlüsselt und sicher übermittelt. Dies verhindert die Möglichkeit von unberechtigter Profilbildung. Zu Zwecken der Anomalieerkennung werden personenbezogene Daten der Leistungserbringer pseudonymisiert ausgewertet.

Zur Wahrung der Transparenz über den Zweck und der Rechtmäßigkeit der Verarbeitung der personenbezogenen (medizinischen) Daten sowie die Intervenierbarkeit zur Wahrung der Betroffenenrechte werden sowohl dem Leistungserbringer als auch dem EU-Bürger vor der Datenverarbeitung Informationen zur Verfügung gestellt. Die Informationen für den EU-Bürger werden sowohl von dessen EU-Zugehörigkeitsland als auch von Deutschland zur Verfügung gestellt. Es sind somit zwei PIN-Dokumente vorhanden. Die Dokumente werden vom LE-DE an den EU-Bürger digital oder physisch übergeben oder es wird dem EU-Bürger ein Link oder eine Information bereitgestellt, welche ihm die Einsichtnahme beider Dokumente ermöglicht. Der EU-Bürger muss zur Wahrung der Betroffenenrechte sich an den NCPeH seines Zugehörigkeitslandes wenden. Der LE-DE erhält ebenfalls eine Information zur Wahrung seiner Betroffenenrechte. Diese wird vom Anbieter des NCPeH-FD bereitgestellt.

Zur Gewährleistung der sicheren Auslieferung und dem Schutz vor Manipulation der Webapp wurden Maßnahmen definiert. Auf die einzelnen Sicherheitsmechanismen wurde bereits in Kapitel 8.1.3 eingegangen.

Betriebliche Sicherheitsanforderungen an die Anbieter der Dienste und Komponenten ergeben sich weiterhin aus der übergreifenden gematik-Spezifikation DS-Anbieter.

2474 Sicherheitsanforderungen an den sicheren Entwicklungsprozess der Hersteller von
2475 Komponenten und Dienste ergeben sich aus der übergreifenden gematik-Spezifikation
2476 DS-Hersteller.
2477

2478 **9.5 Erweiterung der Protokollierung**

2479 Für das Anwendungsszenario ePeD-B ist kein eHDSI Patient Privacy Audittrail Eintrag
2480 notwendig, da die Einsichtnahme über den NCPeH-Land A (des Heimatlandes) erfolgt. Für
2481 das Anwendungsszenario wird jedoch ein Protokolleintrag für den deutschen
2482 Leistungserbringer erstellt um bei Unstimmigkeiten dem Leistungserbringer
2483 Nachvollziehbarkeit zu ermöglichen. Das Protokoll wird HP Assurance (Healthcare
2484 Professional Assurance) genannt. Hier werden neben der Rolle und den
2485 Identifikationsdaten des Leistungserbringers, spezifischen Fehlermeldungen unter
2486 anderem auch der Patient Identifier, also die spezifischen Suchparameter aus der ISM
2487 enthalten sein. Die Festlegung der Protokollierungsinhalte wird in den europäischen
2488 Spezifikationen geregelt. Zur Einsichtnahme der Protokolle wendet sich der LE-DE an den
2489 Betreiber des NCPeH-FD Deutschland und stellt dort eine Anfrage. Bei berechtigtem
2490 Interesse und nach erfolgreicher Identitätsprüfung durch die nationale Kontaktstelle
2491 (DVKA) wird die Einsichtnahme ermöglicht.

2492 **9.6 Grenze der Sicherheitsleistung**

2493 Da der Patient Privacy Audit Trail Eintrag aufgrund der eHDSI-Spezifikation nur im
2494 Zugehörigkeitsland des EU-Bürgers erzeugt und dem EU-Bürger zur Verfügung gestellt
2495 wird, können die Betroffenenrechte vollumfänglich auch lediglich dort ausgeübt werden.
2496 Da die Maßnahmen zum Schutz des autorisierten Zugriffs von jedem Mitgliedsstaat selbst
2497 bestimmt werden, kann die Autorisierungsmaßnahme nicht durch diese Spezifikation
2498 vorgegeben werden. Die Verantwortung zusätzliche Schutzmechanismen zu etablieren,
2499 wie es Deutschland getan hat, liegt somit beim EU-Zugehörigkeitsland.
2500 Der LE-DE hat trotz allen von der gematik geforderten Sicherheitsmechanismen weiterhin
2501 für ein angemessenes Sicherheitsniveau der IT-Infrastruktur in der
2502 Leistungserbringerumgebung zu sorgen und somit eine Mitwirkungspflicht, da lokale
2503 Sicherheitslücken nicht vollständig durch zentrale Maßnahmen ausgeglichen werden
2504 können.

2505 10 Anhang A – Verzeichnisse

2506 10.1 Abbildungsverzeichnis

2507	Abbildung 1: Abgrenzungen ePeD-B	8
2508	Abbildung 2: Systemischer Blick auf das Anwendungsszenario	14
2509	Abbildung 3: Flussdiagramm Anwendungsszenario ePeD-B	15
2510	Abbildung 4: Authentisierung und Autorisierung des Leistungserbringers in Deutschland	
2511	22
2512	Abbildung 5: Information der Betroffenen über ihre Rechte und Pflichten zum Schutz	
2513	ihrer personenbezogenen und gesundheitlichen Daten	25
2514	Abbildung 6: Identifikation des EU-Bürgers in der Apotheke vor Ort	30
2515	Abbildung 7: Bestätigung des Behandlungsverhältnisses zum EU-Bürger	34
2516	Abbildung 8: Auflistung und Abruf der einlösbaren Rezepte des EU-Bürgers	38
2517	Abbildung 9: Schreiben der Dispensierinformation	45
2518	Abbildung 10: Systemübersicht des Anwendungsszenarios ePrescription/eDispensation	
2519	Land B	57
2520	Abbildung 11: Sequenzdiagramm des Anwendungsszenarios ("Main-Flow")	62
2521	Abbildung 12: Aufbau und Nutzung der WebApp-Komponente	68
2522	Abbildung 13: Qualitätsanforderungen an die Ausfallsicherheit der Betriebs- und	
2523	Infrastrukturumgebung des NCPeH-Proxy	77
2524	Abbildung 14: Qualitätsanforderungen an die Informationssicherheit der Betriebs- und	
2525	Infrastrukturumgebung des NCPeH-Proxy	78
2526	Abbildung 15: sonstige Qualitätsanforderungen an die Betriebs- und	
2527	Infrastrukturumgebung des NCPeH-Proxy	79
2528	Abbildung 16: Sequenzdiagramm - Basis-Initialisierung der WebApp und der	
2529	Kommunikation	93
2530	Abbildung 17: Sequenzdiagramm - Authentifizierung und Autorisierung des LE-DE	96
2531	Abbildung 18: Etablierung eines ASL-Kanals in die VAU-Umgebung des NCPeH-FD	97
2532	Abbildung 19: Sequenzdiagramm - Nutzung einer autorisierten Verbindung zum NCPeD-	
2533	FH	101
2534	Abbildung 20: Sequenzdiagramm - International Search Masks abrufen	102
2535	Abbildung 21: Sequenzdiagramm - Demographische Daten eines EU-Bürgers abrufen	105
2536	Abbildung 22: Sequenzdiagramm - Liste der einlösbaren E-Rezepte eines EU-Bürgers	
2537	abrufen	109
2538	Abbildung 23: Sequenzdiagramm - Ausgewählte E-Rezepte eines EU-Bürgers abrufen	112
2539	Abbildung 24: Sequenzdiagramm - Dispensierinformationen an Land-A übermitteln ...	115

10.2 Tabellenverzeichnis

Tabelle 1: Funktionale Schnittstellen und Operationen des EU-Webportals	69
Tabelle 2: Funktionale Schnittstellen und Operationen des NCPeH-Proxy	73
Tabelle 3: Verwendete und vom IDP-Dienst bestätigte Identitätsattribute des HBA	75
Tabelle 4: Verwendete und vom IDP-Dienst bestätigte Identitätsattribute der SMC-B ...	76
Tabelle 5: Funktionale Webschnittstellen und Operationstypen des NCPeH-FD	81
Tabelle 6: Schutzbedarf der Dienste und Komponenten	116
Tabelle 7: Schutzbedarfsfeststellung der maßgeblichen Informationsobjekte	117

10.3 Abkürzungen

Kürzel	Erläuterung
ASL	Additional Security Layer
ATC	Anatomical Therapeutic Chemical
AVS	Apothekenverwaltungssystem
BfArM	Bundesinstitut für Arzneimittel und Medizinprodukte
eGK	elektronische Gesundheitskarte
EHDS	European Health Data Space
eHDSI	eHealth Digital Service Infrastructure
EHIC	European Health Insurance Card - Europäische Krankenversicherungskarte
eHMSEG	eHealth Member States Expert Group
ePeD	ePrescription/eDispensation
ePeD-B	ePrescription/eDispensation Land B
FdV	Frontend des Versicherten
FQDN	Full-qualified Domain Name
HBA	Heilberufsausweis

HCC	Healthcare Confidential Computing
HPIN- (Dokument)	Health Professional Information Notice
LE-DE	Leistungserbringer in Deutschland
LE-EU	Leistungserbringer in einem EU-Mitgliedstaat (nicht Deutschland)
LEI-DE	Leistungserbringerinstitution in Deutschland
LTR	Local Terminology Repository
IdA	Identity Assertion des LE-DE
IDP	Identity Provider Dienst
ISM	International Search Mask
MTC	Master Translation Catalogue
MVC	Master Value Set Catalogue
NdB	Netz des Bundes
PIN- Dokument	Patient Information Notice
PIN	Personal Identification Number
PZN	Pharmazentralnummer
SBOM	Software Bill of Materials
SMC-B	Security Module Card Typ B
TI	Telematikinfrastuktur
TRC	Treatment Relationship Confirmation (Bestätigung des Behandlungsverhältnisses)
VAU	Vertrauenswürdige Ausführungsumgebung
ZETA	Zero Trust Access

2551

2552 **10.4 Inkludierte Dokumente**

2553 Die nachfolgende Tabelle enthält diejenigen Dokumente, die in dieses Dokument virtuell
 2554 inkludiert (und somit Bestandteil dieses Dokument sind), jedoch einen anderen
 2555 Bereitstellungsort (z.B. zwecks besserer Lesbarkeit/Nachvollziehbarkeit/Postprocessing-
 2556 Möglichkeit) haben.

[Quelle]	Link
[domainobj-eped-b.yaml]	https://github.com/gematik/api-ncpeh/blob/master/src/domain/domainobj-eped-b.yaml
[subdomains.yaml]	https://github.com/gematik/api-ncpeh/blob/master/src/domain/subdomains.yaml

2557 **10.5 Referenzierte Dokumente**2558 **10.5.1 Dokumente der gematik**

2559 Die nachfolgende Tabelle enthält die Bezeichnung der in dem vorliegenden Dokument
 2560 referenzierten Dokumente der gematik zur Telematikinfrastruktur.

[Quelle]	Herausgeber: Titel
[gemGlossar]	gematik: Glossar der Telematikinfrastruktur
[gemSpec_HCC]	gematik: Spezifikation Healthcare Confidential Computing (öffentlicher Entwurf)
[gemSpec_Krypt]	Übergreifende Spezifikation Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur
[gemSpec_Perf]	Spezifikation Performance und Mengengerüst TI-Plattform

2561

2562 **10.5.2 Weitere Dokumente**

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[Backends for Frontends]	https://learn.microsoft.com/en-us/azure/architecture/patterns/backends-for-frontends

[Baseline Requirements for the Issuance and Management of Publicly Trusted Certificates]	https://cabforum.org/working-groups/server/baseline-requirements/documents/
[Arzneimittelverschreibungsverordnung §2]	https://www.gesetze-im-internet.de/amvv/_2.html
[Durchführungsrichtlinie 2012/52/EU]	Amtsblatt der Europäischen Union, 20. Dezember 2012 https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=celex%3A32012L0052
[eHDSI_Requirements Catalogue]	eHDSI Solution Provider: Requirements Catalogue Version 10.0.0 https://webgate.ec.europa.eu/fpfis/wikis/pages/viewpage.action?pageId=888398339&spaceKey=EHDSI&title=Requirements%2Bcatalogue%2B-%2BPDF%2Bexports&preview=/888398339/2324764019/eHDSI%20Requirements%20Catalogue%20v10.0.0%20OR.pdf
[eHealth Network Guideline on the electronic exchange of health data under Cross-Border Directive 2011/24/EU ePrescription and eDispensation of Authorised Medicinal Products]	eHealth Network Guideline on the electronic exchange of health data under Cross-Border Directive 2011/24/EU ePrescription and eDispensation of Authorised Medicinal Products (Release 3.1) https://health.ec.europa.eu/system/files/2022-06/ehn_guidelines_eprescriptions_en.pdf
[eHDSI_SAML_Profile]	https://webgate.ec.europa.eu/fpfis/wikis/spaces/EHDSI/pages/888398849/SAML+Profile?preview=/888398849/2136510903/eHDSI_SAML_Profile_v9.0.0.pdf
[eHDSI_Audit_Trail_Profile]	https://webgate.ec.europa.eu/fpfis/wikis/spaces/EHDSI/pages/888398697/Audit+Trail+Profile?preview=/888398697/2136511191/eHDSI_Audit_Trail_Profile_v9.0.0.pdf
[eHDSI_Operations_Framework]	eHDSI Solution Provider: Operations Framework Version 4.1.0 https://webgate.ec.europa.eu/fpfis/wikis/display/EHDSI/6.+eHDSI+Operations+Framework
[MyHealth@EU_Monitoring_Framework]	eHDSI Solution Provider: Monitoring Framework Version 6.1.0 https://webgate.ec.europa.eu/fpfis/wikis/display/EHDSI/MyHealth@E

ork]	U+Monitoring+Framework+-+Version+History
[eHDSI_Audit_Framework]	eHDSI Solution Provider: Audit Framework https://webgate.ec.europa.eu/fpfis/wikis/display/EHDSI/4.+MyHealth@EU+Compliance+Checks+Services
[eHDSI_ISM_XSD]	https://code.europa.eu/ehdsi/ehealth/-/blob/master/openncp-web-manager/openncp-web-manager-backend/src/main/resources/ehdsi-ism-2023.xsd
[eHDSI_NCPeH_Architecture_Specification]	eHDSI Solution Provider: NCPeH Architecture Specifications Version 6.1.0 https://webgate.ec.europa.eu/fpfis/wikis/display/EHDSI/NCPeH+Architecture+Specifications
[eHDSI_Test_Framework]	eHDSI Solution Provider: Test Framework https://webgate.ec.europa.eu/fpfis/wikis/pages/viewpage.action?spaceKey=EHDSI&title=eHDSI+Test+Framework
[eHDSI_CDA_eDispensation]	https://art-decor.ehdsi.eu/publication/epsos-html-20260211T104851/tmp-1.3.6.1.4.1.12559.11.10.1.3.1.1.2-2024-04-19T095620.html
[eHDSI_CDA_ePrescription_L1]	https://art-decor.ehdsi.eu/publication/epsos-html-20260211T104851/tmp-1.3.6.1.4.1.12559.11.10.1.3.1.1.6-2024-04-19T095804.html
[eHDSI_CDA_ePrescription_L3]	https://art-decor.ehdsi.eu/publication/epsos-html-20260211T104851/tmp-1.3.6.1.4.1.12559.11.10.1.3.1.1.1-2024-04-19T095714.html
[eHDSI_XCA_Profile]	https://webgate.ec.europa.eu/fpfis/wikis/display/EHDSI/XCA+Profile
[Figma-Clickdummy]	https://www.figma.com/proto/ELGATKC5yeZmFZqLLb4nZS/Einl%C3%B6sen-im-EU-Ausland?node-id=4900-27265&p=f&viewport=3137%2C-2242%2C2.04&t=6Ig6bUc2q5LATBL6-1&scaling=min-zoom&content-scaling=fixed&starting-point-node-id=4900%3A27265&page-id=4900%3A27246
[ITI-38]	https://profiles.ihe.net/ITI/TF/Volume2/ITI-38.html
[ITI-39]	https://profiles.ihe.net/ITI/TF/Volume2/ITI-39.html
[ITI-55]	https://profiles.ihe.net/ITI/TF/Volume2/ITI-55.html#3.55.4.1.2
[MyHealth@EU_Glossary]	https://webgate.ec.europa.eu/fpfis/wikis/display/EHDSI/MyHealth@EU+Glossary

[MyHealth@EU_Scope_Business_Goals]	MyHealth@EU Scope and Business Goals Version 1.3 https://webgate.ec.europa.eu/fpfis/wikis/pages/viewpage.action?spaceKey=EHDSI&title=MyHealth@EU+Scope+and+Business+Goals
[MyHealth@EU_Cross-Border_Health_Services]	https://health.ec.europa.eu/ehealth-digital-health-and-care/digital-health-and-care/electronic-cross-border-health-services_en
[OpenID Connect Core]	https://openid.net/specs/openid-connect-core-1_0-final.html
[PRPA_MT201306 UV02.xsd]	https://drive.google.com/file/d/1N3dNoF7zKNzYjKYbfX-THGYf_CyYKphj/view
[PRPA_MT201310 UV02.xsd]	https://drive.google.com/file/d/1N4VWfKIO7LqXUa55fkv_RiuU-UO03aYT/view
[RFC 7519]	https://datatracker.ietf.org/doc/html/rfc7519
[RFC 9068]	https://datatracker.ietf.org/doc/html/rfc9068
[SGB V]	Sozialgesetzbuch V https://www.gesetze-im-internet.de/sgb_5/BJNR024820988.html

2563
2564
2565
2566
2567