

Elektronische Gesundheitskarte und Telematikinfrastruktur

Spezifikation NCPeH- Fachdienst

Version: 2.0.1
Revision: 1175014
Stand: 25.03.2025
Status: freigegeben
Klassifizierung: öffentlich
Referenzierung: gemSpec_NCPeH_FD

Dokumentinformationen

Änderungen zur Vorversion

Es handelt sich um die Erstversion des Dokumentes.

Dokumentenhistorie

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitun g
1.0.0	27.03.202 3		Erstversion des Dokumentes	gematik
1.5.0	11.09.202 3		Einarbeitung gemäß Änderungsliste NCPeH_23.1	gematik
1.6.0	15.07.202 4		Anpassung der NCPeH-Schnittstellen zur ePA-Anwendung wegen Änderungen, die mit ePA 3.0 berücksichtigt werden müssen Redaktionelle Änderungen, um übergreifende Themen für den NCPeH nicht auf ePA zu begrenzen	gematik
2.0.0	07.03.202 5		Einarbeitung gemäß Änderungsliste NCPeH_24_2	gematik
2.0.1	25.03.202 5		Einarbeitung Änderung aus ePA- Aktensystem (C_12080) gemäß Änderungsliste NCPeH_24_2-1	

Inhaltsverzeichnis

1 Einordnung des Dokuments.....	8
1.1 Zielsetzung.....	8
1.2 Zielgruppe.....	8
1.3 Geltungsbereich.....	9
1.4 Abgrenzungen.....	9
1.5 Methodik.....	10
1.5.1 Anwendungsfälle.....	10
1.5.2 Technische Use Cases.....	11
1.5.3 Anforderungen.....	11
2 Systemüberblick.....	13
2.1 Patient Summary Land-A.....	13
2.2 ePrescription/eDispensation Land-A.....	15
3 Systemkontext.....	18
3.1 Nachbarsysteme.....	18
3.2 Akteure.....	19
4 Übergreifende Festlegungen.....	23
4.1 Anbindung an die eHDSI.....	23
4.1.1 Konfigurationsparameter.....	23
4.1.2 Datenaustausch mit zugelassenen EU-Ländern.....	27
4.1.3 eHDSI Basisleistungen.....	28
4.1.3.1 <i>Sicherer Kanal: TESTA-ng und TLS.....</i>	<i>28</i>
4.1.3.2 <i>Zeitsynchronisation.....</i>	<i>29</i>
4.1.3.3 <i>eHDSI Identifier.....</i>	<i>29</i>
4.1.3.4 <i>Allgemeine Fehlerbehandlung.....</i>	<i>29</i>
4.1.3.5 <i>Umgang mit Zertifikaten der eHDSI.....</i>	<i>29</i>
4.1.3.6 <i>Validierung von Zertifikaten in eHDSI.....</i>	<i>30</i>
4.1.4 Service Metadata des NCPeH Land-B abrufen.....	32
4.1.5 Validierung der Identity Assertion des LE-EU.....	34
4.1.6 Validierung der TRC Assertion.....	42
4.1.7 Non-Repudiation und Audit Trail Schemas.....	48
4.1.7.1 <i>Non-Repudiation of Origin erstellen.....</i>	<i>48</i>
4.1.7.2 <i>Non-Repudiation of Receipt erstellen.....</i>	<i>51</i>
4.1.7.3 <i>Patient Privacy Audit Trail Eintrag erstellen.....</i>	<i>54</i>
4.1.7.4 <i>Translation Audit Trail Eintrag erstellen.....</i>	<i>55</i>
4.1.7.5 <i>Security Audit Trail Eintrag erstellen.....</i>	<i>60</i>
4.1.8 Festlegungen zur Prüfung der Zugriffsberechtigung auf Fachdienste der TI.....	63
4.1.9 Format und Validierung der KVNR.....	67
4.2 Anschluss an die Telematikinfrastruktur.....	67
4.2.1 Schnittstellen zu Diensten der zentralen TI.....	67
4.2.2 TLS-Verbindungsaufbau zu Diensten der TI.....	69
4.2.2.1 <i>TLS-Verbindungsaufbau zu Diensten der TI über das zentrale Netz der TI.....</i>	<i>69</i>

4.2.3 Prüfung von nonQES-Zertifikaten.....	70
4.2.3.1 Prüfung von X.509 nonQES Zertifikaten der TI.....	71
4.2.3.2 Prüfung von Internet-Zertifikaten.....	73
4.2.4 Registrierung als ePA-Client.....	73
4.2.5 Lokalisierung der Service-Endpunkte der ePA.....	73
4.2.6 Nutzung des IDP-Dienstes.....	74
4.2.6.1 Registrierung beim IDP-Dienst.....	74
4.2.6.2 Verarbeitung des Discovery Document.....	74
4.2.6.3 TLS-Verbindungsaufbau zu Service-Endpunkten des IDP-Dienstes.....	75
4.2.6.4 Authentifizierung per IDP-Dienst für Zugriff auf ePA-Aktensystem.....	75
4.2.7 Login in ein ePA-Aktenkonto.....	79
4.2.7.1 TLS-Verbindungsaufbau zum ePA-Aktensystem.....	79
4.2.7.2 Interne Aktenkontosession für einen Versicherten.....	80
4.2.7.3 Lokalisierung der Akte eines Versicherten.....	81
4.2.7.4 Aufbau eines VAU-Kanals zum ePA-Aktensystem.....	82
4.2.7.5 Nutzung eines etablierten VAU-Kanals zum ePA-Aktensystem.....	84
4.2.7.6 Schließen eines etablierten VAU-Kanals zum ePA-Aktensystem.....	84
4.2.7.7 Authentifizierung mit dem ePA Authorization Service.....	85
4.2.7.8 Adressierung des Aktenkontos.....	87
4.2.8 Befüllung von SOAP Header Elementen für Zugriff auf ePA XDS Document Service.....	87
4.2.9 Elektronische Identitäten des NCPeH-FD.....	88
4.2.10 Übergreifende Vorgaben an die Kommunikation mit E-Rezept-FD.....	90
4.2.10.1 Allgemeine Vorgaben an die Kommunikation mit dem E-Rezept-FD.....	90
4.2.10.2 Lokalisierung und Namensauflösung des E-Rezept-FD.....	90
4.2.10.3 Verschlüsselte Kommunikation zur VAU des E-Rezept-FD.....	90
4.2.10.4 Authentifizierung des NCPeH-FD am E-Rezept-FD.....	92
4.2.10.5 Abruf von Token vom IDP-Dienst.....	93
4.2.10.6 Erstellung des Payload für die Kommunikation mit dem E-Rezept-FD.....	93
4.2.10.7 Regelung zur Unterstützung von mehreren FHIR-Package Versionen.....	102
4.3 Sicherheit und Datenschutz.....	103
4.3.1 Datenschutzrechtliche- und informationssicherheitstechnische Anforderungen an die Vertrauenswürdige Ausführungsumgebung.....	107
4.3.2 Verarbeitungskontext des NCPeH-FD.....	108
4.3.3 Ausschluss von nicht autorisierten Zugriffen aus dem Betriebsumfeld.....	109
4.4 Betrieb.....	110
4.4.1 Schnittstellen und Anwendungsfälle.....	110
4.4.2 Leistungsanforderungen.....	110
4.4.3 Aufnahme eines Country Service Desks.....	110
4.4.4 Monitoring.....	111
4.4.4.1 Erfassung und Lieferung von Rohdaten.....	111
4.4.4.2 Erfassung und Lieferung von eHDSI-Kennzahlen.....	111
4.4.5 Logging.....	114
4.4.6 Betriebshandbuch.....	115
4.4.7 Verwaltung von Einträgen im Verzeichnisdienst FHIR.....	115
4.5 Test des NCPeH-FD.....	115
4.5.1 Durchführung eigenverantwortliche Tests des Herstellers bzw. Betreibers... ..	116
4.5.2 Bereitstellung von Testobjekten des NCPeH-FD in der TI.....	116
4.5.3 Testspezifische Funktionen im NCPeH-FD.....	117
4.5.3.1 Tracing mit ePA-Aktensystemen in Nichtproduktivumgebungen.....	117
4.5.4 Automatisiertes Auslösen von NCPeH-Anwendungsfällen für Tests in der TI... ..	117
4.5.4.1 Daten für das automatisierte Auslösen von Anwendungsfällen.....	118
4.5.5 Testdurchführung nach Vorgaben der eHDSI.....	119
4.5.6 Schematischer Testaufbau.....	120
4.5.6.1 Testaufbau für integrative Tests in der Telematikinfrastruktur.....	120

4.5.6.2 Testaufbau für den (Pre-)PPT.....	122
4.5.6.3 Testaufbau für den PET.....	122
5 Fachliche Anwendungsfälle.....	124
5.1 Anwendungsfälle für Patient Summary Land-A.....	124
5.1.1 NCPeH.UC_1 - Versicherten im Behandlungsland für PS-A identifizieren.....	124
5.1.2 NCPeH.UC_2 - Metadaten über ePKA MIO auflisten.....	125
5.1.3 NCPeH.UC_3 - ePKA MIO des Versicherten abrufen.....	127
5.1.4 NCPeH.UC_4 - ePKA MIO des Versicherten als PDF/A abrufen.....	129
5.2 Anwendungsfälle für ePrescription/eDispensation Land-A.....	131
5.2.1 NCPeH.UC_9 - Versicherten im Behandlungsland für ePeD-A identifizieren....	131
5.2.2 NCPeH.UC_10 - Einlösbare E-Rezepte des Versicherten aus ePeD-A auflisten	132
5.2.3 NCPeH.UC_11 - Ausgewählte E-Rezepte aus ePeD-A abrufen.....	134
5.2.4 NCPeH.UC_12 - Abgabe von Arzneimitteln an Versicherte im Abgabeland.....	136
5.3 Administrative Anwendungsfälle.....	138
5.3.1 NCPeH.UC_5 - Evidence & Audit Trails aus Audit Repository abrufen.....	138
5.3.2 NCPeH.UC_6 - Service Metadata auf eHDSI Configuration Service verwalten.	139
5.3.3 NCPeH.UC_7 - MTC vom eHDSI Terminology Service herunterladen.....	140
5.3.4 NCPeH.UC_8 - Konfigurationsparameter verwalten.....	142
6 Funktionsmerkmale.....	144
6.1 eHDSI.....	144
6.1.1 Operation	
Cross_Gateway_Patient_Discovery::RespondingGateway_PRPA_IN201305UV02.....	144
6.1.1.1 TUC_NCPeH_001: Patient Demographics Query Request für PS-A verarbeiten.....	146
6.1.1.2 TUC_NCPeH_002: Patient Demographics Response für PS-A versenden...155	
6.1.1.3 TUC_NCPeH_023: Patient Demographics Query Request für ePeD-A verarbeiten.....	159
6.1.1.4 TUC_NCPeH_024: Patient Demographics Response mit demographischen Versichertendaten für ePeD-A versenden.....	169
6.1.2 Operation Cross_Gateway_Query::FindDocuments.....	173
6.1.2.1 TUC_NCPeH_003: Cross Gateway Query Request für PS-A verarbeiten....175	
6.1.2.2 TUC_NCPeH_004: Cross Gateway Query Response für PS-A versenden....183	
6.1.2.3 TUC_NCPeH_025: Cross Gateway Query Request für ePeD-A verarbeiten	192
6.1.2.4 TUC_NCPeH_026: Cross Gateway Query Response für ePeD-A versenden	200
6.1.3 Operation Cross_Gateway_Retrieve::RetrieveDocument.....	212
6.1.3.1 TUC_NCPeH_005: Cross Gateway Retrieve Request zur Abfrage der Patient Summary CDA Level 3 verarbeiten.....	215
6.1.3.2 TUC_NCPeH_006: Cross Gateway Retrieve Response mit Patient Summary CDA Level 3 senden.....	224
6.1.3.3 TUC_NCPeH_007: Cross Gateway Retrieve Request zur Abfrage der Patient Summary CDA Level 1 verarbeiten.....	226
6.1.3.4 TUC_NCPeH_008: Cross Gateway Retrieve Response mit dem Patient Summary CDA Level 1 senden.....	234
6.1.3.5 TUC_NCPeH_009: NFD des ePKA MIO transkodieren und transformieren..236	
6.1.3.6 TUC_NCPeH_010: NFD des ePKA MIO ins PDF/A-Format transformieren...237	
6.1.3.7 TUC_NCPeH_027: Cross Gateway Retrieve Request für ePeD-A auf Einhaltung von allgemeinen Kriterien prüfen.....	238
6.1.3.8 TUC_NCPeH_028: Cross Gateway Retrieve Request für ePeD-A CDA verarbeiten.....	243
6.1.3.9 TUC_NCPeH_029: Cross Gateway Retrieve Response mit ePeD-A CDA senden.....	246

6.1.3.10 TUC_NCPeH_030: Abgerufene E-Rezepte transkodieren und transformieren	249
6.1.4 Nutzung der Schnittstelle des zentralen eHDSI Configuration Service	250
6.1.4.1 TUC_NCPeH_011: Service Metadata erstellen	250
6.1.4.2 TUC_NCPeH_012: Signed Service Metadata auf eHDSI Configuration Service hochladen	260
6.1.5 Operation Cross-Enterprise	
Document_Reliable_Interchange::ProvideAndRegisterDocumentSet-b	261
6.1.5.1 TUC_NCPeH_031: Überprüfung des Cross-Enterprise Document Reliable Interchange Request für eD-A auf allgemeine Vorgaben	263
6.1.5.2 TUC_NCPeH_032: Cross-Enterprise Document Reliable Interchange Request für eD-A verarbeiten	269
6.1.5.3 TUC_NCPeH_033: Cross-Enterprise Document Reliable Interchange Response für eD-A senden	275
6.1.5.4 TUC_NCPeH_034: Dispensierdokumente transkodieren und transformieren	277
6.2 Telematikinfrastruktur	278
6.2.1 TUC_NCPeH_013: Metadatenattribute des ePKA MIO abrufen	278
6.2.2 TUC_NCPeH_014: FHIR-Bundle ePKA MIO abrufen	283
6.2.3 TUC_NCPeH_017: Demographische Versichertendaten aus NFD des ePKA MIO übernehmen	288
6.2.4 TUC_NCPeH_035: Demographische Versichertendaten aus E-Rezept extrahieren	289
6.2.5 TUC_NCPeH_036: Liste der einlösbaren E-Rezepte des Versicherten aus dem E-Rezept-FD abrufen	293
6.2.6 TUC_NCPeH_037: Abzugebende E-Rezepte vom E-Rezept-FD abrufen	298
6.2.7 TUC_NCPeH_038: Dispensierdokumente an E-Rezept-FD übermitteln	305
6.3 Administration	310
6.3.1 TUC_NCPeH_018: Systemadministrator oder Prozessverantwortlicher anmelden	310
6.3.2 TUC_NCPeH_019: Änderungen an Konfigurationsparameter planen	311
6.3.3 TUC_NCPeH_020: Änderungen an Konfigurationsparametern und im Truststore aktivieren	312
6.3.4 TUC_NCPeH_021: Ausgewählte Evidence und Audit Trail Einträge ermitteln	314
6.3.5 TUC_NCPeH_022: MTC in der VAU speichern	315
7 Anhang - Europäische Krankenversicherungskarte	317
8 Anhang - Verzeichnisse	319
8.1 Abkürzungen	319
8.2 Begriffe	322
8.3 Abbildungsverzeichnis	323
8.4 Tabellenverzeichnis	323
8.5 Referenzierte Dokumente	326
8.5.1 Dokumente der gematik	326
8.5.2 Weitere Dokumente	329

1 Einordnung des Dokuments

Versicherte im deutschen Gesundheitssystem sollen die Möglichkeit bekommen, die eigenen medizinischen Daten auch im EU-Ausland sinnvoll nutzen zu können. Um das zu erreichen, ist es notwendig, die entsprechenden Voraussetzungen zu schaffen, damit die Telematikinfrastruktur (TI) an die europäische Gesundheitsinfrastruktur eHealth Digital Services Infrastructure (eHDSI), auch als MyHealth@EU bezeichnet, angebunden werden kann.

Um einen vernetzten digitalen Binnenmarkt zu verwirklichen, wurde im Rahmen des Infrastrukturprogramms Connecting Europe Facility (CEF, 2014-2021) die sektorspezifische eHDSI entwickelt. Die unmittelbare Kooperation zwischen den EU-Mitgliedsstaaten und der Europäischen Kommission verfolgt das Ziel, einen zur Regelversorgung geeigneten Austausch von Versichertendaten umzusetzen. Dieser umfasst die ersten medizinischen Basisanwendungen: Die Patient Summary (PS) und das elektronische Rezept (ePrescription) inklusive der Dispensationsmeldung (eDispensation).

Der Austausch medizinischer Daten und die damit einhergehende Bereitstellung von elektronischen Dienstleistungen soll durch die von den beteiligten EU-Mitgliedsstaaten individuell eingerichteten und betriebenen nationalen Kontaktstellen – National Contact Point for eHealth (NCPeH) – unterstützt werden. Der NCPeH unterstützt die eHDSI als landesspezifischer, fachlicher Vermittler, rechtlicher Ankerpunkt sowie technischer Dienstleister für Kommunikations- und Sicherheitsaufgaben (EU Gateway).

Im von der eHDSI spezifizierten Daten- und Kontrollfluss vermitteln die NCPeH zwischen den bestehenden nationalen Gesundheitsinfrastrukturen sowie deren digitalen Diensten. Zur Beschleunigung der Bereitstellung von patientenbezogenen Gesundheitsdaten sind Hilfsmittel seitens des durch das Land-A betriebenen NCPeH-Fachdienst (FD) (ausstellendes oder datenoffenbarendes Land) sowie zur Abfrage und Anzeige von Daten auf Seiten des NCPeH Land-B (datenempfangendes Land) integriert.

Der NCPeH soll zwei grundlegende fachliche Rollen unterstützen. In der Rolle als NCPeH Land-A werden Gesundheitsdaten der Versicherten aus Deutschland zum Abruf durch andere NCPeH bereitgestellt. In der Rolle des NCPeH Land-B werden Gesundheitsdaten über ausländische Patienten vom zuständigen NCPeH Land-A abgefragt. In beiden Rollen werden zusätzliche Aufgaben wahrgenommen, wie bspw. die Transkodierung zwischen den deutschen und europäischen medizinischen Codesystemen beim Abruf sowie die Bereitstellung technischer Sicherheitsleistungen.

1.1 Zielsetzung

Die vorliegende Spezifikation beschreibt die Anforderungen zu Herstellung, Test und Betrieb des NCPeH-FD.

1.2 Zielgruppe

Das Dokument richtet sich zum Zwecke der Realisierung an Anbieter, Betreiber und Hersteller des NCPeH-FD.

1.3 Geltungsbereich

Dieses Dokument enthält normative Festlegungen an den NCPeH-FD.

Wichtiger Schutzrechts-/Patentrechtshinweis

Die nachfolgende Spezifikation ist von der gematik allein unter technischen Gesichtspunkten erstellt worden. Im Einzelfall kann nicht ausgeschlossen werden, dass die Implementierung der Spezifikation in technische Schutzrechte Dritter eingreift. Es ist allein Sache des Anbieters oder Herstellers, durch geeignete Maßnahmen dafür Sorge zu tragen, dass von ihm aufgrund der Spezifikation angebotene Produkte und/oder Leistungen nicht gegen Schutzrechte Dritter verstoßen und sich ggf. die erforderlichen Erlaubnisse/Lizenzen von den betroffenen Schutzrechtsinhabern einzuholen. Die gematik GmbH übernimmt insofern keinerlei Gewährleistungen.

1.4 Abgrenzungen

Die vom NCPeH-FD bereitgestellten (angebotenen) Schnittstellen, über die die grenzüberschreitende Datenübertragung mit NCPeHs anderer europäischer Mitgliedsstaaten erfolgt, sind durch die eHDSI spezifiziert und haben normativen Charakter. In diesem Dokument wird auf die eHDSI-Spezifikationen referenziert (siehe auch [\[8.5.2- Weitere Dokumente\]](#)).

Nationale vom NCPeH-FD verwendete Schnittstellen werden hingegen in der Spezifikation desjenigen Produkttypen beschrieben, der diese Schnittstelle bereitstellt. Auf die entsprechenden Dokumente wird referenziert (siehe [\[8.5.1- Dokumente der gematik\]](#)).

Nicht Bestandteil des vorliegenden Dokumentes sind die Festlegungen zu folgenden Themenbereichen:

- Der Abruf von Daten aus der elektronischen Patientenakte (ePKA) aus Deutschland in Notfallsituationen ("Emergency") durch Leistungserbringer in anderen europäischen Mitgliedsländern (LE-EU),
- Regelung zur Transformierung der Komposition KBV_PR_MIO_NFD_Composition_NFD des FHIR-Bundle ePKA MIO in das eHDSI CDA Pivotformat Level 3,
- Regelung zur Transformation und (semantischen) Transkodierung von strukturierten Inhalten der Komposition KBV_PR_MIO_NFD_Composition_NFD des FHIR-Bundle ePKA MIO in das eHDSI CDA Pivotformat Level 3,
- Regelung zur Transformierung von Inhalten der Komposition KBV_PR_MIO_NFD_Composition_NFD des FHIR-Bundle ePKA MIO ins eHDSI CDA Pivotformat Level 1 embedded PDF/A,
- Bereitstellung und Auswertung von Audit Trails und Non-Repudiation-Einträgen,
- Definition und Festlegung von Technologien von Management-Schnittstellen innerhalb der Umgebung des NCPeH-FD des Anbieters,
- Vertreterregelung (Next of Kin),

sowie

- Schreibender Zugriff auf die ePKA-Anwendung durch LE-EU,
- Zugriff auf andere Fachanwendungen eines Versicherten in DE,

- Umsetzung der grenzüberschreitenden Fachanwendung ePrescription/eDispensation Land-B,
- Es erfolgt keine Umsetzung des optionalen Anwendungsfalls "Option to discard a previously performed dispensation" gemäß [eHDSI_Requirements_Catalogue#07.04],
- Für das europäische Anwendungsszenario ePrescription/eDispensation dürfen folgende E-Rezepte gemäß [MyHealth@EU_Scope_and_Business_Goals#"MyHealth@EU OUT OF SCOPE description"] nicht verarbeitet werden:
 - Betäubungsmittel,
 - Arzneimittel, die nach ärztlicher Verschreibung oder nach den Vorschriften eines Arzneibuchs für den Versicherten zubereitet werden (bezeichnet als "formula magistralis" oder "extemporale Zubereitungen"),
 - Arzneimittel, die nicht durch ein industrielles Verfahren hergestellt oder bei deren Herstellung kein industrielles Verfahren angewandt wurde,
 - Arzneimittel, die nicht als Humanarzneimittel eingestuft sind,
- Lesender und schreibender Zugriff für Leistungserbringer in Deutschland (LE-DE) auf äquivalente ePKA-Daten, die sich in elektronischen Gesundheitsinfrastrukturen anderer EU-Mitgliedsstaaten befinden (Szenario Patient Summary Land-B),
- Spezifikationen oder Konzeptionen zum ePA-Aktensystem, zur ePKA-Anwendung im ePA-Aktensystem sowie zum FdV (Frontend des Versicherten) des ePA-Aktensystems.

1.5 Methodik

Die Spezifikation ist im Stil einer RFC-Spezifikation verfasst. Dies bedeutet:

- **Der gesamte Text in der Spezifikation ist für den Anbieter und den Hersteller des Produktes NCPeH-FD, als auch für dessen Betreiber gemäß [gemKPT_Betr] verbindlich zu betrachten und gilt zusätzlich zu den verbindlichen Steckbriefen von Produkt- und Anbietertyp des NCPeH-FD.**
- Die Verbindlichkeit SOLL durch die dem RFC 2119 [RFC2119] entsprechenden, in Großbuchstaben geschriebenen deutschen Schlüsselworte MUSS, DARF NICHT, SOLL, SOLL NICHT, KANN gekennzeichnet werden.
- Da in dem Beispielsatz „Eine leere Liste DARF NICHT ein Element besitzen.“ die Phrase „DARF NICHT“ semantisch irreführend wäre (wenn nicht ein, dann vielleicht zwei?), wird in diesem Dokument stattdessen „Eine leere Liste DARF KEIN Element besitzen.“ verwendet.
- Die Schlüsselworte KÖNNEN außerdem um Pronomen in Großbuchstaben ergänzt werden, wenn dies den Sprachfluss verbessert oder die Semantik verdeutlicht.

1.5.1 Anwendungsfälle

Anwendungsfälle als Ausdruck normativer Festlegungen werden durch Tests geprüft und nachgewiesen. Sie besitzen eine eindeutige, permanente ID, welche als Referenz verwendet werden SOLL. Die Tests werden im Rahmen einer Abnahme mit dem in diesem Dokument spezifizierten Testaufbau durchgeführt.

Anwendungsfälle werden im Dokument wie folgt dargestellt:

<ID> - <Titel des Anwendungsfalles / Akzeptanzkriteriums>

Text / Beschreibung
[<=]

Die einzelnen Elemente beschreiben:

- **ID:** einen eindeutigen Identifier.
 - Bei einem Anwendungsfall besteht der Identifier aus der Zeichenfolge 'AF_' gefolgt von einer Zahl,
 - Der Identifier eines Akzeptanzkriteriums wird von System vergeben, z.B. die Zeichenfolge 'ML_' gefolgt von einer Zahl
- **Titel des Anwendungsfalles:** Ein Titel, welcher zusammenfassend den Inhalt beschreibt
- **Text / Beschreibung:** Ausführliche Beschreibung des Inhalts. Kann neben Text Tabellen, Abbildungen und Modelle enthalten

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

1.5.2 Technische Use Cases

Jeder Anwendungsfall enthält eine Beschreibung des Standardablaufs (Gutfall). Der Standardablauf besteht aus Aktivitätsschritten, die auf "Technische Use Cases" (TUC) verweisen. Die TUCs sind im [6- Funktionsmerkmale] beschrieben. Die TUCs sind eigene modulare Funktionsmerkmale bzw. Verantwortungsbereiche, die von verschiedenen Anwendungsfällen oder anderen TUC wiederverwendet werden können. In diesen Verantwortungsbereich greifen keine anderen Funktionsmerkmale (TUC) ein.

TUCs werden im Dokument nach folgendem Muster dargestellt:

<TUC_NCPeH_XXX>: <Titel des TUC>

- Relevante Übergreifende Festlegungen,
- Ablauf des TUC inkl. spezifischer Fehlerbehandlung,
- Ausgabeparameter des TUC,

Benutzte Schnittstellen und Operationsbezeichnungen in diesem Dokument auf Seiten der eHDSI orientieren sich anhand eHDSI- bzw. IHE-Namensgebung. Bei Schnittstellen zur TI werden die Bezeichnungen der TI genutzt.

1.5.3 Anforderungen

Zusätzlich zu der obigen Festlegung kommen in einigen Abschnitten dieses Dokumentes weiterhin dedizierte Anforderungen zum Einsatz. Dies ist vor allem dann der Fall, wenn damit ein besonderes Prüfverfahren verknüpft ist (z. B. Produktgutachten), dass sich entsprechend auch im Produkttypsteckbrief [gemProdT_NCPeH_FD] widerspiegeln soll.

Sie werden im Dokument wie folgt dargestellt:

<AFO-ID> - <Titel der Afo>

Text / Beschreibung
[<=]

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

An einigen Stellen wird im Dokument auf übergreifende Anforderungen in anderen Dokumenten der TI verwiesen. In diesen referenzierten Anforderungen können teilweise Formulierungen auftauchen wie z.B. "Produkt der TI", "Produkttypen der TI", "Dienste der

TI". Mit Nennung dieser Anforderungen in diesem Dokument gelten diese auch für den NCPeH-FD, unabhängig davon, ob der NCPeH-FD als Produkt der TI gilt oder nicht.

2 Systemüberblick

Der NCPeH-FD ermöglicht Versicherten, ihre Gesundheitsdaten in andere europäische Mitgliedsstaaten mitzunehmen und sie dort mit behandelnden LE zu teilen. Der NCPeH-FD ist in seiner Rolle als Service Provider beteiligt an der europäischen eHealth Digital Services Infrastructure (eHDSI). Dabei ist der NCPeH-FD zuständig für eine interoperable Kommunikation und Datenaustausch zwischen der eHDSI und TI. Die Gesundheitsdaten der Versicherten werden in Fachdiensten der TI (z.B. ePA-Aktensystem oder E-Rezept-FD) verwaltet. Anfragen von anderen EU-Ländern (Land-B), in denen die medizinische Behandlung einer in Deutschland versicherten Person stattfindet, werden vom NCPeH-FD unter Einhaltung von Sicherheitsschutzziele (z.B. Integrität, Authentizität, etc.) geprüft und an den entsprechenden Fachdienst in der TI weitergeleitet, in dem die angeforderten Gesundheitsdaten der Versicherten enthalten sind.

Jeder NCPeH benötigt als zugelassener Teilnehmer an der eHDSI einen Zugang zu TESTA-ng mittels eines sogenannten "Turnkey Access Point" (TAP), um darüber sicher mit den NCPeH anderer EU-Länder und den zentralen Diensten der eHDSI kommunizieren zu können. Den Zugang zu TESTA-ng gewährt die Kommission einem Mitgliedsstaat, indem sie mit ihm ein "Memorandum of Understanding" (MoU) aufsetzt, in dem die Pflichten aller TESTA-ng Nutzer festgehalten sind. Dieses MoU muss von einer Regierungsorganisation des Mitgliedsstaates unterschrieben werden. Ein eigener TESTA-ng Zugang des Bundesgesundheitsministeriums ist derzeit nicht vorhanden. Es wurde in Deutschland jedoch ein sog. "Bund-Länder-Kommunen-Verbindungsnetz" (Netze des Bundes, NdB) aufgebaut, welches wiederum an einen TESTA-TAP angebunden ist. Die DVKA (eine Abteilung des GKV-SV) verfügt bereits im Rahmen des "elektronischen Austauschs von Sozialversicherungsdaten" (Electronic Exchange of Social Security Information) über einen Zugang zum NdB.

Mit der Anbindung an das Netz der TESTA-ng gewährleistet der NCPeH-FD als Bindeglied zwischen der TI und der nationalen Gesundheitsinfrastruktur eines anderen EU-Mitgliedsstaates eine sichere Übertragung von Identitäts- und Gesundheitsdaten. Der NCPeH-FD realisiert die Vertraulichkeit und Integrität der verarbeiteten Daten über das Konzept der vertrauenswürdigen Ausführungsumgebung (VAU), die eine vertrauenswürdige Verarbeitung und verschlüsselte Persistierung der Daten sicherstellt.

Zusätzlich protokolliert der NCPeH-FD alle Ereignisse im Zusammenhang mit der Verarbeitung von Identitäts- und Gesundheitsdaten. Dies impliziert das Sammeln vollständiger und zeitbezogener Informationen über die Aktionen und Zustände in Bezug auf den NCPeH-FD (Audit Trails). Neben der Protokollierung führt der NCPeH-FD eine Historie von digitalen Beweisen (Evidenzen), so dass nachvollzogen werden kann, welche Akteure eine Aktion im Zusammenhang mit einer eHDSI-NCPeH-Transaktion durchgeführt haben.

Im Zuge des kontinuierlichen Ausbaus und der Integration weiterer grenzüberschreitender Anwendungsszenarien werden deren Systemübersichten aus Sicht des NCPeH-FD in den folgenden Unterkapiteln aufgenommen bzw. bestehende Systemübersichten entsprechend den Anforderungen des eHDSI und der TI angepasst.

2.1 Patient Summary Land-A

Die zentralen Funktionen der ePA für alle (ePA-Aktensystem) sind das integrale Management von definierten Metadaten und den medizinischen Dokumenten als auch die Unterstützung von digitalen Versorgungsprozessen. Das ePA-Aktensystem (ePA-AS) wird

den LE und anderen anerkannten Akteuren des Gesundheitswesens zur Verfügung gestellt. Für den NCPeH-FD ist dies der Zugriff auf die elektronische Patientenakte (ePKA) als technischer Client. Gegenüber dem ePA-Aktensystem agiert der NCPeH-FD als ein anerkannter ePA Client. Der NCPeH-FD bietet den LE-EU als Nutzer den Zugang zur ePKA MIO des Versicherten an. Dabei greift der NCPeH-FD als Repräsentant des Land-B in der TI über ein Kommunikationsprotokoll mit Ende-zu-Ende-Verschlüsselung (VAU-Protokoll) auf die relevanten Dienste der ePA zu.

Die Authentifizierung des Land-B erfolgt durch den zentralen Identity Provider (IDP-Dienst) der TI. Als Authentifizierungsmittel verwendet der NCPeH-FD das im HSM für das Land-B hinterlegte AUT-Zertifikat des Zertifikatsprofils SM-B NCPeH, um damit die TI-Identität des Land-B gegenüber dem IDP-Dienst nachzuweisen. Der Authentifizierungsprozess erfolgt entsprechend dem OpenID Connect Standard sowie dem Challenge-Response Verfahren. Bei erfolgreicher Authentifizierung erhält das ePA-Aktensystem vom IDP-Dienst ein ID_TOKEN mit relevanten Identitätsmerkmalen. Anhand der Identitätsmerkmalen kann im ePA-AS überprüft werden, ob der NCPeH-FD (als Repräsentant für Land-B in der TI) befugt ist auf ePKA MIO zuzugreifen. Wenn dies der Fall ist, wird im ePA-AS eine User Session für das Land-B gestartet.

In der User Session können mehrere Health Record Contexts zu verschiedenen Aktenkonten parallel aufgebaut werden, auf die LE-EU aus dem Land-B dann zugreifen können. Im Health Record Context erfolgt die Verarbeitung der (medizinischen) Daten eines Aktenkontos. In einem Health Record Context werden niemals Daten aus unterschiedlichen Aktenkonten verarbeitet.

Die finale Autorisierung des Land-B für den Zugriff durch NCPeH-FD auf ePKA MIO des Versicherten kann vom ePA-Aktensystem erst erfolgen, wenn der Versicherte selbst über sein ePA FdV eine Zugriffsberechtigung (Befugnisvergabe) für das Land-B erteilt hat. Die Dauer der Zugriffsberechtigung ist fest auf eine Stunde begrenzt. Bei jeder Erteilung oder Verlängerung einer Zugriffsberechtigung durch den Versicherten wird ein neuer Zugriffscod generiert. Der Zugriffscod ist mit der Dauer der Zugriffsberechtigung, der KVNR des Versicherten und dem angegebenen Land-B gekoppelt. Nach Ablauf oder Widerruf der Zugriffsberechtigung durch den Versicherten wird auch der Zugriffscod automatisch ungültig. Dadurch können die LE-EU aus dem Land-B durch den NCPeH-FD keinen weiteren Zugriff auf die ePA des Versicherten erhalten.

Die Prüfung von Zugriffsautorisierungen (inkl. Zugriffscod) auf ePKA MIO des Versicherten erfolgt durch den ePA XDS Document Service. Dabei wird vorausgesetzt, dass der NCPeH-FD den Zugriffscod an den ePA XDS Document Service übermittelt hat, welchen der NCPeH-FD aus der eHDSI-Anfrage des NCPeH Land-B übernommen hat. Nach erfolgreicher Prüfung der Autorisierung erfolgt die Bereitstellung des ePKA MIO des Versicherten.

Der Abruf von Metadaten und ePKA MIO des Versicherten durch NCPeH-FD aus dem ePA XDS Document Service erfolgt gemäß den Festlegungen der IHE und ePA.

Durch die Übermittlung der vom NCPeH-FD transkodierte und transformierte ePKA-Daten des Versicherten an das jeweilige NCPeH Land-B stellt der NCPeH-FD sicher, dass die Bedeutung und Aussagekraft der Inhalte des ePKA MIO erhalten bleibt. Zu diesem Zweck konvertiert der NCPeH-FD die ePKA-Daten in das normative und interoperable eHDSI-Pivot-Format und verwendet die von den am eHDSI beteiligten europäischen Mitgliedsstaaten vereinbarte Kodierungssysteme.

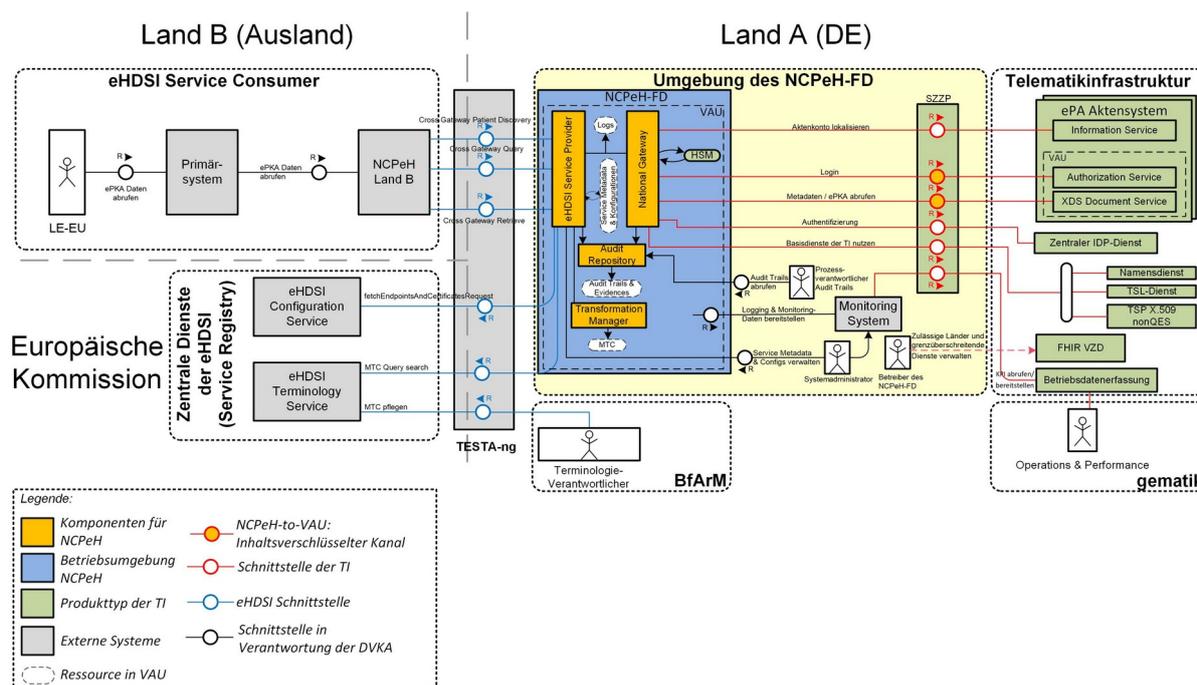


Abbildung 1: Architektur des NCPeH-FD Patient Summary Land-A

Abbildung 1 stellt die Architektur für den NCPeH-FD Anwendungsszenario Patient Summary Land-A dar. Orange dargestellt sind logische Komponenten des NCPeH-FD. Die grün dargestellten Systeme stellen Produkttypen der TI dar. Die grau dargestellten Systeme befinden sich außerhalb der Systemgrenzen des NCPeH-FD. Die blau dargestellten Schnittstellen (blaue Linien) sind bereits durch die eHDSI spezifiziert, sie werden in diesem Dokument referenziert. Die Nutzung der rot dargestellten Schnittstellen (rote Linien) durch den NCPeH-FD werden in diesem Dokument spezifiziert. Die schwarz dargestellten Verbindungen sind in Verantwortung des Anbieters und werden vom NCPeH-FD Betreiber bereitgestellt.

2.2 ePrescription/eDispensation Land-A

Versicherte aus Deutschland sollen die Möglichkeit haben, ihre elektronischen Rezepte (E-Rezepte) in einer Apotheke ihrer Wahl im europäischen Ausland einzulösen. Für dieses Anwendungsszenario stehen den Versicherten die EU-Mitgliedsstaaten zur Verfügung, mit denen bilateral ein Agreement zum Datenaustausch zum Abruf der in Deutschland ausgestellten E-Rezepte getroffen wurde. Anhand dieser Liste der Länder können die Versicherten selbst wählen, in welchem verfügbaren europäischen Mitgliedsstaat sie ihre E-Rezepte einlösen möchten. Die Nutzung dieser Option ist freiwillig, erfordert jedoch eine vorherige Erteilung der Zugriffsberechtigung durch den Versicherten für den jeweiligen europäischen Mitgliedsstaat.

Verwaltung von Zugriffsberechtigungen für E-Rezepte

Vor dem Abruf oder Einlösen von E-Rezepten in anderen EU-Mitgliedsstaaten (Land-B) erteilt eine versicherte Person über seine E-Rezept-FdV einmalig die Einwilligungserklärung in die Nutzung der Anwendung ePrescription/eDispensation. Die Gültigkeit der Einwilligungserklärung ist nicht länderspezifisch. Danach trifft die Person über sein E-Rezept-FdV die Entscheidung, aus welchem anderen europäischen Mitgliedsstaat die Apotheker bzw. Leistungserbringer (LE-EU) auf seine E-Rezepte zugreifen dürfen. Die Speicherung von Zugriffsberechtigungen erfolgt technisch direkt im

E-Rezept-FD. Mit jeder Erteilung einer Zugriffsberechtigung wird ein neuer Zugriffscode generiert. Die erteilte Zugriffsberechtigung inkl. Zugriffscode ist zeitlich auf eine Stunde begrenzt. Mit der Erstellung jeder Zugriffsberechtigung werden Informationen zur KVNR der versicherten Person, zum Ländercode des berechtigten EU-Mitgliedsstaates (Land-B), Zugriffscode und Zeitpunkt der Erstellung der Berechtigung gespeichert. Die gespeicherten Informationen inkl. Zugriffscode werden der Person auf seinem E-Rezept-FdV angezeigt.

Nach Ablauf oder Widerruf der Zugriffsberechtigung durch die versicherte Person wird auch der Zugriffscode automatisch ungültig. Dadurch können die LE-EU keinen weiteren Zugriff auf die E-Rezepte des Versicherten erhalten. Versicherte Personen haben auf ihrem E-Rezept-FdV die Möglichkeit, eine gültige Zugriffsberechtigung mit einer neuen Zugriffsberechtigung zu überschreiben. Dabei wird immer ein neuer Zugriffscode generiert.

Die versicherte Person übergibt die Zugriffsdaten (KVNR und generierter Zugriffscode) an den LE-EU in der Apotheke durch Vorzeigen oder Mitteilen. Durch die Übergabe der Zugriffsdaten hat die Person in dem konkreten EU-Land die Möglichkeit zu steuern, welcher konkrete LE-EU dieses Landes auf seine deutschen E-Rezepte zugreifen darf. Der Abruf oder das Einlösen von E-Rezepten in einer Apotheke im Ausland setzt voraus, dass die Apotheke beim Zugriff auf E-Rezepte die Zugriffsdaten über die Schnittstellen der eHDSI und des NCPeH-FD an den E-Rezept-FD übermittelt.

Berechtigter Zugriff auf E-Rezepte

Der Zugriff auf E-Rezepte der versicherten Person erfolgt für die LE-EU mittels NCPeH-FD. Dieser enthält die E-Rezept-spezifische Clientfunktionalität und baut die Verbindung zu zentralen Diensten der TI auf. Eine Nutzung der Schnittstellen des E-Rezept-FD durch den NCPeH-FD ist nur nach erfolgreicher Autorisierung durch den IDP-Dienst möglich.

Den Authentisierungsprozess initiiert der NCPeH-FD gegenüber dem IDP-Dienst entsprechend dem OpenID Connect Standard sowie dem Challenge Response-Verfahren. Als Authentisierungsmittel verwendet der NCPeH-FD das im HSM für das Land-B hinterlegte AUT-Zertifikat des Zertifikatsprofils SM-B NCPeH, um damit die TI-Identität des Land-B gegenüber dem IDP-Dienst nachzuweisen. Eine Interaktion mit dem Nutzer im Hintergrund ist nicht erforderlich.

Der IDP-Dienst agiert dabei als OAuth2 Authorization Server für das E-Rezept und prüft in dieser Funktion, ob das vorgetragene X.509-nonQES-Signatur-Zertifikat zeitlich gültig und ob seine Integrität sichergestellt ist.

Der IDP-Dienst führt die Identifikation des NCPeH-FD als den Repräsentanten des Land-B innerhalb der TI durch, und stattet diesen anschließend mit ID_TOKEN gemäß [openid-connect-core 1.0 # IDToken] und ACCESS_TOKEN gemäß [[RFC6749#section-1.4](#)] und [[RFC6749#section-5](#)] aus. Dazu wird ein "Authorization Code Grant" gemäß [[RFC6749#section-4.1](#)] genutzt. Um dem erforderlichen Sicherheitsniveau gerecht zu werden, wird zudem PKCE (Proof Key for Code Exchange by OAuth Public Clients) gemäß [RFC7636] angewandt.

Der IDP-Dienst verwendet ACCESS_TOKEN, um die Autorisierung des Zugriffs durch den NCPeH-FD auf den E-Rezept-FD sicherzustellen. Der ACCESS_TOKEN wird vom NCPeH-FD als Bearer Token für den Zugriff auf E-Rezepte versicherten Personen des E-Rezept-FD verwendet. Der ACCESS_TOKEN enthält die bestätigten Identitätsmerkmale, die der E-Rezept-FD benötigt, um die Berechtigung des NCPeH-FD abzuleiten und zu verifizieren.

Der E-Rezept-FD prüft neben der Validierung des ACCESS_TOKEN auch die zusätzlich hinterlegten Berechtigungsinformationen für die konkrete versicherte Person auf Gültigkeit (KVNR der versicherten Person, Ländercode des berechtigten EU-Mitgliedsstaates (Land-B), Zugriffscode und zeitliche Gültigkeit der Berechtigung). Bei erfolgreicher Prüfung wird dem NCPeH-FD der Zugriff auf die angeforderten E-Rezepte der versicherten Person gewährt.

FHIR-Ressourcen

Für den Abruf von E-Rezepten aus dem E-Rezept-FD in diesem Anwendungsszenario wird der Standard FHIR (Fast Healthcare Interoperability Resources) verwendet. In FHIR werden Datenstrukturen und Elemente in "Ressourcen" beschrieben, welche über standardisierte Schnittstellen übertragen werden können. Die Daten werden dabei in XML repräsentiert.

Der NCPeH-FD ruft die Ressource FHIR-Bundle über die entsprechende Schnittstelle des E-Rezept-FD ab. Für eine Beschreibung der FHIR-Ressource siehe [FHIR_Resource_Bundle].

Architektonische Übersicht

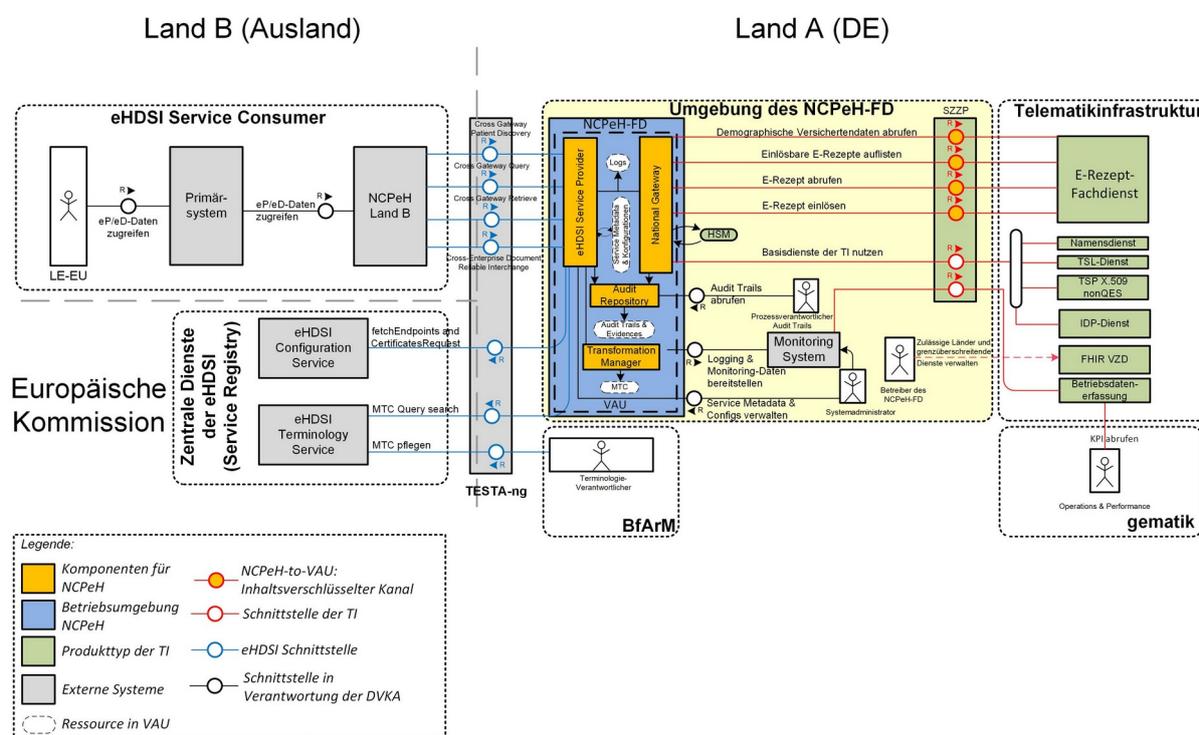


Abbildung 2: Architektur des NCPeH-FD ePrescription/eDispensation Land-A

Die Abbildung stellt die Architektur für den NCPeH-FD Anwendungsszenario ePrescription/eDispensation Land-A dar. Orange dargestellt sind logische Komponenten des NCPeH-FD. Die grün dargestellten Systeme stellen Produkttypen der TI dar. Die grau dargestellten Systeme befinden sich außerhalb der Systemgrenzen des NCPeH-FD. Die blau dargestellten Schnittstellen (blaue Linien) sind bereits durch die eHDSI spezifiziert, sie werden in diesem Dokument referenziert. Die Nutzung der rot dargestellten Schnittstellen (rote Linien) durch den NCPeH-FD werden in diesem Dokument spezifiziert. Die schwarz dargestellten Verbindungen sind in Verantwortung des Anbieters und werden vom Betreiber des NCPeH-FD bereitgestellt.

3 Systemkontext

3.1 Nachbarsysteme

Der NCPeH-FD nutzt Schnittstellen der folgenden Produkttypen der TI:

- ePA-Aktensystem mit den Diensten:
 - Information Service,
 - Authorization Service,
 - XDS Document Service,
- E-Rezept-Fachdienst,
- Zentraler IDP-Dienst,
- Namensdienst,
- TSP X.509 nonQES,
- TSL-Dienst,
- Betriebsdatenerfassung.

Der NCPeH-FD ist über einen Sicheren Zentralen Zugangspunkt (SZZP) an das zentrale Netz der TI (siehe [gemSpec_Net#3]) angebunden und tritt als Document Consumer für die ePA-AS und den E-Rezept-FD auf. Der NCPeH-FD nutzt den IDP-Dienst, um sich gegenüber ePA-AS und E-Rezept-FD zu authentisieren bzw. zu autorisieren. Die Dienste der zentralen TI, wie Namensdienst, TSP X.509 nonQES und TSL-Dienst, werden über die logische Komponente National Gateway genutzt.

Der NCPeH-FD zeichnet sein Leistungsverhalten in den Betriebsdaten auf und stellt diese dem Dienst Betriebsdatenerfassung zur Verfügung. Aus den Rohdaten können die Leistungsparameter für den Produkttyp NCPeH-FD ermittelt werden und als Grundlage für die Feststellung der Einhaltung des Service Levels dienen.

Wenn Gesundheitsdaten von Versicherten über den NCPeH-FD grenzüberschreitend mit einem neuen EU-Land ausgetauscht werden sollen, ist es notwendig, einen entsprechenden Eintrag für das EU-Land im FHIR VZD anzulegen. Ist der Eintrag erstellt, können Versicherte in der FdV nach dem EU-Land suchen. Der Betreiber des NCPeH-FD MUSS über einen organisatorischen Prozess (z.B. Service Request) bei der gematik beantragen, einen Eintrag in der FHIR VZD zu erstellen oder zu verwalten. Der Eintrag MUSS Informationen über das EU-Land und den grenzüberschreitenden Dienst, auf den das EU-Land zugreifen darf, enthalten.

In Richtung der eHDSI kommuniziert NCPeH-FD mit den NCPeH Land-B anderer europäischer Mitgliedsstaaten über die eigene logische Komponente eHDSI Service Provider. Die Kommunikation mit dem eHDSI Configuration Service und eHDSI Terminology Service erfolgt ebenfalls über die logische Komponente eHDSI Service Provider des NCPeH-FD.

3.2 Akteure

Im folgenden Abschnitt werden die am NCPeH-FD beteiligten Akteure betrachtet. Ein Akteur ist eine Person, Institution oder ein technisches System, die/das mit dem NCPeH-FD direkt oder indirekt über einen anderen Akteur interagiert. Diese Interaktion wird durch einen Anwendungsfall ausgelöst.

Tabelle 1: TAB_NCPeH_Übersicht_NCPeH-FD_Akteure

Rolle	Beschreibung
Versicherter/Patient	Im Kontext des NCPeH-FD ist der Patient eine versicherte Person, die in einem Versichertenverhältnis mit einer gesetzlichen Krankenversicherung steht. Für diese Person werden in der TI elektronische Gesundheitsdaten (z.B. Patientenkurzakte oder E-Rezepte) gespeichert. Anhand einer eindeutigen Patientennummer (z.B. Krankenversicherungsnummer (KVNR)) kann der NCPeH-FD in der TI relevante demographische oder gesundheitliche Daten des Versicherten ermitteln und dem behandelnden LE-EU zur Patientenidentifizierung oder medizinischen Behandlung/Beratung zur Verfügung stellen. Nur der Versicherte hat die Hoheit über die gespeicherten Daten. Der Versicherte muss den LE_EU den Zugriff auf seine Gesundheitsdaten gestatten.
Leistungserbringer im EU-Ausland (LE-EU)	Ein LE im EU-Ausland gehört zu einem zugriffsberechtigten Personenkreis nach den gesetzlichen Regelungen des EU-Landes und ist dort sicher authentifiziert. Die Gültigkeit der LE-EU Identität ist innerhalb der eHDSI nach dem Circle of Trust-Prinzip zur allgemeingültigen Vertrauensstellung im Land-A (Deutschland) valide.
Leistungserbringerinstitution im EU-Ausland (LEI-EU)	Eine LEI ist eine organisatorische Einheit oder juristische Person, in der ein oder mehrere LE-EU sowie deren berufsmäßige Gehilfen gemeinsam organisiert werden (z. B. Arztpraxen, Apotheken, Krankenhäuser). Im eHDSI-Kontext wird die LEI-EU zusammen mit der Identität des LE-EU repräsentiert.
ePA-Aktensystem	Das ePA-Aktensystem ist ein Produkttyp der ePA Fachanwendung (siehe [gemKPT_ePAfuerAlle]) und nimmt mehrere Aufgaben wahr, die über verschiedene ePA-Dienste realisiert werden. Für die Umsetzung relevanter grenzüberschreitender Anwendungsfälle wird der NCPeH-FD mit den folgenden ePA-Diensten interagieren: <ul style="list-style-type: none"> • Information Service: Die Nutzergruppen der ePA haben über den Information Service eine einfache Abfragemöglichkeit sowohl über die Existenz von Aktenkonten als auch über die aktuell erteilten oder nicht erteilten Widersprüche der Versicherten. • Authorization Service: Mit Hilfe des Dienstes Authorization Service stellt das ePA-Aktensystem sicher, dass nur authentifizierte und autorisierte Nutzer mit dem ePA Dienst

	<p>XDS Document Service interagieren können.</p> <ul style="list-style-type: none"> XDS Document Service: Der ePA Dienst XDS Document Service agiert als XDS-Akteur "Document Registry" und "Document Repository" und ist zuständig für die Verwaltung von Gesundheitsdaten der Versicherten (z.B. ePKA MIO). <p>Das ePA-Aktensystem verwaltet pro Versicherten-/Aktenkonto alle vom Versicherten legitimierte Zugriffe auf die Akte. Die ePA wird von mehreren Aktenanbietern/Kostenträgern für ihre Versicherten angeboten.</p>
Betreiber des NCPeH-FD	<p>Der Betreiber des NCPeH-FD ist eine Organisation, die die Bereitstellung des Dienstes auf Seiten der TI erbringt und verantwortet.</p> <p>In den Dokumenten der gematik ist dabei der "Serviceprovider TI unterstützender Produkte" gemäß [gemKPT_Betr] gemeint. Der Betreiber des NCPeH-FD kann über einen organisatorischen Prozess die Einträge für die zugelassenen EU-Länder und die Angaben, auf welche grenzüberschreitende Dienste die EU-Länder zugreifen dürfen, im FHIR VZD verwalten.</p>
E-Rezept-Fachdienst	<p>Der E-Rezept-Fachdienst ist ein offener fachanwendungsspezifischer Dienst in der TI, der den Workflow zu den E-Rezepten umsetzt.</p>
FHIR VZD	<p>Der Produkttyp FHIR Verzeichnisdienst (VZD) der TI stellt ein Verzeichnis zur Verfügung, in dem der Betreiber des NCPeH über einen organisatorischen Prozess für jedes EU-Land einen Eintrag anlegen und verwalten kann. Zu jedem Eintrag für ein EU-Land können Informationen darüber hinterlegt werden, auf welche grenzüberschreitenden Dienste aus dem EU-Land der Zugriff zulässig ist.</p> <p>Der Versicherte kann mit seinem FdV im FHIR VZD nach EU-Ländern suchen, aus denen er seine Gesundheitsdaten zum Zwecke der Behandlung bzw. Einlösung abrufen lassen möchte.</p>
Prozessverantwortliche r Audit Trails	<p>Dieser Akteur kann zur NCPeH-Betriebsorganisation gehören, ist zuständig für Analyse und Auswertung von Sicherheitsverletzungen und die Identifikation von relevanten Sicherheitsmaßnahmen. Ferner beantwortet er rechtmäßige Anfragen der betroffenen Personen (Versicherten) oder der befugten nationalen Stellen mit dem Ziel, die für den Fall erforderlichen Beweise (Evidence) zu liefern.</p>
NCPeH Land-B	<p>NCPeH eines anderen EU-Mitgliedsstaates (Nicht Deutschland), sendet Anfragen an einen eHDSI Service Provider, empfängt Daten als Antwort auf die Anfrage und leitet sie an die eigene nationale eHealth-Infrastruktur weiter.</p>
Terminologie-Verantwortlicher	<p>Der Terminologie-Verantwortliche ist ein Akteur, der für die Pflege des Inhalts des MTC (Master Translation/Transcoding</p>

(BfArM)	<p>Catalogue) verantwortlich ist. Dies umfasst unter anderem die Zuordnung von europäisch vereinbarten Valuesets Mappings und Terminologien, die über den zentralen Terminology Service mit dem NCPeH-FD geteilt werden können. Ferner legt der Terminologie-Verantwortliche im MTC ein Rechte- und Rollenkonzept fest, mit dem entsprechende Aktionen durchgeführt werden dürfen (z.B. Mapper, Translator). Der Terminologie-Verantwortliche ist für die Übersetzung der Terminologien zuständig und ist mit den Beziehungen zwischen Codesystemen vertraut, d. h. wie ein bestimmtes medizinisches Konzept zwischen zwei oder mehreren Kodiersystemen in Beziehung gesetzt werden kann. Entsprechend den gesetzlichen Regelungen nach § 219d Absatz 6 Satz 5 & 6 ist die BfArM mit dieser Aufgabe betraut.</p>
eHDSI Terminology Service	<p>Eine Reihe von Systemkomponenten, die für die Darstellung, den Zugriff und die Pflege des terminologischen Inhalts der im Rahmen von eHDSI ausgetauschten elektronischen Dokumente verwendet werden. Der ermöglicht die zentrale Bereitstellung von für den europäischen Austausch vereinbarten Wertelisten (Master Value Catalogue), auf die anschließend auf der Ebene der an der eHDSI teilnehmenden Länder zugegriffen wird (MTC). Eine lokale Synchronisierung des MTC im NCPeH-FD ist vorgesehen.</p>
eHDSI Configuration Service	<p>Der eHDSI Configuration Service ermöglicht allen europäischen NCPeHs die technische Funktionalität und den Ort der Verfügbarkeit der eHDSI-Dienste einzusehen und zuzuordnen. Zusätzliche Informationen und Sicherheitsartefakte der NCPeHs werden gemeinsam über einen Mechanismus geteilt, um die aktuelle Konfiguration dynamisch zu veröffentlichen und untereinander zu synchronisieren.</p>
Operations & Performance	<p>Der IT-Betrieb wird vom Betreiber des NCPeH-FD geleistet. Die Hauptaufgabe ist die robuste, resiliente und fachlich korrekte Zurverfügungstellung des NCPeH-FD und die Übernahme der Aufgaben des IT-Servicemanagements.</p>
Systemadministrator	<p>Dieser Akteur kann zur NCPeH-Betriebsorganisation gehören, ist zuständig für Administration von Metadaten über die angebotenen eHDSI-Dienste durch NCPeH-FD und International Search Mask auf dem eHDSI Configuration Service. Ferner stellt er sicher, dass im NCPeH-FD die aktuelle Version des MTC (Master Translation/Transcoding Catalogue) vorhanden ist und dass eine regelmäßige Auswertung von Logging und Monitoring-Daten stattfindet.</p>
Zentraler IDP-Dienst	<p>Der zentrale IDP-Dienst (weiter im Dokument als IDP-Dienst) verwaltet und steuert den Smartcard-basierten Authentifizierungsprozess für verschiedene Clients und stellt diesen nach erfolgter Authentifizierung einen Authorisation_Code bereit. Das autorisierte Nutzersystem, das im Besitz des Authorisation_Code ist,</p>

	kann den <code>Authorisation_Code</code> gegen den <code>ID_TOKEN</code> mit den Identitätsdaten des Nutzers eintauschen.
Zertifikatsherausgeber SM-B NCPeH	Der Zertifikatsherausgeber signiert die Certificate Signing Requests (CSR) für die SM-B NCPeH Zertifikate und erzeugt initiale Einträge im VZD anhand von Zertifikatsinformationen.

4 Übergreifende Festlegungen

Das folgende Kapitel beschreibt übergreifende Anforderungen an den NCPeH-FD zur Unterstützung der Fachlogik.

4.1 Anbindung an die eHDSI

Analog zu den gesetzlichen Vorgaben der Europäischen Union gilt es zwingend, auch die Spezifikation der eHDSI zu beachten.

Als fundamentale Dokumente zur Spezifikation sind die [eHDSI_System_Architecture_Specifications] und [eHDSI_NCPeH_Architecture_Specification] zu beachten. Der [eHDSI_Requirements_Catalogue] spiegelt das Dokument mit den allgemeinen Anforderungen wider. Spezielle Anforderungen, wie z.B. an die Sicherheit und den Datenschutz sind in den entsprechenden Detaildokumenten zu finden, hier sei beispielsweise die [eHDSI_Security_Services_Specification] genannt. Wenn der NCPeH-FD in den Betrieb überführt werden soll, kann zur Erfassung der notwendigen Schritte auf das [eHDSI_Starting_Toolkit] zurückgegriffen werden.

Einen guten Überblick über die bestehenden Spezifikationen für den Betreiber des NCPeH-FD zur Herstellung der technischen und semantischen Interoperabilität innerhalb der eHDSI bietet [eHDSI_Specifications].

4.1.1 Konfigurationsparameter

Die Verwaltung der in der Tabelle TAB_NCPeH_KONFIGURATIONSPARAMETER aufgelisteten Konfigurationsparameter werden durch den Systemadministrator über eine Managementschnittstelle des NCPeH-FD verwaltet und wird im Anwendungsfall [5.3.4-NCPeH_UC_8 - Konfigurationsparameter verwalten] beschrieben.

Tabelle 2: TAB_NCPeH_Konfigurationsparameter

Konfigurationsparameter	Wert
HOME_COMMUNITY_ID_NCPeH-FD	1.2.276.0.76.4.291 Der Wert ist die eindeutige Kennung des NCPeH-FD und wird im Rahmen der eHDSI im grenzüberschreitenden Austausch von Gesundheitsdaten verwendet. Weitere Informationen zum Wert sind in [DIMDI_HCID_NCPeH] enthalten.
OID_KVNR_ASSIGNING_AUTHORITY	1.2.276.0.76.3.1.580.147
OID_AC_ePKA_ASSIGNING_AUTHORITY	1.2.276.0.76.4.298
OID_AC_eRp_ASSIGNING_AUTHORITY	1.2.276.0.76.4.299

WHITELIST_NCPeH_COUNTRY-B	Die Liste besteht aus Einträgen und enthält Angaben zu den europäischen Ländern, mit denen ein gegenseitiger Betrieb zum grenzüberschreitenden Austausch von Gesundheitsdaten besteht. Jeder Eintrag besteht aus Attributen: Ländercode (ISO 3166-1 Alpha 2) und die HomeCommunityId des NCPeH Land-B.
ABSOLUTE_TIMEOUT_ePA_SESSION	20 Minuten Zeitlicher Dauerablauf einer im NCPeH-FD internen Aktenkontosession zum ePA-Aktensystem. Dieser Konfigurationsparameter gibt die absolute Zeit an, nach der bei Inaktivität einer Aktenkontosession die sämtlichen Daten dieser Session aus flüchtigen Speichern sicher gelöscht werden können.
ePKA_MIO_FORMATCODE	urn:gematik:ig:pka:v1.0 Bezeichnung: "Patientenkurzakte (gematik) v1.0" CodeSystem (Deutsche Dokumentenformate FHIR) mit der OID 1.3.6.1.4.1.19376.3.276.1.5.6
LIST_ePA_ANBIETER_FQDN	Eine Liste von Einträgen mit den relevanten FQDNs der einzelnen Anbieter der ePA-Aktensysteme. Ein FQDN gehört immer genau zu einem Anbieter des ePA-Aktensystems.
CRL_DOWNLOAD_TIMEOUT	5 Sekunden Der Timeout-Parameter definiert hier, zu welchem Zeitpunkt das System ein Timeout bei Nichterreichbarkeit oder ausbleibender Response des Dienstes meldet bzw. bestimmt die maximale Dauer für das Herunterladen der CRL.
OCSP_RESPONSE_TIMEOUT	3 Sekunden Der Timeout-Parameter für OCSP-Abfragen definiert hier, zu welchem Zeitpunkt der NCPeH-FD ein Timeout bei Nichterreichbarkeit bzw. ausbleibender Response des OCSP-Responders meldet.
CRL_CACHE_REFRESH_PERIOD	24 Stunden Bestimmt den Aktualisierungszeitraum für den lokalen CRL-Cache (CRL für den

	Vertrauensraum der eHDSI). Nach Ablauf der Zeit MUSS nach Bedarf ein erneuter Abruf der CRL-Datei erfolgen.
OCSP_CACHE_REFRESH_PERIOD	12 Stunden Der Wert des Parameters bestimmt den Aktualisierungszeitraum für den lokalen Cache der OCSP-Antwort eines Zertifikats (bezogen auf die eindeutige Zertifikatsseriennummer) und stellt die Gültigkeitsdauer der darin zwischengespeicherten OCSP-Antwort dar.
IDP_RESPONSE_TIMEOUT	5 Sekunden Der Timeout-Parameter für die Kommunikation mit dem zentralen IDP-Dienst definiert hier, zu welchem Zeitpunkt der NCPeH-FD ein Timeout bei Nichterreichbarkeit bzw. ausbleibender Response des IDP-Dienstes meldet.
ePA_RESPONSE_TIMEOUT	5 Sekunden Der Timeout-Parameter für die Kommunikation mit dem ePA-Aktensystem definiert hier, zu welchem Zeitpunkt der NCPeH-FD ein Timeout als Nichterreichbarkeit bzw. ausbleibender Response des ePA-Aktensystems meldet.
eRp_RESPONSE_TIMEOUT	5 Sekunden Der Timeout-Parameter für die Kommunikation mit dem E-Rezept-FD definiert hier, zu welchem Zeitpunkt der NCPeH-FD ein Timeout als Nichterreichbarkeit bzw. ausbleibender Response des E-Rezept-FD meldet. Disclaimer: Der Wert für diesen Konfigurationsparameter muss noch definiert werden.
ePA_VAU_CHANNEL_TIME	24 Stunden Der Wert des Parameters ist die Zeit, die eine bestehende VAU-Verbindung zum ePA-Aktensystem nachgenutzt werden darf, bevor sie abgebaut oder neu aufgebaut werden muss.
TERMINOLOGY_SERVICE_BASE_URL	Der Wert des Parameters ist eine Basis-URL, die für alle relativen URLs bei der Kommunikation mit dem eHDSI Terminology Service zu verwenden ist. Der Wert des

	Parameters wird vom eHDSI Solution Provider vorgegeben oder ist auf der Seite [eHDSI_CTS2.0_USER_GUIDE] für die jeweilige Umgebung enthalten.
TERMINOLOGY_SERVICE_USERNAME	Der Wert des Parameters wird durch den eHDSI Solution Provider vorgegeben, sobald NCPeH-FD in der technischen Rolle als "NCPeH User" gemäß [eHDSI_CTS#4.2] beim eHDSI Terminology Service registriert ist. Der Registrierungsprozess ist in [eHDSI_CTS2.0_USER_GUIDE] beschrieben.
TERMINOLOGY_SERVICE_PASSWORD	Der Wert des Parameters wird durch den eHDSI Solution Provider vorgegeben, sobald NCPeH-FD in der technischen Rolle als "NCPeH User" gemäß [eHDSI_CTS#4.2] beim eHDSI Terminology Service registriert ist. Der Registrierungsprozess ist in [eHDSI_CTS2.0_USER_GUIDE] beschrieben.
CLIENT_ID_IDP_DIENST	Der Wert des Parameters wird durch den Anbieter des zentralen IDP-Dienstes vorgegeben, sobald der NCPeH-FD beim IDP-Dienst registriert ist.
DOWNLOAD_DISCOVERY_DOCUMENT	Der Wert des Parameters wird vom Anbieter des zentralen IDP-Dienstes bei der organisatorischen Registrierung des NCPeH-FD beim IDP-Dienst angegeben.
TSL_GRACE_PERIOD	0 Tage Der Wert legt fest, wie lange eine vorhandene TSL gemäß GS-A_4898 nach Ablauf der initialen Gültigkeitsdauer maximal genutzt werden darf.
TSL_DOWNLOAD_TIMEOUT	5 Sekunden Der Timeout-Parameter für die Kommunikation mit dem TSL-Dienst definiert hier, zu welchem Zeitpunkt der NCPeH-FD ein Timeout bei Nichterreichbarkeit bzw. ausbleibender Response meldet.
TSL_UPDATE_INTERVAL	Der Wert legt fest, nach welcher Zeit die Prüfung auf TSL-Aktualisierung (Hashwertprüfung) gemäß GS-A_4899 durchgeführt werden muss.

4.1.2 Datenaustausch mit zugelassenen EU-Ländern

Ein grenzüberschreitender Austausch von Gesundheitsdaten mit anderen europäischen Ländern kann erst dann erfolgen, wenn die dafür notwendigen technischen und organisatorischen Voraussetzungen geschaffen sind. Das jeweilige europäische Land, mit dem die Gesundheitsdaten ausgetauscht werden sollen, muss nachweisen, dass es die Vorgaben zur Interoperabilität, Sicherheit und Datenschutz der eHDSI- und EU durch das Land erfolgreich umgesetzt hat. Ferner bedarf das Land vor der eigentlichen Inbetriebnahme mit einem neuen Dienst, Anwendungsfall oder Feature die offizielle Zustimmung durch das eHealth Network (das höchste Entscheidungsgremium in der EU zur eHealth). Auch die Entscheidung, ob ein Austausch von Gesundheitsdaten mit einem bestimmten europäischen Land erfolgen soll, muss durch Deutschland getroffen werden. Daher ist es notwendig, dass der NCPeH-FD die Länderidentitäten verwaltet, mit denen ein grenzüberschreitender Datenaustausch zulässig ist.

Nach Erhalt einer Anfrage von einem NCPeH Land-B für einen grenzüberschreitenden Anwendungsfall gemäß [eHDSI_Audit_Trail_Profile#1.2.3] MUSS der NCPeH-FD einen Non-Repudiation of Receipt Eintrag gemäß [4.1.7.2- Non-Repudiation of Receipt erstellen] in der Komponente Audit Repository speichern. Im weiteren Verlauf der Verarbeitung der Anfrage MUSS der NCPeH-FD gemäß [eHDSI_Audit_Trail_Profile#1.2.3] einen Audit Trail Eintrag gemäß [4.1.7.3- Patient Privacy Audit Trail Eintrag erstellen] in der Komponente Audit Repository speichern.

Der NCPeH-FD MUSS vor der weiteren Verarbeitung der Anfrage prüfen, ob die Identität des Land-B, von dem die Anfrage stammt, auf der WHITELIST_NCPeH_COUNTRY-B (siehe [4.1.1- Konfigurationsparameter]) enthalten ist. Dabei MUSS der NCPeH-FD die Identität des Land-B vom gültigen TLS-Zertifikat des NCPeH Land-B aus dem Element Subject: C (Country) verwenden. Falls der Ländercode nicht auf der Liste WHITELIST_NCPeH_COUNTRY-B enthalten ist, MUSS der NCPeH-FD eine Verarbeitung der Anfrage abbrechen und dem NCPeH Land-B mit dem Fehlercode ERROR_GENERIC gemäß [eHDSI_NCPeH_Components#6.4] antworten.

Falls Die Prüfung im Zusammenhang mit der Nutzung der Schnittstelle [6.1.1- Operation Cross_Gateway_Patient_Discovery::RespondingGateway_PRPA_IN201305UV02] erfolgt, dann MUSS der NCPeH-FD mit der Fehlermeldung gemäß folgender Tabelle an den NCPeH Land-B antworten:

Tabelle 3: TAB_NCPeH_XCPD_Fehlermeldung_nicht_zugelassenes_EU-Land

Reason Encoding gemäß [eHDSI_XCPD_Profile#2.3.3]	acknowledgementDetail
<pre><mitigatedBy typeCode="MITGT"> <detectedIssueManagement classCode="ACT" moodCode="ENV"> <code code="InsufficientRights" codeSystem="1.3.6.1.4.1.12559.11.10.1.3.2.2.1"/> </detectedIssueManagement> </mitigatedBy></pre>	<pre>acknowledgementDetail.Code= ERROR_P I_GENERIC acknowledgementDetail.Text = Patient Identification Error acknowledgementDetail.Location = There is no agreement on the transfer of patient data with your country.</pre>

Der NCPeH-FD MUSS einen Non-Repudiation of Origin Eintrag gemäß [4.1.7.1- Non-Repudiation of Origin erstellen] in der Komponente Audit Repository speichern.

4.1.3 eHDSI Basisleistungen

Die Schnittstellen des NCPeH-FD sind durch IHE XCPD Profile bzw. IHE XCA Profile definiert. In Anlehnung an das SOA-Modell werden die Nachrichtenstrukturen (Header und Body) durch IHE definiert. In eHDSI wird der SOAP-Header durch WS-Security und SAML geregelt. Der SOAP-Body wird durch den Standard definiert, der die Transaktion regelt und kann auf ebXML für XCA (zum Abrufen von medizinischen Versichertendaten) oder auf HL7V3 für XCPD-Abfragen (zur Versichertenidentifizierung) basieren.

Die eHDSI beschreibt die Nachrichtenstruktur, wie sie zwischen zwei NCPeHs (Service Consumer und Service Provider) fließen soll und stellt in [eHDSI_Messaging_Profile#1] Vorgaben zur Implementierung der eHDSI-Nachrichtenstrukturen und zur Verwendung konkreter Sicherheitsstandards zur Verfügung. Außerdem Vorgaben zur Transport- und Nachrichtenschicht, Einbettung von Sicherheitstokens und allgemeine Verarbeitung von SOAP-Nachrichten sind in [eHDSI_Messaging_Profile#5] enthalten. Weiterführende normative Vorgaben zur Nutzung und Verarbeitung der eHDSI-Nachrichtenformate, Transportschicht, SOAP Binding, SAML-Assertions und Signaturerstellung sind in [eHDSI_NCPeH_Components#4.3] enthalten.

4.1.3.1 Sicherer Kanal: TESTA-ng und TLS

Das Vertrauen zwischen Service Consumer, Service Provider und zentralen Diensten der eHDSI basiert auf gegenseitig vertrauenswürdigen und sicheren Kanälen zwischen den zugrundeliegenden Netzknoten. Der Aufbau des gegenseitigen Vertrauens zwischen NCPeH-FD und anderen NCPeHs und zentralen eHDSI-Diensten MUSS gemäß Vorgaben aus [eHDSI_Messaging_Profile#3] und [eHDSI_NCPeH_Configuration_Production_Environment] zur Einrichtung und Anwendung von TESTA-ng und TLS erfolgen.

Der NCPeH-FD MUSS beim Aufbau von TLS-Verbindungen innerhalb der eHDSI Vorgaben aus [eHDSI_Messaging_Profile#1.2] umsetzen. Dabei MUSS der NCPeH-FD TLS-Version 1.2 und TLS-Version 1.3 unterstützen. Er DARF NUR empfohlene Cipher Suites gemäß Vorgaben aus [SOGIS-IS-2020#6.1] akzeptieren.

Der NCPeH-FD MUSS das beim TLS-Handshake empfangene TLS-Zertifikat des NCPeH Land-B nach Vorgaben aus [4.1.3.6- Validierung von Zertifikaten in eHDSI] prüfen und erst bei erfolgreicher Zertifikatsprüfung eine sichere TLS-Verbindung zum NCPeH Land-B aufbauen.

Falls bei der Überprüfung des TLS-Zertifikats die Gültigkeit erfolgreich bestätigt werden konnte, MUSS der NCPeH-FD aus dem Element Subject: C (Country) den Ländercode des Landes entnehmen, in die Variable `tls_country` zwischenspeichern und in den Kontext der weiteren Verarbeitung der jeweiligen eHDSI-Anfrage bringen.

Tritt bei der Prüfung des TLS-Zertifikats ein Fehler auf, MUSS der NCPeH-FD den Aufbau der TLS-Verbindung zum NCPeH Land-B abbrechen.

4.1.3.2 Zeitsynchronisation

Innerhalb des eHDSI Circle of Trust sind alle Clients und Services (Service Consumer, Service Provider, zentrale Dienste) auf eine konsistente Systemzeit angewiesen. Daher MUSS der NCPeH-FD die Aktualität seiner Systemzeit gemäß Vorgaben aus [eHDSI_Messaging_Profile#4] abfragen und konsistent halten (Synchronisation).

4.1.3.3 eHDSI Identifier

Die eHDSI definiert konkrete URNs, OIDs und Coding Schema gemäß [eHDSI_NCPeH_Components#6.2], die im NCPeH-FD zu verwenden sind.

4.1.3.4 Allgemeine Fehlerbehandlung

Der NCPeH-FD MUSS die Behandlung von Fehler in der Kommunikation, Nachrichten- und Dokumentenkodierung und Nachrichtenverarbeitung gemäß Vorgaben aus [eHDSI_Messaging_Profile#6] umsetzen.

In Abhängigkeit von der jeweiligen Situation wird bei Fehlerfällen auf konkrete Fehlernachrichten bzw. -codes in den einzelnen technischen Use Cases (TUC) im [6-Funktionsmerkmale] näher eingegangen.

4.1.3.5 Umgang mit Zertifikaten der eHDSI

Die Authentizität und Integrität der Dienste in der eHDSI-Kommunikation wird mit digitalen Zertifikaten gesichert. Die eHDSI definiert zwei Zertifikatstypen: Seal- und TLS-Zertifikat (siehe [eHDSI_x509_Certificate_Profile#3.1]). Der NCPeH-FD benötigt das TLS-Zertifikatsprofil für Land-A Szenarien und für Land-B Szenarien sowohl das Seal- als auch TLS-Zertifikatsprofil, um sichere Verbindungen zu anderen NCPeHs oder zentralen Diensten der eHDSI herzustellen. Der Herausgeber (CA) der beiden Zertifikatstypen ist GlobalSign.

Der Prozess zur Antragstellung für TLS-Zertifikate der eHDSI ist in [eHDSI_Certificates_Procedure_Request#II- TLS Certificates] und zur Verlängerung bzw. Erneuerung von Zertifikaten ist in [eHDSI_Certificates_Procedure_Request#IV- Certificates Renewal] beschrieben. Die Beschreibung der Sperrung von Zertifikaten der eHDSI ist in [eHDSI_Certificates_Procedure_Request#III- Certificates Revocation] enthalten.

Der NCPeH-FD MUSS sein privates TLS-Schlüsselmaterial im HSM erzeugen und dort zur Signaturerstellung anwenden. Der NCPeH-FD MUSS die öffentlichen Zertifikate des Herausgebers (Root und Intermediate) gemäß [eHDSI_Certificates_Procedure_Request] in seinem lokalen Truststore in der VAU hinterlegen, die bei der Prüfung von Zertifikatsketten als Vertrauensanker zu betrachten sind. Ferner MUSS der NCPeH-FD die öffentlichen Zertifikate des eHDSI Configuration und Terminology Service in seinem lokalen Truststore in der VAU speichern. Die Aufnahme der öffentlichen Zertifikate in dem lokalen Truststore erfolgt gemäß Anwendungsfall [5.3.4- NCPeH_UC_8 - Konfigurationsparameter verwalten].

Der Systemadministrator muss sicherstellen, dass an den NCPeH-FD über eine Management-Schnittstelle nur gültige, nicht abgelaufene oder nicht gesperrte Zertifikate des CA oder der zentralen Dienste der eHDSI zur Installation im lokalen Truststore übergeben werden. Bei der Installation der Zertifikate MUSS der NCPeH-FD alte Zertifikate der CA und der zentralen eHDSI-Dienste aus dem lokalen Truststore entfernen. Bei der Befüllung des Truststore MUSS der NCPeH-FD alle Service Metadata der berechtigten NCPeH Land-B (gemäß Einträgen im Konfigurationsparameter WHITELIST_NCPeH_COUNTRY-B aus [4.1.1- Konfigurationsparameter]) vom Configuration Service der eHDSI herunterladen, in den lokalen Truststore aufnehmen und alte Zertifikate der NCPeH Land-B aus dem Truststore entfernen (siehe [4.1.4- Service Metadata des NCPeH Land-B abrufen]).

Das Vertrauen zum NCPeH Land-B wird durch die eHDSI-PKI sichergestellt, da die gegenseitige Authentifizierung der beiden Kommunikationsteilnehmer beim Aufbau der TLS-Verbindung unter Nutzung der TLS-Zertifikate erfolgt, deren Zertifikatsherausgeber (CA) der gemeinsame Vertrauensanker ist. Bei Erstellung von SAML-Assertions (Identity und TRC Assertion) durch NCPeH Land-B, deren Signatur mit einem Seal-Zertifikat der eHDSI erstellt wurde, kann durch die Prüfung im NCPeH-FD auf gemeinsamen Zertifikatsherausgeber (CA) das Vertrauen zu dem Seal-Zertifikat herstellen.

Wird für die Signatur der SAML-Assertion im Land-B ein Seal-Zertifikat einer anderen PKI verwendet, muss der NCPeH Land-B eine SMP-Datei inkl. des öffentlichen Seal-Zertifikats einrichten und sie auf dem zentralen eHDSI Configuration Service mit anderen NCPeHs teilen. Damit der NCPeH-FD das Seal-Zertifikat prüfen kann, MUSS im NCPeH-FD das öffentliche Zertifikat des Herausgebers, welches das Seal-Zertifikat ausgestellt hat, in den lokalen Truststore aufgenommen werden (siehe [4.1.1- Konfigurationsparameter]). Der NCPeH-FD MUSS die Prüfung des Seal-Zertifikats gemäß [4.1.3.6- Validierung von Zertifikaten in eHDSI] durchführen. Dadurch kann der NCPeH-FD dem öffentlichen Seal-Zertifikat vertrauen und die Integrität und Authentizität der SAML-Assertion des NCPeH Land-B validieren.

4.1.3.6 Validierung von Zertifikaten in eHDSI

Der NCPeH-FD MUSS das zu prüfende Zertifikat des NCPeH Land-B (SEAL- oder TLS-Zertifikat) gemäß Vorgaben aus [eHDSI_X509_Certificate_Profile#2.4] und nach folgenden Schritten überprüfen:

1. Gültigkeitsprüfung des zu prüfenden Zertifikats:
Prüfung des Zertifikats auf seine aktuelle zeitliche Gültigkeit, damit ist der Zeitraum gemeint, der im Feld `validity` steht. Dabei kommt folgender Algorithmus zu tragen: `notBefore =<Referenzzeitpunkt &¬After >=Referenzzeitpunkt` entspricht einem zeitlich gültigen Zertifikat. Der Referenzzeitpunkt ist die aktuelle Systemzeit des NCPeH-FD.
2. Prüfung der Extension `KeyUsage` auf Vorhandensein:
Zudem muss die `KeyUsage` auf die richtige Belegung entsprechend der vorgesehenen `KeyUsage` gemäß [eHDSI_X509_Certificate_Profile#3.1] geprüft werden.
3. Ermittlung des passenden öffentlichen CA-Zertifikats aus dem lokalen Truststore:
Issuer `DName` des Zertifikats muss identisch mit dem Subject `DName` des CA-Zertifikats sein und `AuthorityKeyIdentifier` des Zertifikats mit `SubjectKeyIdentifier` des CA-Zertifikats
4. Mathematische Prüfung der Signatur des Zertifikats mit Hilfe des ermittelten CA-Zertifikats:
Die Signatur und der verwendete Algorithmus werden aus dem Zertifikat ausgelesen. Verifikation der Signatur und Hashwert-Vergleich (siehe Verfahren in [RFC5280#6.1]).
5. Status- und Sperrprüfung mittels CRL-Prüfung oder OCSP-Abfrage:
Hinweis: Der Downloadpunkt für Status- und Sperrprüfung ist gemäß [eHDSI_X509_Certificate_Profile#3.1] entweder im Element `CRL Distribution Points` oder im Element `Authority Info Access` des TLS-Zertifikats enthalten.
 - a. CRL-Prüfung - Validierung einer CRL und Ermittlung der Sperrinformation zum Zertifikat:
Vor dem Download der CRL-Datei muss geprüft werden, ob unter Berücksichtigung der Dauer des Konfigurationsparameters `CRL_CACHE_REFRESH_PERIOD` ([4.1.1- Konfigurationsparameter]) gültige Sperrliste im NCPeH-FD vorliegt (z. B. im lokalen Cache). Ein Zwang, CRL-Daten zu cachen, existiert nicht.
Falls die CRL-Daten nicht im lokalen Cache vorhanden sind, kann eine CRL gemäß [eHDSI_X509_Certificate_Profile#3.1] (siehe Element `CRL Distribution Points`) heruntergeladen werden, unter Einhaltung der maximalen zeitlichen Dauer des Herunterladens der CRL (siehe Konfigurationsparameter `CRL_DOWNLOAD_TIMEOUT` gemäß [4.1.1- Konfigurationsparameter]). Die zeitliche Gültigkeit der heruntergeladenen CRL (`Systemzeit < crl.NextUpdate`) (siehe [RFC5280#5.1.2.5]) wird geprüft. Es wird anhand der `IssuingDistributionPoint`-Erweiterung in der Sperrliste (CRL) geprüft, ob es sich um eine indirekte CRL (`indirectCRL-bit`) handelt (siehe [RFC5280#5.2.5])

und [X.509#7.12]). Prüfung der Signatur der CRL erfolgt gemäß [RFC5280#6.3.3]. Die Auswertung der CRL-Einträge erfolgt mit der Suche nach der Zertifikatsseriennummer des zu überprüfenden Zertifikats in der CRL (siehe [RFC5280#6.3.3]). Bei der Verarbeitung der CRL sind Vorgaben aus [eHDSI_X509_Certificate_Profile#3.2] zu berücksichtigen. Falls bei der Suche ein oder mehrere Einträge gefunden wurden, wird die CRL-Entry-Erweiterung „CertificateIssuer“ ausgelesen und deren Inhalt mit dem Issuer DName des Zertifikats verglichen. Nur wenn der Inhalt der CertificateIssuer-Erweiterung mit diesem DName übereinstimmt, ist das Zertifikat gesperrt, siehe [RFC5280#6.3.3]. *Hinweis: Die Validierung der CRL kann unabhängig von der Zertifikatsprüfung durchgeführt werden und muss also nicht bei jeder einzelnen CRL-Prüfung eines Zertifikats durchlaufen werden, solange gewährleistet ist, dass die CRL zeitlich gültig ist. Das Cachen der CRL ist optional.*

- b. OCSP-Abfrage - Ermittlung der Statusinformation zum Zertifikat durch Abfrage des zugeordneten OCSP-Dienstes:

Vor der OCSP-Abfrage muss geprüft werden, ob unter Berücksichtigung der Dauer des Konfigurationsparameters OCSP_CACHE_REFRESH_PERIOD (siehe [4.1.1-Konfigurationsparameter]) gültige Statusinformationen zum prüfenden Zertifikat bereits vorliegen (z. B. im lokalen Cache). Ein Zwang, OCSP-Responses zu cachen, existiert nicht.

Ansonsten wird die OCSP-Abfrage für das zu prüfende Zertifikat mit dem Parameter ENFORCE_CERTHASH_CHECK=true gesendet, unter Beachtung des Konfigurationsparameters OCSP_RESPONSE_TIMEOUT (siehe [4.1.1-Konfigurationsparameter]) bei Nicht-Erreichbarkeit oder ohne Antwort vom OCSP-Responder. Die OCSP-Response muss gemäß [RFC6960#4.2] verarbeitet werden. Wenn der zuständige OCSP-Responder die Statusinformation des Zertifikats mit einem Wert „revoked“ oder „unknown“ zurückgibt oder eine erforderliche certHash-Erweiterung fehlt bzw. falsch ist, DARF das Zertifikat NICHT als gültig bewertet werden.

4.1.4 Service Metadata des NCPeH Land-B abrufen

Die eHDSI sieht vor, dass jeder NCPeH seine Service Metadata mittels des SMP/SML-Protokolls an den Configuration Service der eHDSI übermitteln muss, damit bei grenzüberschreitendem Datenaustausch die Vertraulichkeit, Integrität und Nichtabstreitbarkeit gewährleistet wird. Dies gilt auch für NCPeH Land-B. Damit der NCPeH-FD sichere TLS-Verbindungen zu NCPeH Land-B aufbauen und die Authentizität und Integrität der IdA-/TRC Assertions, die durch NCPeH Land-B oder eine andere Entität aus Land-B ausgestellt wurden, validieren kann, muss der NCPeH-FD über die gültigen Service Metadata der NCPeH Land-B verfügen.

Die auf dem eHDSI Configuration Service verfügbaren Service Metadata der NCPeH Land-B befinden sich in einem öffentlichen Verzeichnis, aus dem alle NCPeHs die Service Metadata abrufen können. Der NCPeH-FD MUSS täglich die Service Metadata der NCPeH Land-B (siehe Konfigurationsparameter WHITELIST_NCPeH_COUNTRY-B [4.1.1-Konfigurationsparameter])

) mittels des SMP/SML-Protokolls gemäß Vorgaben aus [eHDSI_Service_Location_and_Capability_Lookup_Profile#3] und [BDX-smp-v1.0] vom eHDSI Configuration Service abrufen. Beim Abruf von länderspezifischen Service Metadata MUSS der NCPeH-FD das Element ServiceGroup/ParticipantIdentifier nach folgender Struktur befüllen und in der Anfrage an den eHDSI Configuration Service senden: "urn:ehhealth:" + Ländercode + ":ncp-idp". Der Ländercode des Land-B muss dem Format gemäß ISO 3166-1 Alpha 2 entsprechen.

Der NCPeH-FD MUSS im Erfolgsfall das in der Rückmeldung enthaltene XML-Dokument (SignedServiceMetadata-Dokument) auf Schemavalidierung nach Vorgaben aus [BDX-smp-v1.0] prüfen. Falls das Dokument schemakonform ist, MUSS der NCPeH-FD die vom eHDSI Configuration Service erstellte Dokumentensignatur aus dem Element SignedServiceMetadata/Signature auf Gültigkeit gemäß Vorgaben aus [BDX-smp-v1.0#3.6.2] prüfen. Bei dem Zertifikat aus dem Element ds:X509Data MUSS es sich um das öffentliche Zertifikat des eHDSI Configuration Service handeln und das Zertifikat MUSS bereits im lokalen Truststore des NCPeH-FD vorhanden sein. Dieses Zertifikat MUSS gemäß [4.1.3.6- Validierung von Zertifikaten in eHDSI] geprüft werden.

Der NCPeH-FD DARF für die Events "IDP Provide HCP Authentication used for proprietary issuance" und "NCP Provide TRC Assertion" gemäß [eHDSI_Audit_Trail_Profile#2.3.5.7] NUR die Service Metadata zur weiteren Datenverarbeitung extrahieren, deren folgende Elemente die Prüfkriterien erfüllen:

Tabelle 4: TAB_NCPeH_Service_Metadata_IDP_Provider

Event	Element aus SignedServiceMetadata-Datei	Prüfkriterium
IDP Provide HCP Authentication used for proprietary issuance	SignedServiceMetadata/ServiceMetadata/ServiceInformation/DocumentIdentifier	MUSS identisch mit dem Wert sein: urn:ehealth:CountryBIdentityProvider::identityProvider::HPAuthentication##epsos-91
	SignedServiceMetadata/ServiceMetadata/ServiceInformation/ProcessList/Process/ProcessIdentifier	MUSS identisch mit dem Wert sein: urn:identityProvider::HPAuthentication
NCP Provide TRC Assertion	SignedServiceMetadata/ServiceMetadata/ServiceInformation/DocumentIdentifier	MUSS identisch mit dem Wert sein: urn:ehealth:CountryBNCP::identityProvider::TRCAssertion##eHDSI-92
	SignedServiceMetadata/ServiceMetadata/ServiceInformation/ProcessList/Process/ProcessIdentifier	MUSS identisch mit dem Wert sein: urn:identityProvider::TRCAssertion

Falls bereits für ein ausgewähltes ProcessIdentifier (siehe *Tabelle TAB_NCPeH_Service_Metadata_IDP_Provider* und unten Abschnitt "Speicherung von Referenzwerten") bezogen auf ein Land-B im Truststore ein Zertifikat vorhanden ist, MUSS der NCPeH-FD die SMP-Datei auf Aktualität prüfen, bevor mit Signatur- und Zertifikatsprüfung der SMP-Datei begonnen wird. Die Prüfung besteht aus einem Vergleich des bereits in der VAU gespeicherten Referenzwertes SignatureValue (siehe unten Abschnitt "Speicherung von Referenzwerten") mit dem Wert des Elementes ServiceMetadata/ServiceInformation/Extension/Signature/SignatureValue aus der neu heruntergeladenen SMP-Datei. Falls die Werte identisch sind, kann davon ausgegangen werden, dass die SMP-Datei keine Änderungen enthält und das im Truststore vorhandene Zertifikat nicht aktualisiert oder entfernt werden muss. An dieser Stelle der NCPeH-FD SOLL die SMP-Datei nicht weiterverarbeiten.

Ansonsten, falls die Werte unterschiedlich sind, MUSS der NCPeH-FD mit der weiteren Verarbeitung der SMP-Datei fortsetzen.

Jede ausgewählte ServiceMetadata-Datei enthält eine Signatur, die mit dem Schlüsselmaterial des NCPeH Land-B erstellt wurde. Die Gültigkeit der Signatur soll die Integrität der jeweiligen ServiceMetadata bestätigen. Der NCPeH-FD MUSS das Zertifikat aus dem Element

ServiceMetadata/ServiceInformation/Extension/Signature extrahieren und die vollständige Zertifikatskette überprüfen, ob das Zertifikat von der vertrauenswürdigen CA der eHDSI ausgestellt wurde. Die Überprüfung des extrahierten Zertifikats MUSS gemäß [\[4.1.3.6- Validierung von Zertifikaten in eHDSI\]](#) durchgeführt werden. Der NCPeH-FD MUSS die Signatur aus dem Element ServiceMetadata/ServiceInformation/Extension/Signature nach Vorgaben aus [\[BDX-smp-v1.0#3.6.2\]](#) validieren.

Nach erfolgreicher Signatur- und Zertifikatsprüfung MUSS der NCPeH-FD das nächste Zertifikat aus dem folgenden Element der ServiceMetadata extrahieren, gemäß Vorgaben im [\[4.1.3.6- Validierung von Zertifikaten in eHDSI\]](#) prüfen und nach erfolgreicher Zertifikatsprüfung NUR dieses Zertifikat in den lokalen Truststore aufnehmen:

- ServiceMetadata/ServiceInformation/ProcessList/Process/ServiceEndpointList/Endpoint/Certificate
(der Wert ist mit Base64 kodiert und muss evtl. vor Aufnahme in den Truststore dekodiert werden)

Speicherung von Referenzwerten

In diesem Zusammenhang MUSS der NCPeH-FD folgende Referenzwerte mit dem vorher extrahierten Zertifikat in Verbindung setzen und in der VAU speichern:

- Ländercode des NCPeH Land-B
- ServiceMetadata/ServiceInformation/ProcessList/Process/ProcessIdentifier
- ServiceMetadata/ServiceInformation/ProcessList/Process/ServiceEndpointList/Endpoint/ServiceActivationDate
- ServiceMetadata/ServiceInformation/ProcessList/Process/ServiceEndpointList/Endpoint/ServiceExpirationDate
- ServiceMetadata/ServiceInformation/Extension/Signature/SignatureValue

Der NCPeH-FD MUSS vor der Aufnahme des Zertifikats aus dem Element ServiceMetadata/ServiceInformation/ProcessList/Process/ServiceEndpointList/Endpoint/Certificate in den lokalen Truststore sicherstellen, dass für das jeweilige Event "IDP Provide HCP Authentication used for proprietary issuance" bzw. "NCP Provide TRC Assertion" gemäß [\[eHDSI_Audit_Trail_Profile#2.3.5.7\]](#) in dem Zeitintervall aus der ServiceMetadata (ServiceActivationDate bis ServiceExpirationDate) kein anderes Zertifikat im lokalen Truststore enthalten ist.

Die Inhalte aus den extrahierten ServiceMetadata, deren Validierung der Signaturen und Zertifikate und Prüfung auf Schemakonformität mit einem Fehler enden, DÜRFEN NICHT in den lokalen Truststore bzw. in der VAU des NCPeH-FD aufgenommen oder für Zwecke der Datenverarbeitung im NCPeH-FD verwendet werden.

Der NCPeH-FD MUSS bei jedem Abruf der ServiceMetadata eines NCPeH Land-B vom zentralen eHDSI Configuration Service einen Audit Trail Eintrag gemäß [\[4.1.7.5- Security Audit Trail Eintrag erstellen\]](#) erstellen und im lokalen Audit Repository speichern.

4.1.5 Validierung der Identity Assertion des LE-EU

Die Identity Assertion ("IdA") des LE-EU wird vom Behandlungsland (Land-B) ausgestellt und enthält Aussagen über die Identität, Authentizität, Zugehörigkeit und Rolle des LE-EU, der demographische oder medizinische Daten des behandelten Versicherten anfordert. Die IdA ist als SAML Assertion obligatorischer Bestandteil jeder eHDSI-Anfrage. Jeder NCPeH Land-B, der die SAML Assertion zusammen mit eHDSI-Anfragen versendet, steht gemäß [eHDSI_SAML_Profile] für die Richtigkeit, Integrität und Authentizität aller in dieser Assertion gekapselten Informationen ein. Die Identity Assertion des LE-EU muss von dem NCPeH Land-B oder einem Identity Provider aus Land-B elektronisch signiert und in den Security Header Envelope/Header/Security/Assertion der SOAP-Nachricht eingetragen werden. Das öffentliche Zertifikat des NCPeH Land-B oder des Identity Providers aus dem Land-B, mit dem die Signatur der IdA geprüft werden kann, muss vom Land-B dem NCPeH-FD über den eHDSI Configuration Service zum Herunterladen bereitgestellt werden (siehe [\[4.1.4- Service Metadata des NCPeH Land-B abrufen\]](#)).

Das Prüfen des öffentlichen Zertifikats aus der IdA auf den gemeinsamen Zertifikatsherausgeber (CA), um das Vertrauen zu dem Zertifikat herzustellen, ist im [\[4.1.3.5- Umgang mit Zertifikaten der eHDSI\]](#) und [\[4.1.4- Service Metadata des NCPeH Land-B abrufen\]](#) beschrieben.

Der NCPeH-FD agiert gegenüber NCPeH Land-B als SAML Assertion Consumer und sorgt für ordnungsgemäße Prüfung der IdA und der Verarbeitung von Inhalten der IdA.

Die eingehende SOAP-Anfrage muss im Security Header genau eine Identity Assertion für einen LE-EU enthalten. Falls die Anfrage eine zusätzliche Identity Assertion für Next of Kin oder für einen weiteren LE-EU enthält, MUSS der NCPeH-FD eine weitere Verarbeitung der Anfrage abbrechen und die Anfrage mit dem Code Sender und Subcode Invalid Security Token gemäß Vorgaben aus [eHDSI_NCPeH_Components#4.4.2.4] zurückweisen.

Der NCPeH-FD MUSS folgende Elemente prüfen:

- Der Wert des Elements Assertion/AuthnStatement/AuthnInstant DARF NICHT in der Zukunft liegen. Eine tolerierbare Zeitabweichung DARF bis maximal eine Minute (60 Sekunden) betragen.
- Falls das Element Assertion/AuthnStatement/SessionNotOnOrAfter angegeben ist, DARF der Wert NICHT in der Vergangenheit liegen. Eine tolerierbare Zeitabweichung DARF bis maximal einer Minute (60 Sekunden) betragen.

Die IdA MUSS die Vorgaben aus [eHDSI_SAML_Profile#2] erfüllen. Der NCPeH-FD MUSS das Profil des öffentlichen Zertifikats aus dem Element Envelope/Header/Security/Assertion/Signature/KeyInfo der IdA gemäß Vorgaben aus [eHDSI_Certificates_Profile] prüfen. Die Validierung des öffentlichen Zertifikats MUSS gemäß Vorgaben aus [\[4.1.3.5- Umgang mit Zertifikaten der eHDSI\]](#) erfolgen.

Der NCPeH-FD MUSS die elektronische Signatur der IdA validieren, indem er den Security Header gemäß Vorgaben aus [OASIS_WS-Security#8.4] verarbeitet. Schlägt die Signaturvalidierung fehl, MUSS der NCPeH-FD die SMP-Datei des NCPeH Land-B gemäß [\[4.1.4- Service Metadata des NCPeH Land-B abrufen\]](#), erneut herunterladen und ggf. das entsprechende Seal-Zertifikat für Identity Assertions im Truststore aktualisieren. Nach erfolgreicher Aktualisierung des Seal-Zertifikats im lokalen Truststore MUSS der NCPeH-FD die elektronische Signatur der IdA gemäß [OASIS_WS-Security#8.4] validieren.

Schlägt die Validierung erneut fehl, so verhält sich die zugehörige Transaktion wie ein Authentifizierungsfehler. Der NCPeH-FD MUSS bei Fehlern, die bei der Verarbeitung und

Validierung der IdA entstehen, mit einer entsprechenden Fehlermeldung gemäß [eHDSI_NCPeH_Components#4.4.2.4] auf die erhaltene SOAP-Anfrage antworten.

Der NCPeH-FD MUSS im Erfolgsfall (erfolgreiche Validierung der IdA) aus der IdA folgende Identitätsattribute des LE-EU einlesen und in die entsprechenden Variablen abspeichern, damit er die Identitätsattribute in den TUCs für Zwecke der Protokollierung und in Prüfschritten weiterverarbeiten kann:

Tabelle 5: TAB_NCPeH_Identitätsattribute_LE-EU

Variable für Zwecke der internen Datenverarbeitung	Element aus Identity Assertion des LE-EU (gemäß Tabelle aus [eHDSI_SAML_Profile#2.3])
ida_name-id	Assertion/Subject/NameID
ida_practitioner_name	urn:oasis:names:tc:xspa:1.0:subject:subject-id
ida_practitioner_role_code	urn:oasis:names:tc:xacml:2.0:subject:role Der Code, der zu der Rolle des LE-EU gehört, ist im Attribut AttributeValue/Role@code enthalten. Dieser Code MUSS der Variable zugewiesen werden. Beispiel: <pre> <saml2:Attribute FriendlyName="XSPA Role" Name="urn:oasis:names:tc:xacml:2.0:subject:role"> <saml2:AttributeValue> <Role xmlns="urn:hl7-org:v3"code="221" codeSystem="2.16.840.1.113883.2.9.6.2.7" codeSystemName="ISCO" displayName="Medical Doctors"/> </saml2:AttributeValue> </saml2:Attribute> </pre>

ida_practitioner_role_code_system	<p>urn:oasis:names:tc:xacml:2.0:subject:role Die OID des Kodiersystems ist im Attribut AttributeValue/Role@codeSystem enthalten. Der Wert MUSS der Variable zugewiesen werden. Beispiel: <saml2:Attribute FriendlyName="XSPA Role" Name="urn:oasis:names:tc:xacml:2.0:subject:role"> <saml2:AttributeValue> <Role xmlns="urn:hl7-org:v3" code="221" codeSystem="2.16.840.1.113883.2.9.6.2.7" codeSystemName="ISCO" displayName="Medical Doctors"/> </saml2:AttributeValue> </saml2:Attribute></p>
ida_point_of_care	urn:oasis:names:tc:xspa:1.0:environment:locality
ida_healthcare_facility_type_code	<p>urn:ehdsi:names:subject:healthcare-facility-type Der Wert ist im Unterelement AttributeValue enthalten und MUSS der Variable zugewiesen werden. Beispiel: <saml2:Attribute FriendlyName="eHealth DSI Healthcare Facility Type" Name="urn:epsos:names:wp3.4:subject:healthcare-facility-type" NameFormat="urn:oasis:names:tc:SAML:2.0:attribute-format:uri"> <saml2:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xsd:string">Hospital</saml2:AttributeValue> </saml2:Attribute></p>
ida_healthcare_facility_type_code_system	<p>1.3.6.1.4.1.12559.11.10.1.3.2.2.2 Gemäß [eHDSI_SAML_Profile#HP Identity Attributes]</p>
ida_permissions	urn:oasis:names:tc:xspa:1.0:subject:hl7:permission
ida_organization-id	urn:oasis:names:tc:xspa:1.0:subject:organization-id

ida_purposeofuse	urn:oasis:names:tc:xspa:1.0:subject:purposeofuse Der Wert ist im Attribut AttributeValue/PurposeOfUse@code enthalten und gehört in die Variable ida_purposeofuse. Der NCPeH DARF NUR den Wert TREATMENT akzeptieren. Beispiel: <saml2:Attribute FriendlyName="XSPA Purpose Of Use" Name="urn:oasis:names:tc:xspa:1.0:subject:pu rposeofuse" NameFormat="urn:oasis:names:tc:SAML:2.0:attr name-format:uri"> <saml2:AttributeValue> <PurposeOfUse xmlns="urn:hl7- org:v3"code="TREATMENT" codeSystem="3bc18518-d305-46c2-a8d6- 94bd59856e9e" codeSystemName="eHDSI XSPA PurposeOfUse" displayName="TREATMENT"/> </saml2:AttributeValue> </saml2:Attribute>
------------------	--

Der NCPeH-FD MUSS die Werte der oben genannten Variablen eindeutig der Session mit dem Fachdienst der TI zuordnen, an die das konkrete Anwendungsszenario (z.B. PS-A), die Identität des Land-B innerhalb der TI, die Identität des LE-EU und die Identität des Versicherten gebunden sind. Durch die Zuordnung der Variablen zu der entsprechenden Session MÜSSEN Identitätsattribute anderer LE-EU in anderen Sessions des NCPeH-FD unberührt bleiben.

Der NCPeH-FD DARF nur Anfragen annehmen und bearbeiten, in denen das Element urn:oasis:names:tc:xspa:1.0:subject:purposeofuse den Wert TREATMENT enthält. Enthält das Element einen anderen Wert oder erfüllt die IdA nicht die Syntaxvorgaben aus [eHDSI_SAML_Profile], MUSS der NCPeH-FD die weitere Bearbeitung der Anfragen abbrechen und die Anfragen mit dem Code Sender und Subcode Invalid Security Token gemäß den Vorgaben aus [eHDSI_NCPeH_Components#4.4.2.4] zurückweisen. Die fachlichen Fehler im Zusammenhang mit der IdA werden in Abhängigkeit vom jeweiligen Anwendungsfall in entsprechenden TUCs behandelt. Die übrigen Fehler MÜSSEN gemäß [eHDSI_NCPeH_Components#4.4.2.4] behandelt werden.

Das folgende Beispiel stellt die Struktur einer Identity Assertion eines LE-EU dar:

```

<soapenv:Envelope
  xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
  <soapenv:Header>
    <wsse:Security
      xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-
secext-1.0.xsd">
      <saml2:Assertion
        xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
        xmlns:soapenv="http://www.w3.org/2003/05/soap-envelope"
        xmlns:wsa="http://www.w3.org/2005/08/addressing"
        xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-secext-1.0.xsd"
        xmlns:xsd="http://www.w3.org/2001/XMLSchema"
        ID="_4beb5801-1d1a-4318-94d5-d95b135db0be"
        IssueInstant="2023-06-16T09:59:59.860Z"
        Version="2.0">
        <saml2:Issuer
NameQualifier="urn:ehdsi:assertions:hcp">urn:idp:HR:countryB</saml2:Issuer>
        <ds:Signature
          xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
            <ds:SignedInfo>
              <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-
exc-c14n#"/>
              <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-
more#rsa-sha256"/>
              <ds:Reference URI="#_4beb5801-1d1a-4318-94d5-d95b135db0be">
                <ds:Transforms>
                  <ds:Transform
Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
                  <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#">
                    <ec:InclusiveNamespaces
                      xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#"
PrefixList="xsd"/>
                    </ds:Transform>
                  </ds:Transforms>
                <ds:DigestMethod
Algorithm="http://www.w3.org/2001/04/xmenc#sha256"/>
                <ds:DigestValue>YWNZ2V6T5Gte...</ds:DigestValue>
              </ds:Reference>
            </ds:SignedInfo>
            <ds:SignatureValue>F3U93Q38...</ds:SignatureValue>
            <ds:KeyInfo>
              <ds:X509Data>
                <ds:X509Certificate>MIIFmFGh...</ds:X509Certificate>
              </ds:X509Data>
            </ds:KeyInfo>
          </ds:Signature>
        <saml2:Subject>
          <saml2:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-
format:emailAddress">marin.ostroski@hzzo.hr</saml2:NameID>
          <saml2:SubjectConfirmation
Method="urn:oasis:names:tc:SAML:2.0:cm:sender-vouches"/>
            </saml2:Subject>
            <saml2:Conditions NotBefore="2023-06-16T09:59:59.860Z"
NotOnOrAfter="2023-06-16T13:59:59.860Z">
              <saml2:AudienceRestriction>
                <saml2:Audience>urn:ehdsi:assertions.audience:x-border</saml2:Audience>
              </saml2:AudienceRestriction>
            </saml2:Conditions>
            <saml2:AuthnStatement AuthnInstant="2023-06-16T09:59:59.860Z">
              <saml2:AuthnContext>
                <saml2:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:SmartcardPKI</
saml2:AuthnContextClassRef>
              </saml2:AuthnContext>
            </saml2:AuthnStatement>
            <saml2:AttributeStatement>
              <saml2:Attribute FriendlyName="XSPA Subject"
Name="urn:oasis:names:tc:xspa:1.0:subject:subject-id"
NameFormat="urn:oasis:names:tc:SAML:2.0:attribute-format:uri">
                <saml2:AttributeValue
                  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"

```

4.1.6 Validierung der TRC Assertion

Die TRC Assertion ist eine SAML-Assertion. Sie bescheinigt das Bestehen einer Behandlungsbeziehung zwischen einem Versicherten und einem LE-EU und liefert Informationen über den Kontext eines bestimmten Behandlungsszenarios. Die Datenstruktur, Empfehlungen und Einschränkungen zur Nutzung der TRC Assertion sind in [eHDSI_SAML_Profile#4] profiliert und beschrieben. In Security Header von XCPD-Anfragen ist nur eine IdA vorgesehen, eine TRC Assertion DARF dort NICHT enthalten sein. Erst nach erfolgreicher Identifizierung des Versicherten im EU-Ausland MUSS mit den nachfolgenden Anwendungsschritten des LE-EU im Security Header der Nachrichten neben der IdA auch eine TRC Assertion übermittelt werden.

Der NCPeH-FD MUSS das öffentliche Zertifikat aus dem Element Envelope/Header/Security/Assertion/Signature/KeyInfo der TRC Assertion gemäß Vorgaben aus [eHDSI_Certificates_Profile] verifizieren.

Der NCPeH-FD MUSS die elektronische Signatur der TRC Assertion validieren, indem er den Security Header gemäß Vorgaben aus [OASIS_WS-Security#8.4] verarbeitet. Schlägt die Signaturvalidierung fehl, MUSS der NCPeH-FD die SMP-Datei des NCPeH Land-B gemäß [4.1.4- Service Metadata des NCPeH Land-B abrufen] erneut herunterladen und ggf. das entsprechende Seal-Zertifikat für TRC Assertion im Truststore aktualisieren. Nach erfolgreicher Aktualisierung des Seal-Zertifikats im lokalen Truststore MUSS der NCPeH-FD die elektronische Signatur der TRC Assertion gemäß [OASIS_WS-Security#8.4] validieren.

Schlägt die Signaturvalidierung erneut fehl, so verhält sich die zugehörige Transaktion wie ein Autorisierungsfehler. Der NCPeH-FD MUSS bei Fehlern, die bei der Verarbeitung und Validierung der TRC Assertion entstehen, mit einer entsprechenden Fehlermeldung gemäß [eHDSI_NCPeH_Components#4.4.2.4] auf die erhaltene SOAP-Anfrage antworten.

Der NCPeH-FD MUSS folgende Elemente prüfen:

- Der Wert des Elements Assertion/Advice/AssertionIDRef MUSS identisch mit dem Wert des Elements Security/Assertion@ID aus der IdA sein
- Der Wert des Elements Assertion/AuthnStatement/AuthnInstant DARF NICHT in der Zukunft liegen. Eine tolerierbare Zeitabweichung DARF bis maximal einer Minute (60 Sekunden) betragen.
- Falls das Element Assertion/AuthnStatement/SessionNotOnOrAfter angegeben ist, DARF der Wert NICHT in der Vergangenheit liegen. Eine tolerierbare Zeitabweichung DARF bis maximal einer Minute (60 Sekunden) betragen.

Neben Vorgaben aus [eHDSI_SAML_Profile#4] MUSS der NCPeH-FD folgende Prüfschritte durchführen und im Erfolgsfall die entnommenen Werte aus der TRC Assertion in die entsprechenden Variablen für Zwecke der internen Verarbeitung der entsprechenden XCA-Anfragen zu der internen Session (bezogen auf Identität des LE-EU, Land-B und Versicherten) zwischenspeichern:

Tabelle 6: TAB_NCPeH_TRC Assertion

Variable für Zwecke der internen Datenverarbeitung	Element aus TRC Assertion (gemäß Tabelle aus [eHDSI_SAML_Profile#4.3])

trc_patient _identifizier	<p>Der Wert aus dem Element Assertion/AttributeStatement/Attribute[@Name=urn:oasis:names:tc:xspa:1.0:subject:subject-id]/AttributeValue</p> <p>Beispiel: B123456789 A2C4E6^^^&;1.2.276.0.76.3.1.580.147&;ISO</p>
trc_kvnr	<p>Der KVNR-Anteil des Wertes aus dem Element Assertion/AttributeStatement/Attribute[@Name="urn:oasis:names:tc:xspa:1.0:subject:subject-id]/AttributeValue muss folgender inhaltlichen Struktur entsprechen:</p> <ol style="list-style-type: none"> 1. Die ersten 17 Stellen haben folgende Struktur: KVNR + " " + Zugriffscode <ol style="list-style-type: none"> a. Die ersten 10 Stellen gehören dem unveränderbaren Teil der KVNR. Der NCPeH-FD MUSS diesen Wert gemäß Vorgaben aus [4.1.9-Format und Validierung der KVNR] prüfen und validieren. Dieser Wert MUSS in die Variable trc_kvnr übernommen werden, wenn alle Bedingungen gemäß [4.1.9-Format und Validierung der KVNR] erfüllt sind. b. Der senkrechte Strich ohne Anführungszeichen " " (nicht Bestandteil der KVNR) c. Die nächsten sechs Zeichen sind der Zugriffscode (nicht Bestandteil der KVNR) 2. "^^^&;" 3. Wert des Konfigurationsparameters OID_KVNR_ASSIGNING_AUTHORITY aus [4.1.1-Konfigurationsparameter] 4. "&;ISO" <p>Beispiel: B123456789 A2C4E6^^^&;1.2.276.0.76.3.1.580.147&;ISO</p>

trc_accesscode	<p>Der Zugriffscode-Anteil des Wertes aus dem Element Assertion/AttributeStatement/Attribute[@Name="urn:oasis:names:tc:xspa:1.0:subject:subject-id"]/AttributeValue muss folgender inhaltlichen Struktur entsprechen:</p> <ol style="list-style-type: none">1. Die ersten 17 Stellen haben folgende Struktur: KVNR + " " + Zugriffscode<ol style="list-style-type: none">a. Die ersten 10 Stellen gehören dem unveränderbaren Teil der KVNR des Versicherten (Nicht Bestandteil des Zugriffscode),b. Der senkrechte Strich ohne Anführungszeichen " " (Nicht Bestandteil des Zugriffscode),c. die nächsten sechs Zeichen stellen den Zugriffscode dar und gehören in die Variable trc_accesscode.2. "^^^&";3. Wert des Konfigurationsparameters <code>OID_KVNR_ASSIGNING_AUTHORITY</code> aus [4.1.1-Konfigurationsparameter]4. "&ISO" <p>Beispiel: B123456789 A2C4E6^^^&;1.2.276.0.76.3.1.580.147&;ISO</p> <p>Der ermittelte Zugriffscode muss eine Länge von genau sechs Zeichen haben und darf keine Sonderzeichen und Umlaute enthalten.</p>
----------------	---

<p>trc_purposeofuse</p>	<p>Der Wert aus dem Element Assertion/AttributeStatement/Attribute[@Name="urn:oasis:names:tc:xspa:1.0:subject:purposeofuse]/AttributeValue/PurposeOfUse@code MUSS identisch mit dem Wert der Variable ida_purposeofuse sein (siehe [4.1.5- Validierung der Identity Assertion des LE-EU]). Der NCPeH-FD DARF NUR den Wert TREATMENT akzeptieren.</p> <p>Beispiel:</p> <pre><saml2:Attribute FriendlyName="XSPA Purpose Of Use" Name="urn:oasis:names:tc:xspa:1.0:subject:purposeofuse" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"> <saml2:AttributeValue> <PurposeOfUse xmlns="urn:hl7-org:v3"code="TREATMENT" codeSystem="3bc18518-d305-46c2-a8d6-94bd59856e9e" codeSystemName="eHDSI PurposeofUse"/> </saml2:AttributeValue> </saml2:Attribute></pre>
<p>trc_nameid</p>	<p>Der Wert des Elementes Assertion/Subject/NameID MUSS identisch mit dem Wert der Variable ida_name-id (siehe [4.1.5- Validierung der Identity Assertion des LE-EU]) sein. Die Angaben zum Format (Assertion/Subject/NameID@Format) aus der TRC Assertion und IdA MÜSSEN identisch sein und die Kriterien aus [eHDSI_SAML_Profile#4.1 und #2.1] einhalten.</p>

Falls es bei der Durchführung der Prüfkriterien zu Fehlern kommt, MUSS der NCPeH-FD eine weitere Verarbeitung der Anfrage abbrechen und die Anfrage mit dem Code Sender und Subcode Invalid Security Token gemäß Vorgaben aus [eHDSI_NCPeH_Components#4.4.2.4] zurückweisen. Dabei MUSS der NCPeH-FD einen Audit Trail Eintrag gemäß Vorgaben aus [eHDSI_SAML_Profile#4.4] erstellen und in das Audit Repository schreiben.

Das folgende Beispiel stellt die Struktur einer TRC Assertion dar:

```

<soapenv:Envelope xmlns:soapenv=" http://schemas.xmlsoap.org/soap/envelope/">
  <soapenv:Header>
    <wsse:Security xmlns:wsse=" http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-secext-1.0.xsd">
      <saml2:Assertion xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
xmlns:xsd=" http://www.w3.org/2001/XMLSchema"
ID="_139caba7-5d62-49ff-8ef8-37df59be8481"
IssueInstant="2019-05-24T08:13:09.780Z"
Version="2.0">
        <saml2:Issuer urn:initgw:AT:countryB</saml2:Issuer>
        <ds:Signature xmlns:ds=" http://www.w3.org/2000/09/xmldsig#">
          <ds:SignedInfo>
            <ds:CanonicalizationMethod Algorithm=" http://www.w3.org/2001/10/xml-exc-
c14n#" />
            <ds:SignatureMethod Algorithm=" http://www.w3.org/2001/04/xmldsig-
more#rsa-sha256" />
            <ds:Reference URI="#_139caba7-5d62-49ff-8ef8-37df59be8481">
              <ds:Transforms>
                <ds:Transform Algorithm="
http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
                <ds:Transform Algorithm=" http://www.w3.org/2001/10/xml-exc-c14n#">
                  <ec:InclusiveNamespaces xmlns:ec=" http://www.w3.org/2001/10/xml-
exc-c14n#"
                    PrefixList="xsd" />
                </ds:Transform>
              </ds:Transforms>
              <ds:DigestMethod Algorithm=" http://www.w3.org/2001/04/xmlenc#sha256" />
              <ds:DigestValue>ofp6HvIKr...</ds:DigestValue>
            </ds:Reference>
          </ds:SignedInfo>
          <ds:SignatureValue>YiBz/mFXn1r...</ds:SignatureValue>
          <ds:KeyInfo>
            <ds:X509Data>
              <ds:X509Certificate>MIIFjjCCBHa...</ds:X509Certificate>
            </ds:X509Data>
          </ds:KeyInfo>
        </ds:Signature>
      </saml2:Assertion>
      <saml2:Subject>
        <saml2:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-
format:emailAddress">
          marin.ostroski@hzzo.hr</saml2:NameID>
        <saml2:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:sender-
vouches" />
      </saml2:Subject>
      <saml2:Conditions NotBefore="2019-05-24T08:13:09.780Z"
NotOnOrAfter="2019-05-24T10:13:09.780Z" />
      <saml2:Advice>
        <saml2:AssertionIDRef>_9a76c3b4-0d6e-492d-ba8b-7c4371fa0b28</saml2:AssertionIDRef>
        </saml2:Advice>
        <saml2:AuthnStatement AuthnInstant="2019-05-24T08:13:09.780Z">
          <saml2:AuthnContext>
            <saml2:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:PreviousSession
            </saml2:AuthnContextClassRef>
          </saml2:AuthnContext>
        </saml2:AuthnStatement>
        <saml2:AttributeStatement>
          <saml2:Attribute FriendlyName="XSPA Subject"
            Name="urn:oasis:names:tc:xspa:1.0:subject:subject-id"
            NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
format:uri">
            <saml2:AttributeValue xmlns:xsi=" http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xsd:string">
              B123456789|A2C4E6^^^&amp;1.2.276.0.76.3.1.580.147&amp;ISO</saml2:AttributeValue>
            </saml2:Attribute>
          <saml2:Attribute FriendlyName="XSPA Purpose Of Use"
            Name="urn:oasis:names:tc:xspa:1.0:subject:purposeofuse"
            NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
format:uri">
            <saml2:AttributeValue>
              <PurposeOfUse xmlns="urn:hl7-org:v3" code="TREATMENT"

```

4.1.7 Non-Repudiation und Audit Trail Schemas

4.1.7.1 Non-Repudiation of Origin erstellen

Die Non-Repudiation of Origin (NRO) ist als SubmissionAcceptanceRejection (SAR) gemäß [ETSI_REM#5.1.1] definiert. Das SAR-Objekt dient als Nachweis (Evidence), dass eine bestimmte Nachricht vom NCPeH-FD (in der Rolle als Absender) zu dem im Nachweis angegebenen Zeitpunkt erfolgreich bzw. nicht erfolgreich versendet wurde.

Der NCPeH-FD MUSS die Struktur und die Werte für die einzelnen Elemente des SAR-Objektes gemäß Definition in [eHDSI_Audit_Trail_Profile#1.2.2] Abschnitt Non-Repudiation of Origin implementieren. Für die Kennzeichnung von Nachrichtentypen bzw. -transaktionen im SAR-Objekt MÜSSEN Werte aus [eHDSI_Audit_Trail_Profile] Table 7 "eHealth DSI Event IDs" verwendet werden. Das erstellte SAR-Objekt MUSS in dem Audit Repository des NCPeH-FD gespeichert werden.

Nachweis für die Kommunikation mit dem entsprechenden Fachdienst der TI

Bei den Anfragen an die entsprechenden Fachdienste der TI zum Abruf von Versichertendaten MUSS der NCPeH-FD in das Element des SAR-Objektes SubmissionAcceptanceRejection/RecipientsDetails/EntityDetails/CertificateDetails/X509Certificate das öffentliche TLS-Zertifikat des jeweiligen Fachdienstes der TI (ePA Aktensystem, E-Rezept-Fachdienst) in Base64-Kodierung eintragen. Der NCPeH-FD MUSS in das Element SubmissionAcceptanceRejection/SenderDetails/CertificateDetails/X509Certificate das eigene öffentliche TLS-Zertifikat der eHDSI eintragen. Beim Element SubmissionAcceptanceRejection/SenderMessageDetails/MessageSubject MUSS der NCPeH-FD in Abhängigkeit vom TUC, in dem die Erstellung des SAR-Objektes initiiert wird, einen der folgenden Werte eintragen:

- bei [[TUC_NCPeH_013: Metadatenattribute des ePKA MIO abrufen](#)] im Zusammenhang mit dem Anwendungsfall [5.1.1- NCPeH.UC_1 - Versicherten im Behandlungsland für PS-A identifizieren] den Wert ITI-55,
- bei [[TUC_NCPeH_014: FHIR-Bundle ePKA MIO abrufen](#)] im Zusammenhang mit dem Anwendungsfall [5.1.1- NCPeH.UC_1 - Versicherten im Behandlungsland für PS-A identifizieren] den Wert ITI-55,
- bei [6.2.4- [TUC_NCPeH_035: Demographische Versichertendaten aus E-Rezept extrahieren](#)] den Wert ITI-55,
- bei [[TUC_NCPeH_013: Metadatenattribute des ePKA MIO abrufen](#)] im Zusammenhang mit dem Anwendungsfall [5.1.2- NCPeH.UC_2 - Metadaten über ePKA MIO auflisten] den Wert ITI-38,
- bei [6.2.5- [TUC_NCPeH_036: Liste der einlösbaren E-Rezepte des Versicherten aus dem E-Rezept-FD abrufen](#)] den Wert ITI-38,
- bei [[TUC_NCPeH_014: FHIR-Bundle ePKA MIO abrufen](#)] im Zusammenhang mit den Anwendungsfällen [5.1.3- NCPeH.UC_3 - ePKA MIO des Versicherten abrufen] und [5.1.4- NCPeH.UC_4 - ePKA MIO des Versicherten als PDF/A abrufen] den Wert ITI-39,
- bei [6.2.6- [TUC_NCPeH_037: Abzugebende E-Rezepte vom E-Rezept-FD abrufen](#)] den Wert ITI-39,
- bei [6.2.7- [TUC_NCPeH_038: Dispensierdokumente an E-Rezept-FD übermitteln](#)] den Wert ITI-41.

Die restlichen Elemente des SAR-Objektes müssen nach Vorgaben aus [eHDSI_Audit_Trail_Profile#1.2.2] verarbeitet werden.

Wenn der NRO Eintrag nicht erstellt oder nicht im Audit Repository gespeichert werden konnte, MUSS der NCPeH-FD die weitere Verarbeitung der Anfrage vom NCPeH-Land-B abbrechen und mit einer Fehlermeldung gemäß [eHDSI_Messaging_Profile#6.2.1] und dem Code "Receiver" und Subcode "Audit Log Failure" aus [eHDSI_Messaging_Profile#6.2.2] antworten. Der NCPeH-FD MUSS das Element "Reason/Text" (siehe [eHDSI_Messaging_Profile#6.2.1]) mit der Fehlernachricht "It was not possible to create the Non-Repudiation of Origin entry in Germany." befüllen.

Das folgende Beispiel stellt die Struktur eines SAR-Objektes dar:

```

<?xml version="1.0" encoding="UTF-8"?>
<SubmissionAcceptanceRejection version="2">
  <EventCode>Acceptance</EventCode>
  <EvidenceIdentifier>b1147b95-1806-43ee-93f9-b025fab6e64b</EvidenceIdentifier>
  <EvidenceIssuerPolicyID>
    <PolicyID>urn:oid:1.2.3.4</PolicyID>
  </EvidenceIssuerPolicyID>
  <EvidenceIssuerDetails>
    <CertificateDetails>
      <X509Certificate>MIIF0zCCBLug...</X509Certificate>
    </CertificateDetails>
  </EvidenceIssuerDetails>
  <SenderAuthenticationDetails>
    <AuthenticationTime>2018-06-25T07:22:15.819Z</AuthenticationTime>
    <AuthenticationMethod>
http://uri.etsi.org/REM/AuthMethod#Strong</AuthenticationMethod>
  </SenderAuthenticationDetails>
  <EventTime>2018-06-25T07:22:15.817Z</EventTime>
  <SubmissionTime>2018-06-25T07:22:15.756Z</SubmissionTime>
  <SenderDetails>
    <CertificateDetails>
      <X509Certificate>MIIFDjCCA...</X509Certificate>
    </CertificateDetails>
  </SenderDetails>
  <RecipientsDetails>
    <EntityDetails>
      <CertificateDetails>
        <X509Certificate>MIIF0zCCBLug...</X509Certificate>
      </CertificateDetails>
    </EntityDetails>
  </RecipientsDetails>
  <SenderMessageDetails isNotification="false">
    <MessageSubject>ITI-55</MessageSubject>
    <UAMessageIdentifier>urn:uuid:60a3fbc3-3c60-41a3-a0e0-ff089e0ede40</
UAMessageIdentifier>
    <MessageIdentifierByREMMD>urn:uuid:60a3fbc3-3c60-41a3-a0e0-ff089e0ede40</
MessageIdentifierByREMMD>
    <DigestMethod Algorithm="SHA256"/>
    <DigestValue>mC5kcXef0...</DigestValue>
  </SenderMessageDetails>
  <Signature
    xmlns:ds=" http://www.w3.org/2000/09/xmldsig#">
    <SignedInfo>
      <CanonicalizationMethod Algorithm=" http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
      <SignatureMethod Algorithm=" http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
      <Reference URI="">
        <Transforms>
          <Transform Algorithm=" http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
          <Transform Algorithm=" http://www.w3.org/TR/2001/REC-xml-c14n-20010315#WithComments"/>
          </Transforms>
          <DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
          <DigestValue>VOKVuhwF2...</DigestValue>
        </Reference>
      </SignedInfo>
      <SignatureValue>nI/TuThMcAtG...</SignatureValue>
    <KeyInfo>
      <X509Data>
        <X509Certificate>MIIF0zCCBLug...</X509Certificate>
      </X509Data>
      <KeyValue>
        <RSAKeyValue>
          <Modulus>8YbeqFFiKip...</Modulus>
          <Exponent>AQAB</Exponent>
        </RSAKeyValue>
      </KeyValue>
    </KeyInfo>
  </Signature>
</SubmissionAcceptanceRejection>

```

4.1.7.2 Non-Repudiation of Receipt erstellen

Die Non-Repudiation of Receipt (NRR) ist als AcceptanceRejectionByRecipient (ARbR) gemäß [ETSI_REM#5.1.7] definiert. Das ARbR-Objektes dient als Nachweis, dass die eingegangene Nachricht vom NCPeH-FD empfangen worden ist.

Nach dem Eingang der Nachricht MUSS der NCPeH-FD ein ARbR-Objekt erstellen und die Struktur und die Werte für die einzelnen Elemente des ARbR-Objektes gemäß [eHDSI_Audit_Trail_Profile#1.2.2] Abschnitt Non-Repudiation of Receipt verwenden. Für die Kennzeichnung von Nachrichtentypen bzw. -transaktionen im ARbR-Objekt MÜSSEN Werte aus der Tabelle in [eHDSI_Audit_Trail_Profile#2.3.5.8] verwendet werden. Das erstellte ARbR-Objekt MUSS in dem Audit Repository des NCPeH-FD gespeichert werden.

Nachweis für die Kommunikation mit entsprechenden Fachdiensten der TI

Beim Erhalt von Antworten von den Fachdiensten der TI MUSS der NCPeH-FD in das Element des ARbR-Objektes

SubmissionAcceptanceRejection/SenderDetails/CertificateDetails/X509Certificate das öffentliche TLS-Zertifikat des jeweiligen Fachdienstes der TI (ePA Aktensystem, E-Rezept-Fachdienst) in Base64-Kodierung eintragen. Ferner MUSS der NCPeH-FD in das Element

AcceptanceRejectionByRecipient/RecipientsDetails/EntityDetails/CertificateDetails/X509Certificate das eigene öffentliche TLS-Zertifikat der eHDSI eintragen.

Beim Element

AcceptanceRejectionByRecipient/SenderMessageDetails/MessageSubject MUSS der NCPeH-FD in Abhängigkeit vom jeweiligen TUC, in dem die Erstellung des ARbR-Objektes initiiert wird, einen der folgenden Werte eintragen:

- bei [6.2.4- TUC_NCPeH_035: Demographische Versichertendaten aus E-Rezept extrahieren] den Wert ITI-55,
- bei [[TUC_NCPeH_013: Metadatenattribute des ePKA MIO abrufen](#)] im Zusammenhang mit dem Anwendungsfall [5.1.1- NCPeH.UC_1 - Versicherten im Behandlungsland für PS-A identifizieren] den Wert ITI-55
- bei [[TUC_NCPeH_014: FHIR-Bundle ePKA MIO abrufen](#)] im Zusammenhang mit dem Anwendungsfall [5.1.1- NCPeH.UC_1 - Versicherten im Behandlungsland für PS-A identifizieren] den Wert ITI-55,
- bei [[TUC_NCPeH_013: Metadatenattribute des ePKA MIO abrufen](#)] im Zusammenhang mit dem Anwendungsfall [5.1.2- NCPeH.UC_2 - Metadaten über ePKA MIO auflisten] den Wert ITI-38,
- bei [6.2.5- TUC_NCPeH_036: Liste der einlösbaren E-Rezepte des Versicherten aus dem E-Rezept-FD abrufen] den Wert ITI-38,
- bei [[TUC_NCPeH_014: FHIR-Bundle ePKA MIO abrufen](#)] im Zusammenhang mit den Anwendungsfällen [5.1.3- NCPeH.UC_3 - ePKA MIO des Versicherten abrufen] und [5.1.4- NCPeH.UC_4 - ePKA MIO des Versicherten als PDF/A abrufen] den Wert ITI-39,
- bei [6.2.6- TUC_NCPeH_037: Abzugebende E-Rezepte vom E-Rezept-FD abrufen] den Wert ITI-39,
- bei [6.2.7- TUC_NCPeH_038: Dispensierdokumente an E-Rezept-FD übermitteln] den Wert ITI-41.

Die restlichen Elemente des ARbR-Objektes müssen nach Vorgaben aus [eHDSI_Audit_Trail_Profile#1.2.2] verarbeitet werden.

Wenn der NRR Eintrag nicht erstellt oder nicht im Audit Repository gespeichert werden konnte, MUSS der NCPeH-FD die weitere Verarbeitung der Anfrage vom NCPeH-Land-B abbrechen und mit einer Fehlermeldung gemäß [eHDSI_Messaging_Profile#6.2.1] und

dem Code "Receiver" und Subcode "Audit Log Failure" aus [eHDSI_Messaging_Profile#6.2.2] antworten. Der NCPeH-FD MUSS das Element "Reason/Text" (siehe [eHDSI_Messaging_Profile#6.2.1]) mit der Fehlernachricht "It was not possible to create the Non-Repudiation of Receipt entry in Germany." befüllen.

Das folgende Beispiel stellt die Struktur eines ARbR-Objektes dar:

```

<?xml version="1.0" encoding="UTF-8"?>
<AcceptanceRejectionByRecipient version="1">
  <EventCode>Acceptance</EventCode>
  <EvidenceIdentifier>f4fbc592-c12d-4a7d-a641-a8770d06dca8</EvidenceIdentifier>
  <EvidenceIssuerPolicyID>
    <PolicyID>urn:oid:1.2.3.5</PolicyID>
  </EvidenceIssuerPolicyID>
  <EvidenceIssuerDetails>
    <CertificateDetails>
      <X509Certificate>MIIF0zCCBLug...</X509Certificate>
    </CertificateDetails>
  </EvidenceIssuerDetails>
  <SenderAuthenticationDetails>
    <AuthenticationTime>2018-06-25T07:22:15.375Z</AuthenticationTime>
  </SenderAuthenticationDetails>
  <AuthenticationMethod>http://uri.etsi.org/REM/AuthMethod#Strong</AuthenticationMethod>
  </SenderAuthenticationDetails>
  <EventTime>2018-06-25T07:22:15.373Z</EventTime>
  <SubmissionTime>2018-06-25T07:22:15.269Z</SubmissionTime>
  <SenderDetails>
    <CertificateDetails>
      <X509Certificate>MIIFDjCCA...</X509Certificate>
    </CertificateDetails>
  </SenderDetails>
  <RecipientsDetails>
    <EntityDetails>
      <CertificateDetails>
        <X509Certificate>MIIF0zCCBLug...</X509Certificate>
      </CertificateDetails>
    </EntityDetails>
  </RecipientsDetails>
  <SenderMessageDetails isNotification="false">
    <MessageSubject>ITI-55</MessageSubject>
    <UAMessageIdentifier>_b0bdd6b9-9a02-498f-bd32-4bfd1e891624</UAMessageIdentifier>
  </SenderMessageDetails>
  <MessageIdentifierByREMMD>_b0bdd6b9-9a02-498f-bd32-4bfd1e891624</MessageIdentifierByREMMD>
  <DigestMethod Algorithm="SHA256"/>
  <DigestValue>Ry5yXa8Fr...</DigestValue>
  </SenderMessageDetails>
  <Signature
    xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    <SignedInfo>
      <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-
20010315"/>
      <SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
      <Reference URI="">
        <Transforms>
          <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-
signature"/>
          <Transform Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-
20010315#WithComments"/>
        </Transforms>
        <DigestMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-
sha256"/>
        <DigestValue>x3oUZL5Re38...</DigestValue>
      </Reference>
    </SignedInfo>
    <SignatureValue>FvLmfVMdyR...</SignatureValue>
  </KeyInfo>
    <X509Data>
      <X509Certificate>MIIF0zCCBLug...</X509Certificate>
    </X509Data>
    <KeyValue>
      <RSAKeyValue>
        <Modulus>8YbeqFFiKip+ti...</Modulus>
        <Exponent>AQAB</Exponent>
      </RSAKeyValue>
    </KeyValue>
  </KeyInfo>
  </Signature>
</AcceptanceRejectionByRecipient>

```

4.1.7.3 Patient Privacy Audit Trail Eintrag erstellen

Der Inhalt und die Struktur von eHDSI Audit Trail Schemata sind in [eHDSI_Audit_Trail_Profile#2] spezifiziert. Der NCPeH-FD MUSS den Audit Trail Eintrag nach dem eHDSI Audit Trail Schema "Patient Privacy" gemäß [eHDSI_Audit_Trail_Profile#2.3.2] erzeugen. Dieses Audit Schema dient zum Schutz der Privatsphäre der Versicherten und der Dokumentation von Verantwortlichkeiten des Anbieters des NCPeH-FD für die Datenverarbeitung in Bezug auf die Rechte des betroffenen Versicherten und der ordnungsgemäßen Erfüllung dieser Pflichten. Folglich dient dieser Audit Trail auch dazu, den Versicherten in die Lage zu versetzen, sich über alle Verwendungen seiner medizinischen Daten zu informieren. Durch die Analyse dieses Audit Trails soll der Versicherte die Rechtmäßigkeit aller Zugriffe auf seine Daten beurteilen können.

Für die Nachvollziehbarkeit und Nichtabstreitbarkeit (Non-Repudiation) von durchgeführten Vorgängen zum Nachrichtenaustausch verlangt die eHDSI gemäß [eHDSI_Audit_Trail_Profile#2.3.4], dass der vollständige Security Header jeder Nachricht vom NCPeH-FD in einem Audit Trail Eintrag erfasst und in dem Audit Repository gespeichert werden muss. Die erfassten Audit Trails MÜSSEN auch die relevanten "Participant Object"-Elemente enthalten, wie es in [eHDSI_Audit_Trail_Profile#2.3.4] beschrieben ist.

Wenn der Audit Trail Eintrag nicht erstellt oder nicht im Audit Repository gespeichert werden konnte, MUSS der NCPeH-FD die weitere Verarbeitung der Anfrage vom NCPeH-Land-B abbrechen und mit einer Fehlermeldung gemäß [eHDSI_Messaging_Profile#6.2.1] und dem Code "Receiver" und Subcode "Audit Log Failure" aus [eHDSI_Messaging_Profile#6.2.2] antworten. Der NCPeH-FD MUSS das Element "Reason/Text" (siehe [eHDSI_Messaging_Profile#6.2.1]) mit der Fehlernachricht "It was not possible to create the Patient Privacy Audit Trail entry in Germany." befüllen.

Das folgende Beispiel stellt die Struktur eines Audit Trail Eintrages nach dem eHDSI Audit Trail Patient Privacy Schema dar:

```

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<AuditMessage>
  <EventIdentification EventActionCode="E" EventDateTime="2018-04-26T08:55:47.847+02:00"
EventOutcomeIndicator="0">
    <EventID code="ITI-55" displayName="XCPD::CrossGatewayPatientDiscovery"
codeSystemName="IHE Transaction"/>
    <EventTypeCode code="EHDSI-11" displayName="eHDSI Identity Service Find Traits"
codeSystemName="eHDSI Transaction"/>
  </EventIdentification>
  <ActiveParticipant UserID="POC" UserIsRequestor="true">
    <RoleIDCode code="Resident Physician"
codeSystem="1.3.6.1.4.1.12559.11.10.1.3.2.2.2"/>
  </ActiveParticipant>
  <ActiveParticipant UserID="CY&lt;peter.max@liferay.com@CY&gt;" AlternativeUserID="Peter
Max" UserIsRequestor="true">
    <RoleIDCode code="medical doctor"/>
  </ActiveParticipant>
  <ActiveParticipant UserID="CN=ncp.sp.test.cy, O=University of Cyprus, C=CY"
UserIsRequestor="true" NetworkAccessPointID="194.42.17.185" NetworkAccessPointTypeCode="2">
    <RoleIDCode code="ServiceConsumer" displayName="eHealth DSI Service Consumer"
codeSystem="eHealth DSI"/>
  </ActiveParticipant>
  <ActiveParticipant UserID="CN=itsg, O=ITSG GmbH, C=DE" UserIsRequestor="false"
NetworkAccessPointID="185.251.178.100" NetworkAccessPointTypeCode="2">
    <RoleIDCode code="ServiceProvider" displayName="eHDSI Service Provider"
codeSystem="eHealth DSI"/>
  </ActiveParticipant>
  <AuditSourceIdentification AuditSourceID="OID des Betreibers des NCPeH-FD"/>
  <ParticipantObjectIdentification
ParticipantObjectID="B123456789^^^&1.2.276.0.76.3.1.580.147&ISO"
ParticipantObjectTypeCode="1" ParticipantObjectTypeCodeRole="1">
    <ParticipantObjectIDTypeCode code="2" displayName="Patient Number"
codeSystemName="RFC-3881"/>
    <ParticipantObjectName>Patient</ParticipantObjectName>
  </ParticipantObjectIdentification>
  <ParticipantObjectIdentification ParticipantObjectID="urn:uuid:0f31268e-261c-43f3-aeae-
9ddd43eb433e" ParticipantObjectTypeCode="4">
    <ParticipantObjectIDTypeCode code="req" displayName="Request Message"
codeSystemName="eHealth DSI Msg"/>
    <ParticipantObjectDetail type="securityheader" value="..."/>
  </ParticipantObjectIdentification>
  <ParticipantObjectIdentification ParticipantObjectID="urn:uuid:cefa11d5-7d80-49a7-833c-
8e8c21834057" ParticipantObjectTypeCode="4">
    <ParticipantObjectIDTypeCode code="rsp" displayName="Response Message"
codeSystemName="eHealth DSI Msg"/>
    <ParticipantObjectDetail type="securityheader" value="..."/>
  </ParticipantObjectIdentification>
</AuditMessage>

```

4.1.7.4 Translation Audit Trail Eintrag erstellen

Der NCPeH-FD MUSS bei jeder Transformation und Transkodierung von Gesundheitsdaten des Versicherten in das entsprechende eHDSI Pivot Dokumentenformat (CDA Level 1 oder Level 3) einen Audit Trail Eintrag erstellen und in das Audit Repository schreiben. Der

Audit Trail Eintrag MUSS dem Audit Schema gemäß [eHDSI_Audit_Trail_Profile#2.3.5.5] entsprechen.

Der NCPeH-FD MUSS Angaben zum Element EventIdentification gemäß Vorgaben in [eHDSI_Audit_Trail_Profile#2.3.1.1 und #2.3.5.5] umsetzen.

Der NCPeH-FD MUSS Vorgaben zum ActiveParticipant gemäß Vorgaben in [eHDSI_Audit_Trail_Profile#2.3.1.5] umsetzen.

Der NCPeH-FD MUSS nach Vorgaben aus [eHDSI_Audit_Trail_Profile#2.3.3.5] für die angeforderten Gesundheitsdaten des Versicherten ein ParticipantObjectIdentification Element erstellen und nach Durchführung der Transformierung und Transkodierung ein weiteres ParticipantObjectIdentification Element erstellen. Das Attribut ParticipantObjectID MUSS bei Abruf von Gesundheitsdaten von Fachdiensten der TI in beiden Elementen den Wert nach folgender Vorschrift enthalten:

1. Identifier der abgerufenen Gesundheitsdaten:
 - a. Für das ePKA MIO MUSS der Wert aus der Variable METADATA_ePKA_MIO_uniqueld übernommen werden, siehe [\[6.1.3.1- TUC_NCPeH_005: Cross Gateway Retrieve Request zur Abfrage der Patient Summary CDA Level 3 verarbeiten\]](#)
 - b. Beim Abruf von ePrescriptions MUSS je "innerem Bundle" aus der Liste fhir_erp_bundle_collection ein eigener Audit-Trail-Eintrag erstellt und dafür die eindeutig zugeordnete E-Rezept-Id übernommen werden, siehe [\[6.1.3.10- TUC_NCPeH_030: Abgerufene E-Rezepte transkodieren und transformieren\]](#).
2. "^"
3. Das entsprechende Kürzel für die grenzüberschreitende Fachanwendung (z.B. PS für Patient Summary, eP für ePrescription), gefolgt von einer Endung ".XML" oder ".PDF"

Beispiele: "PS.XML", "PS.PDF", "eP.XML" oder "eP.PDF"

Nutzungsvorschrift: Die Endung aus dem jeweiligen Eingangsparameter DocumentUniqueId der XCA-Anfrage MUSS mit dem Wert im Schritt 3 identisch sein.

Beispiele:

```
ParticipantObjectID="1.2.84.116.1.800.254.370.349.563.1605.469.534.1338^PS.XML"
```

```
ParticipantObjectID="160.000.000.000.123.76^eP.XML"
```

Das Attribut ParticipantObjectID MUSS beim Senden von Gesundheitsdaten an Fachdienste der TI in beiden Elementen den Wert nach folgender Vorschrift enthalten:

1. Identifier der gesendeten Gesundheitsdaten:
 - a. Beim Übermitteln von Dispensierdokumenten an den E-Rezept-Fachdienst MUSS pro Eintrag in der Liste xdr_request_cda_dispensation_documents ein eigener Audit-Trail-Eintrag erstellt und dafür die E-Rezept-ID aus dem jeweiligen Dispensierdokument übernommen werden, siehe [\[6.1.5.4- TUC_NCPeH_034: Dispensierdokumente transkodieren und transformieren\]](#).

Nutzungsvorschrift: Eine eventuell vorhandene Endung "^eP.XML" oder "^eP.PDF" DARF NICHT in der ID enthalten sein, da die Dispensierung zu einem E-Rezept nur einmalig und unabhängig vom zuvor abgerufenen CDA-Format des E-Rezeptes durchgeführt wird.

Beispiel: ParticipantObjectID="160.000.000.000.123.76"

Ferner MUSS der NCPeH-FD für jede Transaktion (Anfrage und Antwort, außer bei XCPD) einzeln ein ParticipantObjectIdentification Element gemäß Vorgaben aus [eHDSI_Audit_Trail_Profile#2.3.4] erstellen.

Wenn der Audit Trail Eintrag nicht erstellt oder nicht im Audit Repository gespeichert werden konnte, MUSS der NCPeH-FD die weitere Verarbeitung der Anfrage vom NCPeH-Land-B abbrechen und mit einer Fehlermeldung gemäß [eHDSI_Messaging_Profile#6.2.1] und dem Code "Receiver" und Subcode "Audit Log Failure" aus [eHDSI_Messaging_Profile#6.2.2] antworten. Der NCPeH-FD MUSS das Element "Reason/Text" (siehe [eHDSI_Messaging_Profile#6.2.1]) mit der Fehlermeldung "It was not possible to create the Translation Audit Trail entry in Germany." befüllen.

Das folgende Beispiel stellt die Struktur eines Translation Audit Trail Eintrages nach dem Audit Trail Entries on NCP-Internal Activities gemäß eHDSI Schema dar:

Tabelle 7: TAB_NCPeH_Beispiel_Translation_Audit_Trail

```

<AuditMessage>
  <EventIdentification EventActionCode="E" EventDateTime="2021-11-16T09:30:20.880+02:00"
  EventOutcomeIndicator="0">
    <EventID code="EHDSI-94" displayName="eHDSI Transformation Service Translate
  Document" codeSystemName="eHealth DSI Transaction"/>
    <EventTypeCode code="EHDSI-94" displayName="ncpTransformationMgr::Translate"
  codeSystemName="eHDSI Transactions"/>
  </EventIdentification>
  <ActiveParticipant UserID="ncp-ppt.de.ehealth.testa.eu" UserIsRequestor="false"
  NetworkAccessPointID="10.200.200.15" NetworkAccessPointTypeCode="2">
    <RoleIDCode code="ServiceProvider" displayName="Service Provider"
  codeSystem="eHealth DSI"/>
  </ActiveParticipant>
  <AuditSourceIdentification AuditSourceID="DE-1"/>
  <ParticipantObjectIdentification
  ParticipantObjectID="2.16.17.710.813.1000.990.1.1^PS.XML" ParticipantObjectTypeCode="4"
  ParticipantObjectDataLifeCycle="5">
    <ParticipantObjectIDTypeCode code="in" displayName="Input Data"
  codeSystemName="eHealth DSI Translation"/>
  </ParticipantObjectIdentification>
  <ParticipantObjectIdentification
  ParticipantObjectID="2.16.17.710.813.1000.990.1.1^PS.XML" ParticipantObjectTypeCode="4"
  ParticipantObjectDataLifeCycle="5">
    <ParticipantObjectIDTypeCode code="out" displayName="Output Data"
  codeSystemName="eHealth DSI Translation"/>
  </ParticipantObjectIdentification>
  <ParticipantObjectIdentification ParticipantObjectID="urn:uuid:c563d942-7083-400d-9ef7-
  d76cd6568211" ParticipantObjectTypeCode="4">
    <ParticipantObjectIDTypeCode code="req" displayName="Request Message"
  codeSystemName="eHealth DSI Msg"/>
    <ParticipantObjectDetail type="securityheader"
  value="W05vIHNLY3VyaXR5IGhLYWRlciBwcm92aWRlZF0="/>
  </ParticipantObjectIdentification>
  <ParticipantObjectIdentification ParticipantObjectID="urn:uuid:c563d942-7083-400d-9ef7-
  d76cd6568211" ParticipantObjectTypeCode="4">
    <ParticipantObjectIDTypeCode code="rsp" displayName="Response Message"
  codeSystemName="eHealth DSI Msg"/>
    <ParticipantObjectDetail type="securityheader"
  value="W05vIHNLY3VyaXR5IGhLYWRlciBwcm92aWRlZF0="/>
  </ParticipantObjectIdentification>
  <Signature xmlns="http://www.w3.org/2000/09/xmlsig#">
    <SignedInfo>
      <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-
  20010315#WithComments"/>
      <SignatureMethod Algorithm="http://www.w3.org/2001/04/xmlsig-more#rsa-sha256"/>
      <Reference URI="">
        <Transforms>
          <Transform Algorithm="http://www.w3.org/2000/09/xmlsig#enveloped-
  signature"/>
        </Transforms>
        <DigestMethod Algorithm="http://www.w3.org/2001/04/xmllenc#sha256"/>
        <DigestValue>vQWcEwp...</DigestValue>
      </Reference>
    </SignedInfo>
    <SignatureValue>... BASE64 SIGNATURE VALUE ...</SignatureValue>
  </Signature>
  <KeyInfo>
    <KeyValue>
      <RSAKeyValue>
        <Modulus>... BASE64 KEY ...</Modulus>
        <Exponent>AQAB</Exponent>
      </RSAKeyValue>
    </KeyValue>
  </KeyInfo>
</AuditMessage>

```

4.1.7.5 Security Audit Trail Eintrag erstellen

Wenn der NCPeH-FD einen eigenen SMP-Datensatz (Service Metadata) auf dem zentralen eHDSI Configuration Service veröffentlicht oder vom zentralen eHDSI Configuration Service einen SMP-Datensatz eines NCPeH Land-B heruntergeladen hat, dann MUSS der NCPeH-FD einen Audit Trail Eintrag gemäß dem Patient Privacy Audit Schema (siehe [\[4.1.7.3- Patient Privacy Audit Trail Eintrag erstellen\]](#)) erstellen und im Audit Repository speichern. Der Audit Trail Eintrag MUSS dem Audit Schema gemäß [\[eHDSI_Audit_Trail_Profile#2.3.5.4\]](#) entsprechen.

Wenn der Audit Trail Eintrag nicht vollständig im Audit Repository gespeichert werden kann, MUSS der NCPeH-FD die weitere Verarbeitung der Anfrage vom NCPeH-Land-B abbrechen und mit einer Fehlermeldung gemäß [\[eHDSI_Messaging_Profile#6.2.1\]](#) und dem Code Receiver und Subcode Audit Log Failure aus [\[eHDSI_Messaging_Profile#6.2.2\]](#) antworten. Der NCPeH-FD MUSS das Element Reason/Text (siehe [\[eHDSI_Messaging_Profile#6.2.1\]](#)) mit der Fehlermeldung It was not possible to create the Security Audit Trail entry in Germany. befüllen.

Das folgende Beispiel zeigt die Struktur eines Security Audit Trail Eintrages:

Tabelle 8: TAB_NCPeH_Beispiel_Security_Audit_Trail

```

<?xml version="1.0" encoding="UTF-8"?>
<AuditMessage>
  <EventIdentification EventActionCode="E" EventDateTime="2022-03-11T12:55:33.161Z"
EventOutcomeIndicator="0">
    <EventID code="SMP" codeSystemName="EHDSI-194" displayName="SMP::Push"/>
    <EventTypeCode code="EHDSI-194" codeSystemName="eHDSI Transactions"
displayName="SMP::Push"/>
    <EventTypeCode code="SMP" codeSystemName="EHDSI-194" displayName="SMP::Push"/>
  </EventIdentification>
  <ActiveParticipant NetworkAccessPointID="10.200.200.15" NetworkAccessPointTypeCode="2"
UserID="ncp-ppt.de.ehealth.testa.eu" UserIsRequestor="true">
    <RoleIDCode code="ServiceConsumer" codeSystem="eHealth DSI" displayName="Service
Consumer"/>
  </ActiveParticipant>
  <ActiveParticipant NetworkAccessPointID="smp-cert-auth-test.publisher.ehealth.testa.eu"
NetworkAccessPointTypeCode="1" UserID="smp-cert-auth-
test.publisher.ehealth.testa.eu"
UserIsRequestor="false">
    <RoleIDCode code="ServiceProvider" codeSystem="eHealth DSI" displayName="Service
Provider"/>
  </ActiveParticipant>
  <AuditSourceIdentification AuditSourceID="DE-1"/>
  <ParticipantObjectIdentification ParticipantObjectID="... BASE64 ENDPOINT of SMP-
Server ..."
ParticipantObjectTypeCode="2">
    <ParticipantObjectIDTypeCode code="SMP" codeSystemName="eHealth DSI Security"
displayName="SignedServiceMetadata"/>
  </ParticipantObjectIdentification>
  <Signature
xmlns="http://www.w3.org/2000/09/xmldsig#">
    <SignedInfo>
      <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-
20010315#WithComments"/>
      <SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
      <Reference URI="">
        <Transforms>
          <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-
signature"/>
        </Transforms>
        <DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
        <DigestValue>vQWcEwp...</DigestValue>
      </Reference>
    </SignedInfo>
    <SignatureValue>... BASE64 SIGNATURE VALUE ...</SignatureValue>
  <KeyInfo>
    <KeyValue>
      <RSAKeyValue>
        <Modulus>... BASE64 KEY ...</Modulus>
        <Exponent>AQAB</Exponent>
      </RSAKeyValue>
    </KeyValue>
  </KeyInfo>
</Signature>
</AuditMessage>

```

4.1.8 Festlegungen zur Prüfung der Zugriffsberechtigung auf Fachdienste der TI

Zur Prüfung der Zugriffsberechtigung eines LE-EU auf einen fachanwendungsspezifischen Dienst der TI müssen bestimmte Identitätsattribute aus der Identity Assertion de LE-EU ausgewertet werden. Die Zugriffsrechte auf einen jeweiligen Dienst sind abhängig von dem jeweiligen Anwendungsszenario und werden durch Vorgaben der eHDSI zur IdA technisch geregelt nach [eHDSI_SAML_Profile#2.3 HP Identity Attributes] und [eHDSI_SAML_Profile#2.5 Permission Codes]. Das Zugriffsrecht des NCPeH-FD auf zentrale Dienste der TI bleibt hiervon unberührt.

Falls die Variable `ida_permissions` aus [4.1.5- Validierung der Identity Assertion des LE-EU] nicht leer ist, MÜSSEN bei der Prüfung durch die benannten technische Use Cases mindestens die folgenden Permission Codes aus [eHDSI_SAML_Profile#2.5] enthalten sein, um auf einen entsprechenden fachanwendungsspezifischen Dienst zugreifen zu dürfen:

Tabelle 9: TAB_Zugriffsberechtigung_durch_Prüfung_PermissionCodes

prüfender Technical UseCase	erforderliche Permission Codes in <code>ida_permissions</code>	Zugriffsberechtigung auf fachanwendungsspezifische Dienste der TI
[6.1.1.1- TUC_NCPeH_001: Patient Demographics Query Request für PS-A verarbeiten]	Permission Codes für den eHealth DSI Use Case "Patient Identification"	Im Rahmen des Anwendungsfalls [NCPeH.UC_1 - Versicherten im Behandlungsland für PS-A identifizieren] darf auf die ePA-Aktensysteme der TI zugegriffen werden.
[6.1.1.3- TUC_NCPeH_023: Patient Demographics Query Request für ePeD-A verarbeiten]		Im Rahmen des Anwendungsfalls [5.2.1- NCPeH.UC_9 - Versicherten im Behandlungsland für ePeD-A identifizieren] darf auf den E-Rezept-FD der TI zugegriffen werden.
[6.1.2.1- TUC_NCPeH_003: Cross Gateway Query Request für PS-A verarbeiten], [6.1.3.1- TUC_NCPeH_005: Cross Gateway Retrieve Request zur Abfrage der Patient Summary CDA Level 3 verarbeiten] oder [6.1.3.3- TUC_NCPeH_007: Cross Gateway Retrieve Request zur Abfrage der Patient	Permission Codes für den eHealth DSI Use Case "Request for Patient Summary"	Im Rahmen der Anwendungsfälle <ul style="list-style-type: none"> • [5.1.2- NCPeH.UC_2 - Metadaten über ePKA MIO auflisten], • [5.1.3- NCPeH.UC_3 - ePKA MIO des Versicherten abrufen] und • [5.1.4- NCPeH.UC_4 - ePKA MIO des Versicherten als PDF/A abrufen] darf auf die ePA-Aktensysteme der TI zugegriffen werden.

<p>Summary CDA Level 1 verarbeiten]</p>		
<p>[6.1.2.3- TUC_NCPeH_025: Cross Gateway Query Request für ePeD-A verarbeiten],</p> <p>[6.1.3.8- TUC_NCPeH_028: Cross Gateway Retrieve Request für ePeD-A CDA verarbeiten]</p>	<p>Permission Codes für den eHealth DSI Use Case Request for ePrescriptions</p>	<p>Im Rahmen der Anwendungsfälle:</p> <ul style="list-style-type: none"> • [5.2.2- NCPeH.UC_10 - Einlösbare E-Rezepte des Versicherten aus ePeD-A auflisten] und • [5.2.3- NCPeH.UC_11 - Ausgewählte E-Rezepte aus ePeD-A abrufen], <p>darf auf den E-Rezept-FD der TI zugreifen.</p>
<p>[6.1.5.2- TUC_NCPeH_032: Cross-Enterprise Document Reliable Interchange Request für eD-A verarbeiten]</p>	<p>Permission Codes für den eHealth DSI Use Case Notification on Dispensation</p>	<p>Im Rahmen des Anwendungsfalls [5.2.4- NCPeH.UC_12 - Abgabe von Arzneimitteln an Versicherte im Abgabeland] darf auf den E-Rezept-FD der TI zugreifen.</p>

Falls in der Identity Assertion des LE-EU kein Identity Attribut "permission" mitgeliefert wird, dann muss nach [eHDSI_SAML_Profile#2.3] die Prüfung der Zugriffsberechtigung anhand des Rollencodes des LE-EU nach nationalen Vorgaben erfolgen.

Das bedeutet, dass § 352 SGB V zur Prüfung der Zugriffsberechtigung auf ePA-Aktensysteme anhand der Rollencodes des LE-EU herangezogen werden muss. Hebammen aus der EU sind dementsprechend nach § 352 Nr. 13 für den Zugriff auf ePA-Aktensysteme ausgeschlossen, da die notwendige Erfüllung von § 134a Absatz 2 SGB V nicht möglich ist. Heilmittelerbringer aus der EU sind nach § 352 Nr. 13 vom Zugriff auf ePA-Aktensysteme ausgeschlossen, da die notwendige Erfüllung von § 124 Absatz 1 SGB V nicht möglich ist. Hilfsmittelerbringer sind für den Zugriff auf ePA-Aktensysteme nach § 352 SGB V aktuell nicht zugelassen.

In diesem Fall ergeben sich nach Bewertung der nationalen gesetzlichen Regelungen folgende zulässige Rollen eines LE-EU zur Ermittlung der Zugriffsberechtigungen auf den jeweiligen fachanwendungsspezifischen Dienst der TI:

Falls die Variable `ida_permissions` leer ist, dann MUSS die Rolle des LE-EU anhand des Inhalts der Variablen `ida_practitioner_role_code` aus [4.1.5- Validierung der Identity Assertion des LE-EU] geprüft werden und genau einen der Codes aus der folgenden Tabelle (nach [eHDSI_SAML_Profile#2.3]) enthalten:

Tabelle 10: TAB_Zugriffsberechtigung_durch_Prüfung_RollenCodes

<p>prüfender Technical UseCase</p>	<p>erforderlicher Rollen Code in <code>ida_practitioner_role_code</code></p>	<p>Zugriffsberechtigung auf fachanwendungsspezifische Dienste der TI</p>
<p>[6.1.1.1- TUC_NCPeH_001: Patient Demographics]</p>	<ul style="list-style-type: none"> • 221 (Medical Doctors) oder • 2221 (Nursing professionals) oder 	<p>Im Rahmen der Anwendungsfälle</p> <ul style="list-style-type: none"> • [NCPeH.UC_1 - Versicherten im Behandlungsland für PS-A identifizieren],

<p>Query Request für PS-A verarbeiten],</p> <p>[6.1.2.1- TUC_NCPeH_003: Cross Gateway Query Request für PS-A verarbeiten],</p> <p>[6.1.3.1- TUC_NCPeH_005: Cross Gateway Retrieve Request zur Abfrage der Patient Summary CDA Level 3 verarbeiten] oder</p> <p>[6.1.3.3- TUC_NCPeH_007: Cross Gateway Retrieve Request zur Abfrage der Patient Summary CDA Level 1 verarbeiten]</p>	<ul style="list-style-type: none"> • 2262 (Pharmacists) oder • 2261 (Dentists) 	<ul style="list-style-type: none"> • [5.1.2- NCPeH.UC_2 - Metadaten über ePKA MIO auflisten], • [5.1.3- NCPeH.UC_3 - ePKA MIO des Versicherten abrufen] und • [5.1.4- NCPeH.UC_4 - ePKA MIO des Versicherten als PDF/A abrufen] <p>darf auf die ePA-Aktensysteme der TI zugegriffen werden.</p>
<p>[6.1.1.3- TUC_NCPeH_023: Patient Demographics Query Request für ePeD-A verarbeiten],</p> <p>[6.1.2.3- TUC_NCPeH_025: Cross Gateway Query Request für ePeD-A verarbeiten],</p> <p>[6.1.3.8- TUC_NCPeH_028: Cross Gateway Retrieve Request für ePeD-A CDA verarbeiten]</p> <p>oder</p> <p>[6.1.5.2- TUC_NCPeH_032: Cross-Enterprise Document Reliable Interchange</p>	<ul style="list-style-type: none"> • 262 (Pharmacists) oder • 3213 (Pharmaceutical technicians and assistants) 	<p>Im Rahmen der Anwendungsfälle:</p> <ul style="list-style-type: none"> • [5.2.1- NCPeH.UC_9 - Versicherten im Behandlungsland für ePeD-A identifizieren], • [5.2.2- NCPeH.UC_10 - Einlösbare E-Rezepte des Versicherten aus ePeD-A auflisten], • [5.2.3- NCPeH.UC_11 - Ausgewählte E-Rezepte aus ePeD-A abrufen] und • [5.2.4- NCPeH.UC_12 - Abgabe von Arzneimitteln an Versicherte im Abgabeland] <p>darf auf den E-Rezept-FD der TI zugreifen.</p>

Request für eD-A verarbeiten]		
----------------------------------	--	--

A_25349 - Durchsetzung der Zugriffsberechtigung auf fachanwendungsspezifische Dienste der TI

Der NCPeH-FD MUSS sicherstellen, dass Operationen auf fachanwendungsspezifische Dienste der TI nicht durchgeführt und mit einer Fehlermeldung beendet werden, wenn der Zugriff nach den Tabellen TAB_Zugriffsberechtigung_durch_Prüfung_PermissionCodes und TAB_Zugriffsberechtigung_durch_Prüfung_RollenCodes nicht zulässig ist. [<=]

A_25348 - Prüfung der Zugriffsberechtigung anhand der Rolle des LE-EU nur bei fehlender Angabe von Permission Codes

Wenn die Variable `ida_permissions` aus dem Kapitel [4.1.5- Validierung der Identity Assertion des LE-EU NICHT](#) leer ist und somit eine Prüfung der Zugriffsberechtigung anhand von Permission Codes aus der Identity Assertion des LE-EU möglich ist, dann DARF der NCPeH-FD KEINE Prüfung der Zugriffsberechtigung nach TAB_Zugriffsberechtigung_durch_Prüfung_RollenCodes durchführen. [<=]

A_25297 - Änderungen der Zugriffsrechte nicht erlauben

Der NCPeH-FD MUSS durch technische Maßnahmen sicherstellen, dass Änderungen an den Kriterien zur Prüfung der Zugriffsberechtigung auf Fachdienste der TI nach TAB_Zugriffsberechtigung_durch_Prüfung_PermissionCodes und TAB_Zugriffsberechtigung_durch_Prüfung_RollenCodes ausgeschlossen sind. [<=]

4.1.9 Format und Validierung der KVNR

A_26576 - Prüfung der Strukturvorgaben an die KVNR

Der NCPeH-FD MUSS sicherstellen, dass die KVNR die in bestimmten Parametern enthalten ist, die Strukturvorgaben erfüllt: der unveränderbare Teil ist eine 10-stellige KVNR mit dem Format `[A-Z][0-9]{9}` und hat folgenden Aufbau: 1. Stelle: Alpha-Zeichen (Wertebereich A - Z, ohne Umlaute), 2. bis 10. Stelle: 9-stellige Ziffernfolge. [<=]

A_26566 - Validierung der Prüfziffer der KVNR

Bei der Bearbeitung der Anfragen von NCPeH Land-B MUSS der NCPeH-FD die darin enthaltenen Werte der KVNR des unveränderlichen Anteils des Versicherten gemäß `[Anlage-1_Prüfziffernberechnung_KVNR]` des dort beschriebenen Prüfalgorithmus zur Prüfziffernberechnung der KVNR nach § 290 SGB V validieren und bei fehlerhafter Prüfung die weitere Bearbeitung des Antrags abbrechen. [<=]

4.2 Anschluss an die Telematikinfrastruktur

4.2.1 Schnittstellen zu Diensten der zentralen TI

Über einen sicheren zentralen Zugangspunkt (SZZP) stehen dem NCPeH-FD Dienste der zentralen TI und fachanwendungsspezifischen Diensten (Fachdienste) zur Verfügung. Der NCPeH-FD ist zuständig für den Verbindungsaufbau und -abbau zu diesen Diensten. Dieser interagiert mit der TI in der Rolle eines Consumer und enthält die Absicherung gegenüber dem Zugriff auf das zentrale Netz der TI und Fachdienste.

Die Tabelle `TAB_NCPeH_Schnittstellen_TI-Dienste` listet die relevanten Schnittstellen der zentralen Diensten der TI für den NCPeH-FD auf. Diese Schnittstellen werden vom NCPeH-

FD genutzt, um Endpunkte der Fachdienste zu lokalisieren, TI-Zertifikate zu validieren und sichere Verbindungen zu den Fachdiensten herzustellen.

Tabelle 11: TAB_NCPeH_Schnittstellen_TI-Dienste

Schnittstellen der TI-Plattform	Spezifikation
I_TSL_Download	[gemSpec_TSL#6.3.1] enthält die Beschreibung der Schnittstelle. [gemSpec_PKI#8.1 und 8.2] beschreiben die Vorgänge die bei der Initialisierung und Aktualisierung der TSL durchzuführen sind.
	Der NCPeH-FD MUSS die aktuelle, gültige TSL vom TSL-Dienst herunterladen, initialisieren und nachfolgend aktuell halten.
I_DNS_Name_Resolution und I_DNS_Service_Localization	[gemSpec_Net#5.6] enthält die Beschreibung der Schnittstellen.
	Durch eine mit fachlichen Merkmalen parametrisierte Abfrage kann der URI eines Fachdienstes ermittelt werden.
I_IP_Transport	[gemSpec_Net#3] enthält die Beschreibung der Schnittstellen.
	Das Zentrale Netz TI stellt die Transportmechanismen in der zentralen TI bereit.
I_OCSP_Status_Information	[gemSpec_PKI#9], Verweise auf konkrete Anforderungen sind im Produkttypsteckbrief enthalten (siehe gemProdT_NCPeH_FD)
	Über den TSP X.509 nonQES des Zertifikatherausgebers wird bei Zertifikatsprüfungen der aktuelle Status des Zertifikats geprüft. Die Leistung zum Prüfen der zeitlichen und mathematischen Gültigkeit eines Zertifikats setzt der NCPeH-FD in Plattformbausteinen (siehe [gemSpec_Systemprozesse_dezTI]) selbst um. Lediglich der Sperrstatus wird mittels I_OCSP_Status_Information an der zentralen TI-Plattform abgefragt.
Zugang zur TI über einen SZZP	Zentrale Dienste und Fachdienste [gemSpec_Net], Verweise auf konkrete Anforderungen sind im Produkttypsteckbrief enthalten (siehe gemProdT_NCPeH_FD)
	Der SZZP stellt die Verbindung vom NCPeH-FD zum zentralen Netz der TI her. Dazu stellt der SZZP die Schnittstelle I_IP_Transport in Richtung des NCPeH-FD zur Verfügung. Über den

	SZZP kann der NCPeH-FD auf die TI zugreifen, um die oben genannten Schnittstellen nutzen zu können.
Discovery-Endpunkt des IDP-Dienstes	Der Discovery-Endpunkt stellt den zentralen Anlaufpunkt dar, anhand dessen alle weiteren Endpunkte des IDP-Dienstes adressiert werden können (siehe [gemSpec_IDP_Dienst#Authorization-Server Metadata (Discovery Document)]).
Authorization-Endpunkt des IDP-Dienstes	Der IDP-Dienst führt über den Authorization-Endpunkt die Authentisierung des Nutzers durch. Die Beschreibung und Vorgaben zur Nutzung der Schnittstelle sind in [gemSpec_IDP_Dienst#Authorization-Endpunkt] enthalten.
Token-Endpunkt des IDP-Dienstes	Der IDP-Dienst prüft am Token-Endpunkt die Identität zwischen Aufrufer und Initiator und gibt bei Erfolg neben dem ID_TOKEN den ACCESS_TOKEN zur Nutzung am E-Rezept-Fachdienst aus [gemSpec_IDP_Dienst#Token-Endpunkt].

Hinweis: Wenn der Begriff SZZP verwendet wird, sind damit Anbindungstypen SZZP, SZZP-light oder SZZP-light-plus gemeint. Für weitere Informationen zu den einzelnen Anbindungstypen siehe [gemSpec_Net#3.1.1].

4.2.2 TLS-Verbindungsaufbau zu Diensten der TI

Im Rahmen der Weiterentwicklung der TI können zukünftig Dienste der TI sowohl über das geschlossene, zentrale Netz der TI, als auch über das Internet angesprochen werden. Dementsprechend gibt es unterschiedliche Regularien, die bei der sicheren Nutzung von TLS und der Zertifikatsprüfung zu beachten sind. Entsprechende übergreifende oder anwendungsspezifische Vorgaben zum TLS-Handshake werden hier zusammengefasst.

Aktuell werden die vom NCPeH-FD zu nutzenden zentralen und fachanwendungsspezifischen Dienste der TI (hier allgemein als Dienste der TI bezeichnet) nur über das zentrale Netz der TI angesprochen.

Da die Nutzung von RSA mit der Schlüssellänge 2048 nur noch bis Ende 2025 in der TI erlaubt ist, erfolgt in der TI eine Migration auf ECC-basierte Algorithmen (siehe z. B. [gemSpec_Krypt#5]).

A_25639 - Kein RSA im TLS-Handshake zulassen

Der NCPeH-FD DARF RSA-basierte Ciphersuiten beim TLS-Handshake mit Komponenten der TI NICHT anbieten oder nutzen, auch falls solche Ciphersuiten von diesen aktuell noch unterstützt werden sollten.[<=]

4.2.2.1 TLS-Verbindungsaufbau zu Diensten der TI über das zentrale Netz der TI

Wenn der NCPeH-FD TLS-gesicherte Verbindungen zu Diensten der TI über das zentrale Netz der TI aufbaut, dann MUSS er folgende Vorgaben zur sicheren Nutzung von TLS beachten:

- [gemSpec_Krypt#3.3.2 "TLS-Verbindungen"] allgemein,

- beim Verbindungsaufbau zu ePA-Aktensystemen zusätzlich [gemSpec_Krypt#3.15.3 "ePA-spezifische TLS-Vorgaben"]
- beim Verbindungsaufbau zum E-Rezept-Fachdienst zusätzlich [gemSpec_Krypt#A_21332*] (unter Beachtung des Verbots von RSA-basierten Ciphersuiten für den NCPeH-FD nach A_25639),
- [gemSpec_PKI#8.4.1 "TLS-Verbindungsaufbau"].

Hinweis: Umzusetzende Anforderungen aus diesen Dokumenten werden zusätzlich im Produkttypsteckbrief [gemProdT_NCPeH_FD] aufgeführt.

Für die vom NCPeH-FD mittels TLS zu nutzenden Dienste ist nur eine einseitige Authentisierung im TLS-Handshake vorgesehen.

Bei der Server-Authentisierung des jeweiligen Dienstes MUSS der NCPeH-FD eine Prüfung der Zertifikate nach [4.2.3- Prüfung von nonQES-Zertifikaten] durchführen. Zusätzlich MUSS der NCPeH-FD eine Prüfung des FQDN durchführen und sicherstellen, dass der FQDN im Zertifikat mit dem der Komponente zugeordneten FQDN übereinstimmt.

Der NCPeH-FD MUSS den Aufbau der TLS-Verbindung zum entsprechenden Service-Endpunkt des Dienstes der TI abbrechen, wenn eine der obigen Prüfungen mit einem Fehler beendet wird. Eine eventuell weiterführende Fehlerreaktion insbesondere in Richtung NCPeH Land-B wird von den jeweils nutzenden übergreifenden Festlegungen oder Technical Use Cases festgelegt.

4.2.3 Prüfung von nonQES-Zertifikaten

Der NCPeH-FD MUSS alle nonQES Zertifikate, die er aktiv verwendet (z. B. TLS Verbindungsaufbau oder Aufbau eines VAU-Kanals) auf Integrität und Authentizität prüfen.

Falls die Prüfung eines Zertifikats kein positives Ergebnis ("gültig") liefert, so MUSS der NCPeH-FD die von dem Zertifikat und den darin enthaltenen Attributen (bspw. öffentliche Schlüssel) abhängenden Arbeitsabläufe ablehnen.

Der NCPeH-FD MUSS alle öffentlichen Schlüssel, die es verwenden will, auf eine positiv verlaufene Zertifikatsprüfung zurückführen können.

Tabelle 12: TAB_nonQES_Zertifikatsübersicht

Auslöser der Zertifikatsprüfung	Zertifikat der TI	Zertifikatsprofil	Rollen-OID	Nutzung
TLS-Verbindungsaufbau zum TSL-Dienst	ja	C.ZD.TLS-S	oid_tsl_ti	aktiv
TSL-Signaturzertifikat	ja	C.TSL.SIG	n/a	aktiv
TLS-Verbindungsaufbau zur Betriebsdatenerfassung	ja	C.ZD.TLS-S	(keine Vorgabe)	aktiv
TLS-Verbindungsaufbau zum zentralen IDP-Dienst	nein	TLS Internet-Zertifikat	n/a	aktiv
Signaturprüfung des Discovery Document vom IDP-Dienst und	ja	C.FD.SIG	oid_idpd	aktiv

Signatur-Prüfung des ACCESS_TOKEN vom IDP-Dienst für den E-Rezept-Fachdienst				
TLS-Verbindungsaufbau zum ePA-Aktensystem	ja	C.FD.TLS-S	oid_epa_dvw	aktiv
TLS-Verbindungsaufbau zum E-Rezept-Fachdienst	nein	TLS Internet Zertifikat	n/a	aktiv
Aufbau sicherer Kanal zur VAU des E-Rezept-Fachdienstes	ja	C.FD.ENC	oid_erp-vau	aktiv

Hinweis: Der zentrale IDP-Dienst wird vom NCPeH-FD per TLS über die zentrale TI angesprochen, liefert jedoch ein Internet-Zertifikat mit einem TI-spezifischen FQDN zur TLS-Authentisierung aus. Weiterführende Informationen siehe z. B. [gemSpec_IDP_Dienst], A_20587 oder A_20688.

Hinweis: Die OIDs zu Zertifikatsprofilen der TI und die OIDs für technische Rollen können in der [gemSpec_OID] in den Tabellen Tab_PKI_405 bzw. Tab_PKI_406 ermittelt werden. Die Rollen-OIDs sind entsprechend der Zertifikatsprofile im Zertifikat in der Extension "Admission", professionOID zu finden (siehe jeweilige Zertifikatsprofile in [gemSpec_PKI]).

Hinweis: Hier nicht aufgeführte Zertifikatsprofile (z. B. VAU-Zertifikat im "signierten öffentlichen VAU-Schlüssel") durchlaufen einen separat beschriebenen Prüfungsvorgang.

Hinweis: Hier nicht aufgeführte Zertifikatsprofile (z. B. VAU-Zertifikat des ePA Aktensystems im "signierten öffentlichen VAU-Schlüssel") durchlaufen einen separat beschriebenen Prüfungsvorgang.

Da die Nutzung von RSA mit der Schlüssellänge 2048 nur noch bis Ende 2025 in der TI erlaubt ist, erfolgt in der TI eine Migration auf ECC-basierte Algorithmen (siehe u. A. [gemSpec_Krypt#5]).

A_25640 - Keine RSA-signierten nonQES-Zertifikate akzeptieren

Der NCPeH-FD DARF nonQES-Zertifikate NICHT akzeptieren, deren Signatur auf dem RSA-Algorithmus basieren, auch falls solche Zertifikate aktuell noch von Diensten der TI zusätzlich zu ECC-signierten Zertifikaten angeboten werden dürfen. [≤=]

4.2.3.1 Prüfung von X.509 nonQES Zertifikaten der TI

Der NCPeH-FD MUSS die X.509 nonQES Zertifikate der TI nach [gemSpec_PKI#TUC_PKI_018] im Kontext der jeweiligen Aktivität nach TAB_nonQES_Zertifikatsübersicht mit folgenden Parametern prüfen:

Tabelle 13: TAB_Prüfparameter_nonQES_Zertifikate_TI

Parameter	Wert
Zertifikat	entsprechend Zertifikatsprofil nach TAB_nonQES_Zertifikatsübersicht
PolicyList	entsprechend Zertifikatstyp-OID in CertificatePolicies des zu prüfenden Zertifikatsprofils, siehe [gemSpec_PKI]

intendedKeyUsage	Zertifikatsprofile C.ZD.TLS-S, C.FD.TLS-S oder C.FD.SIG: digitalSignature Zertifikatsprofil C.FD.ENC: keyAgreement
intendedExtendedKeyUsage	Zertifikatsprofil C.ZD.TLS-S oder C.FD.TLS-S: id-kp-serverAuth Zertifikatsprofil C.FD.SIG oder C.FD.ENC: leer oder nicht vorhanden
OCSP-Graceperiod	OCSP_CACHE_REFRESH_PERIOD (siehe [4.1.1-Konfigurationsparameter]), falls keine Sperrinformationen vom zu authentifizierenden System mitgesendet werden
Offline-Modus	nein
Prüfmodus	OCSP

Der NCPeH-FD MUSS die Vorgaben zur Prüfung der Sperrinformation von Zertifikaten nach [gemSpec_PKI#A_23225-*] umsetzen. Der NCPeH-FD KANN auf eine Zwischenspeicherung der Sperrinformation von Zertifikaten verzichten, wenn das definierte Prüfintervall eines Zertifikats gleich oder größer als OCSP_CACHE_REFRESH_PERIOD ist. Der Konfigurationswert OCSP_CACHE_REFRESH_PERIOD entspricht dem in A_23225-*, Punkt 2 definierten Wert "D".

Hinweis: Siehe dort auch die Erläuterungen zur Umsetzung der Anforderung in [gemSpec_Krypt], z. B. auch im Falle der Bereitstellung von Sperrinformationen mittels OCSP-Stapling oder im VAU-Verbindungsaufbau (Nachricht 2, siehe [gemSpec_Krypt] A_24608- und A_24425-*).*

Da die Quellen für Sperrinformationen von Zertifikaten teilweise unterschiedlich vorgegeben sind und der Sinn des Caching sich aus Quelle und Prüfintervall ergibt, folgt hier eine informative Übersicht:

Tabelle 14: TAB_NCPeH_OCSP_Übersicht_für_Zertifikate_TI

Auslöser der Zertifikatsprüfung	Quelle der Sperrinformation	Caching ist sinnvoll?
TLS-Verbindungsaufbau zum TSL-Dienst	OCSP-Responder zur CA	nein (Prüfintervall 24h)
TSL-Signaturzertifikat	OCSP-Responder zur CA	nein (Prüfintervall 24h)
TLS-Verbindungsaufbau zur Betriebsdatenerfassung	OCSP-Responder zur CA	ja
Signaturprüfung des Discovery Document vom IDP-Dienst	OCSP-Responder zur CA	ja, falls es das gleiche Zertifikat ist, dass zur Signatur des ACCESS_TOKEN genutzt wird

Signatur-Prüfung des ACCESS_TOKEN vom IDP für den E-Rezept-Fachdienst	OCSP-Responder zur CA	ja
TLS-Verbindungsaufbau zum ePA-Aktensystem	Primär: OCSP-Stapling im TLS-Handshake Backup: OCSP-Responder zur CA	Primär: nein Backup: ja (siehe A_24913*)
Aufbau sicherer Kanal zur VAU des ePA-Aktensystems	ePA VAU-Protokoll (siehe [gemSpec_Krypt#A_24624*])	nein
Aufbau sicherer Kanal zur VAU des E-Rezept-Fachdienstes	E-Rezept-Fachdienst (siehe [gemSpec_Krypt#A_21216*])	ja

Hinweis: Im Rahmen einer Zertifikatsprüfung nach TUC_PKI_018 beschreibt der untergeordnete TUC_PKI_005 die Ermittlung der Adresse des OCSP-Responders der Zertifikats-herausgebenden CA aus der TSL (siehe [gemSpec_PKI#Statusprüfung]).

4.2.3.2 Prüfung von Internet-Zertifikaten

Der NCPeH-FD MUSS bei einem Internet Zertifikat sowohl eine Signaturprüfung als auch eine Prüfung der zeitlichen Gültigkeit durchführen. Falls diese Prüfung negativ ausfällt, MUSS er das Zertifikat als "ungültig" bewerten.

Der NCPeH-FD MUSS das Zertifikat anhand der Signaturprüfung auf ein CA-Zertifikat einer CA, die die "CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly Trusted Certificates" ([<https://cabforum.org/baseline-requirements-documents/>]) erfüllt, zurückführen können. Ansonsten MUSS er das Zertifikat als "ungültig" bewerten.

Hinweis: Eine positiv ausgefallene Signaturprüfung ist gleichbedeutend damit, dass das CA-Zertifikat im Zertifikats-Truststore eines aktuellen Webrowsers vorhanden ist.

4.2.4 Registrierung als ePA-Client

Der Anbieter des NCPeH-FD MUSS sich als ePA-Client gemäß Vorgaben aus [gemSpec_Aktensystem_ePAfuerAlle#Useragent] registrieren.

Der NCPeH-FD MUSS sicherstellen, dass das HTTP Header Element "x-useragent" bei jedem Request sowohl im HTTP-Header der VAU-Nachricht, als auch im HTTP-Header der Nachricht an alle ePA Services gemäß [gemSpec_Aktensystem_ePAfuerAlle#Useragent] übermittelt wird. Der NCPeH-FD DARF das HTTP Header Element "x-clientid" nur im HTTP-Header der VAU-Nachricht (innerer Request) an ePA Services übermitteln.

4.2.5 Lokalisierung der Service-Endpunkte der ePA

Die Anbieter der ePA-Aktensysteme registrieren die Service-Endpunkte der ePA-Aktensysteme über die übergreifende Domäne **epa4a11.de**, die immer auf IP-Adressen der TI verweist. Für die verschiedenen Umgebungen der TI sind third-level Domänen eingerichtet: .ref (RU1), .dev (RU2), .test (TU) und .prod (PU).

Der NCPeH-FD MUSS die FQDNs jedes Anbieters der ePA-Aktensysteme im Konfigurationsparameter LIST_ePA_ANBIETER_FQDN (siehe [4.1.1-Konfigurationsparameter]) in der VAU speichern, die in [gemSpec_Aktensystem_ePAfuerAlle#A_24592-*] fest definiert sind. Die FQDNs MÜSSEN ausschließlich für die Kommunikation mit den ePA-Diensten genutzt werden.

Das Redundanzkonzept der ePA sieht mehrere Instanzen vor, die über verschiedene IP-Adressen angesprochen werden. Folglich liefert die DNS-Namensauflösung verschiedene IP-Adressen zum FQDN zurück. Diese Adressen werden vom DNS-Server in zufälliger Reihenfolge geschickt, sodass es legitim ist, immer den ersten Eintrag für den folgenden Operationsaufruf zu verwenden.

Unspezifiziert ist das Verhalten, wenn die erste Zieladresse nicht erreichbar ist. Empfehlenswert ist die Nutzung der anderen/weiteren IP-Adressen der DNS-Abfrage. Bei Nicht-Erreichbarkeit des Zielhosts der ersten IP-Adresse wird daher empfohlen, weitere Verbindungsversuche auf Basis einer neuen DNS-Abfrage zu tätigen, mit dem Ziel, eine andere IP-Adresse an erster Stelle der DNS-Antwort zu erhalten, als die des nicht erreichbaren Zielhosts.

4.2.6 Nutzung des IDP-Dienstes

Der IDP-Dienst in der zentralen TI muss im Rahmen der Autorisierung des NCPeH an Fachdiensten der TI genutzt werden. Dazu sind folgende Vorgaben einzuhalten.

4.2.6.1 Registrierung beim IDP-Dienst

Der Anbieter des NCPeH-FD MUSS sich über einen organisatorischen Prozess beim Anbieter des IDP-Dienstes für die Dienste registrieren, für die Token abgerufen werden sollen. Der IDP-Dienst vergibt dabei eine client_id. Diese client_id MUSS vom NCPeH-FD bei Nutzung des IDP-Dienstes übertragen werden.

Der Anbieter des NCPeH-FD MUSS die client_id unter dem Konfigurationsparameter CLIENT_ID_IDP_DIENST (siehe [4.1.1-Konfigurationsparameter]) speichern.

Weitere Informationen zur Registrierung von Fachdiensten beim IDP-Dienst sind in [gemSpec_IDP_Dienst#Registrierung Anwendungsfrontend und Fachdienst] enthalten.

4.2.6.2 Verarbeitung des Discovery Document

Das Discovery Document des IDP-Dienstes stellt den zentralen Anlaufpunkt dar, anhand dessen alle weiteren „statischen“ Service-Endpunkte des IDP-Dienstes adressiert werden können (gemäß [RFC8414#OAuth 2.0 Authorization Server Metadata]).

Der NCPeH-FD MUSS das Discovery Document regelmäßig alle 24 Stunden einlesen und auswerten, und danach die darin aufgeführten URI zu den benötigten öffentlichen Schlüsseln (PUKs) und Diensten verwenden. Das Discovery Document ist vom IDP-Dienst unter der URL /.well-known/openid-configuration abrufbar. Die Informationen über die URL des Downloadpunktes des Discovery Document in der zentralen TI sind in [gemSpec_IDP_Dienst#A_19874-05] enthalten.

Der Anbieter des NCPeH-FD MUSS den Downloadpunkt des Discovery Document als Konfigurationsparameter DOWNLOAD_DISCOVERY_DOCUMENT (siehe [4.1.1-Konfigurationsparameter]) speichern.

Der NCPeH-FD MUSS das öffentliche X.509 nonQES Zertifikat des Discovery Document gemäß [4.2.3-Prüfung von nonQES-Zertifikaten] auf Integrität und Authentizität prüfen und dabei sicherstellen, dass im Feld certificatePolicies (2.5.29.32) des Zertifikates der

policyIdentifier oid_fd_sig für das Zertifikatsprofil C.FD.SIG enthalten ist und das Zertifikat auf die Rollen-OID oid_idpd zurückgeführt wird. Der NCPeH-FD MUSS die von dem Zertifikat und den darin enthaltenen Attributen (bspw. öffentliche Schlüssel) abhängenden Arbeitsabläufe ablehnen, wenn die Prüfung kein positives Ergebnis ("gültig") liefert.

Wenn das Ergebnis der Zertifikatsprüfung "gültig" ist, dann MUSS der NCPeH-FD die JWS [RFC7515 # section-3 - Compact Serialization] Signatur des Discovery Documents auf mathematische Korrektheit sowie auf Vorgaben aus [RFC7515#5.2 Message Signature or MAC Validation] auf zeitliche Gültigkeit des ausstellenden Zertifikates innerhalb der TI prüfen. Weiterführende Festlegungen zur Signatur des Discovery Document sind in [gemSpec_IDP_Dienst#A_20591-01] enthalten.

Nach erfolgreicher Zertifikats- und Signaturprüfung des Discovery Document MUSS der NCPeH-FD:

- das öffentliche Zertifikat PUK_IDP_SIG von dem im Element uri_puk_idp_sig des Discovery Document angegebenen URI herunterladen und in der VAU abspeichern,
- das öffentliche Zertifikat PUK_IDP_ENC von dem im Element uri_puk_idp_enc des Discovery Document angegebenen URI herunterladen und in der VAU abspeichern und
- die benötigten URL-Endpunkte für die Kommunikation mit dem IDP-Dienst dem Discovery Document entnehmen, in der VAU zwischenspeichern und zur Kommunikation mit dem IDP-Dienst nutzen.

Hinweis: zur Struktur des Discovery Document siehe auch [[gemSpec_IDP_Dienst#Aufbau des Discovery Documents](#)] und [[gemSpec_IDP_Dienst#Aufbau des Discovery Document](#)].

Falls die Prüfungen kein positives Ergebnis ("gültig") liefern, so MUSS der NCPeH-FD die von den Zertifikaten und den darin enthaltenen Attributen abhängenden Arbeitsabläufe ablehnen.

4.2.6.3 TLS-Verbindungsaufbau zu Service-Endpunkten des IDP-Dienstes

Der NCPeH-FD MUSS sicherstellen, dass die Kommunikation mit allen Service-Endpunkten des IDP-Dienstes TLS-gesichert erfolgt.

Der NCPeH-FD MUSS den TLS-Verbindungsaufbau zu den Service-Endpunkten des IDP-Dienstes in der TI nach den Vorgaben aus [4.2.2- TLS-Verbindungsaufbau zu Diensten der TI] und [4.2.3- Prüfung von nonQES-Zertifikaten] durchführen.

4.2.6.4 Authentifizierung per IDP-Dienst für Zugriff auf ePA-Aktensystem

Der ePA Authorization Service leitet die Authentifizierungsanfrage des NCPeH-FD an den IDP-Dienst weiter. Am IDP-Dienst authentisiert sich der NCPeH-FD mittels des im HSM für das Land-B hinterlegten C.HCI.AUT-Zertifikattyps des Zertifikatsprofils SM-B NCPeH. Bei erfolgreicher Authentisierung erhält der NCPeH-FD einen AUTHORIZATION_CODE.

Die Abbildung *Nachrichtenfluss für die Authentifizierung gegenüber dem zentralen IDP-Dienst* zeigt den allgemeinen Ablauf der Authentifizierung des NCPeH-FD gegenüber dem IDP-Dienst für den Zugriff auf ePA-Aktensysteme. Der folgende Abschnitt enthält eine informative Erläuterung der Abbildung:

Der NCPeH-FD übermittelt den AUTHORIZATION_CODE an den ePA Authorization Service. Der ePA Authorization Service ruft mittels des AUTHORIZATION_CODE das ID_TOKEN für den NCPeH-FD vom IDP-Dienst ab. Das ID_TOKEN ist vom IDP-Dienst signiert. Als Ergebnis ist ein ID_TOKEN des NCPeH-FD in der VAU des ePA-Aktensystems vorhanden. Ist ein gültiges ID_TOKEN des NCPeH-FD in der VAU vorhanden, startet der ePA User Session Manager eine User Session für den NCPeH-FD für das entsprechende Land-B und der NCPeH-FD kann auf das Aktenkonto des Versicherten zugreifen (sofern eine in ePA vom Versicherten erteilte Befugnis vorhanden ist).

Mit einer etablierten VAU Session für eine authentifizierte, Land-B spezifische NCPeH Identität kann der NCPeH den Zugriff verschiedener LE-EU dieses Landes auf unterschiedliche Versichertenkonten durchführen. Eine bestehende Befugnis für den Zugriff dieses Landes auf ein Konto wird beim Öffnen des jeweiligen Health Record Context durch das ePA-Aktensystem besser geprüft. In der User Session des ePA-Aktensystems können mehrere Health Record Context zu verschiedenen Aktenkonten parallel aufgebaut werden.

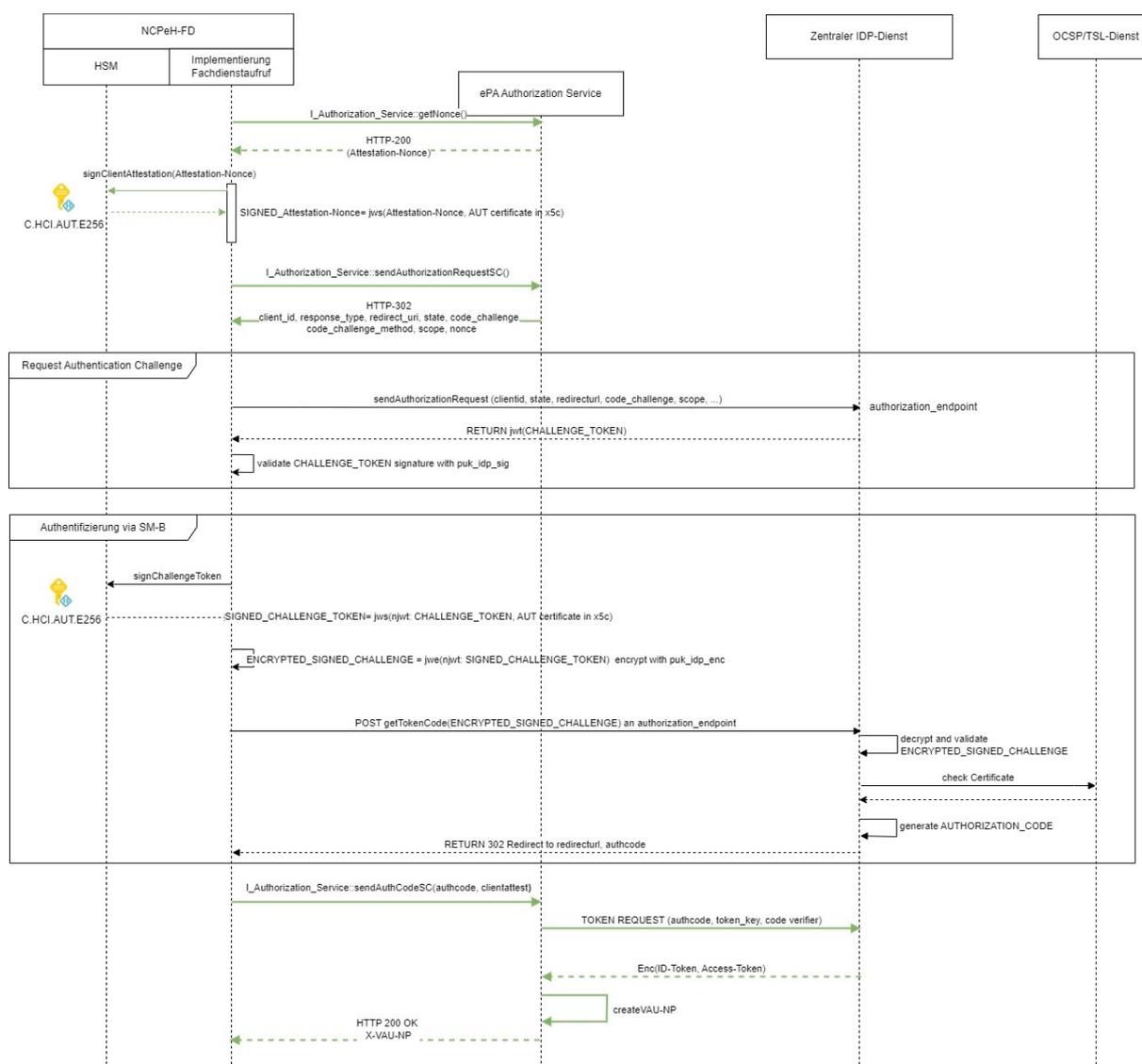


Abbildung 3: Nachrichtenfluss für die Authentifizierung gegenüber dem zentralen IDP-Dienst

Der NCPeH-FD startet die Authentifizierung beim ePA Authorization Service. Dieser Ablauf ist im [4.2.7.7- Authentifizierung mit dem ePA Authorization Service] beschrieben.

Senden der Authentifizierungsanfrage an IDP-Dienst

Bei der folgenden Kommunikation mit dem IDP-Dienst DARF der NCPeH-FD NICHT länger auf eine Antwort des IDP-Dienstes warten als der Zeitwert des Konfigurationsparameter IDP_RESPONSE_TIMEOUT (siehe [4.1.1- Konfigurationsparameter]). Wenn der Zeitwert überschritten wird, MUSS der NCPeH-FD die Kommunikation mit dem IDP-Dienst abbrechen und diesen Fall als einen Fehler behandeln (siehe in diesem Kapitel den Abschnitt "Umgang mit Fehlern und Timeouts").

Nach dem Abruf der Attestation-Nonce und der Delegierung der Authentifizierungsanfrage vom ePA Authorization Service an den IDP-Dienst MUSS der NCPeH-FD den Antrag zum Erhalt eines AUTHORIZATION_CODE für ein ID_TOKEN in Form eines HTTP/1.1 GET AuthorizationRequest beim Authorization-Endpoint (siehe URI_AUTH aus dem Discovery Document) stellen. Dabei MUSS der NCPeH-FD die

folgenden Attribute, die aus der Response von `send_authorization_request_sc` stammen, an den IDP-Dienst übermitteln:

- `response_type`,
- `scope`,
- `nonce2`,
- `client_id`,
- `redirect_uri`,
- `code_challenge` (Hashwert des `code_verifier`) [RFC7636 # section-4.2],
- `code_challenge_method` HASH-Algorithmus (S256) [RFC7636 # section-4.3],
- `state`.

Der Authorization-Endpunkt legt nun eine `session_id` an, stellt alle nötigen Informationen zusammen und erzeugt das `CHALLENGE_TOKEN`. Darüber hinaus stellt der Authorization-Endpunkt den im Claim des ePA-Aktensystems vereinbarten, Consent zusammen, welcher die für dessen Funktion notwendigen Attribute beinhaltet. Diese Informationen liefert der Authorization-Endpunkt als Antwort auf den Authorization-Request des NCPeH-FD.

Challenge/Response-Verfahren

Der NCPeH-FD MUSS die JWS [RFC7515 # section-3 - Compact Serialization] Signatur des `CHALLENGE_TOKEN` auf mathematische Korrektheit sowie auf Vorgaben aus [RFC7515#5.2 Message Signature or MAC Validation] auf zeitliche Gültigkeit gegen den aktuellen öffentlichen Schlüssel des Authorization-Endpunktes "PUK_IDP_SIG" innerhalb der TI prüfen. Die Angaben zum Algorithmus sind in [gemSpec_IDP_Dienst#A_20521-02] enthalten.

Bei erfolgreicher Prüfung der Signatur des `CHALLENGE_TOKEN` MUSS der NCPeH-FD nun im HSM mit dem Signaturzertifikat C.HCI.AUT des SM-B NCPeH für das entsprechende Land-B gemäß Vorgaben aus [4.2.9- Elektronische Identitäten des NCPeH-FD] das `CHALLENGE_TOKEN` des IDP-Dienstes signieren und als zu signierende Daten BinaryString den SHA-256-Hashwert des `CHALLENGE_TOKEN` in Base64-Codierung übergeben. Die Vorgaben für die Anwendung von Algorithmen bei der Erzeugung von Signaturen ist geregelt in [gemSpec_IDP_Dienst#A_21439]. Der NCPeH-FD MUSS beim Signieren des `CHALLENGE_TOKEN` den Signatur-Typ ECDSA-Signatur verwenden.

Anschließend MUSS der NCPeH-FD das `CHALLENGE_TOKEN` zusammen mit der im HSM signierten Challenge-Signatur `SIGNED_CHALLENGE_TOKEN` und dem öffentlichen Authentifizierungszertifikat C.HCI.AUT der SM-B NCPeH, mit dem öffentlichen Schlüssel des Authorization-Endpunktes `PUK_IDP_ENC` verschlüsseln, an diesen in Form eines HTTP-POST-Requests senden. Der Request entspricht dem Aufruf "getTokenCode" aus der Abbildung "Nachrichtenfluss für die Authentifizierung mit dem zentralen IDP-Dienst". Weitere Vorgaben an die Struktur des Request und Algorithmen gelten gemäß Vorgaben aus [gemSpec_IDP_Dienst#7.3].

Hinweis: Der Aufbau der Anfrage, der einzureichenden Objekte und Vorgaben an die Verwendung von Algorithmen sind in [gemSpec_IDP_Dienst#7.3 Authentication Request] enthalten.

Hinweis: Das Signieren und Verschlüsseln des `CHALLENGE_TOKEN` ist durch die Verwendung eines Nested JWT [angelehnt an den folgenden Draft:

<https://tools.ietf.org/html/draft-yusef-oauth-nested-jwt-03>] vom IDP-Dienst realisiert. Im `cty-Header` ist "NJWT" gesetzt, um anzugeben, dass es sich um einen Nested JWT handelt. Das Erstellen der Signatur durch den IDP-Dienst wird dabei durch die Verwendung einer JSON Web Signature (JWS) [RFC7515 # section-3 - Compact Serialization] gewährleistet. Die Verschlüsselung des signierten Token MUSS durch die Nutzung der JSON Web Encryption (JWE) [RFC7516 # section-3] sichergestellt werden. Als Verschlüsselungsalgorithmus MUSS ECDH-ES (Elliptic Curve Diffie-Hellman Ephemeral Static key agreement) vorgesehen.

Erhalt des AUTHORIZATION_CODE

Der Authorization-Endpunkt des IDP-Dienstes verknüpft die `session` mit der Identität aus dem Authentisierungszertifikat und erstellt einen `AUTHORIZATION_CODE`, welchen er als Antwort an den NCPeH-FD zurücksendet.

Der NCPeH-FD MUSS diesen `AUTHORIZATION_CODE` an den ePA Authorization Service senden. Dieser Vorgang ist im [4.2.7.7- Authentifizierung mit dem ePA Authorization Service] beschrieben.

Umgang mit Fehlern und Timeouts

Kommt es während des Authentisierungsprozesses gegenüber IDP-Dienst im Kontext des Anwendungsfalls [[NCPeH.UC_1 - Versicherten im Behandlungsland für PS-A identifizieren](#)] zu einem Fehler oder Timeout, dann MUSS der NCPeH-FD eine weitere Verarbeitung der Anfrage des NCPeH Land-B und der dabei ermittelten Daten abbrechen und dem anfragenden NCPeH Land-B mit einer Fehlermeldung gemäß Tabelle `TAB_NCPeH_Authentifizierung_IDP-Dienst_Fehlerbehandlung_XCPD` antworten.

Tabelle 15: TAB_NCPeH_Authentifizierung_IDP-Dienst_Fehlerbehandlung_XCPD

Reason Encoding gemäß [eHDSI_XCPD_Profile#2.3.3]	acknowledgementDetail
<pre><mitigatedBy typeCode="MITGT"> <detectedIssueManagement classCode="ACT" moodCode="ENV"> <code code="AnswerNotAvailable" codeSystem="1.3.6.1.4.1.19376.1.2.27.3" /> </detectedIssueManagement> </mitigatedBy></pre>	<pre>acknowledgement.typeCode= AA queryAck.queryResponseCode= AE acknowledgementDetail.Code= ERROR_PI_GENERIC acknowledgementDetail.Text = Patient Identification Error acknowledgementDetail.Location = An error occurred during communication with the national identity provider.</pre>

Bei Fehlerfällen oder Timeouts, die im Zusammenhang mit den Anwendungsfällen wie [5.1.2- NCPeH.UC_2 - Metadaten über ePKA MIO auflisten], [5.1.3- NCPeH.UC_3 - ePKA MIO des Versicherten abrufen] oder [5.1.4- NCPeH.UC_4 - ePKA MIO des Versicherten als PDF/A abrufen] entstehen, gilt folgende Anforderung:

Der NCPeH-FD MUSS eine weitere Verarbeitung der Anfrage abbrechen und dem NCPeH Land-B mit dem Fehlercode `ERROR_PS_GENERIC` gemäß [eHDSI_XCA_Profile#2.4] und [eHDSI_NCPeH_Components#6.4] antworten.

Nach einer Fehlerbehandlung, unabhängig vom Anwendungsfall, MUSS der NCPeH-FD den bestehenden VAU-Kanal gemäß Vorgaben in [[4.2.7.6 Schließen eines etablierten VAU-Kanals zum ePA-Aktensystem](#)] schließen.

Nach der Fehlerbehandlung MUSS der NCPeH-FD das Discovery Document und alle zugehörigen Zertifikate aus der VAU löschen, damit diese Objekte technisch nicht mehr verwendet werden können. Danach MUSS der NCPeH-FD das Discovery Document und alle erforderlichen Zertifikate gemäß Vorgaben aus [[4.2.6.2 Verarbeitung des Discovery Document](#)] erneut herunterladen, einlesen, auswerten und in der VAU speichern.

4.2.7 Login in ein ePA-Aktenkonto

Die folgenden Unterkapitel enthalten Vorgaben und Verweise auf entsprechende Dokumente der gematik, die weitere Informationen zum Aufbau von sicheren Verbindungen mit dem ePA-Aktensystem enthalten.

4.2.7.1 TLS-Verbindungsaufbau zum ePA-Aktensystem

Der NCPeH-FD MUSS sicherstellen, dass die Kommunikation mit allen Service-Endpunkten eines ePA Aktensystems TLS-gesichert erfolgt.

Der NCPeH-FD MUSS den TLS-Verbindungsaufbau zum ePA-Aktensystem in der TI nach den Vorgaben aus [4.2.2- TLS-Verbindungsaufbau zu Diensten der TI] und [4.2.3- Prüfung von nonQES-Zertifikaten] durchführen.

Falls beim TLS-Verbindungsaufbau ein Fehler oder Timeout auftritt, MUSS der NCPeH-FD eine weitere Verarbeitung der Anfrage eines NCPeH Land-B und der dabei ermittelten Daten abbrechen und dem anfragenden NCPeH Land-B mit einer Fehlernachricht gemäß Vorgaben aus [eHDSI_Messaging_Profile#6.2.1] und dem Code Receiver und Subcode Busy aus [eHDSI_Messaging_Profile#6.2.2] antworten.

Der NCPeH-FD MUSS das Element Reason/Text gemäß [eHDSI_Messaging_Profile#6.2.1] mit der Fehlernachricht "Unable to connect to the national electronic health record system." befüllen.

Hinweis: Eine Beispielimplementierung für den Aufbau der TLS-Verbindung zu einem ePA-Aktensystem ist unter [github-Link-TLS] veröffentlicht.

4.2.7.2 Interne Aktenkontosession für einen Versicherten

Eine Aktenkontosession im NCPeH-FD bezeichnet die Sitzung, in der fachliche Anwendungsfälle mit dem ePA-Aktenkonto eines Versicherten ausgeführt werden und dabei innerhalb der Sitzung wiederverwendbare Daten in der VAU zwischengespeichert werden.

Der NCPeH-FD SOLL in der VAU nach einer gültigen Aktenkontosession anhand der folgenden Merkmale suchen:

- KVNR des Versicherten gemäß Variable `trc_kvnr` aus [4.1.6- Validierung der TRC Assertion],
- Identifier des LE-EU gemäß Variable `ida_name-id` aus [4.1.5- Validierung der Identity Assertion des LE-EU] und
- Ländercode des Land-B gemäß Variable `tls_country` aus [4.1.3.1- Sicherer Kanal: TESTA-ng und TLS] oder die dem NCPeH Land-B zugeordnete TI-Identität.

Die Liste der Suchergebnisse SOLL NICHT mehr als eine gültige Aktenkontosession enthalten. Wenn mehr als eine gültige Aktenkontosession gefunden wird, dann MUSS der

NCPeH-FD alle gefundenen Aktenkontosessions als ungültig markieren und DARF sie NICHT verwenden. Der NCPeH-FD MUSS dann das Suchergebnis in diesem Fall so behandeln, als ob es keine Suchtreffer gab.

Wenn der NCPeH-FD keine gültige Aktenkontosession findet, dann MUSS er eine Lokalisierung des Aktenkontos des Versicherten (siehe [\[4.2.7.3- Lokalisierung der Akte eines Versicherten\]](#)) durchführen. Wenn der NCPeH-FD die Existenz des Aktenkontos des Versicherten bei einem ePA-Aktensystem ermitteln konnte, dann MUSS er eine neue Aktenkontosession für den Versicherten in der VAU anlegen und die oben genannten Merkmale in der neuen Aktenkontosession abspeichern.

Wenn der NCPeH-FD eine gültige Aktenkontosession gefunden oder erstellt hat, SOLL er dieser Aktenkontosession für die Bearbeitung der fachlichen Anwendungsfälle des Versicherten nutzen und erforderliche Daten zwischenspeichern.

Eine Aktenkontosession KANN mit einem VAU-Kanal fest verknüpft werden. Wenn eine Aktenkontosession mit einem VAU-Kanal verknüpft ist, dann MUSS der NCPeH-FD sicherstellen, dass der VAU-Kanal mit der zugeordneten TI-Identität des NCPeH Land-B authentifiziert wurde (siehe [\[4.2.7.7- Authentifizierung mit dem ePA Authorization Service\]](#)).

A_25966 - Isolation zwischen internen Aktenkontosessions innerhalb der VAU

Der NCPeH-FD MUSS durch einen technischen Separationsmechanismus ausschließen, dass sich die Verarbeitungen einer Aktenkontosession schadhaft auf die Verarbeitungen einer anderen Aktenkontosession innerhalb der VAU auswirken können. Das bedeutet, dass eine gegenseitige inhaltliche Beeinflussung von Aktenkontosessions verhindert werden muss. [**<=**]

Weitere zusätzliche Daten SOLLEN in der Aktenkontosession des Versicherten zwischengespeichert werden:

- Angaben zu Service-Endpunkten des ePA-Aktensystems, in dem das Aktenkonto des Versicherten gehalten wird (siehe [\[4.2.7.3- Lokalisierung der Akte eines Versicherten\]](#)).

Folgende ermittelte Daten KÖNNEN in der Aktenkontosession des Versicherten zwischengespeichert werden:

- Angaben zum LE-EU siehe [\[4.1.5- Validierung der Identity Assertion des LE-EU\]](#),
- Interne Variablen aus [\[4.1.5- Validierung der Identity Assertion des LE-EU\]](#),
- Referenz zu einem VAU-Kanal für das ePA-Aktensystem (siehe [\[4.2.7.4- Aufbau eines VAU-Kanals zum ePA-Aktensystem\]](#) oder [\[4.2.7.5- Nutzung eines etablierten VAU-Kanals zum ePA-Aktensystem\]](#)),
- Metadaten des Versichertendatensatzes: DocumentUniqueld, RepositoryUniqueld.

Folgende Daten DÜRFEN NICHT in der Aktenkontosession des Versicherten zwischengespeichert werden:

- Zugriffscode,
- Medizinische und personenbezogene Daten des Versicherten.

Der NCPeH-FD MUSS bei Inaktivität einer Aktenkontosession nach Ablauf der zeitlichen Dauer gemäß Konfigurationsparameter ABSOLUTE_TIMEOUT_ePA_SESSION (siehe [\[4.1.1- Konfigurationsparameter\]](#)) sicherstellen, dass beim Beenden der Aktenkontosession sämtliche Daten dieser Session aus flüchtigen Speichern sicher gelöscht werden oder ein Zugriff auf diese Daten technisch ausgeschlossen ist.

4.2.7.3 Lokalisierung der Akte eines Versicherten

Die Gesundheitsdaten des Versicherten werden in einem ePA-Aktensystem eines Anbieters gehalten. Ist dem NCPeH-FD nicht bekannt, in welchem ePA-Aktensystem ein Aktenkonto liegt, MUSS der NCPeH-FD den zuständigen ePA Service-Endpunkt ermitteln. Dazu wendet sich der NCPeH-FD an den ePA Information Service außerhalb der VAU eines ePA-Aktensystems, um dort nach der Akte zu fragen.

Der NCPeH-FD MUSS den Status und die Existenz eines Aktenkontos mit Hilfe der Operation `getRecordStatus` des ePA Information Service bei einem Aktensystemanbieter gemäß REST-Schnittstelle [`I_Information_Service`] abfragen. Die Operation ermittelt, ob für die übergebene KVNR ein Aktenkonto existiert und in welchem Status ist es.

Der NCPeH-FD MUSS die Abfrage der Existenz eines Aktenkontos zu einer KVNR gegen die bekannten ePA-Aktensysteme wiederholen, bis diese erfolgreich ist oder alle ePA-Aktensysteme angefragt wurden. Kennt kein ePA-Aktensystem die Akte, hat der Versicherte der ePA widersprochen und es existiert keine Akte. Wenn das ePA-Aktensystem auf die Anfrage mit einem HTTP Status Code 200 OK antwortet, MUSS der NCPeH-FD die relevanten Service-Endpunkte des ePA-Aktensystems in einer neuen Aktenkontosession des Versicherten (siehe [\[4.2.7.2- Interne Aktenkontosession für einen Versicherten\]](#)) abspeichern.

In allen anderen Fällen, wo alle verfügbaren ePA-Aktensysteme nicht mit dem HTTP Status Code 200 OK geantwortet haben und damit die Existenz des Aktenkontos des Versicherten nicht bestätigt wurde, MUSS der NCPeH-FD eine weitere Verarbeitung der Anfrage aus eHDSI abbrechen und dem NCPeH Land-B abhängig vom jeweiligen Anwendungsfall mit einer der folgenden Fehlernachrichten antworten:

Tritt der Fehler im Kontext von Anwendungsfall [\[5.1.1-1- Versicherten im Behandlungsland für PS-A identifizieren\]](#) auf, MUSS der NCPeH-FD eine Fehlernachricht gemäß Tabelle `TAB_NCPeH_Lokalisierung_Akte_Fehler_XCPD_Response` erstellen und an NCPeH Land-B versenden.

Tabelle 16: TAB_NCPeH_Lokalisierung_Akte_Fehler_XCPD_Response

Reason Encoding gemäß [eHDSI_XCPD_Profile#2.3.3]	acknowledgementDetail
<pre><mitigatedBy typeCode="MITGT"> <detectedIssueManagement classCode="ACT" moodCode="ENV"> <code code="AnswerNotAvailable" codeSystem="1.3.6.1.4.1.19376.1.2.27.3"/> </detectedIssueManagement> </mitigatedBy></pre>	<pre>acknowledgement.typeCode= AA queryAck.queryResponseCode= AE acknowledgementDetail.Code= ERROR_PI_NO_MATCH acknowledgementDetail.Text = Patient Identification Error acknowledgementDetail.Location = It was not possible to localise the patient's health record account in the national health record system.</pre>

Hinweis: Weitere Fehlerbehandlungen werden in den für diesen TUC relevanten übergreifenden Festlegungen beschrieben.

Andernfalls, tritt der Fehler in den folgenden Anwendungsfällen wie [\[5.1.2- NCPeH_UC 2 - Metadaten über ePKA MIO auflisten\]](#), [\[5.1.3- NCPeH_UC 3 - ePKA MIO des Versicherten abrufen\]](#) oder [\[5.1.4- NCPeH_UC 4 - ePKA MIO des Versicherten als PDF/A abrufen\]](#) auf, MUSS der NCPeH-FD dem NCPeH Land-B mit dem Fehlercode `ERROR_PS_GENERIC` gemäß [\[eHDSI_XCA_Profile#2.4\]](#) und [\[eHDSI_NCPeH_Components#6.4\]](#) antworten.

4.2.7.4 Aufbau eines VAU-Kanals zum ePA-Aktensystem

Der NCPeH-FD MUSS nach den Vorgaben aus [gemSpec_Krypt#7.1] in seiner Rolle als VAU-Client den Verbindungsaufbau zur VAU eines ePA-Aktensystems durchführen. Dazu muss er den dort beschriebenen Nachrichtenablauf und seine Prüfungen umsetzen:

- Erzeugung und Absenden der Nachricht 1 an das ePA-Aktensystem
- Empfang und Prüfung der Nachricht 2 (Response vom ePA-Aktensystem)
- Erzeugung und Absenden der Nachricht 3 an das ePA-Aktensystem
- Empfang und Prüfung der Nachricht 4 (Response vom ePA-Aktensystem)

Der NCPeH-FD MUSS die Gültigkeitsprüfung der "signierten öffentlichen VAU-Schlüssel" des ePA Aktensystems nach den Anforderungen A_24958-* und A_24624-* aus [gemSpec_Krypt] umsetzen.

A_25729-01 - Aufbau neuer VAU-Kanal zu einem ePA-Aktensystem nur für genau einen NCPeH Land-B

Der NCPeH-FD MUSS sicherstellen, dass ein zu etablierender VAU-Kanal zu einem ePA-Aktensystem nur für genau einen NCPeH Land-B mit seiner zugeordneten TI-Identität aufgebaut und genutzt wird (siehe [[4.2.9 Elektronische Identitäten des NCPeH-FD](#)]).[<=]

Der NCPeH-FD MUSS für unterschiedliche NCPeH Land-B mit ihren zugeordneten TI-Identitäten (entsprechend [[4.2.9- Elektronische Identitäten des NCPeH-FD](#)]) unterschiedliche VAU-Kanäle zum ePA-Aktensystem aufbauen.

Der NCPeH-FD KANN für eine TI-Identität eines NCPeH Land-B mehrere VAU-Kanäle zum ePA-Aktensystem aufbauen. Dies kann z. B. sinnvoll sein, wenn für verschiedene Versicherte aus dem gleichen Land-B parallel fachliche Anwendungsfälle abzarbeiten sind.

Der NCPeH-FD MUSS beim Aufbau der Nachricht 1 ermitteln, ob für die nach A_25729-* zu nutzende Land-B Identität ein VAU-Nutzerpseudonym ("VAU-NP") zwischengespeichert ist. Wenn ein Nutzerpseudonym vorhanden ist, dann MUSS der NCPeH-FD diesen Wert entsprechend [gemSpec_Krypt#A_24757-*] im HTTP-Header der Nachricht 1 mitschicken.

Erläuterung: Obwohl die Authentifizierung, mit der dem Land-B zugeordneten SM-B erst nach Aufbau des VAU-Kanals erfolgt (siehe [4.2.7.7- Authentifizierung mit dem ePA Authorization Service]), muss bereits zu diesem Zeitpunkt klar sein, für welche Land-B Identität der VAU-Kanal genutzt werden soll. Dies wird auch durch die Nutzung des "VAU-NP" klar. Ein Wechsel der NCPeH-Identität in einem VAU-Kanal ist nicht zulässig.

Falls beim Aufbau des VAU-Kanals ein Fehler oder Timeout auftritt MUSS der NCPeH-FD eine weitere Verarbeitung der Anfrage des NCPeH Land-B abbrechen (siehe [gemSpec_Krypt#7.6 Fehlersignalisierung]). Der NCPeH-FD MUSS die Daten zu dem im Aufbau befindlichen VAU-Kanal wie in [4.2.7.6- Schließen eines etablierten VAU-Kanals zum ePA-Aktensystem] behandeln. Bei einem Fehler oder Timeout im Kontext des Anwendungsfalls [5.1.1-1- Versicherten im Behandlungsland für PS-A identifizieren] MUSS der NCPeH-FD dem anfragenden NCPeH Land-B mit einer Fehlernachricht gemäß Vorgaben aus der Tabelle TAB_NCPeH_Aufbau_VAU-Kanal_ePA_Fehlerbehandlung_XCPD antworten.

Tabelle 17: TAB_NCPeH_Aufbau_VAU-Kanal_ePA_Fehlerbehandlung_XCPD

Reason Encoding gemäß [eHDSI_XCPD_Profile#2.3.3]	acknowledgementDetail
--	-----------------------

<pre><mitigatedBy typeCode="MITGT"> <detectedIssueManagement classCode="ACT" moodCode="ENV"> <code code="AnswerNotAvailable" codeSystem="1.3.6.1.4.1.19376.1.2.27.3" /> </detectedIssueManagement> </mitigatedBy></pre>	<pre>acknowledgement.typeCode= AA queryAck.queryResponseCode= AE acknowledgementDetail.Code= ERROR_PI_GENERIC acknowledgementDetail.Text = Patient Identification Error acknowledgementDetail.Location = Unable to connect to the national electronic health record system.</pre>
---	---

Bei Fehlerfällen oder Timeouts, die im Zusammenhang mit den Anwendungsfällen wie [5.1.2- NCPeH.UC_2 - Metadaten über ePKA MIO auflisten](#), [\[5.1.3- NCPeH.UC_3 - ePKA MIO des Versicherten abrufen\]](#) oder [\[5.1.4- NCPeH.UC_4 - ePKA MIO des Versicherten als PDF/A abrufen\]](#) entstehen, gilt folgende Anforderung:

Der NCPeH-FD MUSS eine weitere Verarbeitung der Anfrage abbrechen und dem anfragenden NCPeH Land-B mit dem Fehlercode ERROR_PS_GENERIC gemäß [\[eHDSI_XCA_Profile#2.4\]](#) und [\[eHDSI_NCPeH_Components#6.4\]](#) antworten.

Hinweis: Eine Beispielimplementierung für den Aufbau der VAU-Kanals zu einem ePA-Aktensystem ist unter [\[github-Link-VAU\]](#) veröffentlicht.

4.2.7.5 Nutzung eines etablierten VAU-Kanals zum ePA-Aktensystem

Der NCPeH-FD MUSS die Nutzung eines etablierten VAU-Kanals in seiner Rolle als VAU-Client nach [\[gemSpec_Krypt#7.2 Transport und Sicherung der Nutzdaten\]](#) umsetzen.

Der NCPeH-FD DARF im etablierten VAU-Kanal fachliche Requests NICHT an das ePA-Aktensystem senden, solange er sich über diesen Kanal nicht am ePA Authorization Service erfolgreich authentifiziert hat (siehe [\[4.2.7.7- Authentifizierung mit dem ePA Authorization Service\]](#)).

Hinweis: Weitere Hintergründe sind [\[gemSpec_Krypt#7.3 OIDC-Authentisierung eines Clients\]](#) zu entnehmen.

Der NCPeH-FD KANN einen für eine Land-B Identität etablierten VAU-Kanal für Operationen auf Konten unterschiedlicher Versicherter nutzen, wenn die zu bearbeitenden UseCases dem gleichen NCPeH Land-B zuzuordnen sind.

Der NCPeH-FD MUSS die serielle Nutzung eines VAU-Kanals sicherstellen (Request-Response-Verfahren, kein Pipelining).

Erläuterung: Es entsteht durch die benötigte Authentifizierung des VAU-Clients ein beidseitig authentifizierter VAU-Kanal und somit eine feste Verknüpfung von einem bestimmten NCPeH Land-B mit diesem VAU-Kanal. Ist ein beidseitig authentifizierter VAU-Kanal idle, so kann dieser für die Abarbeitung eines eingehenden Requests aus dem zugeordneten NCPeH Land-B genutzt werden.

Der NCPeH-FD MUSS als VAU-Client den Neustart/die Wiederholung eines VAU-Verbindungsaufbaus nach [\[gemSpec_Krypt#A_24773-*\]](#) unterstützen. In diesem Fall ist der zuvor etablierte VAU-Kanal als geschlossen zu behandeln (siehe [\[4.2.7.6- Schließen eines etablierten VAU-Kanals zum ePA-Aktensystem\]](#)).

Falls bei der Nutzung eines etablierten VAU-Kanals ein Timeout oder ein Fehler nach [\[gemSpec_Krypt#A_24633-*\]](#) und [\[gemSpec_Krypt#7.6 "Fehlersignalisierung"\]](#) auftritt MUSS der NCPeH-FD eine weitere Verarbeitung der Anfrage abbrechen. Er MUSS dann dem anfragenden NCPeH Land-B mit einer Fehlernachricht gemäß Vorgaben aus [\[eHDSI_Messaging_Profile#6.2.1\]](#) und dem CodeReceiver und Subcode Busy aus [\[eHDSI_Messaging_Profile#6.2.2\]](#) antworten. Der NCPeH-FD MUSS das

Element Reason/Text gemäß [eHDSI_Messaging_Profile#6.2.1] mit der Fehlernachricht "Error while communicating with the national electronic health record system." befüllen.

4.2.7.6 Schließen eines etablierten VAU-Kanals zum ePA-Aktensystem

Ein ePA-Aktensystem schließt nach 20 Minuten Inaktivität automatisch die Session mit dem ePA-Client (gemSpec_Aktensystem_ePAfuerAlle#A_25006). Dies erfordert einen zeitlich dazu passenden Umgang mit den VAU-Kanal-Daten, die beim NCPeH-FD verwaltet werden.

Der NCPeH-FD MUSS nach 19 Minuten Inaktivität eines etablierten VAU-Kanals diesen schließen.

Der NCPeH-FD KANN einen etablierten VAU-Kanal über eine rechtzeitige Abfrage von /VAU-Status (gemSpec_Krypt#A_25143-*) offenhalten (z. B. Abfrage alle 15 Minuten). Das im Verlauf der Autorisierung vom IDP-Dienst an das Aktensystem ausgegebene ID-Token wird im Aktensystem in ein HSM-ID-Token mit einer Gültigkeitsdauer von 24h umgewandelt und gespeichert.

Der NCPeH-FD MUSS den VAU-Kanal spätestens nach Ablauf der im Konfigurationsparameter ePA_VAU_CHANNEL_TIME hinterlegten Zeitdauer schließen. Bei Bedarf ist ein neuer VAU-Kanal zu etablieren (neuer Verbindungsaufbau VAU-Protokoll + anschließende Authentifizierung).

A_25900 - Schließen eines VAU-Kanals zum ePA-Aktensystem

Der NCPeH-FD MUSS sicherstellen, dass beim Schließen eines VAU-Kanals sämtliche Daten dieses Kanals aus flüchtigen Speichern sicher gelöscht werden oder ein Zugriff auf diese Daten technisch ausgeschlossen ist. [\leq]

Hinweis: Das Schließen eines VAU-Kanals erfolgt nur durch das Löschen der lokalen, zum Kanal gehörenden Daten. Eine Information über das Schließen des VAU-Kanals vom NCPeH-FD an das ePA-Aktensystem erfolgt nicht.

4.2.7.7 Authentifizierung mit dem ePA Authorization Service

A_25897-01 - Bindung des Authentifizierungsvorgangs an einen mit einem ePA Aktensystem etablierten VAU-Kanal

Der NCPeH-FD MUSS sicherstellen, dass pro etablierten VAU-Kanal mit einem ePA-Aktensystem nur genau ein Authentifizierungsvorgang mit einem Land-B erfolgt und somit der VAU-Kanal zur Nutzung an dieses Land-B gebunden ist. [\leq]

Für weitere Informationen zur Nutzung des VAU-Kanals durch die Land-B Identität siehe A_25729-*

Die Authentifizierung des NCPeH-FD, als Repräsentant des Land-B in der TI, wird durch eine eHDSI-Anfrage aus dem Land-B getriggert, die zu einem Zugriff des NCPeH-FD auf den ePA Authorization Service führt.

Bei der folgenden Kommunikation mit dem ePA Authorization Service DARF der NCPeH-FD NICHT länger auf eine Antwort warten, als der Zeitwert des Konfigurationsparameter ePA_RESPONSE_TIMEOUT (siehe [4.1.1- Konfigurationsparameter]). Wenn der Zeitwert überschritten wird, MUSS der NCPeH-FD die Kommunikation abbrechen und diesen Fall als einen Fehler behandeln (siehe in diesem Kapitel den Abschnitt "Umgang mit Fehlern und Timeouts").

Vorbereitend zum OIDC-Flow (siehe [4.2.6.4- Authentifizierung per IDP-Dienst für Zugriff auf ePA-Aktensystem]) MUSS der NCPeH-FD beim ePA Authorization Service über den zuvor aufgebauten VAU-Kanal (siehe [4.2.7.4- Aufbau eines VAU-Kanals zum ePA-

Aktensystem]) eine Attestation-Nonce abfragen. Dazu MUSS der NCPeH-FD über die REST-Schnittstelle `I_Authorization_Service` des ePA Authorization Service die `getNonce`-Operation für Authentifizierungszwecke in Übereinstimmung mit den Vorgaben aus `[I_Authorization_Service]` verwenden.

Die `getNonce`-Operation bezieht einen eindeutigen einmalig generierten Zufallswert für die Client Attestierung (Attestation-Nonce). Der Wert wird im IDP-Dienst verwendet, um eine Client-Sitzung mit einem `ID_TOKEN` zu verknüpfen und CSRF-Angriffe abzuschwächen. Der Wert wird unverändert von der Authentifizierungsanfrage an das `ID_TOKEN` weitergegeben.

Der NCPeH-FD MUSS nach Erhalt der Attestation-Nonce, diese im HSM mit dem Signaturzertifikat `C.HCI.AUT` des SM-B NCPeH für das entsprechende Land-B gemäß Vorgaben aus `[4.2.9- Elektronische Identitäten des NCPeH-FD]` signieren. Beim Signieren der Nonce MUSS der Signatur-Typ ECDSA-Signatur mit Kurve P-256 und SHA-256 verwendet werden.

Beginn der Authentifizierung - Authentifizierungsanfrage an ePA Authorization Service

Der eigentliche IDP-Flow startet mit der Authentifizierungsanfrage des NCPeH-FD an den ePA Authorization Service. Dazu MUSS der NCPeH-FD über die REST-Schnittstelle `I_Authorization_Service` des ePA Authorization Service die `send_authorization_request_sc`-Operation gemäß Vorgaben aus `[I_Authorization_Service]` nutzen. Mit dieser Operation wird die Authentifizierung des NCPeH-FD durch den zentralen IDP-Dienst initiiert.

Die Response-Nachricht enthält `clientId` des ePA-Aktensystems, `response_type`, `redirect_uri`, `state`, `code_challenge`, `code_challenge_method`, `scope` und `nonce`. Die Delegation der Anfrage und die Kommunikation mit dem IDP-Dienst ist im `[4.2.6.4- Authentifizierung per IDP-Dienst für Zugriff auf ePA-Aktensystem]` beschrieben.

Abschluss der Authentifizierung - Senden des AUTHORIZATION_CODE an ePA Authorization Service

Nach erfolgreicher Authentifizierung beim IDP-Dienst und Erhalt des `AUTHORIZATION_CODE` (siehe `[4.2.6.4- Authentifizierung per IDP-Dienst für Zugriff auf ePA-Aktensystem]`) MUSS der NCPeH über die REST-Schnittstelle `I_Authorization_Service` des ePA Authorization Service die Operation `send_authcode_sc` gemäß Vorgaben aus `[I_Authorization_Service]` nutzen. Mittels der Operation übermittelt der NCPeH-FD den vom IDP-Dienst erhaltenen `AUTHORIZATION_CODE` an den ePA Authorization Service.

Mit einer gültigen `send_authcode_sc`-Response entsteht zwischen dem NCPeH-FD und einer VAU-Instanz des ePA-Aktensystems ein beidseitig authentifizierter VAU-Kanal und damit ist die Ausführung von fachlichen Operationen im ePA-Aktensystem für den NCPeH-FD möglich.

Der NCPeH-FD MUSS nach jeder erfolgreichen Authentisierung die Informationen über VAU-NP nach `[gemSpec_Krypt#A24757-*`] aus der `send_authcode_sc`-Response entnehmen und für jede Land-B-spezifische SM-B die vom ePA-Aktensystem vergebene VAU-NP zwischenspeichern. Der NCPeH-FD MUSS die VAU-NP Informationen getrennt pro lokalisiertem ePA-Aktensystem zwischenspeichern (siehe [\[4.2.5 Lokalisierung der Service-Endpunkte der ePA\]](#)). Für weiterführende Informationen zur Verwendung des VAU-NP siehe [\[4.2.7.4 Aufbau eines VAU-Kanals zum ePA-Aktensystem\]](#).

Umgang mit Fehlern und Timeouts

Kommt es während des Verlaufs im Kontext des Anwendungsfalls [5.1.1-1- Versicherten im Behandlungsland für PS-A identifizieren] zu einem Fehler oder Timeout, dann MUSS der NCPeH-FD eine weitere Verarbeitung der Anfrage des NCPeH Land-B und der dabei ermittelten Daten abbrechen und dem anfragenden NCPeH Land-B mit einer Fehlermeldung gemäß Tabelle

TAB_NCPeH_Authentifizierung_ePA_Auth_Service_Fehlerbehandlung_XCPD antworten. Der NCPeH-FD MUSS den bestehenden VAU-Kanal gemäß Vorgaben in [4.2.7.6 Schließen eines etablierten VAU-Kanals zum ePA-Aktensystem] schließen.

Tabelle 18: TAB_NCPeH_Authentifizierung_ePA_Auth_Service_Fehlerbehandlung_XCPD

Reason Encoding gemäß [eHDSI_XCPD_Profile#2.3.3]	acknowledgementDetail
<pre><mitigatedBy typeCode="MITGT"> <detectedIssueManagement classCode="ACT" moodCode="ENV"> <code code="AnswerNotAvailable" codeSystem="1.3.6.1.4.1.19376.1.2.27.3" /> </detectedIssueManagement> </mitigatedBy></pre>	<pre>acknowledgement.typeCode= AA queryAck.queryResponseCode= AE acknowledgementDetail.Code= ERROR_PI_GENERIC acknowledgementDetail.Text = Patient Identification Error acknowledgementDetail.Location = An error occurred during communication with the national identity provider.</pre>

Bei Fehlerfällen oder Timeouts, die im Zusammenhang mit den Anwendungsfällen wie [5.1.2- NCPeH.UC_2 - Metadaten über ePKA MIO auflisten], [5.1.3- NCPeH.UC_3 - ePKA MIO des Versicherten abrufen] oder [5.1.4- NCPeH.UC_4 - ePKA MIO des Versicherten als PDF/A abrufen] entstehen, dann gilt folgende Anforderung:

Der NCPeH-FD MUSS eine weitere Verarbeitung der Anfrage abbrechen und dem NCPeH Land-B mit dem Fehlercode ERROR_PS_GENERIC gemäß [eHDSI_XCA_Profile#2.4] und [eHDSI_NCPeH_Components#6.4] antworten.

4.2.7.8 Adressierung des Aktenkontos

Der NCPeH-FD adressiert das gewünschte Aktenkonto über die KVNR des Versicherten.

Der NCPeH-FD MUSS bei Aufrufen der ePA-Dienste innerhalb der VAU zur Adressierung des Aktenkontos ein HTTP Header Element mit dem Namen "x-insurantId" und der Angabe der KVNR des Versicherten senden. Die KVNR ist der internen Aktenkontosession zu entnehmen (siehe [4.2.7.2- Interne Aktenkontosession für einen Versicherten]).

4.2.8 Befüllung von SOAP Header Elementen für Zugriff auf ePA XDS Document Service

Der NCPeH-FD MUSS beim Aufruf der Operation RegistryStoredQuery und RetrieveDocumentSet (Schnittstelle I_Document_Management_Ncpeh) die Elemente im SOAP Header der Anfrage gemäß Vorgaben aus der Schemadefinition [Schema_ePA_XDSDocumentService] nutzen. Dabei MUSS die Befüllung der Elemente gemäß Tabelle TAB_Befüllung_Elemente_SOAP_Header_XDS_Document_Service erfolgen.

Tabelle 19: TAB_Befüllung_Elemente_SOAP_Header_XDS_Document_Service

Element im	Wert der Variable
------------	-------------------

SOAP Header	
accessCode	xcpd_accesscode_epka (siehe [6.1.1.1-TUC_NCPeH_001: Patient Demographics Query Request für PS-A verarbeiten]) oder trc_accesscode (siehe [4.1.6- Validierung der TRC Assertion])
healthProfessionalName	ida_practitioner_name (siehe [4.1.5- Validierung der Identity Assertion des LE-EU])
healthProfessionalRole/code	ida_practitioner_role_code (siehe [4.1.5- Validierung der Identity Assertion des LE-EU])
healthProfessionalRole/system	ida_practitioner_role_code_system (siehe [4.1.5- Validierung der Identity Assertion des LE-EU])
healthcareFacilityType/code	ida_healthcare_facility_type_code (siehe [4.1.5- Validierung der Identity Assertion des LE-EU])
healthcareFacilityType/system	ida_healthcare_facility_type_code_system (siehe 4.1.5- Validierung der Identity Assertion des LE-EU)
leiName	ida_point_of_care (siehe [4.1.5- Validierung der Identity Assertion des LE-EU])

4.2.9 Elektronische Identitäten des NCPeH-FD

Der NCPeH-FD ermöglicht es anderen europäischen Mitgliedsstaaten bzw. den durch sie vertretenen technischen Akteuren NCPeH Land-B, als Nutzer an der TI teilzunehmen. Dabei stellt der NCPeH-FD sicher, dass jedem NCPeH Land-B innerhalb der TI eine kryptographische Identität zugeordnet ist, die er für die Identitätsbestätigung gegenüber einem Dienst der TI verwenden muss.

Der NCPeH-FD MUSS privates Schlüsselmaterial vom Zertifikatsprofil "SM-B NCPeH" (C.HCI.AUT, C.HCI.ENC, C.HCI.OSIG), die dem NCPeH Land-B als Repräsentation in der TI eindeutig zugeordnet sind, in einem HSM, dessen Eignung durch eine erfolgreiche Evaluierung nachgewiesen wurde, integritätsgeschützt und vertraulich erzeugen. Die Prüftiefe für Einsatz von HSM MUSS gemäß Vorgaben aus [4.3- Sicherheit und Datenschutz] entsprechen.

Der Anbieter des NCPeH-FD MUSS einen sicheren Prozess zur Personalisierung des HSM definieren und etablieren, der die in Tabelle *Tab_NCPeH_Personalisierung_HSM* genannten Aspekte beinhaltet. Der NCPeH-FD MUSS fest kryptographisch mit dem HSM gekoppelt sein, sodass eine hinsichtlich Vertraulichkeit und Integrität geschützte, beidseitig authentifizierte Verbindung zwischen NCPeH-FD und HSM besteht und ausschließlich der NCPeH-FD die auf dem HSM gespeicherten TI-Identitäten nutzen kann. Parallel zu diesen Anforderungen siehe auch die Sicherheitsanforderung [4.3-14- Anbieter des NCPeH-Fachdienstes - Sicherer Betrieb und Nutzung eines HSMs].

Tabelle 20: Tab_NCPeH_Personalisierung_HSM

Aspekt	Beschreibung
Schlüsselmaterial nach dem Zertifikatsprofil "SM-B NCPeH"	Das Schlüsselmaterial wird sicher im HSM erzeugt. Das private Schlüsselmaterial verlässt das HSM nicht oder nur zum Zwecke eines Backups auf einem Backup-HSM, wobei die Übertragung hinsichtlich Vertraulichkeit geschützt sein muss. Das Schlüsselmaterial dient als Repräsentation des NCPeH Land-B bei der Bestätigung der Identitätsbehauptungen gegenüber dem IDP-Dienst.
Zertifikatsrequest	Die benötigten Zertifikatsrequests werden im HSM erzeugt und exportiert. Die Zertifikatsrequests werden unter Wahrung der Authentizität und Integrität dem TSP übermittelt.
Zertifikat	Das Zertifikat wird vom TSP zum Betreiber übermittelt.

Hinweis: Der NCPeH-FD verwendet Schlüsselmaterial "SM-B NCPeH" gemäß [gemSpec_PKI#"SM-B NCPeH"] mit der OID-Referenz "oid_ncpeh" gemäß [gemSpec_OID#Tab_PKI_403].

Im Zusammenhang mit HSM insb. zur sicheren Aufbewahrung von privaten Schlüssel, die von der TI und eHDSI ausgestellt wurden, sind für HSM-Kryptographieschnittstelle, Integritätsprüfung der VAU, Managementprozesse des HSM, sicherer Betrieb und Einsatz zertifizierter HSM im [4.3- Sicherheit und Datenschutz] weitere relevante Anforderungen enthalten.

Auswahl der NCPeH Identität für ein Land-B

Um das passende Signaturzertifikat als Repräsentation des NCPeH Land-B innerhalb der TI im HSM referenzieren zu können, muss der NCPeH-FD zuerst die Identität (Ländercode) des NCPeH Land-B innerhalb der eHDSI ermitteln. Im Rahmen der gegenseitigen TLS-Authentisierung mit dem NCPeH Land-B MUSS der NCPeH-FD aus dem eHDSI-TLS-Zertifikat des NCPeH Land-B die Landidentität ermitteln, den Ländercode (ISO 3166-1 Alpha 2) gemäß [eHDSI_Certificate_Profile#3.1] Element Subject C (Country) bzw. siehe auch Variable `tls_country` im [4.1.3.1- Sicherer Kanal: TESTA-ng und TLS]. Im nächsten Schritt kann der NCPeH-FD anhand der ermittelnden Länderidentität über das Zertifikatselement "commonName" des Zertifikatsprofils "SM-B NCPeH" (siehe [gemSpec_PKI#"SM-B NCPeH"]) das passende Signaturzertifikat als Repräsentation des NCPeH Land-B im HSM eindeutig referenzieren und verwenden. Dabei MUSS der NCPeH-FD die inhaltliche Struktur des Zertifikatselements `commonName` beachten:

<Kurzform des Ländernamens> (<zweistelliger Ländercode>)

Beschreibung des Aufbaus:

1. Teilstring: deutsche amtliche Kurzform eines Ländernamens gemäß [LVZ],
2. Teilstring: " (",
3. Teilstring: zweibuchstabiger Ländercode nach DIN EN ISO 3166-1 gemäß [LVZ],
4. Teilstring: ")".

Beispiel Zuordnung des Zertifikats zu dem NCPeH Frankreich: Frankreich (FR)

4.2.10 Übergreifende Vorgaben an die Kommunikation mit E-Rezept-FD

4.2.10.1 Allgemeine Vorgaben an die Kommunikation mit dem E-Rezept-FD

Der NCPeH-FD MUSS bei der Kommunikation mit dem E-Rezept-FD in allen HTTP-Requests im äußeren Request den HTTP-Header "user-agent" nach der Vorgabe [gemILF_PS_eRp#A_20015*] erstellen und befüllen.

Der NCPeH-FD MUSS bei der Kommunikation mit dem E-Rezept-FD in allen HTTP-Requests im äußeren Request den HTTP-Header "X-erp-user" nach der Vorgabe [gemILF_PS_eRp#A_21568*] erstellen und dabei den Wert "n" als NCPeH-FD einfügen.

Der NCPeH-FD MUSS bei der Kommunikation mit dem E-Rezept-FD in allen HTTP-Requests im äußeren Request den HTTP-Header "X-erp-resource" nach der Vorgabe [gemILF_PS_eRp#A_21569*] setzen und dabei den entsprechenden Wert gemäß der Tabelle "TAB_NCPeH_HTTP-Header_X-erp-resource" einfügen.

Tabelle 21: TAB_NCPeH_HTTP-Header_X-erp-resource

Operation	X-erp-resource
POST /Task/<id>/\$eu-close	Task
POST /get-eu-prescriptions	Prescription

4.2.10.2 Lokalisierung und Namensauflösung des E-Rezept-FD

Der E-Rezept-FD ist gemäß den Festlegungen in [gemSpec_FD_eRp#Servicelokalisierung] lokalisierbar. Dabei nutzt der NCPeH-FD die Lokalisierungsinformationen gemäß Vorgabe aus [gemILF_PS_eRp#A_19451*]. Die URL für die Kommunikation mit dem E-Rezept-FD bildet der NCPeH-FD nach der Vorgabe aus [gemILF_PS_eRp#A_19744*].

Hinweis: Für den Verbindungsaufbau mit dem E-Rezept-FD sind verschiedene Endpunkte in [github_Endpunkte_E-Rezept-FD_IDP-Dienst] angegeben.

Das Redundanzkonzept sieht mehrere Instanzen vor, die über verschiedene IP-Adressen angesprochen werden. Folglich liefert die DNS-Namensauflösung verschiedene IP-Adressen zum FQDN zurück. Diese Adressen werden vom DNS-Server in zufälliger Reihenfolge geschickt, sodass es legitim ist, immer den ersten Eintrag für den folgenden Operationsaufruf zu verwenden.

Unspezifiziert ist das Verhalten, wenn die erste Zieladresse nicht erreichbar ist. Die möglichen Reaktionen darauf sind entweder eine erneute DNS-Abfrage für den Erhalt einer neuen IP-Adresse durchzuführen oder eine der weiteren IP-Adressen aus der letzten DNS-Abfrage zu nutzen.

4.2.10.3 Verschlüsselte Kommunikation zur VAU des E-Rezept-FD

Für die Kommunikation mit dem E-Rezept-FD gelten die Vorgaben zur TLS-gesicherten Kommunikation nach [gemILF_PS_eRp#Kommunikation zu den Diensten der TI] und [4.2.2.1- TLS-Verbindungsaufbau zu Diensten der TI über das zentrale Netz der TI].

Die Kommunikation zum E-Rezept-FD wird zusätzlich zu TLS über einen sicheren Kanal zwischen der VAU-Umgebung des NCPeH-FD und der VAU im E-Rezept-FD gesichert

(Verschlüsselung auf HTTP-Ebene). Beim Aufruf der Operationen des E-Rezept-FD muss eine verschlüsselte Kommunikation gemäß der Vorgabe [gemILF_PS_eRp#A_19741*] gewährleistet werden.

Der NCPeH-FD MUSS in der Rolle als E-Rezept-Client beim Aufbau von VAU-Kanälen zum E-Rezept-FD die Vorgaben aus [gemSpec_Krypt#VAU-Protokoll für E-Rezept] umsetzen.

A_27101 - NCPeH - ePeD-A - Prüfung von VAU-Zertifikaten des E-Rezept-FD

Der NCPeH-FD MUSS die VAU-Zertifikate (X.509-Zertifikate) des E-Rezept-FD gemäß den Vorgaben aus [[4.2.3 Prüfung von nonQES-Zertifikaten](#)] mit der Rollen-OID oid_erp_vau auf Gültigkeit prüfen. Bei Abweichungen MUSS der NCPeH-FD die Benutzung des Zertifikats für einen Verbindungsaufbau zur VAU ablehnen. [**<=**]

Wenn der NCPeH-FD das VAU-Zertifikat des E-Rezept-FD mit dem Ergebnis gültig geprüft hat, dann KANN er dieses Zertifikat für 12h zwischenspeichern und nutzen.

A_27259 - Verwaltung der VAU-Zertifikate des E-Rezept-FD in der lokalen VAU

Wenn der NCPeH-FD das gültig geprüfte VAU-Zertifikat des E-Rezept-FD für 12h zwischenspeichert, dann MUSS er es in der VAU sicher speichern. Nach Ablauf der gültigen Zwischenspeicherung MUSS der NCPeH-FD das VAU-Zertifikat des E-Rezept-FD sicher löschen, erneut beziehen und auf Gültigkeit prüfen.

[**<=**]

Hinweis zum Fehlerhandling: Nur wenn der äußere Response des E-Rezept-FD den Response-Code 200 liefert, enthält der Payload eine mittels VAU-Protokoll verschlüsselte Response.

A_27056 - NCPeH - ePeD-A - Patient Identification - Umgang mit Fehlern beim Aufbau des VAU-Kanals zum E-Rezept-FD

Wenn beim Aufbau des VAU-Kanals zum E-Rezept-FD im Rahmen des Anwendungsfalls [5.2.1- NCPeH_UC_9 - Versicherten im Behandlungsland für ePeD-A identifizieren] ein Fehler auftritt, indem der E-Rezept-FD in der äußeren Response einen HTTP Status Code ≥ 400 liefert, MUSS der NCPeH-FD die weitere Bearbeitung der Anfrage abbrechen und dem NCPeH Land-B mit einer Fehlermeldung antworten, wobei Teile der Antwortnachricht wie folgt zu befüllen sind:

- Reason Encoding (reasonOf-Element) gemäß [eHDSI_XCPD_Profile#2.3.3]=

```
<mitigatedBy typeCode="MITGT">
  <detectedIssueManagement
    classCode="ACT" moodCode="ENV">
    <code code="InternalError"
      codeSystem="1.3.6.1.4.1.19376.1.2.27.3"/>
    </detectedIssueManagement>
  </mitigatedBy>
```
- Acknowledgement =

```
acknowledgement.typeCode= AA queryAck.queryResponseCode= AE
acknowledgementDetail.Code= ERROR_PI_INTERNAL_ERROR
acknowledgementDetail.Text = Patient Identification Error
acknowledgementDetail.Location = "No provision of patient data due to an
internal error."
```

[**<=**]

A_27057 - NCPeH - ePeD-A - Abruf oder Dispensierung von E-Rezepten - Umgang mit Fehlern beim Aufbau des VAU-Kanals zum E-Rezept-FD

Wenn beim Aufbau des VAU-Kanals zum E-Rezept-FD im Rahmen der Anwendungsfälle [5.2.2- NCPeH_UC_10 - Einlösbare E-Rezepte des Versicherten aus ePeD-A auflisten], [5.2.3- NCPeH_UC_11 - Ausgewählte E-Rezepte aus ePeD-A abrufen] und [5.2.4- NCPeH_UC_12 - Abgabe von Arzneimitteln an Versicherte im Abgabeland] ein Fehler auftritt, indem der E-Rezept-FD in der äußeren Response eine HTTP Status Code ≥ 400

liefert, MUSS der NCPeH-FD die weitere Bearbeitung der Anfrage abbrechen und dem NCPeH Land-B mit einer Fehlermeldung antworten, wobei Teile der Antwortnachricht wie folgt zu befüllen sind:

- `AdhocQueryResponse@status = urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Failure`
- `errorCode` gemäß [eHDSI_XCA_Profile#2.2.3] und [eHDSI_NCPeH_Components#6.4] = `ERROR_INTERNAL_ERROR`
- `codeContext = Internal error when querying the patient's ePrescriptions`
- `severity = urn:oasis:names:tc:ebxml-regrep:ErrorSeverityType:Error`
- `location = "The VAU connection to the national e-prescription service could not be established"`

[<=]

4.2.10.4 Authentifizierung des NCPeH-FD am E-Rezept-FD

Der NCPeH-FD, als Repräsentant des NCPeH Land-B in der TI, authentisiert sich gegenüber dem IDP-Dienst für Zugriffe auf Dienste der TI im Rahmen der Anwendung E-Rezept.

Wenn für die TI-Identität des NCPeH Land-B für den Zugriff auf E-Rezept-FD kein gültiges `ACCESS_TOKEN` vorliegt, dann beantragt der NCPeH-FD das benötigte `ACCESS_TOKEN` beim IDP-Dienst. Hierfür wird am Authorization-Endpunkt des IDP-Dienstes ein `AUTHORIZATION_CODE` beantragt, der nach erfolgreicher Verifikation am Token-Endpunkt des IDP-Dienstes gegen ein `ID_TOKEN` und einen `ACCESS_TOKEN` getauscht wird.

Die für die Beantragung des `AUTHORIZATION_CODE` im Challenge-Response-Verfahren notwendige elektronische Signatur erstellt der NCPeH-FD mittels entsprechender AUT-Identität der SM-B für das Land-B gemäß Vorgaben aus [[4.2.9 Elektronische Identitäten des NCPeH-FD](#)].

Der IDP-Dienst führt die Identifikation des NCPeH-FD durch, und stattet diese anschließend mit `ID_TOKEN` gemäß [openid-connect-core#IDToken] und `ACCESS_TOKEN` gemäß [RFC6749 # section-1.4] & [RFC6749 # section-5] aus. Dabei wurde aus Sicherheitsaspekten der "authorization code grant" gemäß [RFC6749 # section-4.1] gewählt. Um dem erforderlichen Sicherheitsniveau gerecht zu werden, wird zudem die Verwendung von PKCE (Proof Key for Code Exchange by OAuth Public Clients) gemäß [RFC7636] vorgesehen.

Der IDP-Dienst selbst teilt sich in mehrere statisch adressierte Teildienste auf. Diese umfassen:

- Discovery-Endpunkt ("OAuth 2.0 Authorization Server Metadata" [RFC8414]),
- Authorization-Endpunkt (Teil des "The OAuth 2.0 Authorization Framework" [RFC6749]),
- Token-Endpunkt [RFC6749#section-3.2].

Für weitere Informationen zum IDP-Dienst und zum Ablauf der Authentisierung siehe [gemSpec_IDP_Dienst] und [gemILF_PS_eRp#Abruf von Token beim IDP-Dienst].

Für die Nutzung des IDP-Dienstes im Zusammenhang mit dem E-Rezept-FD gelten die übergreifenden Vorgaben aus [[4.2.6.1 Registrierung beim IDP-Dienst](#)], [[4.2.6.2 Verarbeitung des Discovery Document](#)] und [[4.2.6.3 TLS-Verbindungsaufbau zu Service-Endpunkten des IDP-Dienstes](#)].

4.2.10.5 Abruf von Token vom IDP-Dienst

Der folgende Abschnitt umfasst Vorgaben, die den Ablauf der Beantragung und Ausgabe von Token bestimmen.

Der Abruf von Token vom IDP-Dienst für den E-Rezept-FD folgt den Vorgaben aus [gemILF_PS_eRp#Abruf von Token beim IDP-Dienst], die dort auch für den NCPeH-FD vorgegeben werden. In diesem Abschnitt erfolgen zusätzlich einige Präzisierungen für den NCPeH-FD.

A_27077 - NCPeH - ePeD-A - Signatur der Challenge des IdP-Dienstes

Der NCPeH-FD MUSS für die Signatur der Challenge des IdP-Dienstes nach [gemILF_PS_eRp#A_20665*] die Auswahl des korrekten Signaturzertifikat C.HCI.AUT als NCPeH-Identität Land-B gemäß Vorgaben aus [[4.2.9 Elektronische Identitäten des NCPeH-FD](#)] durchführen.[<=]

A_27078 - NCPeH - ePeD-A - Response auf die Challenge des Authorization-Endpunktes

Der NCPeH-FD MUSS für die Response auf die Challenge des Authorization-Endpunktes nach [gemILF_PS_eRp#A_20667*] das in A_27077 gewählte Signaturzertifikat C.HCI.AUT als NCPeH-Identität Land-B nutzen.[<=]

A_27080 - NCPeH - ePeD-A - Gültigkeitsprüfung der Signatur des ID_TOKEN innerhalb der TI

Der NCPeH-FD MUSS zur Prüfung der Signaturzertifikates des ACCESS_TOKEN nach [gemILF_PS_eRp#A_20674*] und [gemILF_PS_eRp#A_20675*] die Vorgaben aus [[4.2.3 Prüfung von nonQES-Zertifikaten](#)] umsetzen.[<=]

A_27127 - NCPeH - ePeD-A - Sicheres Löschen des ID_TOKEN und AUTHORIZATION_CODE

Der NCPeH-FD MUSS, nach Erhalt des ID_TOKEN und des ACCESS_TOKEN, vorhandene ID_TOKEN und AUTHORIZATION_CODE-Objekte sicher löschen.[<=]

Hinweis: Für weitere Informationen siehe auch in der Dokumentation [api-erp] auf github [[Als Nutzer gegenüber der Telematikinfrastruktur authentisieren](#)].

4.2.10.6 Erstellung des Payload für die Kommunikation mit dem E-Rezept-FD

A_27144 - NCPeH - ePeD-A - Übermittlung des HTTP-Header Authorization an E-Rezept-FD

Der NCPeH-FD MUSS sicherstellen, dass im inneren Request für die Operationen /get-eu-prescriptions und /Task/<id>/\$eu-close ein HTTP-Header Authorization mit einem gültigen ACCESS_TOKEN an den E-Rezept-FD übermittelt wird.[<=]

Hinweis: ACCESS_TOKEN ist ein vom IDP-Dienst ausgestellter ACCESS_TOKEN. Für mehr Informationen siehe [4.2.10.4- Authentifizierung des NCPeH-FD am E-Rezept-FD].

A_26952 - NCPeH - ePeD-A - Befüllung der Payload-Parameter für Aufruf der Operation /get-eu-prescriptions

Der NCPeH-FD MUSS im inneren Request beim Aufruf der Operation /get-eu-prescriptions eine Payload nach dem FHIR-Profil [GEM_ERPEU_PR_PAR_GET_Prescription_Input] erstellen, darin ein parameter-Element mit dem Namen requestData anlegen und innerhalb des Elements part-Elemente entsprechend den Vorgaben aus der Tabelle "TAB_NCPeH_Payload_Aufruf_Operation_get-eu-prescriptions" erstellen und befüllen.

Tabelle 22: TAB_NCPeH_Payload_Aufruf_Operation_get-eu-prescriptions

name	value oder code	system	display
------	-----------------	--------	---------

<p>requesttype</p>	<p>Der entsprechende Wert MUSS in dem Element gesetzt werden, wenn die Operation /get-eu-prescriptions im Zusammenhang mit dem entsprechenden Anwendungsfall aufgerufen wird (für weitere Informationen zum Parameter siehe [gemSpec_eRp_FD#Http-Operation POST get-eu-prescriptions] und [API_EU_E-Rezepte#Abfragen von E-Rezepten des E-Rezept-Fachdienst]):</p> <ul style="list-style-type: none"> • Beim Anwendungsfall "Versicherten im Behandlungsland für ePeD-A identifizieren" MUSS der Wert gesetzt werden: demographics • Beim Anwendungsfall "Einlösbare E-Rezepte des Versicherten aus ePeD-A auflisten" MUSS der Wert gesetzt werden: e-prescriptions-list • Beim Anwendungsfall "Ausgewählte E-Rezepte abrufen" MUSS der Wert gesetzt werden: e-prescriptions-retrieval 	<p>Der folgende Wert MUSS gesetzt werden: "https://gematik.de/fhir/erp-eu/CodeSystem/GEM_ERPEU_CS_RequestType"</p>	<p>Keine Angaben</p>
<p>kvnr</p>	<p>Wenn die Befüllung dieses Parameters</p>	<p>Der folgende Wert MUSS gesetzt werden:</p>	<p>Keine Angaben</p>

	<p>im Zusammenhang mit dem Anwendungsfall [5.2.1- NCPeH.UC_9 - Versicherten im Behandlungsland für ePeD-A identifizieren] erfolgt, dann MUSS der folgende Wert in dem Parameter gesetzt werden:</p> <ul style="list-style-type: none"> • Wert aus der Variable xcpd_kvnr (siehe [6.1.1.3- TUC_NCPeH_023: Patient Demographics Query Request für ePeD-A verarbeiten]). <p>Ansonsten bei allen anderen Anwendungsfällen MUSS der folgende Wert in dem Parameter gesetzt werden:</p> <ul style="list-style-type: none"> • Wert aus der Variable trc_kvnr (siehe [4.1.6 - Validierung der TRC-Assertion]). 	<p>"http://fhir.de/sid/gkv/kvid-10"</p>	
<p>access Code</p>	<p>Wenn die Befüllung dieses Parameters im Zusammenhang mit dem Anwendungsfall [5.2.1- NCPeH.UC_9 - Versicherten im Behandlungsland für ePeD-A identifizieren] erfolgt, dann MUSS der folgende Wert in dem Parameter gesetzt werden:</p> <ul style="list-style-type: none"> • Wert aus der Variable xcpd_accesscod 	<p>Der folgende Wert MUSS gesetzt werden: "https://gematik.de/fhir/erp/NamingSystem/GEM_ERP_NS_EU_AccessCode"</p>	<p>Keine Angaben</p>

	<p>e_erp (siehe [6.1.1.3-TUC_NCPeH_023: Patient Demographics Query Request für ePeD-A verarbeiten]).</p> <p>Ansonsten bei allen anderen Anwendungsfällen MUSS der folgende Wert in dem Parameter gesetzt werden:</p> <ul style="list-style-type: none"> • Wert aus der Variable trc_acc esscode (siehe [4.1.6 - Validierung der TRC-Assertion]). 		
countryCode	<p>Der Wert der Variable tls_country aus dem TLS-Zertifikat des NCPeH Land-B MUSS gesetzt werden (siehe [4.1.3.1 - Sicherer Kanal: TESTA-ng und TLS])</p>	<p>Der folgende Wert MUSS gesetzt werden: "urn:iso:std:iso:3166"</p>	Keine Angaben
practitionerName	<p>Der Wert der Variable ida_practitioner_name aus der Identity Assertion des LE-EU MUSS gesetzt werden (siehe [4.1.5 - Validierung der Identity Assertion des LE-EU])</p>	Keine Angaben	Keine Angaben
practitionerRole	<p>Ausgehend vom Wert der Variable ida_practitioner_role aus der Identity Assertion des LE-EU (siehe [4.1.5 - Validierung der Identity Assertion</p>	<p>Der folgende Wert MUSS gesetzt werden: "urn:oid:2.16.840.1.113883.2.9.6.2.7"</p>	<p>Ausgehend vom Wert der Variable ida_practitioner_role aus der Identity Assertion des LE-EU (siehe [4.1.5 - Validierung der Identity Assertion des LE-EU]) MUSS der NCPeH-FD eine</p>

	<p>des LE-EU) MUSS der NCPeH-FD den Code in den Parameter aufnehmen. Der NCPeH-FD DARF NICHT die Bezeichnung aus dem Wert der Variable <code>ida_practitioner_role</code> dem Parameter zuweisen.</p> <p>Beispiel: Die Variable <code>ida_practitioner_role</code> kann folgenden Wert enthalten: "2262 - Pharmacists". Der Code aus dem Wert wird extrahiert, so dass dem Parameter "practitionerRole" unter dem ElementvalueCoding/code-Element der Wert 2262 gesetzt wird.</p>		<p>passende Bezeichnung in Deutsch nach Mapping-Regeln des BfArM ermitteln und in den Parameter aufnehmen. Der NCPeH-FD MUSS sicherstellen, dass nur menschen-lesbare Informationen (also keine Code-Werte) in den Parameter aufgenommen werden.</p>
pointOfCare	<p>Der Wert der Variable <code>ida_point_of_care</code> aus der Identity Assertion des LE-EU MUSS gesetzt werden (siehe [4.1.5 - Validierung der Identity Assertion des LE-EU])</p>	Keine Angaben	Keine Angaben
health care-facility-type	<p>Der NCPeH-FD MUSS auf Basis des Wertes aus der Variable <code>ida_health_care_facility_type_code</code> aus der Identity Assertion des LE-EU (siehe [4.1.5 - Validierung der Identity Assertion des LE-EU]) und den</p>	<p>Der folgende Wert MUSS gesetzt werden: "https://gematik.de/fhir/directory/CodeSystem/OrganizationProfessionOID"</p>	<p>Ausgehend vom Wert der Variable <code>ida_health_care_facility_type_code</code> aus der Identity Assertion des LE-EU MUSS der NCPeH-FD eine passende Bezeichnung in Deutsch nach Mapping-Regeln des BfArM ermitteln und in</p>

	<p>Mapping-Regeln des BfArM einen passenden Code aus [https://gematik.de/fhir/erp-eu/ValueSet/GEM_ERPEU_VS_HealthCareFacilityType] ermitteln und in den Parameter aufnehmen.</p>		<p>den Parameter aufnehmen. Wenn ein Mapping nicht erfolgreich durchgeführt werden kann, dann MUSS der originale Texteintrag aus der Variable <code>ida_healthcare_facility_type_code</code> in den Parameter übernommen werden.</p>
--	--	--	--

[<=]

A_27247 - NCPeH - ePeD-A - Befüllung der Payload-Parameter für Aufruf der Operation /Task/<id>/\$eu-close

Der NCPeH-FD MUSS im inneren Request beim Aufruf der Operation /Task/<id>/\$eu-close eine Payload nach dem FHIR-Profil [GEM_ERPEU_PR_PAR_CloseOperation_Input] erstellen, darin ein parameter-Element mit dem Namen `requestData` anlegen und innerhalb des Elements `part`-Elemente entsprechend den Vorgaben aus der Tabelle "TAB_NCPeH_Payload_Aufruf_Operation_Task_id_eu-close" erstellen und befüllen.

Tabelle 23: TAB_NCPeH_Payload_Aufruf_Operation_Task_id_eu-close

name	value oder code	system	display
kvnr	<p>Der Wert aus der Variable <code>trc_kvnr</code> (siehe [4.1.6 - Validierung der TRC-Assertion]) MUSS gesetzt werden</p>	<p>Der folgende Wert MUSS gesetzt werden: "http://fhir.de/sid/gkv/kvid-10"</p>	Keine Angaben
access Code	<p>Der Wert aus der Variable <code>trc_access code</code> (siehe [4.1.6 - Validierung der TRC-Assertion]) MUSS gesetzt werden</p>	<p>Der folgende Wert MUSS gesetzt werden: "https://gematik.de/fhir/erp/NamingSystem/GEM_ERP_NS_EU_AccessCode"</p>	Keine Angaben
countryCode	<p>Der Wert der Variable <code>tls_country</code> aus dem TLS-Zertifikat des NCPeH Land-B MUSS gesetzt werden (siehe [4.1.3.1 - Sicherer Kanal: TESTA-ng und TLS])</p>	<p>Der folgende Wert MUSS gesetzt werden: "urn:iso:std:iso:3166"</p>	Keine Angaben
practit	Der Wert der	Keine Angaben	Keine Angaben

<p>practitionerName</p>	<p>Variable ida_practitioner_name aus der Identity Assertion des LE-EU MUSS gesetzt werden (siehe [4.1.5 - Validierung der Identity Assertion des LE-EU])</p>		
<p>practitionerRole</p>	<p>Ausgehend vom Wert der Variable ida_practitioner_role aus der Identity Assertion des LE-EU (siehe [4.1.5 - Validierung der Identity Assertion des LE-EU]) MUSS der NCPeH-FD den Code in den Parameter aufnehmen. Der NCPeH-FD DARF NICHT die Bezeichnung aus dem Wert der Variable ida_practitioner_role dem Parameter zuweisen.</p> <p>Beispiel: Die Variable ida_practitioner_role kann folgenden Wert enthalten: "2262 - Pharmacists". Der Code aus dem Wert wird extrahiert, so dass dem Parameter "practitionerRole" unter dem ElementvalueCoding/code-Element der Wert 2262 gesetzt wird.</p>	<p>Der folgende Wert MUSS gesetzt werden: "urn:oid:2.16.840.1.113883.2.9.6.2.7"</p>	<p>Ausgehend vom Wert der Variable ida_practitioner_role aus der Identity Assertion des LE-EU (siehe [4.1.5 - Validierung der Identity Assertion des LE-EU]) MUSS der NCPeH-FD eine passende Bezeichnung in Deutsch nach Mapping-Regeln des BfArM ermitteln und in den Parameter aufnehmen. Der NCPeH-FD MUSS sicherstellen, dass nur menschen-lesbare Informationen (also keine Code-Werte) in den Parameter aufgenommen werden.</p>
<p>pointOfCare</p>	<p>Der Wert der Variable ida_point_of_care aus der</p>	<p>Keine Angaben</p>	<p>Keine Angaben</p>

	Identity Assertion des LE-EU MUSS gesetzt werden (siehe [4.1.5 - Validierung der Identity Assertion des LE-EU])		
health care-facility-type	Der NCPeH-FD MUSS auf Basis des Wertes aus der Variable ida_healthcare_facility_type_code aus der Identity Assertion des LE-EU (siehe [4.1.5 - Validierung der Identity Assertion des LE-EU]) und den Mapping-Regeln des BfArM einen passenden Code aus [https://gematik.de/fhir/erp-eu/ValueSet/GEM_ERPEU_VS_HealthCareFacilityType] ermitteln und in den Parameter aufnehmen.	Der folgende Wert MUSS gesetzt werden: "https://gematik.de/fhir/directory/CodeSystem/OrganisationProfessionOID"	Ausgehend vom Wert der Variable ida_healthcare_facility_type_code aus der Identity Assertion des LE-EU MUSS der NCPeH-FD eine passende Bezeichnung in Deutsch nach Mapping-Regeln des BfArM ermitteln und in den Parameter aufnehmen. Wenn ein Mapping nicht erfolgreich durchgeführt werden kann, dann MUSS der originale Texteintrag aus der Variable ida_healthcare_facility_type_code in den Parameter übernommen werden.

[<=]

4.2.10.7 Regelung zur Unterstützung von mehreren FHIR-Package Versionen

Der NCPeH-FD setzt für ePeD-A FHIR-Profilen aus den folgenden FHIR-Profil-Packages um:

- "kbv.ita.erp" [<https://simplifier.net/erezept>],
- "de.gematik.erezept.eu" [<https://simplifier.net/erezept-workflow-eu>].

Das Package "kbv.ita.erp" definiert das Datenmodell für Verordnungsdaten. Es wird durch die Kassenärztliche Bundesvereinigung (KBV) sowie dem GKV-SV verantwortet und durch die KBV veröffentlicht. Die zeitliche Gültigkeit der Versionen des Packages "kbv.ita.erp" ist in [KBV_ITA_VGEX_Technische_Anlage_ERP] beschrieben. Eine neue Version des Package wird in der Regel mit einem Vorlauf von 9 Monaten vor Gültigkeit in der Produktivumgebung veröffentlicht. Diese Regelung schließt einen anderen Vorlauf der Veröffentlichung und Inkraftsetzung nicht aus.

Für die Einführung in den Produktivbetrieb wird den Verordnungsausstellenden Leistungserbringerinstitution (LEI) eine Übergangsfrist von mehreren Monaten nach Gültigkeitsbeginn (beim letzten Profilwechsel 6 Monate) eingeräumt. In diesem Zeitraum akzeptiert der E-Rezept-Fachdienst Verordnungen in der alten und neuen Profilversion. D.h. der NCPeH muss für diesen Zeitraum und zusätzlich für die Dauer der Gültigkeit der Verordnungen (maximal 365 Tage nach Ende des Übergangszeitraumes) in der

Verarbeitung der Response der Operation POST /\$get-eu-prescriptions mehrere (ggf. mehr als zwei) Profilversionen unterstützen.

In den Informationen zu einer Verordnung werden Wertekataloge (bspw. Darreichungsform) verwendet, welche durch die Informationsstelle für Arzneispezialitäten – IFA GmbH (IFA) veröffentlicht werden. Sie werden spätestens 3 Monate vor Gültigkeit in der Produktivumgebung veröffentlicht.

Das Package "de.gematik.erezept.eu" definiert das Datenmodell für die Übermittlung der Dispensierinformationen. Es wird durch die gematik verantwortet und veröffentlicht. Die zeitliche Gültigkeit der Versionen des Packages "de.gematik.erezept.eu" wird in [FHIR_Version_E-Rezept_EU] beschrieben. Eine neue Version des Package wird mit einem Vorlauf von 6 Monaten vor Gültigkeit in der Produktivumgebung veröffentlicht.

Für die Einführung in den Produktivbetrieb wird eine Übergangsfrist von 3 Monaten nach Gültigkeitsbeginn eingeräumt. D.h. der NCPeH muss innerhalb dieses Übergangszeitraumes die für die Operation POST /\$get-eu-prescriptions und POST /Task/\$eu-close unterstützte Profilversion von der alten auf die neue Profilversion umstellen.

Die Planung von neuen Profilversionen wird von der gematik auf [api-erp] veröffentlicht.

Hinweise zu anstehenden Veränderungen in FHIR-Profilen sind auch in der [[E-Rezept API-Dokumentation#Aktuelles](#)] zu finden.

4.3 Sicherheit und Datenschutz

Die Akzeptanz des NCPeH-FD durch die Nutzer wird maßgeblich durch die Gewährleistung des Datenschutzes und - damit verbunden - die Sicherheit der personenbezogenen medizinischen Daten beeinflusst. Der Datenschutz und die Informationssicherheit des NCPeH-FD wird durch das Aufstellen von umfassenden, prüfbar Anforderungen durch die gematik sichergestellt. Die Überprüfung dieser Anforderungen geschieht sowohl vor der ersten Inbetriebnahme durch die gematik, als auch regelmäßig im laufenden Betrieb durch den Betreiber des NCPeH-FD selbst. Qualitätsgesicherte Prozesse in Form von Audits der gematik und der EU halten die Überprüfungsergebnisse fest.

Die aufgestellten Anforderungen des Datenschutzes und der Informationssicherheit entsprechen dem Gebot der Angemessenheit dadurch, dass sie einerseits den Schutzbedarf der zu verarbeitenden Daten und andererseits die Umsetzungsfähigkeit durch den Hersteller des Frontend des Versicherten und den Betreiber des NCPeH-FD berücksichtigen. Die Angemessenheit der Anforderungen hinsichtlich des Schutzbedarfs wird durch die Nutzung der Methoden zur Informationssicherheit und des Datenschutzes der TI unter Beachtung der Risiko-Policy der TI erreicht. Die Angemessenheit hinsichtlich der Umsetzbarkeit wird in den spezifizierten Technologien berücksichtigt.

Die Sicherheitsanforderungen an den NCPeH-FD leiten sich zum einen vom Schutzbedarf der zu verarbeiteten Daten und zum anderen von der potenziellen negativen Beeinflussung der TI durch diesen Dienst ab.

Für die Aufrechterhaltung des Datenschutz- und Informationssicherheitsniveaus der TI ist es erforderlich, dass die TI durch die Nutzung des NCPeH-FD nicht negativ beeinflusst wird. Eine Beeinträchtigung kann insbesondere über den Anschluss des NCPeH-FD erfolgen. Um dies zu verhindern, werden dem Betreiber des NCPeH-FD entsprechend dem Modularisierungskonzept in [gemSpec_DS_Anbieter] Module der Informationssicherheit und des Datenschutzes zugeordnet.

Über diese Module bzw. die zugehörigen Anforderungen wird der Betreiber auch verpflichtet, Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der

Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung einzurichten.

Die folgenden Anforderungen verhindern Profilbildungen über Versicherte und Leistungserbringer(-institutionen) durch den Anbieter bzw. dessen Mitarbeiter.

A_22897 - Anbieter des NCPeH-Fachdienstes - Ordnungsgemäße IT-Administration

Der Anbieter des NCPeH-Fachdienstes MUSS die Maßnahmen für erhöhten Schutzbedarf des BSI-Bausteins „OPS.1.1.2 Ordnungsgemäße IT-Administration“ [BSI-Grundschutz] während des gesamten Betriebs des NCPeHs umsetzen. [<=]

Hinweis: Die Anforderungen des BSI-Bausteins sind entsprechend des dort genannten Schlüsselwortes („MUSS, DARF NICHT/ DARF KEIN, SOLLTE; SOLLTE NICHT/SOLLTE KEIN, KANN/DARF“) umzusetzen.

A_22899 - Anbieter des NCPeH-Fachdienstes - Zwei-Faktor-Authentisierung von Administratoren

Der Anbieter des NCPeH-Fachdienstes MUSS sicherstellen, dass sich Administratoren mindestens mit einer Zwei-Faktor-Authentisierung anmelden. [<=]

A_22913 - Sicherer Betrieb des Produkts nach Handbuch

Der Anbieter des NCPeH-Fachdienstes MUSS die im Handbuch des eingesetzten NCPeH beschriebenen Voraussetzungen für den sicheren Betrieb des Produktes gewährleisten. [<=]

A_22914 - Darstellen der Voraussetzungen für sicheren Betrieb des Produkts im Handbuch

Der Hersteller des NCPeH-Fachdienstes MUSS für sein Produkt im dazugehörigen Handbuch leicht ersichtlich darstellen, welche Voraussetzungen vom Betreiber und der Betriebsumgebung erfüllt werden müssen, damit ein sicherer Betrieb des Produktes gewährleistet werden kann. [<=]

A_22898 - Anbieter des NCPeH-Fachdienstes- Sichere Speicherung von Daten

Der Anbieter des NCPeH-Fachdienstes MUSS die Daten der Komponente Audit Repository bei der Speicherung verschlüsseln. [<=]

Hinweis: für die Verschlüsselung gelten die Anforderungen aus [gemSpec_Krypt].

A_22900 - Anbieter des NCPeH-Fachdienstes - Keine unzulässige Weitergabe von Daten

Der Anbieter des NCPeH-Fachdienstes MUSS sicherstellen, dass die in dem NCPeH-Fachdienst verarbeiteten Daten, außer an berechnigte Nutzer, nicht weitergegeben werden, auch nicht in pseudonymisierter oder anonymisierter Form [<=]

A_22901 - Anbieter des NCPeH-Fachdienstes - Löschkonzept

Der Anbieter des NCPeHs MUSS in einem Löschkonzept für die im NCPeH-Fachdienst verarbeiteten personenbezogenen Daten mindestens folgende Aspekte beschreiben:

- die umgesetzten organisatorischen und technischen Löschrmaßnahmen (dies beinhaltet insbesondere auch die Löschung von Backups, Audit Daten etc.),
- die Löschrregeln und Löschrfristen zusammen mit einer nachvollziehbaren Begründung für die getroffenen Fristfestlegungen,
- wie sichergestellt wird, dass alle Auftragnehmer die Löschrpflichten ihrerseits umsetzen.

[<=]

Hinweis: Das Löschkonzept kann Teil des Sicherheits- oder Datenschutzkonzeptes des Anbieters sein. Es ist nicht notwendigerweise ein eigenes Dokument erforderlich.

A_22902 - Anbieter des NCPeH-Fachdienstes - Information des Versicherten zur Wahrnehmung der Betroffenenrechte bei der Einwilligung der Nutzung des Übermittlungsverfahrens

Der Anbieter des NCPeH-Fachdienstes MUSS Versicherte bei der Einwilligung der Nutzung des Übermittlungsverfahrens in einfacher und verständlicher Form darüber informieren, wie sie ihre Betroffenenrechte nach DSGVO in Verbindung mit BDSG gegenüber dem Anbieter wahrnehmen können, insbesondere auch, an welche datenschutzrechtliche Aufsichtsbehörde sie sich bei Datenschutzbeschwerden bzgl. des Anbieters wenden müssen. [≤]

A_22903 - Anbieter des NCPeH-Fachdienstes - Ausreichende Informationen für eine informierte Einwilligung bei der Einwilligung der Nutzung des Übermittlungsverfahrens

Der Anbieter des NCPeH-Fachdienstes MUSS sicherstellen, dass den Versicherten bei der Einwilligung der Nutzung des Übermittlungsverfahrens Informationen in allgemein verständlicher Form bereitgestellt werden, die für eine informierte Einwilligung notwendig sind; neben den Informationen gemäß Art. 13 DSGVO sind dies insbesondere die Funktionsweise des NCPeHs und die wesentlichen Datenschutz- und Sicherheitsmaßnahmen. [≤]

A_22904 - Anbieter des NCPeH-Fachdienstes - Information der Versicherten zur Wahrnehmung der Betroffenenrechte während der Nutzung des NCPeH-Fachdienstes

Der Anbieter des NCPeH-Fachdienstes MUSS sicherstellen, dass sich Versicherte jederzeit in einfacher Weise beim Anbieter darüber informieren können, wie sie ihre Betroffenenrechte nach DSGVO in Verbindung mit BDSG gegenüber dem Anbieter wahrnehmen können. [≤]

A_22906 - Anbieter des NCPeH-Fachdienstes - Ermittlung von Standard-Nutzung

Der Anbieter des NCPeH-Fachdienstes MUSS mindestens einmal im Jahr Werte zu einer Standard-Nutzung von LE-EU durch die Profilierung anonymer Zugriffsstatistiken auf den NCPeH-Fachdienst zum Zweck der Erkennung von Zugriffen gemäß A_22907 ermitteln. [≤]

A_22907 - Anbieter des NCPeH-Fachdienstes - Abweichung von Standard-Nutzung

Der Anbieter des NCPeH-Fachdienstes MUSS Zugriffe und Zugriffsmuster, die nicht einer Standard-Nutzung entsprechen, erkennen und Maßnahmen zur Schadensreduzierung umsetzen. [≤]

A_22908-01 - Anbieter des NCPeH-FD - Einsatz zertifizierter HSM

Der Anbieter des NCPeH-FD MUSS beim Einsatz eines HSM sicherstellen, dass dessen Eignung durch eine erfolgreiche Evaluierung nachgewiesen wurde. Als Evaluierungsschemata kommen dabei Common Criteria oder Federal Information Processing Standard (FIPS) in Frage. Die Prüftiefe MUSS mindestens

1. FIPS 140-2 Level 3 oder
2. FIPS 140-3 Level 3 oder
3. Common Criteria EAL 4+ (mit AVA_VAN.5)

[≤]

A_22909 - Anbieter des NCPeH-Fachdienstes - Sicherer Betrieb und Nutzung eines HSMs

Der Anbieter des NCPeH-Fachdienstes MUSS sicherstellen, dass die auf dem HSM verarbeiteten privaten Schlüssel, Konfigurationen und eingesetzte Software nicht unautorisiert ausgelesen, unautorisiert verändert, unautorisiert ersetzt oder in anderer Weise unautorisiert benutzt werden können. [≤]

A_22910 - Anbieter des NCPeH-Fachdienstes - Angriffen entgegenwirken

Der Anbieter des NCPeH-Fachdienstes MUSS Maßnahmen zur Erkennung von Angriffen und zur Reduzierung bzw. Verhinderung von Schäden aufgrund von Angriffen in allen Komponenten des NCPeHs umsetzen. [≤]

A_22911 - Anbieter des NCPeH-Fachdienstes - Social Engineering Angriffen entgegenwirken

Der Anbieter des NCPeH-Fachdienstes MUSS Maßnahmen zur Erkennung und Verhinderung von Social Engineering Angriffen umsetzen. [≤]

A_23136 - Eingabevalidierung von Operationen

Der NCPeH-Fachdienst MUSS alle Operationsaufrufe seiner Schnittstellen (Requests) sowie die Antwortmeldung auf seine Anfragen (Responses) auf Wohlgeformtheit und Zulässigkeit gemäß Protokoll SOAP 1.2 prüfen und bei Schema-, Semantik- oder Protokollverletzungen die Operation abbrechen. [≤]

Hinweis: Die Prüfung der eingehenden Nachrichten auf Syntax-, Semantik- und Protokollverletzungen soll insbesondere den Angriffstypen XML Injection, XPath Query Tampering, XML External Entity Injection und XML Signature Wrapping entgegenwirken.

A_22912 - Anbieter des NCPeH-Fachdienstes - Verbot vom dynamischen Inhalt

Die Komponenten des NCPeH-Fachdienstes DÜRFEN dynamischen Inhalt von Drittanbietern NICHT herunterladen und verwenden.

[≤]

A_23135 - Akzeptieren der Identity Assertion des anfragenden LE-EU

Der NCPeH-Fachdienst MUSS die LE-EU Identity Assertion von EU Ländern ablehnen, wenn keine Vereinbarung zum Datenaustausch zwischen Deutschland und dem EU-Land existiert. [≤]

A_23140 - Korrekte Zuordnung der NCPeH Land-B Identitäten

Beim Abruf der Daten des ePA-Aktensystems MUSS der NCPeH-Fachdienst sicherstellen, dass die technische Identität des NCPeH Land-B zu dem anfragenden Land korrekt zugeordnet ist. [≤]

A_23166 - Keine Zwischenspeicherung ePKA MIO

Der NCPeH-Fachdienst DARF das ePKA MIO NICHT zwischenspeichern.

[≤]

Hinweis: Zwischenspeicherung entspricht nicht einer Verarbeitung im RAM innerhalb der VAU.

A_23188 - Kontrollierte Änderungen der Konfigurationsparameter

Der Anbieter des NCPeH-Fachdienstes MUSS sicherstellen, dass Änderungen der Konfigurationsparametern aus dem Kapitel [4.1.1- Konfigurationsparameter](#) nur im 4-Augen-Prinzip erfolgt. [≤]

A_23176 - Eingeschränkte Nutzung des Audit Repositories

Der Anbieter des NCPeH-Fachdienstes MUSS durch technische und organisatorische Maßnahmen sicherstellen, dass die Daten des Audit Repository nur zum Zweck der Audit-Auskunft oder zur Aufrechterhaltung der Sicherheit verwendet werden kann. [≤]

A_23177 - Eingeschränkter Zugriff auf Audit Repository

Der Anbieter des NCPeH-Fachdienstes MUSS sicherstellen, dass Zugriff auf die Daten des Audit Repository nur durch sonderberechtigte Personen (Prozessverantwortlicher Audit Trails) nur im 4-Augen-Prinzip erfolgt. [≤]

A_23138 - Tamper Proof Audit

Der Anbieter des NCPeH-Fachdienstes MUSS sicherstellen, dass das Audit Repository nicht vom Administratoren oder anderen System-Benutzern manipuliert oder gelöscht werden kann. [≤]

A_22933 - Anbieter des NCPeH-Fachdienstes - Wiederherstellung von Audit Server Daten

Der Anbieter des NCPeH-Fachdienstes MUSS sicherstellen, dass die Audit Server Daten zu jeder Zeit wiederhergestellt werden kann. [≤]

A_23178-01 - Sicherheitsprüfung sicherheitsrelevante Anforderung

Der Anbieter des NCPeH-FD MUSS sicherstellen, dass alle Anforderungen aus dem folgenden Kapiteln in vollem Umfang umgesetzt werden:

- 4.1.4 - Service Metadata des NCPeH Land-B abrufen
- 4.1.5 - Validierung der Identity Assertion des LE-EU
- 4.1.6 - Validierung der TRC-Assertion
- 4.1.7.1 - Non-Repudiation of Origin erstellen
- 4.1.7.2 - Non-Repudiation of Receipt erstellen
- 4.1.7.3 - Patient Privacy Audit Trail Eintrag erstellen
- 4.1.7.4 - Translation Audit Trail Eintrag erstellen
- 4.1.7.5 - Security Audit Trail Eintrag erstellen
- 6.1.3.5 - TUC_NCPeH_009: NFD des ePKA MIO transkodieren und transformieren
- 6.1.3.6 - TUC_NCPeH_010: NFD des ePKA MIO ins PDF/A-Format transformieren

[≤]

A_24119 - Anbieter des NCPeH-Fachdienstes - Zugriffscodes Brute-force Angriffen entgegenwirken

Der Anbieter des NCPeH-Fachdienstes MUSS Maßnahmen zur Erkennung und Verhinderung von dem Erraten eines Zugriffscodes umsetzen. [≤]

A_27493 - Aufbewahrungsdauer der Non-Repudiations und Audit Trail Einträge

Der NCPeH-FD MUSS die zum Zwecke der Datenschutzkontrolle für den Versicherten erstellten

Non-Repudiation of Origin, Non-Repudiation of Receipt und Audit Trail Einträge für den Zeitraum von drei Jahren aufbewahren. Danach sind sie vom NCPeH-FD automatisch zu löschen. [≤]

Die Non-Repudiations und Audit Trail Einträge können durch den Versicherten, durch einen befugten Vertreter oder der befugten nationalen Stelle eingesehen werden. Versicherte können bei dem Anbieter des NCPeH-FD beantragen, die Non-Repudiations und Audit Trail Einträge zur Verfügung gestellt zu bekommen.

4.3.1 Datenschutzrechtliche- und informationssicherheitstechnische Anforderungen an die Vertrauenswürdige Ausführungsumgebung

In diesem Abschnitt werden die Anforderungen an den NCPeH-FD zur Umsetzung einer Vertrauenswürdigen Ausführungsumgebung (VAU) gestellt. Die VAU dient der datenschutzrechtlich zulässigen und sicheren Verarbeitung von schützenswerten unverschlüsselten Daten innerhalb des NCPeH-FD. Die VAU stellt dazu einen Verarbeitungskontext bereit, in dem die Verarbeitung sensibler Daten unverschlüsselt erfolgen kann. Dieser Verarbeitungskontext ist entsprechend zu schützen.

A_22517-03 - Umsetzung des NCPeH-FD in einer Vertrauenswürdigen Ausführungsumgebung (VAU)

Der NCPeH-FD MUSS die Verarbeitung aller fachlichen Operationen und Schnittstellen in der eHDSI, zur TI und die Schnittstellen „Audit Trails abrufen“, „Logging und Monitoring“ und „Service Metadaten & Configs verwalten“ des NCPeH-FD im Verarbeitungskontext der Vertrauenswürdigen Ausführungsumgebung (VAU) umsetzen.

[<=]

4.3.2 Verarbeitungskontext des NCPeH-FD

Die Gesamtheit aus der für eine Verarbeitung der unverschlüsselten Daten erforderlichen Software, dem für diese Verarbeitung genutzten physikalischen System sowie den für die Integrität dieser Verarbeitung erforderlichen organisatorischen und physischen Rahmenbedingungen bildet den Verarbeitungskontext der Vertrauenswürdigen Ausführungsumgebung.

Der Verarbeitungskontext grenzt sich von allen weiteren, im betrieblichen Kontext beim Betreiber des NCPeH-FD vorhandenen Systemen und Prozessen dadurch ab, dass die unverschlüsselten Daten von Komponenten innerhalb des Verarbeitungskontextes aus erreichbar sind oder sein können, während sie dies von außerhalb des Verarbeitungskontextes nicht sind. Die schützenswerten Daten verlassen den Verarbeitungskontext ausschließlich gemäß wohldefinierten (Zugriffs-)Regeln und in verschlüsselter Form.

Zur Vertrauenswürdigen Ausführungsumgebung gehören neben den Verarbeitungskontexten alle für ihre Erreichbarkeit und betriebliche Steuerung erforderlichen Komponenten. Sie dürfen nur soweit unbedingt erforderlich als Teil des Verarbeitungskontextes implementiert sein.

Der Verarbeitungskontext umfasst sämtliche physikalischen Systemkomponenten sowie sämtliche Softwarekomponenten, deren Sicherheitseigenschaften sich auf den Schutz der personenbezogenen medizinischen Daten vor Zugriff durch Unbefugte bei ihrer unverschlüsselten Verarbeitung auswirken können.

Die VAU muss die Verarbeitungslogik in Verarbeitungskontexten mittels Komponenten umsetzen, die ein hohes Maß an Gewissheit bei der Feststellung der Sicherheitseigenschaften der Anwendung ermöglichen und dazu auf Ebene des Codes (der Trusted Computing Base) möglichst kompakt gehalten werden.

A_21917-02 - Geschützte Weitergabe von Daten an autorisierte Nutzer durch die VAU

Der Verarbeitungskontext MUSS sicherstellen, dass sämtliche schützenswerten Daten ausschließlich über sichere Verbindungen an autorisierte Nutzer weitergegeben werden.

[<=]

A_21918-02 - Transportverschlüsselte Übertragung von Daten

Der Verarbeitungskontext MUSS sicherstellen, dass er nur transportverschlüsselt mit Clients kommuniziert.[<=]

Hinweis: für die Qualität der Transportverschlüsselung gelten die Anforderungen aus [gemSpec_Krypt].

A_22973-01 - TLS Endpunkt in der VAU

Der Verarbeitungskontext MUSS sicherstellen, dass der TLS-Endpunkt für die transportverschlüsselte Übertragung von Daten mit dem ePA-Aktensystem, mit dem zentralen IDP-Dienst und dem NCPeH Land-B in dem Verarbeitungskontext endet. [<=]

A_22385-02 - Keine Speicherung von schützenswerten Daten

Der Verarbeitungskontext DARF sämtliche schützenswerten Daten, mit der Ausnahme der eHDSI Audit Trail Daten, NICHT speichern.[<=]

A_23189 - Isolation der I_Management_Configuration Schnittstelle

Der Verarbeitungskontext MUSS die Datenverarbeitungsprozesse des Verarbeitungskontexts trennen und damit gewährleisten, dass Einfluss oder Zugriff auf schützenswerten Daten durch die Verwendung der I_Management_Configuration Schnittstelle ausgeschlossen sind. [\leq]

A_23190 - Isolation der „Audit Trails Abrufen“ Schnittstelle

Der Verarbeitungskontext MUSS sicherstellen, dass nur Auditdaten über die „Audit Trails Abrufen“ Schnittstelle abgerufen werden kann. [\leq]

4.3.3 Ausschluss von nicht autorisierten Zugriffen aus dem Betriebsumfeld

Der Schutzbedarf der in der VAU verarbeiteten unverschlüsselten Daten erfordert den technischen Ausschluss von Zugriffen des Anbieters. Dies umfasst insbesondere Zugriffe durch Personen aus dem betrieblichen Umfeld des Anbieters.

A_21922-02 - Isolation der VAU von Datenverarbeitungsprozessen des Anbieters

Die VAU MUSS die in ihren Verarbeitungskontexten ablaufenden Datenverarbeitungsprozesse von allen sonstigen Datenverarbeitungsprozessen des Anbieters trennen und damit gewährleisten, dass der Anbieter des Dienstes vom Zugriff auf die in der VAU verarbeiteten schützenswerten unverschlüsselten Daten ausgeschlossen ist. [\leq]

A_21923-02 - Ausschluss von Manipulationen an der Software der VAU

Die VAU MUSS eine Manipulation der für Verarbeitungskontexte eingesetzten Software oder ihrer Konfiguration erkennen und eine Ausführung der manipulierten Software verhindern. [\leq]

A_21924-02 - Ausschluss von Manipulationen an der Hardware der VAU

Die VAU MUSS die Integrität der für Verarbeitungskontexte eingesetzten Hardware und ihrer Konfiguration schützen und damit insbesondere Manipulationen an der Hardware durch den Anbieter des Dienstes ausschließen. [\leq]

A_21925-02 - Kontinuierliche Wirksamkeit des Manipulationsschutzes der VAU

Die VAU MUSS den Ausschluss von Manipulationen an der für Verarbeitungskontexte eingesetzten Hardware und Software durch den Anbieter des Dienstes mit Mitteln umsetzen, deren dauerhafte und kontinuierliche Wirksamkeit gewährleistet werden kann. [\leq]

A_21926-02 - Kein physischer Zugang des Anbieters zu Systemen der VAU

Die VAU MUSS mit technischen Mitteln sicherstellen, dass niemand, auch nicht der Anbieter des Dienstes, während der Verarbeitung personenbezogener medizinischer Daten Zugriff auf physische Schnittstellen der Systeme erlangen kann, auf denen Verarbeitungskontexte ausgeführt werden. [\leq]

A_21927-02 - Nutzdatenbereinigung vor physischem Zugang zu Systemen der VAU

Die VAU MUSS mit technischen Mitteln sicherstellen, dass physischer Zugang zu Hardware-Komponenten der Verarbeitungskontexte nur erfolgen kann, nachdem gewährleistet ist, dass aus ihnen keine Nutzdaten extrahiert werden können. [\leq]

A_22389-02 - Private Schlüssel der TI im HSM

Die VAU MUSS das private Schlüsselmaterial der TI-Identität des NCPeH-Fachdienstes und das private Schlüsselmaterial, die dem NCPeH Land-B als Repräsentation in der TI eindeutig zugeordnet sind, in einem Hardware Security Module (HSM) erzeugen und anwenden. [\leq]

A_23184 - Private Schlüssel der eHDSI im HSM

Die VAU MUSS privates Schlüsselmaterial der eHDSI-PKI des NCPeH-Fachdiensts in einem Hardware Security Module (HSM) erzeugen und anwenden.

[<=]

A_22391-02 - HSM-Kryptographieschnittstelle verfügbar nur für Verarbeitungskontexte der VAU

Die VAU MUSS mit technischen Mitteln, die auch Manipulationen durch den Anbieter des Dienstes ausschließen, gewährleisten, dass nur integrierte Verarbeitungskontexte der VAU Zugriff auf die Kryptographieschnittstelle des HSM zur Nutzung des privaten Schlüsselmaterials für ihr Dienstzertifikat erhalten kann.[<=]

A_22390-02 - Integritätsprüfung der VAU

Das HSM des NCPeH-Fachdienstes MUSS sicherstellen, dass es der VAU den benötigten privaten Schlüssel des Dienstzertifikates oder der NCPeH Land-B Identität erst zur Verfügung stellt bzw. für den Verbindungsaufbau zum NCPeH Land-B oder zum ePA-Aktensystem verwendet werden kann, nachdem der Verarbeitungskontext seine Integrität gegenüber dem HSM nachgewiesen hat.[<=]

A_21934-02 - Datenschutzkonformes Logging und Monitoring des Verarbeitungskontextes der VAU

Die VAU MUSS die für den Betrieb des NCPeH-Fachdienstes erforderlichen Logging- und Monitoring-Informationen in solcher Art und Weise erheben und verarbeiten, dass mit technischen Mitteln ausgeschlossen ist, dass dem Anbieter des Dienstes vertrauliche oder zur Profilbildung geeignete Daten zur Kenntnis gelangen. [<=]

A_21935-02 - Managementprozesse des HSM

Der NCPeH-Fachdienst MUSS die Managementprozesse des HSM so gestalten, dass ein Missbrauch des Schlüsselmaterials durch den Betreiber des Dienstes ausgeschlossen wird.[<=]

4.4 Betrieb

In diesem Kapitel werden übergreifende, betriebliche Anforderungen getroffen oder auf Kapitel mit speziellen Ausprägungen für den NCPeH Deutschland in normativen Querschnittsdokumenten verwiesen.

4.4.1 Schnittstellen und Anwendungsfälle

Die durch den NCPeH-FD zur Verfügung gestellten Schnittstellen und Anwendungsfälle werden in [[gemKPT_Betr#National Contact Point for E-Health \(PDT69\)](#)] dargestellt.

4.4.2 Leistungsanforderungen

Die vom NCPeH-FD zu leistenden Vorgaben werden übersichtlich in [[gemSpec_Perf#Performancevorgaben NCPeH-Fachdienst](#)] dargestellt.

4.4.3 Aufnahme eines Country Service Desks

Der Country Service Desk agiert in erster Linie als First-Level Service Desk für den abgegrenzten Nutzerkreis des NCPeHs. Er erfüllt damit sowohl Aufgaben eines User Help Desks (UHD), als auch Aufgaben eines Versicherten Help-Desks (VHD).

Die Anforderungen an den Country Service Desk werden in [[gemKPT_Betr#3.6.3](#)] näher beschrieben. Weitere Referenzen finden sich in [[gemKPT_Betr#6.3 "Country Service](#)

Desk") des [eHDSI_Operations_Framework] und in [gemKPT_Betr#03.01] sowie [gemKPT_Betr#03.02] des [eHDSI_Requirements_Catalogue].

Der Anbieter des NCPeH-FD DARF nachfolgende Nutzerkreise gemäß [6.3.1#eHDSI_Operations_Framework] temporär ausschließen, sofern die jeweils angegebenen Bedingungen erfüllt sind:

- Health professional (Leistungserbringer) und Third party vendors / Software integrators (Hersteller): Nur solange keine Funktionalität zum Abruf von Daten europäischer Mitgliedsstaaten (Land-B) über den NCPeH-FD in Umsetzung ist.

Auf Anfrage der gematik MUSS der Anbieter des NCPeH-FD darlegen können, welche Nutzerkreise am Country Service Desk teilnehmen.

Der Anbieter des NCPeH-FD SOLL zusätzlich zur eHDSI-Kategorisierung des Country Service Desks, weitere Datenfelder aufnehmen, welche nachfolgend beschrieben werden:

- Requester Name/Identification: Die Person oder Entität, welche den Incident/die Information an den Country Service Desk meldete.
- Submission Date: Das Datum, an dem der Incident/Service Request erstellt wurde.
- Registration Date: Das Datum, an dem der Incident/Service Request zu den technischen Lösungen hinzugefügt wurde.
- Status: Der Status des Incidents/Service Requests nach dem definierten Workflow.

Die Möglichkeit zur Aufnahme dieser Felder zwingt NICHT zur verpflichtenden Nutzung. Die Nutzung der zusätzlichen Felder ist auch stets nach Gesichtspunkten der DSGVO auszurichten. Dies bedeutet vor allem, dass der im Prozess verankerte Zweck zur Erhebung und Speicherung von teils personenbezogenen Daten deutlich ist.

4.4.4 Monitoring

Das Monitoring ist als Teil des Event-Managements gemäß [ITIL] anzusehen. Es umfasst die kontinuierliche Aufnahme und Überwachung von Ereignissen und stellt die Informationsgrundlage zu den verfügbaren IT-Services her. Sowohl der NCPeH-FD, als auch die darunterliegenden Systeme erzeugen zu jeder Zeit Informationen, um den Zustand des jeweiligen Systems zu analysieren und zu bewerten.

4.4.4.1 Erfassung und Lieferung von Rohdaten

Die durch den NCPeH-FD und den Betreiber zu erfüllenden Anforderungen hinsichtlich der Erfassung und Lieferung von Rohdaten an die gematik, werden in [gemSpec_Perf#Betriebsdatenerfassung v2 Spezifika NCPeH-FD] dargestellt.

Der Betreiber muss sicherstellen, dass die vom NCPeH-FD zugänglich gemachten Informationen des folgenden Kapitels im spezifizierten Maß sicher sowohl an die eHDSI, als auch an die gematik erfolgen.

4.4.4.2 Erfassung und Lieferung von eHDSI-Kennzahlen

Um die Anforderungen der eHDSI zur Erfassung und Lieferung von eHDSI-Kennzahlen zu konkretisieren, werden in diesem Kapitel weiterführende Festlegungen dazu getroffen. Der Inhalt und die Implementierungsrichtlinien von eHDSI-Kennzahlen werden genauer unter Kapitel 3, Tabellen 2 bis 25 [eHDSI_Monitoring_Framework] beschrieben.

Der NCPeH-FD MUSS eHDSI-Kennzahlen nach [eHDSI Monitoring Framework] automatisiert erheben.

Alle eHDSI-Kennzahlen zur Erfassung unterschiedlicher Nutzer (distinct users), werden als

kritisch eingestuft.

Die restlichen eHDSI-Kennzahlen werden als unkritisch eingestuft.

Vor allem die kritischen eHDSI-Kennzahlen MÜSSEN auf eine Weise im NCPeH-FD verarbeitet werden, welche keine Rückschlüsse auf personenbezogene Informationen in den zur Verfügung gestellten Daten zulässt.

Der NCPeH-FD MUSS jede eHDSI-Kennzahl nach folgendem Schema zugänglich machen:

- für unkritische eHDSI-Kennzahl: unmittelbar nach der Erhebung,
- für kritische eHDSI-Kennzahl: je nach Implementation entweder unmittelbar nach der Erhebung oder via eines anonymisierten Dateixports am Ende des vorgegebenen Berichtsintervalls.

Das Berichtsintervall für die eHDSI-Kennzahlen sind unter Kapitel 2, Tabelle 1, Spalte "Frequency" des [eHDSI_Monitoring_Framework] zu finden.

Die Erhebung von kritischen Kennzahlen muss innerhalb der VAU erfolgen. Für die konkrete Verarbeitung von kritischen Kennzahlen kommen zwei Ansätze in Frage:

1. Unmittelbares Herausschreiben der eHDSI-Kennzahl mit speziellen Maßnahmen,
2. Sammeln der Daten zur eHDSI-Kennzahl in der VAU und Export am Ende des Berichtsintervalls nach außen.

Für jeden Ansatz wird ein Implementierungsbeispiel grob skizziert:

1. Unmittelbares Herausschreiben

Da bei kritischen eHDSI-Kennzahlen eine Erhebung und Verarbeitung von personenbezogenen Daten - hier der Identifier des Versicherten, also die KVNR - unumgänglich ist, müssen spezielle Maßnahmen umgesetzt werden. Mit Hilfe dieser Maßnahmen muss es dem Betreiber des NCPeH-FD ermöglicht werden, die eHDSI-Kennzahl im eigenen Monitoringsystem auszuwerten und im Berichtszeitraum für das Reporting an die eHDSI zu ermitteln.

Diese Maßnahmen umfassen die starke Pseudonymisierung des identifizierenden Merkmals, der KVNR, sodass ohne Kenntnis des Pseudonymisierungsgeheimnisses, kein Rückschluss auf den Originalwert stattfinden kann. Dafür soll ein sicheres Pseudonymisierungsgeheimnis genutzt werden, welche nach jedem Berichtsintervall (quartalsweise) vollständig erneuert wird. Damit wird verhindert, dass die Pseudonyme über Quartalsgrenzen im Monitoring verfolgt werden können und eine Profilbildung stattfindet.

Als Beispiel wird eine KVNR mit einem 256-bit Pseudonymisierungsgeheimnis mittels SHA256-Algorithmus state-of-the-art pseudonymisiert. Der Hashwert und entsprechende eHDSI-Kennzahl werden herausgeschrieben und der Datensatz im Monitoringsystem des Betreibers zur Laufzeit hinterlegt. Dem Betreiber ist es nun auch während des Berichtszeitraumes möglich, Auswertungen über diese Kennzahl inmitten des Berichtsintervalls durchzuführen. Zur Erstellung des eHDSI-Kennzahlreports ist es dem Betreiber ebenso möglich, diese eHDSI-Kennzahlen mit dem Verlauf über dem Berichtsintervall darzustellen.

Die Problematik dieses Ansatzes besteht in der sicheren Erzeugung und Wiedererzeugung des Pseudonymisierungsgeheimnisses und der Anwendung von starken State-of-the-Art Hashingalgorithmen zur Laufzeit im NCPeH-FD. Dieser Prozess bindet Verarbeitungsressourcen zur Laufzeit für die Generation des Hashes.

2. Sammeln der Daten und Export

In der VAU können personenbezogene Daten nachgehalten und diese in Form einer Datenstruktur für die Datensammlung im Berichtszeitraum weitergenutzt werden. Am Ende eines Berichtsintervalls wird dann pro kritische eHDSI-Kennzahl ein Dateixport

angelegt, welcher die Informationen in anonymisierter Form enthält und diese Informationen für den Betreiber zugänglich macht.

Am Beispiel: KPI-1.12 "Number of citizens who have used the Patient Summary service" wird folgende beispielhafte Datenstruktur in der VAU gehalten:

Tabelle 24: TAB_NCPeH_VAU-Datenstruktur_zu_kritischer_KPI-1.12

KVNR	Anzahl an Transaktionen
1234567890	8
0987654321	3
0987654300	1

Anstatt der KVNR kann auch ein pseudonymer Wert, basierend auf der KVNR, genutzt werden, bspw. mithilfe eines Hashings, jedoch muss weiterhin eine direkte Zuordenbarkeit innerhalb des Berichtszeitraumes für subsequente Anfragen des Versicherten gewährleistet sein.

Am Ende des Berichtszeitraumes wird eine anonymisierte Datei daraus erzeugt und aus der VAU exportiert, welche folgenden beispielhaften Inhalt hat:

Tabelle 25: TAB_NCPeH_Berichtsdatenstruktur_zu_kritischer_KPI-1.12

ID	Count
1	8
2	3
3	1

Als Problematik wird hier das Verhalten über mehrere Laufzeiten hinweg angesehen. Die gespeicherten Daten müssen auch nach einem Neustart/Update der Applikation im Berichtszeitraum zur Verfügung stehen und damit statisch nachgehalten werden. Es werden dadurch in erster Linie Ressourcen zur Verarbeitung und Speicherung gebunden. Zusätzlich zum Exportzeitpunkt auch noch weitere Ressourcen für den Export und das Bereinigen der Datenstrukturen.

Sowohl das Exportprozedere, als auch die Speicherung der Daten muss zum jeweiligen Zeitpunkt den höchsten Sicherheitsanforderungen entsprechen und fehlerfrei funktionieren.

Darüber hinaus stehen die Werte von kritischen eHDSI-Kennzahlen nur einmal im Quartal gesammelt zur Verfügung, sodass es nur vier definierte Datenpunkte pro Jahr geben kann und weitere Rückschlüsse auf Nutzungsverhalten unterbunden sind.

Der Betreiber des NCPeH-FD MUSS eHDSI-Kennzahlen im vorgeschriebenen Intervall und Format an die eHDSI und die gematik liefern. Dabei sind die unterschiedlichen Anlieferwege zu beachten.

Folgende Tabelle listet alle derzeit relevanten eHDSI-Kennzahlen nach [eHDSI Monitoring Framework] auf, die für den implementierten NCPeH geliefert werden müssen:

Tabelle 26: TAB_NCPeH_eHDSI-Kennzahlen

KPI-ID	Beschreibung	Erfassungszeitraum	Referenz
KPI-1.2	Anzahl der Transaktionen zwischen EU-Mitgliedsstaaten	Quartalsweise	Table 2
KPI-1.5	Anzahl der ausgetauschten Patient Summaries	Quartalsweise	Table 5
KPI-1.12	Anzahl der Bürger, die den Patient Summary Service genutzt haben	Quartalsweise	Table 15
KPI-3.3	NCPeH Verfügbarkeit	Quartalsweise	Table 20
KPI-3.4	NCPeH Zeiträume der Nichtverfügbarkeit	Quartalsweise	Table 21

Bei Erweiterung des NCPeH mit zusätzlichen Anwendungsfällen (bspw. ePrescription/Land-B-Szenario) oder bei Aktualisierung der eHDSI-Dokumente folgt "Tabelle 12: eHDSI-Kennzahlen" der normativen eHDSI-Spezifikation und wird entsprechend der dann geltenden eHDSI-Kennzahlen an die geltende Normative angepasst.

4.4.5 Logging

Das Logging ist ebenfalls als Teil des Event-Managements gemäß [ITILv4] anzusehen. Es umfasst die kontinuierliche Aufnahme und Analyse von Informationen rund um vordefinierte Ereignisse (Logeinträge), jedoch mit dem Fokus auf der Nachhaltung von Einträgen aus bestimmten Quellen. Vom NCPeH-FD erzeugte Applikationslogs oder von der VAU ausgegebene Informationen werden hier konkret gesammelt und können dadurch jedoch erst nachgelagert ausgewertet und analysiert werden. Das Logging dient hauptsächlich zur Fehlersuche und dem Nachvollziehen von internen Prozessen des NCPeH-FD, ohne personenbezogene Daten preiszugeben.

Alle erfassten Daten zum Logging MÜSSEN mindestens 90 Tage lang vollständig aufbewahrt werden, um eine nachfolgende Fehlersuche und Tracing zu ermöglichen.

Alle aufgetretenen Fehlermeldungen müssen nach den Vorgaben der eHDSI mit den entsprechenden Codes in das Logging aufgenommen werden. Eine tabellarische Auflistung von Fehlerzuständen und eindeutigen Identifikationsmerkmalen findet sich in Kapitel 6.4 "eHealth DSI Error Codes" [eHDSI_NCPeH_Components] in den Tabellen 1-4. Darüber hinaus sind auch weitere Vorgaben aus spezielleren Transaktionsprofilen einzuhalten. Dazu vor allem die IHE-Profile der eHDSI.

4.4.6 Betriebshandbuch

Das Betriebshandbuch dient zur Dokumentation von operationalisiertem Wissen im Rahmen der Betriebstätigkeiten um den NCPeH-FD. Es ermöglicht einen Wissensaustausch und erleichtert die Abbildung vorhandener Prozesse in lesbarer und

verständlicher Form. Die Erstellung und Pflege eines Betriebshandbuches geschieht vorrangig digital und gehört zu den anzufertigenden Dokumentationen des Anbieters.

Da der NCPeH-FD als gegebene Besonderheit sowohl im deutschen, als auch übergreifend im europäischen (und damit englischen) Sprachraum agiert, wird zusätzlich zur Festlegung GS-A_5343 in [gemRL_Betr_TI#2.2.1 Auszüge aus dem Betriebshandbuch der TI-ITSM-Teilnehmer] in Verbindung mit GS-A_4090, eine Erweiterung der Sprachregelung von zu liefernden Dokumentationen in [gemRL_Betr_TI#2.1.2 Kommunikation] mit A_24012 spezifiziert.

4.4.7 Verwaltung von Einträgen im Verzeichnisdienst FHIR

Um Berechtigungen zum Abruf bzw. der Nutzung des NCPeHs als Versicherter hinterlegen zu können, werden zwingend aktuelle Informationen im Verzeichnisdienst FHIR benötigt. Diese Informationen setzen sich sowohl aus dem Angebot des in Betrieb befindlichen NCPeH-FD, als auch aus den von ihm verwalteten SM-B Zertifikaten zusammen.

A_27240 - NCPeH-Fachdienst - Management der Einträge im Verzeichnisdienst FHIR

Der Anbieter NCPeH-Fachdienst MUSS Einträge im Verzeichnisdienst FHIR stets aktuell halten. Werden beispielsweise geänderte Dienste für ein europäisches Mitgliedsland angeboten, so sind die Änderungsaufträge der entsprechenden Einträge selbstständig zu beauftragen. Dabei ist zu gewährleisten, dass für jedes angebotene EU-Land ein gültiges ENC-Zertifikat im Verzeichnisdienst hinterlegt ist. [≤]

Hinweis: Das Management von Einträgen im Verzeichnisdienst FHIR kann im Moment über Service-Requests des Anbieters zentrale Dienste gestellt werden. Die gematik stellt dem Anbieter des NCPeH-FD den nötigen Servicekatalogeintrag zur Verfügung.

Weitere Informationen zum Verzeichnisdienst / Verzeichnisdienst FHIR finden sich hier: [<https://github.com/gematik/api-vzd/>]

4.5 Test des NCPeH-FD

Zum Test des NCPeH-FD werden hier im engeren Sinne die technischen Aktivitäten zur Prüfung der Funktionalität der Anwendungsszenarien "Patient Summary Land-A", "ePrescription/eDispensation Land-A" und die Integration des NCPeH-FD in die Telematikinfrastruktur betrachtet.

Themen zum Compliance Check und dem zugehörigen Self-Assessments werden von der eHDSI vorgegeben und beschrieben, siehe dazu [eHDSI Compliance Check Framework] und [eHDSI Compliance Check Services].

Zur Sicherung der Funktionalität, Interoperabilität und Nutzbarkeit der Anwendungsszenarien "Patient Summary Land-A" und "ePrescription/eDispensation Land-A" ergeben sich für den Test verschiedenste Aufgaben. Allgemein lassen sich diese aber in folgende Abschnitte aufteilen:

1. Test der Anwendung während der Entwicklung in der eigenen Entwicklungsumgebung mit Integration in die Testumgebung RU der Telematikinfrastruktur.
2. Abnahmetest des NCPeH-FD zum Nachweis der Interoperabilität mit der TI durch die gematik mit Integration in die Testumgebung TU, Unterstützung bei Zulassungstests anderer am Anwendungsverlauf beteiligter TI-Produkte (ePA FdVs, ePA-Aktensysteme, IDP-Dienst).
3. Tests der Anwendung mit Integration in die Umgebung der eHDSI.
4. Test der Anwendung in der Produktivumgebung (PU).

4.5.1 Durchführung eigenverantwortliche Tests des Herstellers bzw. Betreibers

Der Hersteller bzw. Anbieter des NCPeH-FD MUSS eigenverantwortliche Tests ("EvT") des NCPeH-FD durchführen. Dabei wird davon ausgegangen, dass sich Hersteller und Anbieter untereinander abstimmen, wer für die Durchführung der verschiedenen Testarten verantwortlich ist.

Für die Durchführung der EvTs gilt als Grundlage [[gemKpt_Test#2.4.1 Eigenverantwortlicher Test](#)]. Abweichend von den dortigen Vorgaben erfolgt eine Prüfung der EvTs nicht über die Bereitstellung von Testprotokollen und Testberichten, sondern über einer Vorführung, bei dem der gematik die wichtigsten Ergebnisse der Tests in einem Vor-Ort-Termin präsentiert und Funktionalitäten vorgeführt werden. Der Umfang und Fokus der Vorführung wird vorab mit der gematik abgestimmt. Das mit der gematik abgestimmte Protokoll der Vorführung wird als Dokumentation des EvT von der gematik aufgenommen.

Ergänzend zu den Festlegungen von [[gemKpt_Test#2.4.1 Eigenverantwortlicher Test](#)] KANN der Produkttest als Teil des EvT ohne weitere Abstimmung mit dem Testmanager mit Simulatoren in einer eigenen Testumgebung durchgeführt werden (ohne Anbindung an die RU). Damit soll insbesondere die Durchführung von negativen Tests erleichtert werden. Es gilt jedoch weiterhin, dass der produktübergreifende Test als Teil des EvT gemäß [gemKpt_Test] in der RU integriert durchgeführt werden muss.

4.5.2 Bereitstellung von Testobjekten des NCPeH-FD in der TI

Im Rahmen der Entwicklung der Anwendungsszenarien PS-A und ePeD-A sind integrative Tests mit den daran beteiligten Produkten der TI (NCPeH-FD, ePA FdV, ePA-Aktensystem, E-Rezept-FdV, E-Rezept-Fachdienst, IDP-Dienst und zentrale Produkte der TI) durchzuführen. Dies erfolgt zum einen entwicklungsbegleitend in der Umgebung RU und zum anderen zu Abnahme- bzw. Zulassungszwecken in der TU (siehe [gemKpt_Test]).

Der Anbieter des NCPeH-FD MUSS jeweils ein Testobjekt NCPeH-FD in den Umgebungen RU und TU bereitstellen. Er MUSS eigene integrative Tests mit Produkten der TI in der RU durchführen. Der Anbieter MUSS anderen Herstellern bzw. Betreibern von beteiligten TI-Produkten die Durchführung integrativer Tests in der RU und der gematik die Durchführung von Zulassungs- bzw. Abnahmetests in der TU ermöglichen. Er MUSS der BfArM im Rahmen der Entwicklung und Pflege des MTCs die Durchführung von Tests ermöglichen. Er MUSS sich mit der gematik zur Durchführung gemeinsamer, integrativer Tests (Connectathon) abstimmen, um die Verfügbarkeit der zu integrierenden Produkte und die Teilnahme der Hersteller dieser Produkte sicherzustellen.

Der Anbieter des NCPeH-FD MUSS der gematik Abnahmetests zur Prüfung der korrekten Integration in die TI - insbesondere der Anwendungen ePA und E-Rezept - ermöglichen. Die Durchführung dieser Tests sind gemeinsam zu koordinieren.

Für die Bereitstellung der Produkte in den beiden Umgebungen gilt [[gemKpt_Test#3 Systemumgebungen](#)]. Die konkret umzusetzenden Anforderungen sind im [gemProdT_NCPeH_FD] aufgeführt.

4.5.3 Testspezifische Funktionen im NCPeH-FD

4.5.3.1 Tracing mit ePA-Aktensystemen in Nichtproduktivumgebungen

Für die Fehlersuche in Nichtproduktivumgebungen -- insbesondere bei IOP-Problemen zwischen Produkten verschiedener Hersteller in einer fortgeschrittenen Entwicklungsphase -- hat es sich als notwendig erwiesen, dass der Klartext der

Kommunikation zwischen ePA-Client und VAU-Instanz eines ePA-Aktensystems lesbar sein muss.

Der NCPeH-FD MUSS die Vorgaben aus [[gemSpec_Krypt#7.7 Tracing in Nichtproduktivumgebungen](#)] als ePA-Client umsetzen.

Der NCPeH-FD MUSS sicherstellen, dass die Mechanismen für das Tracing mit dem ePA-Aktensystem gemäß [gemSpec_Krypt#A_24477*] in der Produktivumgebung nicht zum Einsatz kommen und dass der VAU-Kanal im Produktivsystem entsprechend Vorgaben aus [[gemSpec_Krypt#Transport und Sicherung von Nutzdaten](#)] als produktiv gekennzeichnet werden.

Die umzusetzenden Anforderungen sind in [gemProdT_NCPeH_FD] aufgeführt.

Als weiterführende Information siehe auch [[gemSpec_Aktensystem_ePAfueralle#3.19.4 Tracing in Nichtproduktivumgebungen](#)].

4.5.4 Automatisiertes Auslösen von NCPeH-Anwendungsfällen für Tests in der TI

Um anderen Herstellern, der BfArM als auch der gematik eine eigenständige und automatisierte Durchführung von integrativen Tests in den Umgebungen RU und TU zu ermöglichen, MUSS der Anbieter des NCPeH-FD eine Schnittstelle zum Auslösen von Anwendungsfällen in beiden Umgebungen bereitstellen (NCPeH-Testinterface). Das NCPeH-Testinterface MUSS die parallele Durchführung von Tests ermöglichen, um mehrere Nutzer parallel bedienen zu können.

Das NCPeH-Testinterface SOLL in Form einer Simulation eines NCPeH Land-B erfolgen, in der auch die eHDSI-Schnittstellen zur Kommunikation mit dem NCPeH-FD genutzt werden. In den nachfolgenden schematischen Darstellungen der Testaufbauten wird sie als Simulation des NCPeH Land-B dargestellt.

Der Zugang zum NCPeH-Testinterface MUSS mittels Gateway über das Internet ermöglicht werden. Das NCPeH-Testinterface SOLL über TLS mit beidseitiger Authentifizierung abgesichert werden.

Die konkrete technische Beschreibung der Triggerschnittstelle [gemTestTriggerNCPeH] wird in GitHub bereitgestellt.

4.5.4.1 Daten für das automatisierte Auslösen von Anwendungsfällen

Das NCPeH-Testinterface nutzt für einige Eingabeparameter Objekte, an die zu definierende Datenprofile gekoppelt sind (EuCountryCode, IdAssertionProfile/ProfileName, TRCAssertionProfile/ProfileName, DispenseProfile, PatientProfile).

Ein Datenprofil fungiert einerseits wie ein Template, in dem die Daten hinterlegt sind, die für die Kommunikation über die eHDSI-Schnittstelle verwendet werden sollen, so dass diese nicht alle über das NCPeH-Testinterface bereitgestellt werden müssen. Damit soll auch die Komplexität der Schnittstelle reduziert werden. Andererseits definiert es auch Daten, die in die Kommunikation mit dem NCPeH-FD eingehen. Am wichtigsten ist hier die Referenz auf die zu verwendende Zertifikate.

Datenprofile, die von der gematik oder Herstellern beteiligter TI-Produkte benötigt werden, MÜSSEN im Rahmen der Bereitstellung der Schnittstelle zwischen dem Betreiber des NCPeH-Testinterface und der gematik abgestimmt werden. Die gemeinsam definierten Datenprofile MÜSSEN mit dem NCPeH-Testinterface zur Nutzung bereitgestellt werden. Es MUSS möglich sein, Datenprofile hinzuzufügen, zu ändern oder zu löschen.

Das Objekt EuCountryCode referenziert folgendes Datenprofil:

- Das TLS-Zertifikat, das für die Kommunikation mit dem NCPeH-FD genutzt werden soll.
- Die HomeCommunityId, die in dem Profil per Default für den NCPeH Land-B genutzt werden soll.

Das Objekt IdAssertionProfile referenziert folgendes Datenprofil:

- Das Signatur-Zertifikat, das zum Signieren der IdA-Assertion zum Einsatz kommen soll.
- Der Wert, der im SAML-Element Assertion/Subject/NameID einzutragen ist (Identifizier des LE-EU) als auch das Format des Wertes (Attribut @Format).
- Die Werte, die in dem Profil per Default in den Attributen der Struktur AttributeStatement einzutragen oder wegzulassen sind:
 - urn:oasis:names:tc:xspa:1.0:subject:subject-id,
 - urn:oasis:names:tc:xacml:2.0:subject:role,
 - urn:ehdsi:names:subject:clinical-speciality,
 - urn:ehdsi:names:subject:on-behalf-of,
 - urn:oasis:names:tc:xspa:1.0:subject:organization,
 - urn:oasis:names:tc:xspa:1.0:subject:organization-id,
 - urn:ehdsi:names:subject:healthcare-facility-type,
 - urn:oasis:names:tc:xspa:1.0:environment:locality,
 - urn:oasis:names:tc:xspa:1.0:subject:hl7:permission.

Das Objekt TRCAssertionProfile referenziert folgendes Datenprofil:

- Das Signatur-Zertifikat, das zum Signieren der TRC Assertion zum Einsatz kommen soll.
- Der Wert, der im SAML-Element Assertion/Subject/NameID einzutragen ist (Identifizier des LE-EU) als auch das Format des Wertes (Attribut @Format).

Das DispenseProfile wird definiert, da für den Test der Dispensierung ein oder mehrere Dokumente im eHDSI CDA-Pivotformat generiert werden müssen, die aus einem Land-B stammen. Die Erstellung dieser Dokumente MUSS der Land-B Simulator durchführen, bei denen die angegebenen DispenseProfile und den weiteren übergebenen Parametern zugrunde liegen.

Das Objekt DispenseProfile definiert benötigte Datenanteile für ein Dispense-Dokument nach [eHDSI_CDA_Format]:

- Medicinal Product Identifier,
- Medicinal Product Brand Name,
- Medicinal Product Classification,
- Medicinal Product Package Data,
- Active Ingredients Data,
- Marketing Authorization Holder,
- Falls nötig und in gemeinsamer Abstimmung, weitere benötigte medizinische Daten zur Dispensierung.

Mit der KVNR wird für die Generierung von Dispensier-Dokumenten zukünftig auch ein PatientProfile referenziert. Neben der KVNR selbst werden dafür folgende weitere Daten benötigt:

- Insurance Number,
- Given Name,
- Family Name,
- Gender.

Das NCPeH-Testinterface gibt als Response auf die REST-Requests die Inhalte der Nachrichten von der eHDSI-Schnittstelle zurück (siehe [gemTestTriggerNCPeH]). Also den jeweiligen IHE-Request und die IHE-Responses, die mit dem NCPeH-FD ausgetauscht wurden. Beides wird jeweils aufgeteilt in die HTTP-Request bzw. HTTP-Response-Zeile, den http-Header und den http-Body, jeweils Base64-kodiert. Damit soll dem aufrufenden Testfall die Möglichkeit gegeben werden, die Reaktion des NCPeH-FD direkt zu prüfen und zu bewerten.

4.5.5 Testdurchführung nach Vorgaben der eHDSI

Die eHDSI beschreibt in [eHDSI Test Services], insbesondere im [eHDSI Test Framework] ihre Anforderungen und das Vorgehen für den Test der verschiedenen Anwendungsszenarien. Die dort definierten Testphasen "Formal / Upgrade Pre-Production Test" (PPT) und "Produktion Environment Test" (PET), sind verpflichtend. Der Anbieter MUSS an diesen Testphasen teilnehmen und die Vorgaben aus dem [eHDSI Test Framework] umsetzen. Verantwortlich für Organisation und Teilnahme an den eHDSI Testevents ist der deutsche Anbieter des NCPeH.

Der Anbieter des NCPeH-FD SOLL frühzeitig Tests mit einem europäischen Partner durchführen, um die beidseitige Interoperabilität der NCPeHs zu prüfen. Der Anbieter SOLL zusätzlich an den Testphasen Connectivity Testing und Preparatory Pre-Production Testing (Pre-PPT) teilnehmen.

Zur Teilnahme an den Testphasen PPT und Pre-PPT MUSS es mindestens eine rechtzeitige Abstimmung mit der gematik geben (mind. 12 Wochen vor Beginn der Testphase). Über die gematik muss hierbei die zeitliche Verfügbarkeit der benötigten Produkte der TI in einer der Umgebungen RU oder TU sichergestellt werden (z. B. zum Ausschluss von eventuellen Wartungsphasen von Fachdiensten in der TI). Es ist außerdem zu klären, welche Unterstützung seitens der gematik im Verlauf der Testdurchführung benötigt werden.

4.5.6 Schematischer Testaufbau

In den folgenden Kapiteln wird informativ der geplante bzw. mögliche Aufbau der Testumgebungen für die verschiedenen Testphasen dargestellt. Abweichungen können auftreten und sind zwischen Anbieter und der gematik im Rahmen der Entwicklung abzustimmen.

4.5.6.1 Testaufbau für integrative Tests in der Telematikinfrastruktur

Der integrative Test des NCPeH-FD mit Produkten der TI (ePA FdV, ePA-AS, E-Rezept-FdV, E-Rezept-Fachdienst, IDP-Dienst und zentrale Produkte der TI) erfordert eine unabhängige Testdurchführung, da verschiedene Produkthersteller, das BfArM und die gematik Bedarf an einer eigenen Qualitätssicherung haben. Da in dieser Entwicklungsphase die Tests noch auf das deutsche Umfeld beschränkt sind, muss es eine Möglichkeit geben, die verschiedenen Anwendungsfälle der Szenarien automatisiert anzustoßen, die die integrativen Aktivitäten mit den Produkten der TI auslösen. Dies sind die Anwendungsfälle, die eine Interaktion mit den Produkten der TI bewirken. Um den verschiedenen testdurchführenden Instanzen diese Testmöglichkeit zu bieten, wurde

das NCPeH-Testinterface in [[4.5.4 Automatisiertes Auslösen von NCPeH-Anwendungsfällen für Tests in der TI](#)] definiert.

Der mögliche Aufbau der Testumgebung für den Anbieter des NCPeH-FD in der RU wird in der folgenden Grafik schematisch dargestellt. Je nach testdurchführender Instanz kann die Zuordnung zu den herstellereigenen Umgebungsanteilen variieren.

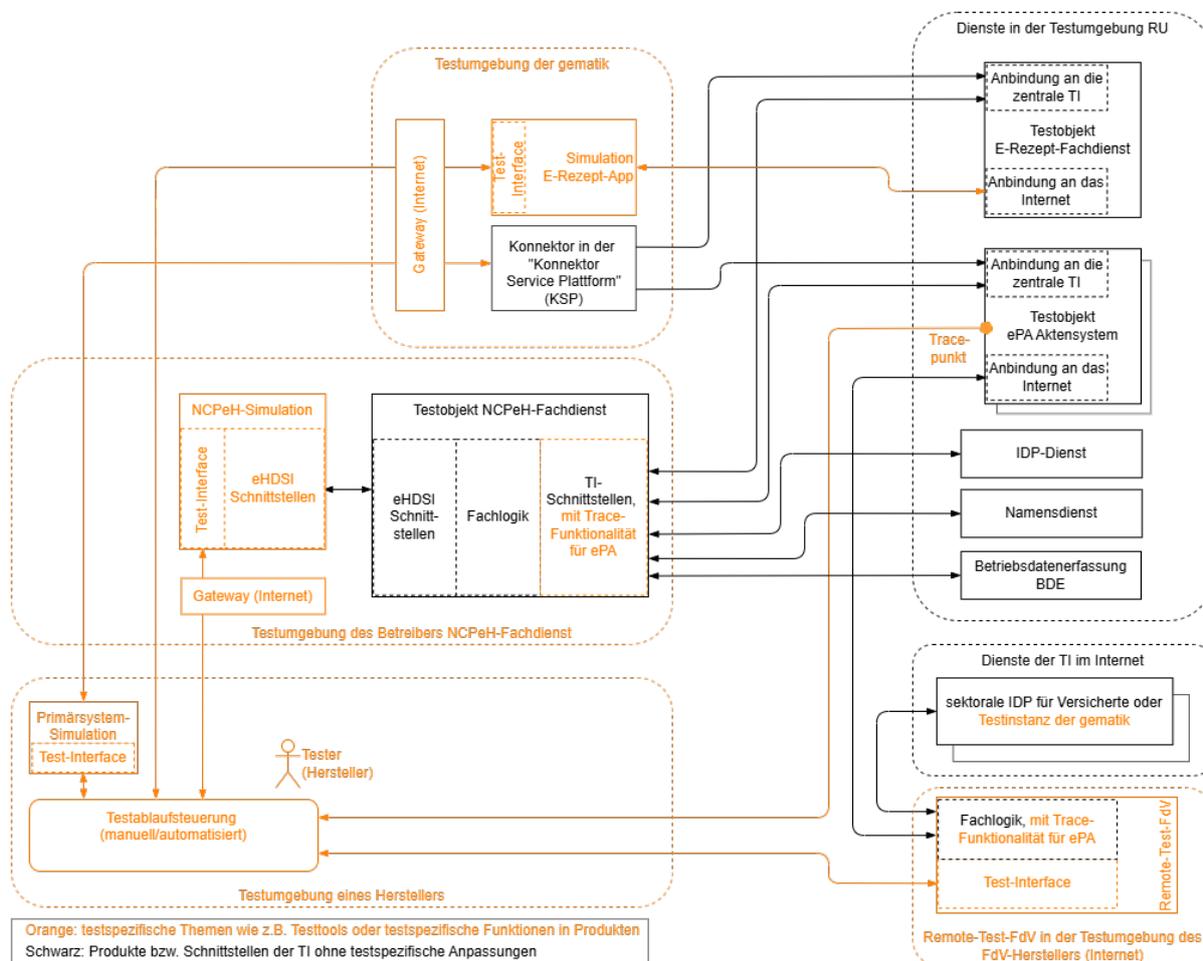


Abbildung 4: Schematischer Testaufbau für den integrativen Test des NCPeH-FD mit der Telematikinfrastruktur

Die Simulation der E-Rezept-App und die Primärsystemsimulation werden zusammen mit der Konnektor Service Plattform KSP von der gematik bereitgestellt. Dies soll vor allem die Möglichkeit bieten, in einem testvorbereitenden Schritt jeweils ein spezifisches, zum Testfall passende Dokumente im relevanten Fachdienst der TI einzustellen (automatisiertes Testdatenmanagement für Testdokumente und Berechtigungsmanagement).

Verschiedene Test-FdVs müssen für die Berechtigung des NCPeH-FD in ePA-Aktensystemen bzw. dem E-Rezept-Fachdienst zum Einsatz kommen. Wenn die Mechanismen zur Berechtigung des NCPeH-FD in den Anwendungen ePA und E-Rezept einsatzbereit sind, wird damit eine NCPeH-FD-Identität mit Repräsentation eines EU-Landes berechtigt. Vor diesem Zeitpunkt kann mit einer deutschen LE-Identität anstelle einer NCPeH-FD-Identität getestet werden. Das Test-FdV wird nach [[gemKpt_Test#9.1 Bereitstellung von Remote-Test-FdVs](#)] von den Herstellern der FdVs bereitgestellt.

Die ePA-Aktensysteme müssen in den Umgebungen RU und TU einen Sensorpunkt zum Aufzeichnen der TLS-entschlüsselten Kommunikation mit den ePA-Clients bereitstellen. Der Sensorpunkt ist über das Access Gateway des ePA-Aktensystems nach [[gemSpec_Aktensystem_ePAfueralle#3.19.4 Tracing in Nichtproduktivumgebungen](#)] erreichbar. Das von der gematik zur externen Nutzung bereitgestellte Tool [gemTigerProxy] kann mit Hilfe der Vorgaben aus [gemSpec_Krypt] und dem Sensorpunkt die VAU-Kommunikation entschlüsseln (siehe auch [[4.5.3.1 Tracing mit ePA-Aktensystemen in Nichtproduktivumgebungen](#)]). Auf diese Weise wird eine Überprüfbarkeit der VAU-verschlüsselten Kommunikation eines ePA-Clients mit einer VAU-Instanz eines ePA Aktensystems ermöglicht.

Ein ähnlicher Aufbau ergibt sich für die Hersteller der ePA- und E-Rezept-Produkte und bei Bedarf für die BfArM in der RU. Abweichungen können hier je nach Nutzer im (Nicht-)Bedarf eines Konnektors oder eines FdVs zum Dokumenten- und Berechtigungsmanagement auftreten.

Abweichend von der schematischen Darstellung erfolgt der Testaufbau für den Test durch die gematik in der TU.

4.5.6.2 Testaufbau für den (Pre-)PPT

In den eHDSI-Testphasen Pre-PPT und PPT liegt der Testfokus auf der Interoperabilität der eHDSI-Schnittstellen, der Konformität der Dokumente Patient Summary, ePrescription/eDispensation und der Usability des Gesamtablaufs aus Sicht des europäischen LE. Der PPT ist dabei Bestandteil des Zulassungsverfahrens der EU. Die Forderung der eHDSI nach verschiedenen, realitätsnahen Dokumenten macht es wiederum notwendig, unterschiedliche ePKA-Dokumente im ePA-Aktensystem und verschiedene E-Rezepte im E-Rezept-Fachdienst bereitstellen zu können. Hierfür sollen Komponenten aus dem Testaufbau wiederverwendet werden (Dokument oder E-Rezept einstellen via Primärsystemsimulation und KSP).

Da der zeitliche Rahmen für die Entwicklung der Produkte der TI und die zeitliche Organisation der Testphasen in der EU nicht leicht in Übereinstimmung zu bringen sind, muss für die Durchführung des PPT eine Entscheidung über die zu nutzende Umgebung in Abstimmung mit der gematik getroffen werden. Die Herausforderungen zur Festlegung einer Umgebung werden vor allem auf die Neu-Entwicklung von EU-Szenarien zutreffen. Ziel ist es, den PPT möglichst nicht auf Produktinstanzen der RU durchzuführen, die zur Weiterentwicklung der jeweiligen Produkte genutzt werden ("RU-Dev"). Ein Prep-PPT oder PPT DARF jedoch NICHT in der PU durchgeführt werden.

Die Sicherstellung der Verfügbarkeit der TI-Produkte erfolgt über die in [[4.5.5 Testdurchführung nach Vorgaben der eHDSI](#)] geforderte Abstimmung mit der gematik. Je nach Absprache und Vorbereitung kann hier auch eine Unterstützungsleistung durch die gematik notwendig werden.

4.5.6.3 Testaufbau für den PET

Das [eHDSI Test Framework] definiert eine Durchführung von Tests in der Produktivumgebung nach Erteilung der Betriebserlaubnis (Product Environment Test - PET). Diese Tests MÜSSEN im Rahmen der Inbetriebnahme eines neuen Anwendungsszenarios bzw. des Upgrades auf eine neue eHDSI Releaseversion ("Wave") erfolgen. Dementsprechend muss produktübergreifend eine Möglichkeit geschaffen werden, diese Tests mit der Produktivumgebung der TI durchzuführen.

In Vorbereitung des PET MUSS sich die DVKA Versichertenidentitäten zu Prüfzwecken mit zugehörigen Konten in den ePA-Aktensystemen beschaffen. Dazu können eGK Prüfkarten für die Rolle und Identität eines Prüfversicherten über den gematik WEB-Shop [gemWebShop] bestellt werden. In [[gemSpec_Aktensystem_ePAfueralle#2.4 Validierungskonto](#)] werden Festlegungen getroffen, um Validierungskonten mit Hilfe der

KVNR der eGK Prüfkarten erstellen lassen zu können. Diese eGK Prüfkarten sind auch für die Durchführung von PETs mit E-Rezepten und dem produktiven E-Rezept-FdV zu nutzen.

Die DVKA MUSS sich um LE-DE (Ärzte oder Zahnärzte) kümmern, um für den PET realitätsnahe ePKA-Dokumente in den Validierungskonten eines ePA-Aktensystems und realitätsnahe E-Rezepte in den E-Rezept-Fachdienst einstellen zu können. Das Einstellen der ePKA-Dokumente und E-Rezepte erfolgt dabei in der Umgebung des jeweiligen LE-DE.

Die Erteilung der Zugriffsbefugnis des NCPeH-FD auf das ePKA-Dokument der Prüfidentität kann mittels ePA-FdV einer Krankenversicherung erfolgen, für die der Betreiber eines ePA-Aktensystems die Prüfidentität bereitstellt. Die Erteilung der Zugriffsberechtigung des NCPeH-FD auf E-Rezepte der Prüfidentität kann mittels gematik E-Rezept-App erfolgen.

Da die eHDSI im [eHDSI Test Framework] auch festlegt, dass im PET Nachweise zu durchgeführten Anpassungen bzw. zur Erfüllung von Auflagen erbracht werden können bzw. sollen, ist - je nach konkreter Situation - mit umfangreicheren Testaktivitäten und Bedarf an ePKA-Testdokumenten oder E-Rezepten zu rechnen. Demzufolge sollten friendly User LE-DE mit verschiedenen Primärsystemen und Konnektoren zum Einsatz kommen können, um unterschiedlich erzeugte ePKA-Dokumente oder E-Rezepte bereitzustellen. Je nach Situation kann dabei die Bereitstellung von Dokumenten vorbereitend erfolgen oder sie muss zum Zeitpunkt der Testdurchführung erfolgen.

Die Testdurchführung ist mit dem Betrieb der gematik abzustimmen. Insbesondere die Sicherstellung der Verfügbarkeit der TI Produkte und passenden Produktversionen ist hier relevant.

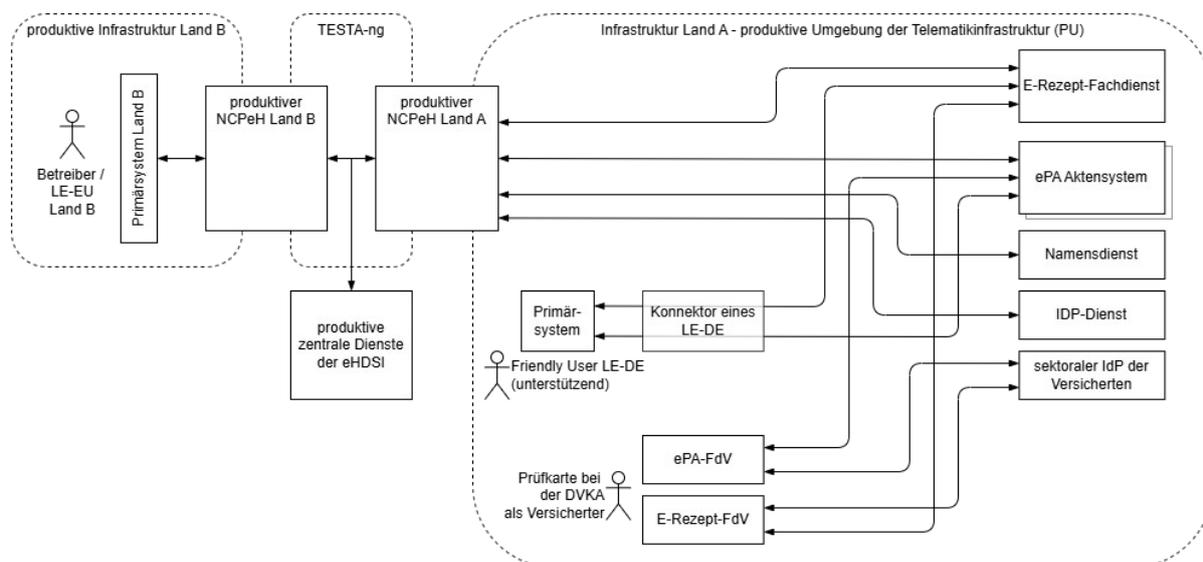


Abbildung 5: Schematischer Aufbau für den Produktivtest des NCPeH-FD mit der eHDSI

5 Fachliche Anwendungsfälle

5.1 Anwendungsfälle für Patient Summary Land-A

5.1.1 NCPeH.UC_1 - Versicherten im Behandlungsland für PS-A identifizieren

AF_10107-01 - Versicherten im Behandlungsland für PS-A identifizieren

Mit diesem Anwendungsfall kann der LE-EU die notwendigen demographischen Versichertendaten abrufen, um den Versicherten Vorort im Behandlungsland identifizieren zu können. Für den Abruf von demographischen Versichertendaten MUSS der NCPeH-FD die Schnittstelle [6.1.1- Operation Cross_Gateway_Patient_Discovery::RespondingGateway_PRPA_IN201305UV02] gemäß [eHDSI_XCPD_Profile] bereitstellen. Diese wird von NCPeH anderer Mitgliedsstaaten (Land-B) verwendet. Die initiale Anfrage enthält neben der Identität des LE-EU auch die technische Versichertenkennung (KVNR) und den Zugriffscode auf das ePKA MIO des Versicherten.

Nach erfolgreicher technischer Ermittlung des ePKA-Kontos des Versicherten unter Verwendung der KVNR und des Zugriffscode werden anhand der TI-Identität (Repräsentation des NCPeH Land-B in der TI) die demographischen Versichertendaten aus dem ePKA-Konto abgerufen. Die Bedingung für den erfolgreichen Zugriff des anfragenden NCPeH Land-B auf die demographischen Versichertendaten ist eine Zugriffsfreigabe durch den Versicherten.

Der Versicherte erteilt für das Land-B die Zugriffsberechtigung bereits vor der eigentlichen Anfrage der LE-EU mittels seines ePA FdV. Mit der Zugriffsberechtigung wird ein Zugriffscode generiert. Die erteilte Zugriffsberechtigung inkl. Zugriffscode ist zeitlich auf eine Stunde begrenzt. Nach Ablauf der Zugriffsberechtigung wird auch der Zugriffscode automatisch ungültig. Dadurch können die LE-EU keinen weiteren Zugriff auf die ePKA-Daten des Versicherten erhalten. Erteilt der Versicherte erneut eine Zugriffsberechtigung für denselben EU-Mitgliedsstaat, wird auf dem FdV des Versicherten ein neuer Zugriffscode generiert, um den Missbrauch eines bereits abgelaufenen Zugriffscode zu verhindern.

Die Verifikation des Zugriffscode erfolgt durch das jeweilige ePA-Aktensystem bei der Suche nach und dem Zugriff auf das ePKA MIO des Versicherten. Bei erfolgreichem Abruf des ePKA MIO sendet der NCPeH-FD eine Antwort mit den demographischen Versichertendaten inkl. der KVNR an den anfordernden NCPeH Land-B. Mit den übermittelten Versichertendaten kann der LE-EU die Identifikation des Versicherten vollständig abschließen.

Tabelle 27: TAB_NCPeH_Versicherten_im_Behandlungsland_für_PS-A_identifizieren

	Versicherten im Behandlungsland für PS-A identifizieren
Akteur	NCPeH Land-B in der Rolle als eHDSI Service Consumer im Behandlungsland.

Auslöser	Ein behandelnder LE-EU (Land-B) möchte den Versicherten identifizieren und braucht dafür demographische Versichertendaten.
Aufgerufene Schnittstelle	[6.1.1- Operation <u>Cross_Gateway_Patient_Discovery::RespondingGateway_PRPA_IN201305UV02</u>]
Vorbedingung	<ul style="list-style-type: none"> • Der Anwendungsfall [5.3.2- NCPeH.UC_6 - Service Metadata auf eHDSI Configuration Service verwalten] ist erfolgreich durchgeführt worden. • Die Service Metadata des NCPeH Land-B sind erfolgreich im NCPeH-FD installiert. • Das private Schlüsselmaterial zum Aufbau von sicheren TLS-Verbindungen in der eHDSI ist im HSM erzeugt und gültig. • Im HSM ist eine gültige TI-Identität (privates Schlüsselmaterial) als Repräsentation des NCPeH Land-B vorhanden. • Der grenzüberschreitende Austausch von Versichertendaten mit einem Land-B ist nur nach Durchführung der Prüfung gemäß den Vorgaben aus [4.1.2- Datenaustausch mit zugelassenen EU-Ländern] zulässig.
Standardablauf	<ol style="list-style-type: none"> 1. [6.1.1.1- TUC_NCPeH_001: Patient Demographics Query Request für PS-A verarbeiten] 2. [6.2.1- TUC_NCPeH_013: Metadatenattribute des ePKA MIO abrufen] 3. [6.2.2- TUC_NCPeH_014: FHIR-Bundle ePKA MIO abrufen] 4. [6.2.3- TUC_NCPeH_017: Demographische Versichertendaten aus NFD des ePKA MIO übernehmen] 5. [6.1.1.2- TUC_NCPeH_002: Patient Demographics Response für PS-A versenden]
Nachbedingungen	<ul style="list-style-type: none"> • Die ermittelten demographischen Versichertendaten wurden an NCPeH Land-B übermittelt • Non-Repudiation of Origin und Non-Repudiation of Receipt gemäß [4.1.7.1- Non-Repudiation of Origin erstellen] und [4.1.7.2- Non-Repudiation of Receipt erstellen] wurden in dem Audit Repository gespeichert • Ein Audit Trail Eintrag gemäß [4.1.7.3- Patient Privacy Audit Trail Eintrag erstellen] wurde in der Komponente Audit Repository gespeichert. Bei der Erstellung des Audit Trail Eintrages MUSS der NCPeH-FD die Vorgaben aus [eHDSI_XCPD_Profile#3.3] umsetzen.

[<=]

5.1.2 NCPeH.UC_2 - Metadaten über ePKA MIO auflisten

AF_10121-01 - Metadaten über ePKA MIO auflisten

Der NCPeH-FD soll in diesem Anwendungsfall auf berechnete Anfrage des behandelnden LE-EU die Metadaten über das ePKA MIO des Versicherten bereitstellen können, um

nachfolgend medizinische relevante ePKA-Daten in einem entsprechenden Dokumentenformat (CDA oder CDA embedded PDF/A) adressieren und lesen zu können. Dafür stellt der NCPeH-FD innerhalb der eHDSI die Schnittstelle [6.1.2- Operation Cross_Gateway_Query::FindDocuments] gemäß [eHDSI_XCA_Profile#2] bereit. Die Anfrage vom NCPeH Land-B enthält neben der Identität des LE-EU, der KVNR des Versicherten auch die elektronische Zusicherung vom Behandlungsland (Land-B) über das Bestehen einer medizinischen Behandlung zwischen dem anfragenden LE-EU und dem Versicherten.

Die Ermittlung der relevanten Metadaten erfolgt durch eine Abfrage des NCPeH-FD am zuständigen ePA XDS Document Service, in dem die ePKA-Daten des Versicherten enthalten sind. Bedingung für die erfolgreiche Ermittlung von Metadaten des ePKA MIO ist eine Zugriffsfreigabe durch den Versicherten. Die Zugriffsfreigabe erteilt der Versicherte mittels seines ePA FdV. Der gesamte Ablauf endet mit der Sendung der Metadaten des ePKA MIO an den NCPeH Land-B.

Tabelle 28: TAB_NCPeH_Metadaten_des_ePKA_MIO_auflisten

AF_10121	Metadaten über ePKA MIO auflisten
Akteur	NCPeH Land-B in der Rolle als eHDSI Service Consumer im Behandlungsland.
Auslöser	Ein behandelnder LE-EU im Ausland (Land-B) ruft in seinem Primärsystem die Metadaten des ePKA MIO des Versicherten ab.
Aufgerufene Schnittstellen	[6.1.2- Operation Cross_Gateway_Query::FindDocuments]
Vorbedingung	<ul style="list-style-type: none"> • Der Anwendungsfall [5.3.2- NCPeH.UC_6 - Service Metadata auf eHDSI Configuration Service verwalten] ist erfolgreich durchgeführt worden • Die gültigen Service Metadata des NCPeH Land-B sind erfolgreich im NCPeH-FD installiert • Das private Schlüsselmaterial zum Aufbau von sicheren TLS-Verbindungen in der eHDSI ist im HSM erzeugt und gültig • Im HSM ist eine gültige TI-Identität (privates Schlüsselmaterial) als Repräsentation des NCPeH Land-B vorhanden • Der grenzüberschreitende Austausch von Versichertendaten mit einem Land-B ist nur nach Durchführung der Prüfung gemäß den Vorgaben aus Kapitel [4.1.2- Datenaustausch mit zugelassenen EU-Ländern] zulässig
Standardablauf	<ol style="list-style-type: none"> 1. [6.1.2.1- TUC_NCPeH_003: Cross Gateway Query Request für PS-A verarbeiten] 2. [6.2.1- TUC_NCPeH_013: Metadatenattribute des ePKA MIO abrufen] 3. [6.1.2.2- TUC_NCPeH_004: Cross Gateway Query Response für PS-A versenden]

Nachbedingungen	<ul style="list-style-type: none"> Die ermittelten Metadatenattribute über verfügbare Versichertendatensätze wurden an NCPeH Land-B übermittelt Non-Repudiation of Origin und Non-Repudiation of Receipt gemäß [4.1.7.1- Non-Repudiation of Origin erstellen] und [4.1.7.2- Non-Repudiation of Receipt erstellen] wurden in dem Audit Repository gespeichert Ein Audit Trail Eintrag gemäß Kapitel [4.1.7.3- Patient Privacy Audit Trail Eintrag erstellen] wurde in der Komponente Audit Repository gespeichert. Bei der Erstellung des Audit Trail Eintrages MUSS der NCPeH-FD die Vorgaben aus [eHDSI_XCA_Profile#4.3] umsetzen
-----------------	---

[<=]

5.1.3 NCPeH.UC_3 - ePKA MIO des Versicherten abrufen

AF_10122-01 - ePKA MIO des Versicherten abrufen

Nachdem ein NCPeH Land-B die Metadaten über das ePKA MIO eines Versicherten im vorherigen Anwendungsfall erhalten hat, kann er nun eine Anfrage an den NCPeH-FD senden, um das ePKA MIO abzurufen. In diesem Anwendungsfall antwortet der NCPeH-FD auf die berechtigte Anfrage vom NCPeH Land-B mit strukturierten medizinischen Daten aus dem ePKA MIO des Versicherten. Dafür stellt der NCPeH-FD die Schnittstelle [6.1.3- Operation Cross_Gateway_Retrieve::RetrieveDocument] gemäß [eHDSI_XCA_Profile#2.4] in der eHDSI bereit. Dabei sorgt der NCPeH-FD dafür, dass die ermittelten medizinischen Daten aus dem ePKA MIO vor der Übermittlung an den NCPeH Land-B zur Laufzeit transformiert und die maschinenlesbaren Elemente des ePKA MIO korrekt in das eHDSI CDA-Pivotformat transkodiert werden. Die vollständige Durchführung der Abfrage setzt das Vorhandensein einer Zugriffsberechtigung für das Land-B auf die ePKA MIO des Versicherten im ePA-Aktensystem voraus. Die Zugriffsfreigabe erteilt der Versicherte mittels seines FdV im ePA-Aktensystem. Der gesamte Ablauf endet mit der Übermittlung der medizinischen Daten aus dem ePKA MIO des Versicherten an den anfragenden NCPeH Land-B im eHDSI CDA-Pivotformat.

Tabelle 29: TAB_NCPeH_ePKA_MIO_des_Versicherten_abrufen

AF_10122-1	ePKA MIO des Versicherten abrufen
Akteur	NCPeH Land-B in der Rolle als eHDSI Service Consumer im Behandlungsland.
Auslöser	Ein behandelnder LE-EU im Ausland (Land-B) ruft in seinem Primärsystem medizinische Daten aus dem ePKA MIO des Versicherten in der Landessprache des Land-B auf.
Aufgerufene Schnittstellen	[6.1.3- Operation Cross_Gateway_Retrieve::RetrieveDocument]
Vorbedingung	<ul style="list-style-type: none"> Der Anwendungsfall [5.3.2- NCPeH.UC_6 - Service Metadata auf eHDSI Configuration Service verwalten] ist erfolgreich durchgeführt worden

	<ul style="list-style-type: none"> • Die gültigen Service Metadata des NCPeH Land-B sind erfolgreich im NCPeH-FD installiert • Das private Schlüsselmaterial zum Aufbau von sicheren TLS-Verbindungen in der eHDSI ist im HSM erzeugt und gültig • Im HSM ist eine gültige TI-Identität (privates Schlüsselmaterial) als Repräsentation des NCPeH Land-B vorhanden • Der grenzüberschreitende Austausch von Versichertendaten mit einem Land-B ist nur nach Durchführung der Prüfung gemäß den Vorgaben aus Kapitel [4.1.2- Datenaustausch mit zugelassenen EU-Ländern] zulässig
Standardablauf	<ol style="list-style-type: none"> 1. [6.1.3.1- TUC_NCPeH_005: Cross Gateway Retrieve Request zur Abfrage der Patient Summary CDA Level 3 verarbeiten] 2. [6.2.2- TUC_NCPeH_014: FHIR-Bundle ePKA MIO abrufen] 3. [6.1.3.5- TUC_NCPeH_009: NFD des ePKA MIO transkodieren und transformieren] 4. [6.1.3.2- TUC_NCPeH_006: Cross Gateway Retrieve Response mit Patient Summary CDA Level 3 senden]
Nachbedingungen	<ul style="list-style-type: none"> • Die medizinischen Daten aus dem ePKA MIO des Versicherten wurden im eHDSI Patient Summary CDA Pivotformat Level 3 an NCPeH Land-B übermittelt • Non-Repudiation of Origin und Non-Repudiation of Receipt gemäß 4.1.7.1- Non-Repudiation of Origin erstellen und [4.1.7.2- Non-Repudiation of Receipt erstellen] wurden in dem Audit Repository gespeichert • Ein Audit Trail Eintrag gemäß Kapitel [4.1.7.3- Patient Privacy Audit Trail Eintrag erstellen] wurde in der Komponente Audit Repository gespeichert. Bei der Erstellung des Audit Trail Eintrages MUSS der NCPeH-FD die Vorgaben aus [eHDSI_XCA_Profile#4.3] umsetzen • Ein Audit Trail Eintrag gemäß Kapitel [4.1.7.4- Translation Audit Trail Eintrag erstellen] wurde in der Komponente Audit Repository gespeichert. Bei der Erstellung des Audit Trail Eintrages MUSS der NCPeH-FD die Vorgaben aus [eHDSI_XCA_Profile#4.3] umsetzen

[<=]

5.1.4 NCPeH.UC_4 - ePKA MIO des Versicherten als PDF/A abrufen

Dieser Anwendungsfall ist weitgehend identisch mit dem Anwendungsfall [5.1.3- NCPeH.UC_3 - ePKA MIO des Versicherten abrufen]. In diesem Anwendungsfall stellt der NCPeH-FD auf Anfrage des NCPeH Land-B die medizinischen ePKA-Daten des Versicherten im PDF/A-Format bereit. Das ePKA MIO des Versicherten wird dazu in dieses Format transformiert. Dabei bleiben die medizinischen Daten des ePKA MIO so wie sie vom LE in DE im ePA-Aktensystem eingestellt wurden und werden nicht zusätzlich auf englische Begriffe gemäß MTC abgebildet (keine Transkodierung). Bedingung für den erfolgreichen

Abruf von ePKA MIO ist eine vorherige Zugriffsfreigabe durch den Versicherten. Die Zugriffsfreigabe erteilt der Versicherte mittels seines FdV im ePA-Aktensystem.

AF_10123-01 - ePKA MIO des Versicherten als PDF/A abrufen

Tabelle 30: TAB_NCPeH_ePKA_MIO_des_Versicherten_als_PDF/A_abrufen

	ePKA MIO des Versicherten als PDF/A abrufen
Akteur	NCPeH Land-B in der Rolle als eHDSI Service Consumer im Behandlungsland.
Auslöser	Ein behandelnder LE_EU (Land-B) ruft in seinem Primärsystem die medizinischen Daten des Versicherten im Originalzustand als CDA embedded PDF/A Pivotformat Level 1 ab.
Aufgerufene Schnittstellen	[6.1.3- Operation Cross_Gateway_Retrieve::RetrieveDocument]
Vorbedingung	<ul style="list-style-type: none"> • Der Anwendungsfall [5.3.2- NCPeH.UC_6 - Service Metadata auf eHDSI Configuration Service verwalten] ist erfolgreich durchgeführt worden • Die gültigen Service Metadata des NCPeH Land-B sind erfolgreich im NCPeH-FD installiert • Das private Schlüsselmaterial zum Aufbau von sicheren TLS-Verbindungen in der eHDSI ist im HSM erzeugt und gültig • Im HSM ist eine gültige TI-Identität (privates Schlüsselmaterial) als Repräsentation des NCPeH Land-B vorhanden • Der grenzüberschreitende Austausch von Versichertendaten mit einem Land-B ist nur nach Durchführung der Prüfung gemäß den Vorgaben aus [4.1.2- Datenaustausch mit zugelassenen EU-Ländern] zulässig
Standardablauf	<ol style="list-style-type: none"> 1. [6.1.3.3- TUC_NCPeH_007: Cross Gateway Retrieve Request zur Abfrage der Patient Summary CDA Level 1 verarbeiten] 2. [6.2.2- TUC_NCPeH_014: FHIR-Bundle ePKA MIO abrufen] 3. [6.1.3.6- TUC_NCPeH_010: NFD des ePKA MIO ins PDF/A-Format transformieren] 4. [6.1.3.4- TUC_NCPeH_008: Cross Gateway Retrieve Response mit dem Patient Summary CDA Level 1 senden]
Nachbedingungen	<ul style="list-style-type: none"> • Die medizinischen Daten aus ePKA MIO des Versicherten wurden im Originalzustand, wie sie vom LE in DE im ePA-Aktensystem eingestellt wurden, im eHDSI Patient Summary CDA embedded PDF/A Pivotformat Level 1 an den NCPeH Land-B gesendet. • Eine Transkodierung von medizinischen Daten nach Vorgaben aus MTC ist nicht erfolgt.

	<ul style="list-style-type: none"> • Non-Repudiation of Origin und Non-Repudiation of Receipt gemäß [4.1.7.1- Non-Repudiation of Origin erstellen] und [4.1.7.2- Non-Repudiation of Receipt erstellen] wurden in dem Audit Repository gespeichert. • Ein Audit Trail-Eintrag gemäß [4.1.7.3- Patient Privacy Audit Trail Eintrag erstellen] wurde in der Komponente Audit Repository gespeichert. Bei der Erstellung des Audit Trail Eintrages MUSS der NCPeH-FD die Vorgaben aus [eHDSI_XCA_Profile#4.3] umsetzen. • Ein Audit Trail-Eintrag gemäß [4.1.7.4- Translation Audit Trail Eintrag erstellen] wurde in der Komponente Audit Repository gespeichert. Bei der Erstellung des Audit Trail-Eintrages MUSS der NCPeH-FD die Vorgaben aus [eHDSI_XCA_Profile#4.3] umsetzen.
--	---

[<=]

5.2 Anwendungsfälle für ePrescription/eDispensation Land-A

5.2.1 NCPeH.UC_9 - Versicherten im Behandlungsland für ePeD-A identifizieren

Der Anwendungsfall zur Patient Identification für das Szenario ePeD-A ähnelt dem Kapitel [5.1.1- NCPeH.UC_1 - Versicherten im Behandlungsland für PS-A identifizieren]. Der Unterschied zum Anwendungsfall besteht darin, dass dem LE-EU unter Verwendung der KVNR und des Zugriffscodes des Versicherten die demographischen Versichertendaten aus dem zuletzt im E-Rezept-FD eingestellten E-Rezept übermittelt werden. Die Ermittlung des E-Rezepts erfolgt durch eine Anfrage des NCPeH-FD beim E-Rezept-FD. Voraussetzung für die Ermittlung und Bereitstellung des E-Rezepts ist das Vorliegen einer gültigen Zugriffsberechtigung im E-Rezept-FD. Die Zugriffsberechtigung erteilt der Versicherte im Voraus mit seinem E-Rezept-FdV. Die Verifikation der Zugriffsberechtigung des Versicherten erfolgt durch den E-Rezept-FD.

AF_10379 - ePeD-A - Versicherten im Behandlungsland für ePeD-A identifizieren

Der NCPeH-FD MUSS Vorgaben gemäß Tabelle "TAB_NCPeH_UC_09_Versicherten_im_Behandlungsland_für_ePeD-A_identifizieren" umsetzen.

Tabelle 33: TAB_NCPeH_UC_09_Versicherten_im_Behandlungsland_für_ePeD-A_identifizieren

	Versicherten im Behandlungsland für ePeD-A identifizieren
Akteur	NCPeH Land-B in der Rolle eHDSI Service Consumer im Behandlungsland
Auslöser	Ein behandelnder LE_EU (Land-B) möchte den Versicherten im Kontext der Anwendung ePrescription/eDispensation identifizieren und braucht dafür demographische Versichertendaten.
Aufgerufene Schnittstelle	[6.1.1- Operation Cross_Gateway_Patient_Discovery::RespondingGateway_PRPA_IN2013

	05UV02]
Vorbedingung	<ul style="list-style-type: none"> • Der Anwendungsfall [5.3.2- NCPeH.UC_6 - Service Metadata auf eHDSI Configuration Service verwalten] ist erfolgreich durchgeführt worden. • Die Service Metadata des NCPeH Land-B sind erfolgreich im NCPeH-FD installiert. • Das private Schlüsselmaterial zum Aufbau von sicheren TLS-Verbindungen in der eHDSI ist im HSM erzeugt und gültig. • Im HSM ist eine gültige TI-Identität (privates Schlüsselmaterial) als Repräsentation des NCPeH Land-B vorhanden. • Die Prüfung auf den zulässigen grenzüberschreitenden Austausch von Versichertendaten mit dem Land-B ist gemäß den Vorgaben aus [4.1.2- Datenaustausch mit zugelassenen EU-Ländern] erfolgreich durchgeführt worden. • Aktuelle, von der BfArM freigegebene Mapping- und Transkodierregeln sind aktiv und alle aktuell gültigen FHIR-Profilversionen für E-Rezepte können verarbeitet werden.
Standardablauf	<ol style="list-style-type: none"> 1. [6.1.1.3- TUC_NCPeH_023: Patient Demographics Query Request für ePeD-A verarbeiten] 2. [6.2.4- TUC_NCPeH_035: Demographische Versichertendaten aus E-Rezept extrahieren] 3. [6.1.1.4- TUC_NCPeH_024: Patient Demographics Response mit demographischen Versichertendaten für ePeD-A versenden]
Nachbedingungen	<ul style="list-style-type: none"> • Die ermittelten demographischen Versichertendaten wurden an NCPeH Land-B übermittelt. • Non-Repudiation of Origin und Non-Repudiation of Receipt gemäß [4.1.7- Non-Repudiation und Audit Trail Schemas] sind in dem Audit Repository gespeichert. • Ein Audit Trail Eintrag gemäß [4.1.7.3- Patient Privacy Audit Trail Eintrag erstellen] wurde in der Komponente Audit Repository gespeichert. Bei der Erstellung des Audit Trail Eintrages MUSS der NCPeH-FD die Vorgaben aus [eHDSI_XCPD_Profile#3.3] umsetzen.

[<=]

5.2.2 NCPeH.UC_10 - Einlösbare E-Rezepte des Versicherten aus ePeD-A auflisten

In diesem Anwendungsfall muss der NCPeH-FD in der Lage sein, auf berechtigte Anfrage des NCPeH Land-B Informationen über die einlösbaren E-Rezepte des Versicherten bereitzustellen. Die Anfrage des NCPeH Land-B enthält die Identität des LE-EU, die KVNR des Versicherten, den Zugriffscode und die elektronische Zusicherung des Abgabelandes (Land-B) über das Bestehen einer Behandlungsbeziehung zwischen dem anfragenden LE-EU und dem Versicherten. Die Ermittlung der einlösbaren E-Rezepte erfolgt durch eine Abfrage des NCPeH-FD beim E-Rezept-FD. Voraussetzung für die Ermittlung von E-Rezepten ist das Vorliegen einer gültigen Zugriffsberechtigung im E-Rezept-FD. Die Zugriffsberechtigung erteilt der Versicherte im Voraus mit seinem E-Rezept-FdV. Der

gesamte Prozess endet mit der Übermittlung einer Liste in der EU einlösbarer E-Rezepte des Versicherten an den NCPeH Land-B.

AF_10380 - Einlösbare E-Rezepte des Versicherten aus ePeD-A auflisten

Der NCPeH-FD MUSS Vorgaben gemäß Tabelle "TAB_NCPeH_Einlösbare_E-Rezepte_des_Versicherten_aus_ePeD-A_auflisten" umsetzen.

Tabelle 31: TAB_NCPeH_Einlösbare_E-Rezepte_des_Versicherten_aus_ePeD-A_auflisten

	Einlösbare E-Rezepte des Versicherten aus ePeD-A auflisten
Akteur	NCPeH Land-B in der Rolle als eHDSI Service Consumer im Abgabeland.
Auslöser	Ein behandelnder LE_EU (Land-B) ruft in seinem Primärsystem Informationen über die einlösbaren E-Rezepte ab.
Aufgerufene Schnittstelle	6.1.2 - Operation Cross_Gateway_Query::FindDocuments
Vorbedingung	<ul style="list-style-type: none"> • Der Anwendungsfall aus [5.3.2- NCPeH_UC_6 - Service Metadata auf eHDSI Configuration Service verwalten] ist erfolgreich durchgeführt worden. • Die gültigen Service Metadata des NCPeH Land-B sind erfolgreich im NCPeH-FD installiert. • Das private Schlüsselmaterial zum Aufbau von sicheren TLS-Verbindungen in der eHDSI ist im HSM erzeugt und gültig • Im HSM ist eine gültige TI-Identität (privates Schlüsselmaterial) als Repräsentation des NCPeH Land-B vorhanden. • Die Prüfung auf den zulässigen grenzüberschreitenden Austausch von Versichertendaten mit dem Land-B ist gemäß den Vorgaben aus [4.1.2- Datenaustausch mit zugelassenen EU-Ländern] erfolgreich durchgeführt worden. • Aktuelle, von der BfArM freigegebene Mapping- und Transkodierregeln sind aktiv und alle aktuell gültigen FHIR-Profilversionen für E-Rezepte können verarbeitet werden.
Standardablauf	<ol style="list-style-type: none"> 1. [6.1.2.3- TUC_NCPeH_025: Cross Gateway Query Request für ePeD-A verarbeiten] 2. [6.2.5- TUC_NCPeH_036: Liste der einlösbaren E-Rezepte des Versicherten aus dem E-Rezept-FD abrufen] 3. [6.1.2.4- TUC_NCPeH_026: Cross Gateway Query Response für ePeD-A versenden]
Nachbedingungen	<ul style="list-style-type: none"> • Die ermittelten Informationen über einlösbare E-Rezepte des Versicherten wurden an NCPeH Land-B übermittelt. • Non-Repudiation of Origin und Non-Repudiation of Receipt gemäß [4.1.7 - Non-Repudiation und Audit Trail Schemas] sind in dem Audit Repository gespeichert.

	<ul style="list-style-type: none"> Ein Audit Trail Eintrag ist gemäß den Vorgaben aus [eHDSI_XCA_Profile#4.3] im Audit Repository gespeichert.
--	---

[<=]

5.2.3 NCPeH.UC_11 - Ausgewählte E-Rezepte aus ePeD-A abrufen

Anhand der Übersicht der einlösbaren E-Rezepte, die dem LE-EU bereitgestellt werden, wählt dieser die E-Rezepte aus, die der Versicherte einlösen möchte. Nach der Abstimmung zwischen LE-EU und Versichertem stellt der LE-EU über den NCPeH Land-B eine Anfrage an den NCPeH-FD, um die E-Rezepte in mindestens einem der beiden Dokumentformaten (eHDSI Pivotformat CDA Level 1 und Level 3) abzurufen.

In diesem Anwendungsfall antwortet der NCPeH-FD auf die berechtigte Anfrage aus Land-B, indem er die E-Rezepte des Versicherten in den angeforderten Dokumentformaten bereitstellt. Hierfür stellt der NCPeH-FD die Schnittstelle gemäß [[6.1.3 Operation Cross_Gateway_Retrieve::RetrieveDocument](#)] und nach [eHDSI_XCA_Profile#2.4] zur Verfügung. Die Ermittlung der angeforderten E-Rezepte erfolgt durch eine Anfrage des NCPeH-FD beim E-Rezept-FD. Voraussetzung für die Ermittlung und Bereitstellung der E-Rezepte ist das Vorliegen einer gültigen Zugriffsberechtigung im E-Rezept-FD. Die Zugriffsberechtigung erteilt der Versicherte im Voraus mit seinem E-Rezept-FdV. Die Verifikation der Zugriffsberechtigung des Versicherten erfolgt durch den E-Rezept-FD.

Der NCPeH-FD stellt sicher, dass die ermittelten E-Rezepte vor der Übermittlung an den NCPeH von Land-B zur Laufzeit transformiert werden und die maschinenlesbaren Elemente der E-Rezepte korrekt transkodiert sind.

AF_10400 - Ausgewählte E-Rezepte abrufen

Der NCPeH-FD MUSS Vorgaben gemäß Tabelle "TAB_NCPeH_UC_11_Ausgewählte_E-Rezepte_abrufen" umsetzen.

Tabelle 32: TAB_NCPeH_UC_11_Ausgewählte_E-Rezepte_abrufen

	Ausgewählte E-Rezepte abrufen
Akteur	NCPeH Land-B in der Rolle als eHDSI Service Consumer im Behandlungsland.
Auslöser	Ein behandelnder LE_EU (Land-B) ruft in seinem Primärsystem E-Rezepte des Versicherten in der Landessprache des Land-B auf.
Aufgerufene Schnittstellen	[6.1.3 Operation Cross_Gateway_Retrieve::RetrieveDocument]
Vorbedingung	<ul style="list-style-type: none"> Der Anwendungsfall aus [NCPeH.UC_6 - Service Metadata auf eHDSI Configuration Service verwalten] ist erfolgreich durchgeführt worden Die gültigen Service Metadata des NCPeH Land-B sind erfolgreich im NCPeH-FD installiert Das private Schlüsselmaterial zum Aufbau von sicheren TLS-Verbindungen in der eHDSI ist im HSM erzeugt und gültig Im HSM ist eine gültige TI-Identität (privates Schlüsselmaterial) als Repräsentation des NCPeH Land-B vorhanden Die Prüfung des zulässigen grenzüberschreitenden Austauschs

	<p>von Versichertendaten mit dem Land-B ist gemäß den Vorgaben aus [Kapitel 4.1.2 - Datenaustausch mit zugelassenen EU-Ländern] erfolgreich durchgeführt worden</p> <ul style="list-style-type: none"> • Aktuelle, von der BfArM freigegebene Mapping- und Transkodierregeln sind aktiv und alle aktuell gültigen FHIR-Profilversionen für E-Rezepte können nach der Regelung im [4.2.10.7- Regelung zur Unterstützung von mehreren FHIR-Package Versionen] verarbeitet werden
Standardablauf	<ol style="list-style-type: none"> 1. [6.1.3.7- TUC_NCPeH_027: Cross Gateway Retrieve Request für ePeD-A auf Einhaltung von allgemeinen Kriterien prüfen] 2. [6.1.3.8- TUC_NCPeH_028: Cross Gateway Retrieve Request für ePeD-A CDA verarbeiten] 3. [6.2.6- TUC_NCPeH_037: Abzugebende E-Rezepte vom E-Rezept-FD abrufen] 4. [6.1.3.10- TUC_NCPeH_030: Abgerufene E-Rezepte transkodieren und transformieren] 5. [6.1.3.9- TUC_NCPeH_029: Cross Gateway Retrieve Response mit ePeD-A CDA senden]
Nachbedingungen	<ul style="list-style-type: none"> • Die angeforderten E-Rezepte des Versicherten wurden im eHDSI ePrescription CDA Pivotformat an NCPeH Land-B übermittelt. • Non-Repudiation of Origin und Non-Repudiation of Receipt sind gemäß den Vorgaben aus [4.1.7 Non-Repudiation und Audit Trail Schemas] im Audit Repository gespeichert. • Ein Audit Trail Eintrag ist gemäß den Vorgaben aus [eHDSI_XCA_Profile#4.3 und #2.4] im Audit Repository gespeichert.

[<=]

5.2.4 NCPeH.UC_12 - Abgabe von Arzneimitteln an Versicherte im Abgabeland

Im Anwendungsfall im [5.2.3- NCPeH.UC_11 - Ausgewählte E-Rezepte aus ePeD-A abrufen] hat der LE-EU Informationen zu den E-Rezepten eines Versicherten abgerufen. Für die E-Rezepte, die er abgeben möchte, sendet der LE-EU Dispensierinformationen im eHDSI eDispensation CDA-Pivotformat über den NCPeH Land-B an den NCPeH-FD. Der NCPeH-FD bestätigt daraufhin den Abschluss des E-Rezept-Workflows für den betreffenden Task und lässt die übermittelten Dispensierinformationen im E-Rezept-FD für den Versicherten speichern.

Der NCPeH-FD übernimmt in diesem Kontext zwei wesentliche Aufgaben. Zunächst stellt er innerhalb der eHDSI eine spezifische Schnittstelle bereit. Diese Schnittstelle entspricht den Vorgaben, die im [6.1.5- Operation Cross-Enterprise Document Reliable Interchange::ProvideAndRegisterDocumentSet-b] sowie in [eHDSI_XCA_Profile#2.4] definiert sind. Darüber hinaus ist der NCPeH-FD für die Verarbeitung der Dispensierinformationen verantwortlich. Bevor diese Informationen an den E-Rezept-FD weitergeleitet werden, führt der NCPeH-FD eine Laufzeittransformation

durch. Zusätzlich werden die maschinenlesbaren Elemente gemäß den Vorgaben des BfArM transkodiert.

AF_10401 - Abgabe von Arzneimitteln an Versicherte im Abgabeland

Der NCPeH-FD MUSS Vorgaben aus der Tabelle

TAB_NCPeH_UC_1X_Abgabe_von_Arzneimitteln_an_Versicherte_im_Abgabeland umsetzen.

Tabelle: TAB_NCPeH_UC_1X_Abgabe_von_Arzneimitteln_an_Versicherte_im_Abgabeland

	Abgabe von Arzneimitteln an Versicherte im Abgabeland
Akteur	NCPeH Land-B in der Rolle als eHDSI Service Consumer im Behandlungsland
Auslöser	Ein LE_EU (Land-B) möchte über sein Primärsystem die Dispensierinformationen für ausgewählte E-Rezepte des Versicherten nach Deutschland übermitteln.
Aufgerufene Schnittstellen	[6.1.5- Operation Cross-Enterprise Document Reliable Interchange::ProvideAndRegisterDocumentSet-b]
Vorbedingung	<ul style="list-style-type: none"> • Der Anwendungsfall [NCPeH.UC_6 - Service Metadata auf eHDSI Configuration Service verwalten] ist erfolgreich durchgeführt worden. • Die gültigen Service Metadata des NCPeH Land-B sind erfolgreich im NCPeH-FD installiert. • Das private Schlüsselmaterial zum Aufbau von sicheren TLS-Verbindungen in der eHDSI ist im HSM erzeugt und gültig. • Im HSM ist eine gültige TI-Identität (privates Schlüsselmaterial) als Repräsentation des NCPeH Land-B vorhanden. • Die Prüfung auf den zulässigen grenzüberschreitenden Austausch von Versichertendaten mit dem Land-B ist gemäß den Vorgaben aus [Kapitel 4.1.2 - Datenaustausch mit zugelassenen EU-Ländern] erfolgreich durchgeführt worden. • Aktuelle, von der BfArM freigegebene Mapping- und Transkodierregeln sind aktiv und alle aktuell gültigen FHIR-Profilversionen für E-Rezepte können verarbeitet werden.
Standardablauf	<ol style="list-style-type: none"> 1. [6.1.5.1- TUC_NCPeH_031: Überprüfung des Cross-Enterprise Document Reliable Interchange Request für eD-A auf allgemeine Vorgaben] 2. [6.1.5.2- TUC_NCPeH_032: Cross-Enterprise Document Reliable Interchange Request für eD-A verarbeiten] 3. [6.1.5.4- TUC_NCPeH_034: Dispensierdokumente transkodieren und transformieren] 4. [6.2.7- TUC_NCPeH_038: Dispensierdokumente an E-Rezept-FD übermitteln] 5. [6.1.5.3- TUC_NCPeH_033: Cross-Enterprise Document Reliable Interchange Response für eD-A senden]

Nachbedingungen	<ul style="list-style-type: none"> Die Dispensierinformationen wurden im E-Rezept-FD hinterlegt. Das E-Rezept kann vom NCPeH-FD nicht mehr als einlösbares E-Rezept aufgelistet und abgerufen werden. Non-Repudiation of Origin und Non-Repudiation of Receipt sind gemäß Vorgaben aus [4.1.7- Non-Repudiation und Audit Trail Schemas] im Audit Repository gespeichert. Ein Audit Trail Eintrag ist gemäß Vorgaben aus [eHDSI_XDR_Profile#3.2 und #2.4] im Audit Repository gespeichert.
-----------------	--

[<=]

5.3 Administrative Anwendungsfälle

5.3.1 NCPeH.UC_5 - Evidence & Audit Trails aus Audit Repository abrufen

In diesem Anwendungsfall MUSS der berechnigte Prozessverantwortliche über eine technische Schnittstelle Evidence und Audit Trail Einträge aus dem Audit Repository auswählen, die im Zusammenhang mit der Verarbeitung von Identitäts- und medizinischen Daten von Versicherten stehen, um sie anschließend in seinem Monitoringsystem abzurufen und ggf. auszuwerten. Dies kann z. B. in einem Szenario geschehen, in dem überprüft werden muss, ob personenbezogene oder administrative Daten im NCPeH-FD manipuliert wurden (siehe [eHDSI Section II - Security Services#6.5]). Ferner MUSS der berechnigte Prozessverantwortliche Anfragen von betroffenen Versicherten oder der befugten nationalen Stelle beantworten und dabei die für den Fall erforderlichen Nachweise (Evidence) aus dem Audit Repository abrufen und dem Antragsteller bereitstellen.

Zuletzt soll darauf hingewiesen werden, dass ebenfalls die Vorgaben aus [eHDSI_NCPeH_Architecture_Specification] Kapitel „Audit Repository“ für die Umsetzung heranzuziehen sind.

Hinweis: Die Definition und Festlegung der Technologie zur Umsetzung der technischen Schnittstelle liegt in Hoheit des Anbieters des NCPeH-FD (siehe [1.4- Abgrenzungen] und [2- Systemüberblick]).

AF_10126 - Evidences & Audit Trails aus Audit Repository abrufen

Tabelle 33: TAB_NCPeH_Evidences_Audit_Trails_abrufen

AF_10126	Evidence & Audit Trails aus Audit Repository abrufen
Akteur	Prozessverantwortlicher Audit Trails
Auslöser	Der Prozessverantwortlicher Audit Trails möchte über einen Client (z.B. Monitoringsystem) Evidence und Audit Trails eines Versicherten aus dem Audit Repository abrufen
Aufgerufene Schnittstelle	Operation I_Management_Configuration (Hinweis: Definition erfolgt durch Anbieter des NCPeH-Fachdienstes)
Vorbedingung	<ul style="list-style-type: none"> Der Prozessverantwortliche für Audit Trails ist im NCPeH-

	<p>Fachdienst berechtigt Evidence und Audit Trails aus dem Audit Repository abzurufen</p> <ul style="list-style-type: none"> Evidence und Audit Trails sind im Audit Repository enthalten
Standardablauf	<ol style="list-style-type: none"> [6.3.1- TUC_NCPeH_018: Systemadministrator oder Prozessverantwortlicher anmelden] [6.3.4- TUC_NCPeH_021: Ausgewählte Evidence und Audit Trail Einträge ermitteln]
Nachbedingungen	<p>Informationen zur Anmeldung des Prozessverantwortlichen, Zeitangaben, Nutzung der Schnittstelle und Operationen, Zugriff auf Ressourcen in dem Audit Repository und aufgetretenen Fehlerfällen und -gründen sind gemäß Vorgaben aus Kapitel [4.4.5- Logging] im NCPeH-Fachdienst protokolliert.</p>

[<=]

5.3.2 NCPeH.UC_6 - Service Metadata auf eHDSI Configuration Service verwalten

In diesem Anwendungsfall verwalten die berechtigten Systemadministratoren über eine Management-Schnittstelle in einem 4-Augen-Prinzip. Diese enthaltenen Informationen (Service Metadata) über die angebotenen Dienste des NCPeH-FD in der eHDSI. Die Systemadministratoren MÜSSEN in der Lage sein, die Service Metadata anderen Teilnehmern (NCPeH Land-B) zur Verfügung zu stellen. Die Service Metadata enthalten Metadaten über einen Dienst, den ein NCPeH Land-B kennen muss, um eine Nachricht an diesen Dienst senden zu können. Dazu gehören unter anderem Angaben zu Netzwerkadressen, Webdienst-Endpunkten, öffentliche Zertifikate, aber auch Angaben für LE-EU zur Identifizierung von Versicherten aus Deutschland im Ausland. Die Systemadministratoren MÜSSEN die Service Metadata auf dem zentralen Configuration Service der eHDSI hochladen bzw. verwalten. Dadurch werden die Service Metadata den NCPeH Land-B zum Download zur Verfügung gestellt. Anhand der Service Metadata können NCPeH Land-B die Dienste des NCPeH-FD lokalisieren, den Aufbau von sicheren TLS-Verbindungen zum NCPeH-FD initiieren sowie IHE-Anfragen an die angebotenen Schnittstellen senden.

Hinweis: Die Definition und Festlegung der Technologie zur Umsetzung der Management-Schnittstelle liegt in Hoheit des Anbieters des NCPeH-FD (Siehe [1.4- Abgrenzungen] und [2- Systemüberblick]).

AF_10124 - Service Metadata auf eHDSI Configuration Service verwalten

Tabelle 34: TAB_NCPeH_Service_Metadata_verwalten

AF_10124	Service Metadata auf eHDSI Configuration Service verwalten
Akteur	Systemadministrator
Auslöser	Systemadministrator möchte Service Metadata der Dienste des NCPeH-Fachdienstes verwalten

<p>Aufgerufene Schnittstelle</p>	<p>Schnittstelle I_Management_Configuration (Hinweis: Definition erfolgt durch Anbieter des NCPeH-Fachdienstes)</p>
<p>Vorbedingung</p>	<ul style="list-style-type: none"> • Der Systemadministrator ist im NCPeH-Fachdienst berechtigt Service Metadata für einzelne Dienste zu erstellen und zu signieren • Ein anderer Systemadministrator ist im NCPeH-Fachdienst berechtigt eine Prüfung (siehe Vier-Augen-Prinzip) der signierten Service Metadata durchzuführen und die Service Metadata auf dem eHDSI Configuration Service hochzuladen • Die Adresse des eHDSI Configuration Service ist im NCPeH-Fachdienst enthalten • Das öffentliche und gültige Zertifikat des eHDSI Configuration Service ist im Truststore des NCPeH-Fachdienstes enthalten
<p>Standardablauf</p>	<ol style="list-style-type: none"> 1. [6.3.1- TUC_NCPeH_018: Systemadministrator oder Prozessverantwortlicher anmelden] 2. [6.1.4.1- TUC_NCPeH_011: Service Metadata erstellen] 3. [6.1.4.2- TUC_NCPeH_012: Signed Service Metadata auf eHDSI Configuration Service hochladen]
<p>Nachbedingungen</p>	<ul style="list-style-type: none"> • Ausgewählte signierte Service Metadata sind erfolgreich auf dem eHDSI Configuration Service hochgeladen • Die erstellten Service Metadata sind weiterhin im NCPeH-Fachdienst in der VAU vorhanden und können von Systemadministratoren als Vorlage verwendet und geändert werden • Ein Audit-Trail-Eintrag gemäß Kapitel [4.1.7.5- Security Audit Trail Eintrag erstellen] ist in der Komponente Audit Repository gespeichert • Informationen zur Anmeldung des Systemadministrators, Zeitangaben, Nutzung der Schnittstelle und Operationen, Erstellung und Aktualisierung von Service Metadata, Signaturerstellung, Identitätsangaben zum prüfenden Systemadministrator und aufgetretenen Fehlerfällen und -gründen sind gemäß Vorgaben aus Kapitel [4.4.5- Logging] im NCPeH-Fachdienst protokolliert

[<=]

5.3.3 NCPeH.UC_7 - MTC vom eHDSI Terminology Service herunterladen

Das BfArM ist in seiner Rolle als Terminologie-Verantwortlicher für die Pflege und korrekte Zuordnung von Codes, Codierungssystemen und Terminologien im MTC verantwortlich (siehe [\[3.2- Akteure\]](#)). Sobald das BfArM eine neue Version des MTC für die Nutzung in Deutschland auf dem eHDSI Terminology Service freigegeben hat, MUSS der NCPeH-FD

die Version des MTC herunterladen und lokal in der VAU aktivieren. Das Herunterladen und die Aktivierung des MTC kann vom Systemadministrator über eine automatische Aktualisierung und zusätzlich über eine manuelle Aktualisierung beim NCPeH-FD ausgelöst werden.

AF_10127 - MTC vom eHDSI Terminology Service herunterladen

Tabelle 35: TAB_NCPeH_MTC_Terminology-Service_herunterladen

AF_10127	MTC vom eHDSI Terminology Service herunterladen
Akteur	Systemadministrator
Auslöser	Systemadministrator möchte den aktuellen MTC vom Central Terminology Service herunterladen und aktivieren
Aufgerufene Schnittstelle	Operation I_Management_Configuration (Hinweis: Definition erfolgt durch Anbieter des NCPeH-Fachdienstes)
Vorbedingung	<ul style="list-style-type: none"> • Der Systemadministrator ist im NCPeH-Fachdienst berechtigt das Herunterladen des MTC vom eHDSI Terminology Service auszulösen • Die Zieladresse des eHDSI Terminology Service ist im NCPeH-Fachdienst konfiguriert • Der NCPeH-Fachdienst verfügt über gültige Zugangsdaten für den eHDSI Terminology Service (Benutzername und Passwort) • Das öffentliche und gültige Zertifikat des eHDSI Terminology Service ist im Truststore des NCPeH-Fachdienstes enthalten
Standardablauf	<ol style="list-style-type: none"> 1. [6.3.1- TUC_NCPeH_018: Systemadministrator oder Prozessverantwortlicher anmelden] 2. [6.3.5- TUC_NCPeH_022: MTC in der VAU speichern]
Nachbedingungen	<ul style="list-style-type: none"> • MTC ist erfolgreich in der VAU gespeichert und nur diese Version des MTC kann für Zwecke der Transkodierung von strukturierten Elementen aus ePKA MIO verwendet werden • Ein Audit-Trail-Eintrag gemäß Kapitel [4.1.7.5- Security Audit Trail Eintrag erstellen] ist in der Komponente Audit Repository gespeichert • Informationen zur Anmeldung des Systemadministrators, Zeitangaben, Nutzung der Schnittstelle und Operationen, Version der heruntergeladenen MTC und aufgetretenen Fehlerfällen und -gründen sind gemäß Vorgaben aus Kapitel [4.4.5- Logging] im NCPeH-Fachdienst protokolliert

[<=]

5.3.4 NCPeH.UC_8 - Konfigurationsparameter verwalten

In diesem Anwendungsfall verwalten die berechtigten Systemadministratoren über eine Management-Schnittstelle in einem 4-Augen-Prinzip die Konfigurationsparameter des NCPeH-FD, die im [4.1.1- Konfigurationsparameter] definiert sind.

Hinweis: Die Definition und Festlegung der Technologie zur Umsetzung der Management-Schnittstelle liegt in Hoheit des Anbieters des NCPeH-FD (Siehe [1.4- Abgrenzungen] und [2- Systemüberblick]).

AF_10125 - Konfigurationsparameter verwalten

Tabelle 36: TAB_NCPeH_Konfigurationsparameter_verwalten

AF_10125	Konfigurationsparameter verwalten
Akteur	Systemadministrator
Auslöser	Systemadministrator möchte Konfigurationsparameter und Zertifikate im NCPeH-Fachdienst verwalten
Aufgerufene Schnittstelle	Operation I_Management_Configuration (Hinweis: Definition erfolgt durch Anbieter des NCPeH-Fachdienstes)
Vorbedingung	<ul style="list-style-type: none"> • Der Systemadministrator ist im NCPeH-Fachdienst berechtigt Änderungen an Konfigurationsparametern und Aktualisierung von Zertifikaten im NCPeH-Fachdienst durchzuführen • Ein anderer Systemadministrator ist im NCPeH-Fachdienst berechtigt eine Prüfung (siehe Vier-Augen-Prinzip) der geänderten Konfigurationsparametern und abschließende Speicherung von Konfigurationsparametern durchzuführen
Standardablauf	<ol style="list-style-type: none"> 1. [6.3.1- TUC_NCPeH_018: Systemadministrator oder Prozessverantwortlicher anmelden] 2. [6.3.2- TUC_NCPeH_019: Änderungen an Konfigurationsparameter planen] 3. [6.3.3- TUC_NCPeH_020: Änderungen an Konfigurationsparametern und im Truststore aktivieren]
Nachbedingungen	<ul style="list-style-type: none"> • Aktualisierte Konfigurationsparameter sind im NCPeH-Fachdienst gespeichert • Die übrigen Konfigurationsparameter, die von den Systemadministratoren nicht geändert wurden, blieben davon unberührt • Bei der Erstellung von neuen Einträgen in der WHITELIST_NCPeH_COUNTRY-B sind gültige Zertifikate des jeweiligen NCPeH Land-B in den lokalen Truststore des NCPeH-Fachdienstes aufgenommen • Für jeden neuen Eintrag in der WHITELIST_NCPeH_COUNTRY-B ist ein Audit Trail Eintrag gemäß Kapitel [4.1.7.5- Security Audit Trail Eintrag]

	<p>erstellen] in der Komponente Audit Repository gespeichert</p> <ul style="list-style-type: none">• Für jeden neuen Eintrag in der WHITELIST_NCPeH_COUNTRY-B sind in der VAU relevante Referenzwerte gemäß [4.1.4- Service Metadata des NCPeH Land-B abrufen] gespeichert, die mit den neuen Zertifikaten des NCPeH Land-B verknüpft sind• Bei der Aktualisierung von Einträgen in der WHITELIST_NCPeH_COUNTRY-B sind die Zertifikate des jeweiligen NCPeH Land-B in den lokalen Truststore des NCPeH-Fachdienstes aktualisiert• Bei der Entfernung von Ländercodes und HomeCommunityId einzelner Länder (Land-B) aus der WHITELIST_NCPeH_COUNTRY-B sind Zertifikate, die zu dem NCPeH Land-B zugeordnet wurden, in den lokalen Truststore nicht mehr vorhanden• Informationen zur Anmeldung des Systemadministrators, Zeitangaben, Nutzung der Schnittstelle und Operationen, Aktualisierung von Konfigurationsparameter, Identitätsangaben zum prüfenden Systemadministrator und aufgetretenen Fehlerfällen und -gründen sind gemäß Vorgaben aus Kapitel [4.4.5- Logging] im NCPeH-Fachdienst protokolliert
--	---

[<=]

6 Funktionsmerkmale

6.1 eHDSI

6.1.1 Operation

Cross_Gateway_Patient_Discovery::RespondingGateway_PRPA_IN201305UV02

Tabelle 37: TAB_NCPeH_Cross_Gateway_Patient_Discovery

Operation	RespondingGateway_PRPA_IN201305UV02	
Beschreibung	<p>Die Schnittstelle Cross Gateway Patient Discovery stellt bei berechtigten Anfragen über die Operation RespondingGateway_PRPA_IN201305UV02 demographische Versichertendaten bereit. Sie wird vom NCPeH-FD gemäß [eHDSI_XCPD_Profile] implementiert und NCPeHs anderer europäischen Mitgliedsstaaten (Land-B) zur Nutzung angeboten. Hierbei sendet der anfragende NCPeH Land-B in der Rolle als XCPD-"Initiating Gateway" eine Anfrage zusammen mit der Kennung (KVNR) und dem Zugriffscode des Versicherten. Die Daten aus der Anfrage werden vom NCPeH-FD in der Rolle als XCPD-"Responding Gateway" verarbeitet und an den zum jeweiligen Anwendungsszenario passenden Fachdienst der TI zur Ermittlung der demographischen Versichertendaten weitergeleitet. Bei einer erfolgreichen Rückmeldung vom Fachdienst der TI übermittelt der NCPeH-FD in seiner Antwort die ermittelten demographischen Versichertendaten an das anfragende NCPeH Land-B. (Hinweis: Operationsname nach [ITI-55#3.55.6.1])</p>	
Eingangsparameter		
Name	Beschreibung	Typ
Patient Demographic s Query Request	Eingangsnachricht zur Abfrage von demographischen Versichertendaten gemäß [eHDSI_XCPD_Profile#2.1]	HL7v3 Patient Registry Find Candidates Query [ITI-55]
X-User Assertion	Authentication Assertion des authentifizierten LE-EU	SAML 2.0 Assertion gemäß [eHDSI_SAML_Profile#2] inkl. X.509 öffentliches Signaturzertifikat des NCPeH Land-B [eHDSI_X.509_Certificates_Profile]
Ausgangsparameter		

Name	Beschreibung	Typ
Patient Demographics Response	Ausgangsnachricht gemäß [eHDSI_XCPD_Profile#2.3] inkl. der demographischen Versichertendaten (KVNR, Vorname, Nachname und Geburtstag)	HL7v3 Patient Registry Find Candidates Query Response

Die Zuordnung von IHE XCPD-Anfragen zu passenden Anwendungsszenarien MUSS anhand des root-Attributs aus dem livingSubjectID/value-Element erfolgen. Es MUSS das livingSubjectID/value-Element genutzt werden, in dem der Zugriffscode enthalten ist, mit dem der LE-EU vom Versicherten zum Zugriff auf die demographischen Versichertendaten berechtigt worden ist. Der NCPeH-FD MUSS in der Lage sein, anhand der IHE XCPD-Anfrage und den Kriterien aus der Tabelle TAB_NCPeH_Kriterien_Zuordnung_IHE_XCPD-Anfragen_zu_Anwendungsszenarien eindeutig das Anwendungsszenario zu adressieren. Darüber hinaus MUSS er den richtigen TUC aufrufen, in dem die Anfrage weiterbearbeitet wird.

Tabelle 38: TAB_NCPeH_Kriterien_Zuordnung_IHE_XCPD-Anfragen_zu_Anwendungsszenarien

root-Attribute	Technischer Use Case (TUC)
Ist identisch mit dem Wert des Konfigurationsparameters OID_AC_ePKA_ASSIGNING_AUTHORITY (siehe 4.1.1-Konfigurationsparameter)	[6.1.1.1- TUC_NCPeH_001: Patient Demographics Query Request für PS-A verarbeiten] (Anwendungsszenario: Patient Summary Land-A)
Ist identisch mit dem Wert des Konfigurationsparameters OID_AC_eRp_ASSIGNING_AUTHORITY (siehe [4.1.1 - Konfigurationsparameter])	[6.1.1.3- TUC_NCPeH_023: Patient Demographics Query Request für ePeD-A verarbeiten] (Anwendungsszenario: ePrescription/eDispensation Land-A)
Der Wert entspricht nicht dem oberen Wert	Anwendungsszenario: nicht bekannt Nach Eingang der Anfrage MUSS der NCPeH-FD einen Non-Repudiation of Receipt Eintrag gemäß [4.1.7.2- Non-Repudiation of Receipt erstellen] und einen Audit Trail Eintrag gemäß [4.1.7.3- Patient Privacy Audit Trail Eintrag erstellen] in der Komponente Audit Repository speichern. Bei der Erstellung des Audit Trail Eintrages der NCPeH-FD MUSS Vorgaben aus [eHDSI_XCPD_Profile#3.3] umsetzen. Der NCPeH-FD DARF die Anfrage NICHT weiter bearbeiten und MUSS dem NCPeH Land-B mit dem folgenden Reason Encoding gemäß [eHDSI_XCPD_Profile#2.3.3] antworten: <mitigatedBy typeCode="MITGT"> <detectedIssueManagement

	<pre>classCode="ACT" moodCode="ENV"> <code code="AnswerNotAvailable" codeSystem="1.3.6.1.4.1.19376.1.2.27.3"/> </detectedIssueManagement> </mitigatedBy></pre> <p>Zusätzliche Informationen, die den Grund beschreiben, MÜSSEN in die Antwort aufgenommen werden:</p> <pre>acknowledgementDetail.Code= ERROR_PI_GENERIC acknowledgementDetail.Text = Patient Identification Error acknowledgementDetail.Location = "Service unknown. Please contact your service provider or administrator."</pre> <p>Nach Versand der Fehlermeldung an den jeweiligen NCPeH Land-B MUSS der NCPeH-FD einen Non-Repudiation of Origin Eintrag gemäß [4.1.7.1 Non-Repudiation of Origin erstellen] und einen Audit Trail Eintrag gemäß [4.1.7.3- Patient Privacy Audit Trail Eintrag erstellen] in der Komponente Audit Repository speichern. Bei der Erstellung des Audit Trail Eintrages der NCPeH-FD MUSS Vorgaben aus [eHDSI_XCA_Profile#4.3] umsetzen.</p>
--	---

6.1.1.1 TUC_NCPeH_001: Patient Demographics Query Request für PS-A verarbeiten

Für diesen TUC gelten folgende übergreifende Festlegungen

- [[4.1.1- Konfigurationsparameter](#)]
- [[4.1.3- eHDSI Basisleistungen](#)]
- [[4.1.5- Validierung der Identity Assertion des LE-EU](#)]
- [[4.1.7.2- Non-Repudiation of Receipt erstellen](#)]
- [[4.1.7.3- Patient Privacy Audit Trail Eintrag erstellen](#)]
- [[4.1.8- Festlegungen zur Prüfung der Zugriffsberechtigung auf Fachdienste der TI](#)]
- [[4.1.9- Format und Validierung der KVNR](#)]
- [[4.2.1- Schnittstellen zu Diensten der zentralen TI](#)]
- [[4.2.7.3- Lokalisierung der Akte eines Versicherten](#)]
- [[4.2.7- Login in ein ePA-Aktenkonto](#)]
- [[4.2.9- Elektronische Identitäten des NCPeH-FD](#)]

Ablauf des TUC

Nach Eingang der Anfrage MUSS der NCPeH-FD einen Non-Repudiation of Receipt Eintrag gemäß [[4.1.7.2 - Non-Repudiation of Receipt erstellen](#)] und einen Audit Trail Eintrag gemäß [[4.1.7.3 Patient Privacy Audit Trail Eintrag erstellen](#)] in der Komponente Audit

Repository speichern. Bei der Erstellung des Audit Trail Eintrages MUSS der NCPeH-FD die Vorgaben aus [eHDSI_XCPD_Profile#3.3] umsetzen. Wenn zum Zeitpunkt der Erstellung des Audit Trail Eintrags nicht alle erforderlichen Daten im NCPeH-FD verfügbar sind, MÜSSEN die Daten in den Audit Trail Eintrag aufgenommen werden, sobald sie im NCPeH-FD verfügbar sind, spätestens aber nachdem die Antwort an NCPeH Land-B gesendet wurde.

Die eingehende Anfrage MUSS dem Nachrichtentyp Patient Registry Find Candidates Query entsprechen, wie er in [eHDSI_XCPD_Profile#2.1] beschrieben ist.

Das Element QueryByParameter.responsePriorityCode aus der Anfrage MUSS den Wert "I" (Immediate) haben. Nur das Verarbeiten und Senden einer sofortigen Antwort ist zulässig. Falls das Element

QueryByParameter.responsePriorityCode einen anderen Wert als "I" enthält, MUSS der NCPeH-FD eine weitere Verarbeitung der Anfrage abbrechen und dem NCPeH Land-B mit der Fehlernachricht gemäß Vorgaben aus [ITI-55#3.55.4.1.3] antworten.

Der NCPeH-FD MUSS überprüfen, ob aus der XCPD-Anfrage die zwei livingSubjectID-Elemente die Prüfkriterien aus der Tabelle TAB_NCPeH_XCPD_Prüfkriterien_PSA erfüllen.

Tabelle 39: TAB_NCPeH_XCPD_Prüfkriterien_PSA

Element	Nutzungskonvention für Attribut root	Nutzungskonvention für Attribut extension
PRPA_IN201305UV02/controlActProcess/queryByParameter/parameterList/livingSubjectID/value	Der Wert des Attributs root MUSS identisch mit dem Wert der Variablen OID_KVNR_ASSIGNING_AUTHORITY sein.	Der Wert des Attributs extension MUSS gemäß Vorgaben aus [4.1.9- Format und Validierung der KVNR] geprüft und valide sein. Falls die Kriterien erfüllt sind, MUSS der Wert des Attributs extension in der lokalen Variable xcpd_kvnr zwischengespeichert werden.
PRPA_IN201305UV02/controlActProcess/queryByParameter/parameterList/livingSubjectID/value	Der Wert des Attributs root MUSS identisch mit dem Wert der Variablen OID_AC_ePKA_ASSIGNING_AUTHORITY sein.	Der Wert des Attributs extension MUSS folgende Kriterien erfüllen: <ul style="list-style-type: none"> • DARF NICHT leer sein, • DARF Sonderzeichen und Umlaute NICHT

		<p>enthalten,</p> <ul style="list-style-type: none"> MUSS eine Länge von sechs Zeichen haben. <p>Wenn die Kriterien erfüllt sind, dann MUSS der Wert des Attributs extension in der lokalen Variable xcpd_accesscode_e pka zwischengespeichert werden.</p>
--	--	---

Die Variablen OID_KVNR_ASSIGNING_AUTHORITY und OID_AC_ePKA_ASSIGNING_AUTHORITY sind im [4.1.1- Konfigurationsparameter] definiert.

Die KVNR und der Zugriffscode werden bei der Kommunikation mit dem ePA-Aktensystem verwendet, um das zugehörige ePA-Konto des Versicherten eindeutig ermitteln zu können. Durch die Übermittlung des Zugriffscode an das jeweilige ePA-Aktensystem des Versicherten wird dort geprüft, ob das europäische Mitgliedsland vom Versicherten ermächtigt ist, durch NCPeH-FD die ePKA-Daten des Versicherten abzurufen.

Der NCPeH-FD MUSS folgende Prüfschritte durchführen und bei Abweichung mit entsprechender Fehlermeldung (siehe Spalte Reason Encoding und acknowledgementDetail) an den NCPeH Land-B antworten und die weitere Verarbeitung der Anfrage abbrechen:

Tabelle 40: TAB_NCPeH_XCPD_Prüfschritte_Fehlermeldungen_PSA

Prüfschritt	Reason Encoding gemäß [eHDSI_XCPD_Profile #2.3.3]	acknowledgementDetail
<p>root-Attribute der folgenden Elemente aus der Anfrage MÜSSEN identisch mit dem Wert des Konfigurationsparameters HOME_COMMUNITY_ID_NCPeH-FD sein (siehe [4.1.1 - Konfigurationsparameter]):</p> <ul style="list-style-type: none"> PRPA_IN201305UV02/receiver/device/id PRPA_IN201305UV02/receiver/device/asAgent/representedOrganization/id (falls vorhanden). 	<pre><mitigatedBy typeCode="MITGT"> <detectedIssueManagement classCode="ACT" moodCode="ENV"> <code code="PolicyViolation" codeSystem="1.3.6.1.4.1.12559.11.10.1.3.2.2.1"/> </detectedIssueManagement> </mitigatedBy></pre>	<p>acknowledgement.typeCode= AA queryAck.queryResponseCode= AE acknowledgementDetail.Code= ERROR_PI_GENERIC acknowledgementDetail.Text = "Connection to Germany not allowed." acknowledgementDetail.Location = "The service request is incorrectly configured and is intended for a different country. Please contact your service provider or</p>

<p>Der Wert des Attributes PRPA_IN201305UV02/sender/device/id@root MUSS im Konfigurationsparameter WHITELIST_NCPeH_COUNTRY-B als HomeCommunityId des NCPeH Land-B enthalten sein (siehe [4.1.1 - Konfigurationsparameter]).</p>		<p>administrator."</p> <p>acknowledgement.typeCode= AA queryAck.queryResponseCode= AE acknowledgementDetail.Code= ERROR_PI_GENERIC acknowledgementDetail.Text = "Connection to Germany not allowed." acknowledgementDetail.Location = "There is currently no agreement with your country on the exchange of demographic data for the use of patient summary service."</p>
<p>Die XCPD-Anfrage MUSS ein livingSubjectID-Element mit einem Zugriffscode enthalten. Der Zugriffscode erfüllt die Prüfkriterien gemäß Tabelle TAB_NCPeH_XCPD_Prüfkriterien_PSA.</p>	<pre><mitigatedBy typeCode="MITGT"> <detectedIssueManagement classCode="ACT" moodCode="ENV"> <code code="PatientAuthenticationRequired" codeSystem="1.3.6.1.4.1.12559.11.10.1.3.2.2.1"/> </detectedIssueManagement> </mitigatedBy></pre>	<p>acknowledgement.typeCode= AA queryAck.queryResponseCode= AE acknowledgementDetail.Code= ERROR_PI_GENERIC acknowledgementDetail.Text = Patient Identification Error acknowledgementDetail.Location = "A respective access code has not been transmitted or has not been transmitted properly. Please ask the patient for access authorisation."</p>
<p>Die XCPD-Anfrage MUSS ein livingSubjectID-Element mit einer KVNR enthalten. Die KVNR erfüllt die Prüfkriterien gemäß Tabelle "TAB_NCPeH_XCPD_Prüfkriterien_PSA".</p>	<pre><triggerFor typeCode="TRIG"> <actOrderRequired classCode="ACT" moodCode="ENV"> <code code="DemographicsQueryNotAllowed" codeSystem="1.3.6.1</pre>	<p>acknowledgement.typeCode= AA queryAck.queryResponseCode= AE acknowledgementDetail.Code= ERROR_PI_GENERIC acknowledgementDetail.Text = Patient Identification</p>

	<pre> .4.1.12559.11.10.1. 3.2.2.1"/> </actOrderRequired> </triggerFor> </pre>	<p>Error acknowledgementDetail.Location = "Please make sure the health insurance number is correct."</p>
<p>Die XCPD-Anfrage DARF neben den livingSubjectID-Elementen für KVNR und Zugriffscode keine weiteren Identifikationsmerkmale enthalten. XCPD-Anfragen mit Elementen wie z. B. weitere livingSubjectID, livingSubjectName, livingSubjectBirthTime, livingSubjectAdministrativeGender oder patientAddress MÜSSEN abgelehnt werden.</p>	<pre> <mitigatedBy typeCode="MITGT"> <detectedIssueManagement classCode="ACT" moodCode="ENV"> <code code="PrivacyViolation" codeSystem="1.3.6.1 .4.1.12559.11.10.1. 3.2.2.1"/> </detectedIssueManagement> </mitigatedBy> </pre>	<p>acknowledgement.typeCode= AA queryAck.queryResponseCode= AE acknowledgementDetail.Code= ERROR_PI_GENERIC acknowledgementDetail.Text = Patient Identification Error acknowledgementDetail.Location = "Only the health insurance number and access code are acceptable for patient identification."</p>
<p>Die Bedingungen zur Erlangung einer Zugriffsberechtigung auf ePA-Aktensystem nach <u>[4.1.8- Festlegungen zur Prüfung der Zugriffsberechtigung auf Fachdienste der TI]</u> MÜSSEN erfüllt sein.</p>	<pre> <mitigatedBy typeCode="MITGT"> <detectedIssueManagement classCode="ACT" moodCode="ENV"> <code code="InsufficientRights" codeSystem="1.3.6.1 .4.1.12559.11.10.1. 3.2.2.1"/> </detectedIssueManagement> </mitigatedBy> </pre>	<p>acknowledgement.typeCode= AA queryAck.queryResponseCode= AE acknowledgementDetail.Code= ERROR_PI_GENERIC acknowledgementDetail.Text = Patient Identification Error acknowledgementDetail.Location = "Please check the access rights for your health professional role in your country."</p>
<p>Die Variable ida_healthcare_facility_type_code DARF NICHT leer sein und MUSS identisch mit einem der in [eHDSI_SAML_Profile#2.3] für das Identitätsattribut urn:ehdsi:names:subject:healthcare-facility-type angegeben Werte</p>		<p>acknowledgement.typeCode= AA queryAck.queryResponseCode= AE acknowledgementDetail.Code= ERROR_PI_GENERIC acknowledgementDetail.Text =</p>

<p>sein.</p>		<p>Patient Identification Error acknowledgementDetail.Location = "The type of your healthcare facility is missing or does not comply with the authorised type of healthcare facility."</p>
<p>Mindestens eine der Variablen ida_name-id oder ida_practitioner_role ist leer.</p>		<p>acknowledgement.typeCode= AA queryAck.queryResponseCode= AE acknowledgementDetail.Code= ERROR_HPI_INSUFFICIENT_INFORMATION acknowledgementDetail.Text = Patient Identification Error acknowledgementDetail.Location = "Information about the health professional are missing."</p>
<p>Die Variable ida_point_of_care ist leer.</p>		<p>acknowledgement.typeCode= AA queryAck.queryResponseCode= AE acknowledgementDetail.Code= ERROR_HPI_POC_NO_INFORMATION acknowledgementDetail.Text = Patient Identification Error acknowledgementDetail.Location = "No information has been provided about the name of the medical facility, where the patient care takes place."</p>

Hinweis: Die Variablen `ida_healthcare_facility_type_code`, `ida_name-id`, `ida_practitioner_role` und `ida_point_of_care` sind im [\[4.1.5 - Validierung der Identity Assertion des LE-EU\]](#) definiert.

Das folgende Beispiel eines Patient Demographics Query Request stellt das IHE XCPD-Profil des Interaktionstyps HL7 PRPA_IN201305UV02 dar. Die Nachricht enthält die Versichertenkennung (KVNR), mit der die zugehörigen demographischen Versichertendaten eindeutig ermittelt werden können, sowie den Zugriffscode, der in den nachgelagerten eHDSI-Anfragen zum Abruf von ePKA-Daten zu verwenden ist. Aus Gründen der Übersichtlichkeit enthält die Nachricht in dem `soapenv:Header-Element` keine Angaben zum Sicherheitsobjekt (Assertion), hierfür siehe [\[4.1.5 - Validierung der Identity Assertion des LE-EU\]](#).

```

<?xml version="1.0" encoding="UTF8" standalone="yes"?>
<Envelope>
  <Header> ... </Header>
  <Body>
    <PRPA_IN201305UV02 ITSVersion="XML_1.0"
      xmlns="urn:hl7-org:v3">
      <id extension="35423" root="1.2.840.114350.1.13.0.1.7.1.1"/>
      <creationTime value="20170922"/>
      <versionCode code="V3PR1"/>
      <interactionId extension="PRPA_IN201305UV02" root="2.16.840.1.113883.1.6"/>
      <processingCode code="P"/>
      <processingModeCode code="T"/>
      <acceptAckCode code="AL"/>
      <receiver typeCode="RCV">
        <device classCode="DEV" determinerCode="INSTANCE">
          <id root="1.2.276.0.76.4.291"/>
        </device>
      </receiver>
      <sender typeCode="SND">
        <device classCode="DEV" determinerCode="INSTANCE">
          <id root="2.16.17.710.803.1000.990.1"/>
        </device>
      </sender>
      <controlActProcess classCode="CACT" moodCode="EVN">
        <code code="PRPA_TE201305UV02" codeSystem="2.16.840.1.113883.1.6"/>
        <queryByParameter>
          <queryId extension="1.263507841149"
            root="1.2.840.114350.1.13.28.1.18.5.999"/>
          <statusCode code="new"/>
          <responseModalityCode code="R"/>
          <responsePriorityCode code="I"/>
          <matchCriterionList/>
          <parameterList>
            <!-- Zugriffscode -->
            <livingSubjectId>
              <value extension="A2C4E6" root="1.2.276.0.76.4.298"/>
              <semanticsText>LivingSubject.id</semanticsText>
            </livingSubjectId>
            <!-- Versichertenkennung (KVNR) -->
            <livingSubjectId>
              <value extension="B123456789" root="1.2.276.0.76.3.1.580.147"/>
              <semanticsText>LivingSubject.id</semanticsText>
            </livingSubjectId>
          </parameterList>
        </queryByParameter>
      </controlActProcess>
    </PRPA_IN201305UV02>
  </Body>
</Envelope>

```

Ausgabeparameter des TUC

Nach erfolgreicher Durchführung dieses TUC stehen folgende Ausgabeparameter zur Verfügung und können im entsprechenden Anwendungsfall verwendet werden:

- xcpd_kvnr
- xcpd_accesscode_epka

6.1.1.2 TUC_NCPeH_002: Patient Demographics Response für PS-A versenden

Für diesen TUC gelten folgende übergreifende Festlegungen

- [\[4.1.3- eHDSI Basisleistungen\]](#)
- [\[4.1.7.1 Non-Repudiation of Origin erstellen\]](#)
- [\[4.1.7.3- Patient Privacy Audit Trail Eintrag erstellen\]](#)

Ablauf des TUC

Der Inhalt und die Struktur der XCPD-Rückmeldung basiert auf der HL7 Patient Registry Find Candidates Query Response gemäß Vorgaben aus [\[eHDSI_XCPD_Profile#2.3\]](#).

Darüber hinaus MÜSSEN folgende Einschränkungen vom NCPeH-FD geprüft werden.

- Die XCPD-Rückmeldung MUSS ein Element `/PRPA_IN201306UV02/controlActProcess/subject/registrationEvent/subject1/patient` enthalten.
- `patient/id@extension` MUSS den Wert nach folgender Vorschrift enthalten:
 1. Der Wert des Parameters `patient_kvnr` (siehe [\[6.2.3- TUC_NCPeH_017: Demographische Versichertendaten aus NFD des ePKA MIO übernehmen\]](#))
 2. Der senkrechte Strich ohne Anführungszeichen: `"|"`
 3. Der Wert des Zugangscodes aus der XCPD-Anfrage, zwischengespeichert in der Variable `xcpd_accesscode_epka` (siehe [\[6.1.1.1- TUC_NCPeH_001: Patient Demographics Query Request für PS-A verarbeiten\]](#))

Beispiel für den gesamten Wert im Attribut `patient/id@extension`: `B123456789|A2C4E6`

- `patient/id@root` MUSS den Wert des Konfigurationsparameters `OID_KVNR_ASSIGNING_AUTHORITY` aus [\[4.1.1- Konfigurationsparameter\]](#) enthalten
- Der NCPeH-FD MUSS die ermittelten demographischen Versichertendaten aus [\[6.2.3- TUC_NCPeH_017: Demographische Versichertendaten aus NFD des ePKA MIO übernehmen\]](#) den untergeordneten Elementen des `patientPerson`-Elements entsprechend folgenden Regelungen zuordnen:

Element	Verwendungskonvention
<code>name/given</code>	<code>patient_vorname</code>
<code>name/family</code>	Der Wert des Element MUSS aus ermittelten Werten in folgender Reihenfolge bestehen, die Werte sind durch ein Leerzeichen getrennt:

	patient_namenszusatz patient_vorsatzwort patient_nachname
birthTime	patient_geburtsdatum Die Vorgaben zum Datumsformat MÜSSEN gemäß [IHE_XCPD_Profile] umgesetzt werden.

Die

Variablen patient_kvnr, patient_vorname, patient_prefix, patient_namenszusatz, patient_vorsatzwort, patient_nachname und patient_geburtsdatum sind im [6.2.3- TUC_NCPeH_017: Demographische Versichertendaten aus NFD des ePKA MIO übernehmen] definiert.

Der NCPeH-FD MUSS einen Non-Repudiation of Origin Eintrag gemäß [4.1.7.1 - Non-Repudiation of Origin erstellen] in der Komponente Audit Repository speichern.

Das folgende Beispiel einer Patient Demographics Response stellt das IHE XCPD-Profil des Interaktionstyps HL7 PRPA_IN201306UV02 dar. Die Nachricht enthält neben der KVNR des Versicherten auch die ermittelten demographischen Versichertendaten:

```

<?xml version="1.0" encoding="UTF8" standalone="yes"?>
<Envelope>
  <Header> ... </Header>
  <Body>
    <PRPA_IN201306UV02
      xmlns="urn:hl7-org:v3" ITSVersion="XML_1.0">
        <id extension="8432007378986" root="f6171fa9-2cdc-4dea-8796-5ec215ccc9af"/>
        <creationTime value="20170922105159.148+0000"/>
        <versionCode code="V3PR1"/>
        <interactionId extension="PRPA_IN201306UV02" root="2.16.840.1.113883.1.6"/>
        <processingCode code="P"/>
        <processingModeCode code="T"/>
        <acceptAckCode code="NE"/>
        <receiver typeCode="RCV">
          <device classCode="DEV" determinerCode="INSTANCE">
            <id root="2.16.17.710.803.1000.990.1"/>
          </device>
        </receiver>
        <sender typeCode="SND">
          <device classCode="DEV" determinerCode="INSTANCE">
            <id root="1.2.276.0.76.4.291"/>
          </device>
        </sender>
        <acknowledgement>
          <typeCode code="AA"/>
          <targetMessage>
            <id extension="35423" root="1.2.840.114350.1.13.0.1.7.1.1"/>
          </targetMessage>
        </acknowledgement>
        <controlActProcess classCode="CACT" moodCode="EVN">
          <code code="PRPA_TE201306UV02"/>
          <subject typeCode="SUBJ">
            <registrationEvent classCode="REG" moodCode="EVN">
              <id nullFlavor="NA"/>
              <statusCode code="active"/>
              <subject1 typeCode="SBJ">
                <patient classCode="PAT">
                  <id extension="B123456789|A2C4E6"
root="1.2.276.0.76.3.1.580.147"/>
                  <statusCode code="active"/>
                  <patientPerson classCode="PSN" determinerCode="INSTANCE">
                    <name>
                      <family>Gräfin von Oberberg</family>
                      <given>Johanna</given>
                    </name>
                    <birthTime value="19820515"/>
                  </patientPerson>
                  <subjectOf1>
                    <queryMatchObservation classCode="OBS" moodCode="EVN">
                      <code code="IHE_PDQ"
codeSystem="2.16.840.1.113883.1.11.19914"/>
                      <value xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance"
                          value="MATCH" xsi:type="INT"/>
                    </queryMatchObservation>
                  </subjectOf1>
                </patient>
              </subject1>
            </registrationEvent>
          </subject>
        </queryAck>
        <queryAck>
          <queryId root="1.263507841149"/>
          <queryResponseCode code="OK"/>
        </queryAck>
        <queryByParameter>
          <queryId root="1.263507841149"/>
          <statusCode code="new"/>
          <parameterList>
            <livingSubjectId>
              <value extension="A2C4E6" root="1.2.276.0.76.4.298"/>
              <semanticsText>LivingSubject.id</semanticsText>
            </livingSubjectId>
            <livingSubjectId>

```

Ausgabeparameter des TUC

Dieser TUC hat keine Ausgabeparameter.

6.1.1.3 TUC_NCPeH_023: Patient Demographics Query Request für ePeD-A verarbeiten

Für diesen TUC gelten folgende übergreifende Festlegungen

- [[4.1.1 - Konfigurationsparameter](#)]
- [[4.1.2 - Datenaustausch mit zugelassenen EU-Ländern](#)]
- [[4.1.3 - eHDSI Basisleistungen](#)]
- [[4.1.5 - Validierung der Identity Assertion des LE-EU](#)]
- [[4.1.7 - Non-Repudiation und Audit Trail Schemas](#)]
- [[4.1.8 - Festlegungen zur Prüfung der Zugriffsberechtigung auf Fachdienste der TI](#)]
- [[4.1.9- Format und Validierung der KVNR](#)]
- [[4.2.1 - Schnittstellen zu Diensten der zentralen TI](#)]
- [[4.2.9 - Elektronische Identitäten des NCPeH-FD](#)]

Ablauf des TUC

Nach Eingang der Anfrage MUSS der NCPeH-FD einen Non-Repudiation of Receipt Eintrag gemäß [4.1.7.2 - Non-Repudiation of Receipt erstellen] und einen Audit Trail Eintrag gemäß [4.1.7.3 - Patient Privacy Audit Trail Eintrag erstellen] in der Komponente Audit Repository speichern. Bei der Erstellung des Audit Trail Eintrages MUSS der NCPeH-FD die Vorgaben aus [eHDSI_XCPD_Profile#3.3] umsetzen. Wenn zum Zeitpunkt der Erstellung des Audit Trail Eintrags nicht alle erforderlichen Daten im NCPeH-FD verfügbar sind, MÜSSEN die Daten in den Audit Trail Eintrag aufgenommen werden, sobald sie im NCPeH-FD verfügbar sind, spätestens aber nachdem die Antwort an NCPeH Land-B gesendet wurde.

Die eingehende Anfrage MUSS dem Nachrichtentyp Patient Registry Find Candidates Query entsprechen, wie er in [eHDSI_XCPD_Profile#2.1] beschrieben ist.

Das Element QueryByParameter.responsePriorityCode aus der Anfrage MUSS den Wert "I" (Immediate) haben. Nur das Verarbeiten und Senden einer sofortigen Antwort ist zulässig. Falls das Element

QueryByParameter.responsePriorityCode einen anderen Wert als "I" enthält, MUSS der NCPeH-FD eine weitere Verarbeitung der Anfrage abbrechen und dem NCPeH Land-B mit der Fehlernachricht gemäß Vorgaben aus [ITI-55#3.55.4.1.3] antworten.

Der NCPeH-FD MUSS überprüfen, ob die XCPD-Anfrage zwei livingSubjectID-Elemente und die zugehörigen Attribute die Prüfkriterien aus der Tabelle "TAB_NCPeH_XCPD_Prüfkriterien_ePeD-A" erfüllen.

Tabelle 41: TAB_NCPeH_XCPD_Prüfkriterien_ePeD-A

Element	Nutzungskonvention für Attribut root	Nutzungskonvention für Attribut extension
PRPA_IN201305UV02/controlActProcess/	Der Wert des	Der NCPeH-FD

<p>queryByParameter/parameterList/ livingSubjectID/value</p>	<p>Attributs root MUSS identisch mit dem Wert der Variablen <code>OID_KVNR_ASSIGNING_AUTHORITY</code> sein.</p>	<p>MUSS diesen Wert gemäß Vorgaben aus [4.1.9- Format und Validierung der KVNR] prüfen und validieren.</p> <p>Wenn die Prüfung und Validierung der KVNR erfolgreich war, MUSS der Wert des Attributs <code>extension</code> in der lokalen Variablen <code>xcpd_kvnr</code> zwischengespeichert werden.</p>
<p>PRPA_IN201305UV02/controlActProcess/ queryByParameter/parameterList/ livingSubjectID/value</p>	<p>Der Wert des Attributs root MUSS identisch mit dem Wert der Variablen <code>OID_AC_erp_ASSIGNING_AUTHORITY</code> sein.</p>	<p>Der Wert des Attributs <code>extension</code> MUSS folgende Kriterien erfüllen:</p> <ul style="list-style-type: none"> • DARF NICHT leer sein, • DARF Sonderzeichen und Umlaute NICHT enthalten, • MUSS eine Länge von sechs Zeichen haben. <p>Falls die Kriterien erfüllt sind, MUSS der Wert des Attributs <code>extension</code> in der lokalen Variablen <code>xcpd_accesscode_erp</code> zwischengespeichert werden.</p>

Die Variablen `OID_KVNR_ASSIGNING_AUTHORITY` und `OID_AC_erp_ASSIGNING_AUTHORITY` sind im [\[4.1.1 - Konfigurationsparameter\]](#) definiert.

Die KVNR und der Zugriffscode werden vom NCPeH-FD beim Zugriff auf E-Rezepte an den E-Rezept-FD übermittelt. Mit der KVNR kann der E-Rezept-FD die demographischen Versichertendaten und die einlösbaren E-Rezepte des Versicherten eindeutig ermitteln. Der Zugriffscode ist Teil der vom Versicherten erteilten Zugriffsberechtigung und wird im E-Rezept-FD gespeichert. Mit der Übermittlung des Zugriffscode wird dieser dort vom E-

Rezept-FD auf Gültigkeit geprüft, bevor der Zugriff auf angefragte E-Rezepte gestattet wird.

Der NCPeH-FD MUSS folgende Prüfschritte durchführen und bei Abweichung mit entsprechender Fehlermeldung (siehe Spalten Reason Encoding und Acknowledgement) an den NCPeH Land-B antworten und die weitere Verarbeitung der Anfrage abbrechen:

Tabelle 42: TAB_NCPeH_XCPD_Prüfschritte_Fehlermeldungen_ePeD-A

Prüfschritt	Reason Encoding (reasonOf-Element) gemäß [eHDSI_XCPD_Profile#2.3.3]	Acknowledgement
<p>Die Variable <code>tls_country</code> aus dem TLS-Zertifikat des NCPeH Land-B DARF NICHT leer sein (siehe [4.1.3.1 Sicherer Kanal: TESTA-ng und TLS]).</p>	<pre><mitigatedBy typeCode="MITGT "></pre>	<pre>acknowledgem t.typeCode= AA queryAck.queryR esponseCode= AE</pre>
<p>root-Attribute der folgenden Elemente aus der Anfrage MÜSSEN identisch mit dem Wert des Konfigurationsparameters <code>HOME_COMMUNITY_ID_NCPeH-FD</code> sein (siehe [4.1.1 - Konfigurationsparameter]):</p> <ul style="list-style-type: none"> • <code>PRPA_IN201305UV02/receiver/device/id</code> • <code>PRPA_IN201305UV02/receiver/device/asAgent/representedOrganization/id</code> (falls vorhanden). 	<pre><detectedIssueM anagement classCode="ACT" moodCode="ENV"> <code code="PolicyVio lation" codeSystem="1.3 .6.1.4.1.12559. 11.10.1.3.2.2.1 "/> </detectedIssue Management> </mitigatedBy></pre>	<pre>acknowledgem tDetail.Code= ER ROR_PI_GENERIC acknowledgem tDetail.Text = "Unknown receiver device id." acknowledgem tDetail.Location = "The service request is incorrectly configured and is intended for a different country. Please contact your service provider or administrator."</pre>
<p>Der Wert des Attributes <code>PRPA_IN201305UV02/sender/device/id@root</code> MUSS im Konfigurationsparameter <code>WHITELIST_NCPeH_COUNTRY-B</code> als <code>HomeCommunityId</code> des NCPeH Land-B enthalten sein (siehe [4.1.1 - Konfigurationsparameter]).</p>		<pre>acknowledgem t.typeCode= AA queryAck.queryR esponseCode= AE acknowledgem tDetail.Code= ER ROR_PI_GENERIC acknowledgem tDetail.Text = "Connection to Germany not</pre>

		<p>allowed." acknowledgementDetail.Location = "There is currently no agreement with your country on the exchange of demographic data for the use of ePrescription service."</p>
<p>Die Variable ida_permissions, falls sie nicht leer ist, MUSS alle Permission Codes gemäß Vorgaben aus [4.1.8 - Festlegungen zur Prüfung der Zugriffsberechtigung auf Fachdienste der TI] für den eHDSI Use Case "Patient Identification" enthalten.</p>	<pre><mitigatedBy typeCode="MITGT "> <detectedIssueManagement classCode="ACT" moodCode="ENV"> <code code="InsufficientRights" codeSystem="1.3.6.1.4.1.12559.11.10.1.3.2.2.1 "/> </detectedIssueManagement> </mitigatedBy></pre>	<p>acknowledgement.typeCode= AA queryAck.queryResponseCode= AE AEacknowledgementDetail.Code= ERROR_PI_GENERIC acknowledgementDetail.Text = Patient Identification Error acknowledgementDetail.Location = "Access is not permitted. Please check the access rights for your health professional role in your country."</p>
<p>Wenn die Variable ida_permissions leer ist, dann MÜSSEN die Bedingungen zur Erlangung einer Zugriffsberechtigung auf E-Rezept-FD nach [4.1.8 - Festlegungen zur Prüfung der Zugriffsberechtigung auf Fachdienste der TI] erfüllt sein.</p>		<p>acknowledgement.typeCode= AA queryAck.queryResponseCode= AE AEacknowledgementDetail.Code= ERROR_PI_GENERIC acknowledgementDetail.Text = Patient Identification Error</p>

		<p>acknowledgementDetail.Location = "Please check the access rights for your health professional role in your country."</p>
<p>Die XCPD-Anfrage MUSS ein livingSubjectID-Element mit einem Zugriffscode enthalten. Der Zugriffscode muss die Prüfkriterien aus der Tabelle "TAB_NCPeH_XCPD_Prüfkriterien_ePeD-A" erfüllen. Die Variable xcpd_accesscode_erp DARF NICHT leer sein.</p>	<pre><mitigatedBy typeCode="MITGT "> <detectedIssueManagement classCode="ACT" moodCode="ENV"> <code code="PatientAuthenticationRequired" codeSystem="1.3.6.1.4.1.12559.11.10.1.3.2.2.1 "/> </detectedIssueManagement> </mitigatedBy></pre>	<p>acknowledgement.typeCode= AA queryAck.queryResponseCode= AE acknowledgementDetail.Code= ERROR_PI_GENERIC acknowledgementDetail.Text = Patient Identification Error acknowledgementDetail.Location = "A respective access code has not been transmitted or has not been transmitted properly. Please ask the patient for an access authorisation."</p>
<p>Die XCPD-Anfrage MUSS ein livingSubjectID-Element mit einer KVNR enthalten. Die KVNR MUSS die Prüfkriterien aus der Tabelle "TAB_NCPeH_XCPD_Prüfkriterien_ePeD-A" erfüllen. Die Variable xcpd_kvnr DARF NICHT leer sein.</p>	<pre><triggerFor typeCode="TRIG" > <actOrderRequired classCode="ACT" moodCode="ENV"> <code code="DemographicsQueryNotAllowed" codeSystem="1.3.6.1.4.1.12559.11.10.1.3.2.2.1 "/></pre>	<p>acknowledgement.typeCode= AA queryAck.queryResponseCode= AE AEacknowledgementDetail.Code= ERROR_PI_GENERIC acknowledgementDetail.Text = Patient Identification error acknowledgementDetail.Location</p>

	<pre></actOrderRequired> </triggerFor></pre>	<pre>= "Please make sure the health insurant number is correct."</pre>
<p>Die XCPD-Anfrage DARF neben den zwei livingSubjectID-Elementen keine weitere Identifikationsmerkmale enthalten. XCPD-Anfragen mit Elementen wie z. B. weitere livingSubjectID, livingSubjectName, livingSubjectBirthTime, livingSubjectAdministrativeGender oder patientAddress MÜSSEN abgelehnt werden.</p>	<pre><mitigatedBy typeCode="MITGT" "> <detectedIssueManagement classCode="ACT" moodCode="ENV"> <code code="PrivacyViolation" codeSystem="1.3 .6.1.4.1.12559. 11.10.1.3.2.2.1" "/> </detectedIssueManagement> </mitigatedBy></pre>	<pre>acknowledgment.typeCode= AA queryAck.queryResponseCode= AE AEacknowledgmentDetail.Code= ERROR_PI_GENERIC acknowledgmentDetail.Text = Patient Identification Error acknowledgmentDetail.Location = "Only the health insurant number and access code are acceptable for patient identification ."</pre>
<p>Die Variable ida_healthcare_facility_type_code DARF NICHT leer sein und MUSS identisch mit einem der in [eHDSI_SAML_Profile#2.3] für das Identitätsattribut urn:ehdsi:names:subject:healthcare-facility-type angegebenen Werte sein.</p>	<pre><mitigatedBy typeCode="MITGT" "> <detectedIssueManagement classCode="ACT" moodCode="ENV"> <code code="InsufficientRights" codeSystem="1.3 .6.1.4.1.12559. 11.10.1.3.2.2.1" "/> </detectedIssueManagement> </mitigatedBy></pre>	<pre>acknowledgment.typeCode= AA queryAck.queryResponseCode= AE AEacknowledgmentDetail.Code= ERROR_PI_GENERIC acknowledgmentDetail.Text = Patient Identification Error acknowledgmentDetail.Location = "The type of your healthcare facility is missing or</pre>

		<p>does not comply with the authorised types of healthcare facilities."</p>
<p>Die Variablen ida_name-id und ida_practitioner_role DÜRFEN NICHT leer sein.</p>		<p>acknowledgement.typeCode= AA queryAck.queryResponseCode= AE acknowledgementDetail.Code= ERROR_HPI_INSUFFICIENT_INFORMATION acknowledgementDetail.Text = Patient Identification Error acknowledgementDetail.Location = "Information about the health professional are missing."</p>
<p>Die Variable ida_point_of_care DARF NICHT leer sein.</p>		<p>acknowledgement.typeCode= AA queryAck.queryResponseCode= AE acknowledgementDetail.Code= ERROR_HPI_POC_NO_INFORMATION acknowledgementDetail.Text = Patient Identification Error acknowledgementDetail.Location = "No information has been provided about the name of the medical facility, where the patient care</p>

		takes place."
<p>Die Variable ida_practitioner_name DARF nicht leer sein.</p>		<p>acknowledgement.typeCode= AA queryAck.queryResponseCode= AE acknowledgementDetail.Code= ERROR_HPI_POC_NO_INFORMATION acknowledgementDetail.Text = Patient Identification Error acknowledgementDetail.Location = "No information has been provided about the name of the health professional."</p>

Hinweis: Die Variablen ida_healthcare_facility_type_code, ida_name-id, ida_practitioner_name, ida_practitioner_role und ida_point_of_care sind im [[4.1.5 - Validierung der Identity Assertion des LE-EU](#)] definiert.

Das folgende Beispiel eines Patient Demographics Query Request stellt das IHE XCPD-Profil des Interaktionstyps HL7 PRPA_IN201305UV02 dar. Die Nachricht enthält eine Krankenversicherungsnummer (KVNR) sowie einen Zugriffscode. Aus Gründen der Übersichtlichkeit enthält das Beispiel in dem soapenv:Header-Element keine Angaben zum Sicherheitsobjekt (Assertion), (siehe [[4.1.5 - Validierung der Identity Assertion des LE-EU](#)]).

```

<?xml version="1.0" encoding="UTF8" standalone="yes"?>
<Envelope>
  <Header> ... </Header>
  <Body>
    <PRPA_IN201305UV02 ITSVersion="XML_1.0"
      xmlns="urn:hl7-org:v3">
      <id extension="35423" root="1.2.840.114350.1.13.0.1.7.1.1"/>
      <creationTime value="20170922"/>
      <versionCode code="V3PR1"/>
      <interactionId extension="PRPA_IN201305UV02" root="2.16.840.1.113883.1.6"/>
      <processingCode code="P"/>
      <processingModeCode code="T"/>
      <acceptAckCode code="AL"/>
      <receiver typeCode="RCV">
        <device classCode="DEV" determinerCode="INSTANCE">
          <id root="1.2.276.0.76.4.291"/>
        </device>
      </receiver>
      <sender typeCode="SND">
        <device classCode="DEV" determinerCode="INSTANCE">
          <id root="2.16.17.710.803.1000.990.1"/>
        </device>
      </sender>
      <controlActProcess classCode="CACT" moodCode="EVN">
        <code code="PRPA_TE201305UV02" codeSystem="2.16.840.1.113883.1.6"/>
        <queryByParameter>
          <queryId extension="1.263507841149"
            root="1.2.840.114350.1.13.28.1.18.5.999"/>
          <statusCode code="new"/>
          <responseModalityCode code="R"/>
          <responsePriorityCode code="I"/>
          <matchCriterionList/>
          <parameterList>
            <livingSubjectId>
              <value extension="B123456789" root="1.2.276.0.76.3.1.580.147"/>
              <semanticsText>LivingSubject.id</semanticsText>
            </livingSubjectId>
            <livingSubjectId>
              <value extension="A2C4E6" root="1.2.276.0.76.4.299"/>
              <semanticsText>LivingSubject.id</semanticsText>
            </livingSubjectId>
          </parameterList>
        </queryByParameter>
      </controlActProcess>
    </PRPA_IN201305UV02>
  </Body>
</Envelope>

```

Ausgabeparameter des TUC

Nach erfolgreicher Durchführung dieses TUC stehen folgende Ausgabeparameter zur Verfügung und können im entsprechenden Anwendungsfall verwendet werden:

- xcpd_kvnr
- xcpd_accesscode_erp

6.1.1.4 TUC_NCPeH_024: Patient Demographics Response mit demographischen Versichertendaten für ePeD-A versenden

Für diesen TUC gelten folgende übergreifende Festlegungen

- [[4.1.3 - eHDSI Basisleistungen](#)]
- [[4.1.7 - Non-Repudiation und Audit Trail Schemas](#)]

Ablauf des TUC

Der Inhalt und die Struktur der XCPD-Rückmeldung basiert auf der HL7 Patient Registry Find Candidates Query Response gemäß Vorgaben aus [eHDSI_XCPD_Profile#2.3].

Darüber hinaus MUSS der NCPeH-FD folgende Vorgaben umsetzen:

- Die XCPD-Rückmeldung DARF nur ein Element /PRPA_IN201306UV02/controlActProcess/subject/registrationEvent/subject1/patient enthalten.
- patient/id@extension MUSS den Wert nach folgender Vorschrift enthalten:
 1. den Wert des Parameters patient_kvnr,
 2. den senkrechte Strich ohne Anführungszeichen: "|",
 3. den Wert des Zugriffscode aus der XCPD-Anfrage, zwischengespeichert in der Variable xcpd_accesscode_erp (siehe [6.1.1.3- TUC_NCPeH_023: Patient Demographics Query Request für ePeD-A verarbeiten]).

Beispiel für den gesamten Wert des Attributs patient/id@extension: B123456789|A2C4E6

- patient/id@root muss den Wert des Konfigurationsparameters OID_KVNR_ASSIGNING_AUTHORITY enthalten (siehe [[4.1.1 - Konfigurationsparameter](#)]).
- Der NCPeH-FD MUSS die ermittelten demographischen Versichertendaten aus dem [6.2.4- TUC_NCPeH_035: Demographische Versichertendaten aus E-Rezept extrahieren] den untergeordneten Elementen des patientPerson-Elements entsprechend folgender Regelungen zuordnen:

Element	Verwendungskonvention
name/given	Der Wert der Variable patient_vorname MUSS in das Element übernommen werden.
name/family	Der Wert des Elementes MUSS aus ermittelten Werten in folgender Reihenfolge bestehen, die Werte sind durch ein Leerzeichen getrennt: patient_prefix patient_namenszusatz patient_vorsatzwort

	patient_nachname.
birthTime	Der Wert der Variable patient_geburtsdatum MUSS in das Element übernommen werden. Die Vorgaben zum Datumsformat MÜSSEN gemäß [IHE_XCPD_Profile] eingehalten werden.

Die Variablen patient_kvnr, patient_vorname, patient_prefix, patient_namenszusatz, patient_vorsatzwort, patient_nachname und patient_geburtsdatum sind im [6.2.4- TUC_NCPeH_035: Demographische Versichertendaten aus E-Rezept extrahieren] definiert.

Der NCPeH-FD MUSS einen Non-Repudiation of Origin Eintrag gemäß [4.1.7.1 - Non-Repudiation of Origin erstellen] in der Komponente Audit Repository speichern.

Das folgende Beispiel einer Patient Demographics Response stellt das IHE XCPD-Profil des Interaktionstyps HL7 PRPA_IN201306UV02 dar. Die Nachricht enthält neben der KVNR des Versicherten auch die ermittelten demographischen Versichertendaten:

```

<?xml version="1.0" encoding="UTF-8"?>
<PRPA_IN201306UV02>
  <id extension="5221910906" root="5ff741d0-f87d-43c1-b239-811d8b13cb0b"/>
  <creationTime value="20230927104903.031+0000"/>
  <versionCode code="V3PR1"/>
  <interactionId extension="PRPA_IN201306UV02" root="2.16.840.1.113883.1.6"/>
  <processingCode code="P"/>
  <processingModeCode code="T"/>
  <acceptAckCode code="NE"/>
  <receiver typeCode="RCV">
    <device classCode="DEV" determinerCode="INSTANCE">
      <id root="2.16.17.710.803.1000.990.1"/>
      <asAgent classCode="AGNT">
        <representedOrganization classCode="ORG" determinerCode="INSTANCE">
          <id root="2.16.17.710.803.1000.990.1"/>
        </representedOrganization>
      </asAgent>
    </device>
  </receiver>
  <sender typeCode="SND">
    <device classCode="DEV" determinerCode="INSTANCE">
      <id root="1.2.276.0.76.4.291"/>
    </device>
  </sender>
  <acknowledgement>
    <typeCode code="AA"/>
    <targetMessage>
      <id extension="35423" root="1.2.840.114350.1.13.0.1.7.1.1"/>
    </targetMessage>
  </acknowledgement>
  <controlActProcess classCode="CACT" moodCode="EVN">
    <code code="PRPA_TE201306UV02"/>
    <subject typeCode="SUBJ">
      <registrationEvent classCode="REG" moodCode="EVN">
        <id nullFlavor="NA"/>
        <statusCode code="active"/>
        <subject1 typeCode="SBJ">
          <patient classCode="PAT">
            <id extension="B123456789|A2C4E6" root="1.2.276.0.76.3.1.580.147"/>
            <statusCode code="active"/>
            <patientPerson classCode="PSN" determinerCode="INSTANCE">
              <name>
                <family>Gräfin von Oberberg</family>
                <given>Johanna</given>
              </name>
              <birthTime value="19820515"/>
            </patientPerson>
            <subjectOf1>
              <queryMatchObservation classCode="OBS" moodCode="EVN">
                <code code="IHE_PDQ"
                  codeSystem="2.16.840.1.113883.1.11.19914"/>
                <value value="100" xsi:type="INT"/>
              </queryMatchObservation>
            </subjectOf1>
          </patient>
        </subject1>
        <custodian typeCode="CST">
          <assignedEntity classCode="ASSIGNED">
            <id root="2.16.17.710.820.1000.990.1"/>
            <code code="NotHealthDataLocator"
              codeSystem="1.3.6.1.4.1.19376.1.2.27.2"/>
          </assignedEntity>
        </custodian>
      </registrationEvent>
    </subject>
    <queryAck>
      <queryId root="1.263507841149"/>
      <statusCode code="OK"/>
      <queryResponseCode code="OK"/>
    </queryAck>
    <queryByParameter>
      <queryId root="1.263507841149"/>
      <statusCode code="new"/>
    </queryByParameter>
  </controlActProcess>

```

Ausgabeparameter des TUC

- Dieser TUC hat keine Ausgabeparameter.

6.1.2 Operation Cross_Gateway_Query::FindDocuments

Tabelle 43: TAB_NCPeH_Cross_Gateway_Queries

Operation	Cross_Gateway_Query::FindDocuments	
Beschreibung	Diese Operation wird aufgerufen, wenn das Initiating Gateway (NCPeH Land-B) ein Ereignis vom behandelnden LE-EU empfängt und die Anfrage an die Operation sendet. Die Operation MUSS vom Responding Gateway (NCPeH-FD) gemäß den Vorgaben aus [eHDSI_XCA_Profile] implementiert und NCPeH Land-B zur Nutzung in der eHDSI bereitgestellt werden. Der NCPeH-FD MUSS die Anfrage verwenden, um semantische Bezeichnungen oder Identifikatoren über die verfügbaren Gesundheitsdatensätze (z.B. ePKA MIO, E-Rezepte) des Versicherten aus dem zum jeweiligen Anwendungsszenario passenden Fachdienst der TI zu ermitteln und sie dem NCPeH Land-B mit der Antwort-Nachricht zu senden.	
Eingangsparameter		
Name	Beschreibung	Typ
Cross Gateway Query Request	Eingangsnachricht zur Abfrage von Metadaten der verfügbaren Versichertendatensätze gemäß [eHDSI_XCA_Profile#2.1]	AdhocQueryRequest [ITI-38]
X-User Assertion	Authentication Assertion des anfragenden LE-EU	SAML 2.0 Assertion gemäß [eHDSI_SAML_Profile#2] inkl. X.509 öffentliches Signaturzertifikat des NCPeH Land-B [eHDSI_X.509_Certificates_Profile]
TRC Assertion	Bestätigung über das Bestehen einer Behandlungsbeziehung zwischen LE-EU und Versichertem	SAML 2.0 Assertion gemäß [eHDSI_SAML_Profile#4] inkl. X.509 öffentliches Signaturzertifikat des NCPeH Land-B [eHDSI_X.509_Certificates_Profile]
Ausgangsparameter		
Name	Beschreibung	Typ
Cross Gateway Query	Ausgangsnachricht gemäß [eHDSI_XCA_Profile#2.2]	AdhocQueryResponse [ITI-38]

Response		
-----------------	--	--

Die eHDSI klassifiziert die Anwendungsszenarien bzw. Dokumentenklassen auf der Grundlage von so genannten semantischen Signifiers. Daher MUSS der NCPeH-FD in der Lage sein, die auf LOINC-Codes abgebildeten semantischen eHDSI-Signifiers aus der XCA.FindDocuments-Anfrage (siehe XSDDocumentEntryClassCode) eindeutig zu erkennen, um sie dem entsprechenden Anwendungsszenario zuordnen zu können. In der Anfrage MUSS die Information über das Klassifikationsschema des Signifiers mit der OID 2.16.840.1.113883.6.1 identisch sein. Der Wert des Parameters XSDDocumentEntryClassCode MUSS folgendem Format entsprechen:

1. "("
 2. Ein LOINC-Code
 3. "^^"
 4. "2.16.840.1.113883.6.1"
 5. ")"
- Beispiel: ('60591-5^^2.16.840.1.113883.6.1')

Die folgende Tabelle enthält Kriterien für die Zuordnungen von IHE XCA-Anfragen zu den entsprechenden TUCs, in denen die Anfragen durch den NCPeH-FD weiterverarbeitet werden.

Tabelle 44: TAB_NCPeH_Kriterien_Zuordnung_IHE-XCA.Query_Anfragen_zu_Anwendungsszenarien

XSDDocumentEntryClassCode	Technischer Use Case (TUC)
60591-5	[6.1.2.1- TUC_NCPeH_003: Cross Gateway Query Request für PS-A verarbeiten] Anwendungsszenario: Patient Summary Land-A
57833-6	[6.1.2.3- TUC_NCPeH_025: Cross Gateway Query Request für ePeD-A verarbeiten] Anwendungsszenario: ePrescription/eDispensation Land-A
Ein anderer Code oder das Format des XSDDocumentEntryClassCode entspricht nicht den oben genannten Vorgaben für die Inhaltsstruktur	<p>ERROR_GENERIC_SERVICE_SIGNIFIER_UNKNOWN Anwendungsszenario: nicht bekannt</p> <p>Der NCPeH-FD DARF die Anfrage NICHT weiterverarbeiten und MUSS dem NCPeH Land-B mit dem Fehlercode antworten.</p> <p>Nach Versand der Fehlernachricht MUSS der NCPeH-FD einen Non-Repudiation of Origin Eintrag gemäß [4.1.7.1 Non-Repudiation of Origin erstellen] in die Komponente Audit Repository speichern. Bei der Vervollständigung des Patient Privacy Audit Trail Eintrages MÜSSEN Vorgaben aus [eHDSI_XCA_Profile#4.3] umgesetzt werden.</p>

6.1.2.1 TUC_NCPeH_003: Cross Gateway Query Request für PS-A verarbeiten

Für diesen TUC gelten folgende übergreifende Festlegungen

- [[4.1.2 - Datenaustausch mit zugelassenen EU-Ländern](#)]
- [[4.1.3- eHDSI Basisleistungen](#)]
- [[4.1.5- Validierung der Identity Assertion des LE-EU](#)]
- [[4.1.6- Validierung der TRC Assertion](#)]
- [[4.1.7.2- Non-Repudiation of Receipt erstellen](#)]
- [[4.1.7.3- Patient Privacy Audit Trail Eintrag erstellen](#)]
- [[4.1.8- Festlegungen zur Prüfung der Zugriffsberechtigung auf Fachdienste der TI](#)]
- [[4.1.9- Format und Validierung der KVNR](#)]

Ablauf des TUC

Der NCPeH-FD MUSS die Umsetzung der Operation Cross_Gateway_Query::FindDocuments gemäß den Vorgaben, Einschränkungen und der definierten Ablauflogik in [eHDSI_XCA_Profile] implementieren.

Nach Eingang der Anfrage MUSS der NCPeH-FD einen Non-Repudiation of Receipt Eintrag gemäß [4.1.7.2 - Non-Repudiation of Receipt erstellen] und einen Audit Trail Eintrag gemäß [4.1.7.3 - Patient Privacy Audit Trail Eintrag erstellen] in der Komponente Audit Repository speichern. Bei der Erstellung des Audit Trail Eintrages müssen Vorgaben aus [eHDSI_XCA_Profile#4.3] umgesetzt werden. Wenn zum Zeitpunkt der Erstellung des Audit Trail Eintrags nicht alle erforderlichen Daten im NCPeH-FD verfügbar sind, MÜSSEN die Daten in den Audit Trail Eintrag aufgenommen werden, sobald sie im NCPeH-FD verfügbar sind, spätestens nach dem Versand der Antwort an NCPeH Land-B.

Der NCPeH-FD MUSS Inhalte des Parameters XSDDocumentEntryPatientId aus der Anfrage auf folgende Kriterien prüfen:

- Der Wert des Parameters XSDDocumentEntryPatientId muss inhaltlich nach der folgenden Vorschrift strukturiert sein:
 1. ""
 2. Der unveränderbare Teil der KVNR des Versicherten (10 Stellen)
Der Wert MUSS gemäß Vorgaben aus [4.1.9- Format und Validierung der KVNR] geprüft und valide sein.
 3. Der senkrechte Strich ohne Anführungszeichen: "|"
 4. 6-stelliger Zugriffscode
 5. "^^^&";
 6. Wert des Konfigurationsparameters OID_KVNR_ASSIGNING_AUTHORITY aus dem [4.1.1- Konfigurationsparameter]
 7. "&ISO"

Beispiel des Wertes: 'B123456789|
A2C4E6^^^&;1.2.276.0.76.3.1.580.147&ISO'

- Der Wert des Parameters muss mit Hochkomma beginnen und enden

- Die in dem Parameter enthaltene Versichertenkennung muss identisch mit dem Wert der Variable `trc_kvnr` (siehe [4.1.6- Validierung der TRC Assertion]) sein
- Der in dem Parameter enthaltene Zugriffscode muss identisch mit dem Wert der Variable `trc_accesscode` (siehe [4.1.6- Validierung der TRC Assertion]) sein
- Die im Parameter enthaltene OID muss identisch mit dem Wert des Konfigurationsparameters `OID_KVNR_ASSIGNING_AUTHORITY` (siehe [4.1.1- Konfigurationsparameter]) sein.

Falls es bei der Prüfung der oben angegebenen Kriterien zu Fehlern bzw. Abweichungen kommt, MUSS der NCPeH-FD eine weitere Verarbeitung der Anfrage abbrechen und dem NCPeH Land-B mit einer Fehlernachricht antworten. Neben Vorgaben zur Fehlerbehandlung aus [eHDSI_XCA_Profile#2.2.3] und [eHDSI_NCPeH_Components#6.4] MUSS der NCPeH-FD beim Auftreten von Fehlerbedingungen folgende Zuordnung von Fehlernachrichten umsetzen:

Tabelle 45: TAB_NCPeH_XCA_QUERY_Fehlerbedingungen_Fehlercodes_PS-A

Fehlerbedingung	errorCode gemäß [eHDSI_NCPeH_Components#6.4]	codeContext	severity	location
Die Validierungsprüfung der Versichertenkennung aus dem Wert des <code>XSDocumentEntryPatientId</code> ist gemäß Vorgaben aus [4.1.9- Format und Validierung der KVNR] nicht erfolgreich.	ERROR_PS_GENERIC	"Please make sure that the health insurant identifier is correct."	urn:oasis:names:tc:ebxml-regrep:ErrorSeverityType:Error	"Received XSDocumentEntryPatientId=" + Wert aus dem <code>XSDocumentEntryPatientId-Slot</code>
Die Versichertenkennung aus dem Wert des <code>XSDocumentEntryPatientId</code> ist nicht identisch mit der KVNR aus TRC Assertion (siehe Variable <code>trc_kvnr</code>).				
Die OID aus dem Parameter <code>XSDocumentEntryPatientId</code> ist nicht identisch mit dem Wert des Konfigurationsparameters <code>OID_KVNR_ASSIGNING</code>		"Unknown type of health insurant identifier. Please		"The service request is incorrectly configured for the health insurant identifier. Received OID of <code>XSDocumentEntryPatientId-Slot</code> =

<p>_AUTHORITY (siehe [4.1.1 - Konfigurationsparameter]).</p>		<p>contact your service provider or administrator."</p>		<p>" + der Wert der OID aus dem Slot XSDocumentEntry PatientId</p>
<p>Der Wert für den Zugriffscode aus dem Element des XSDocumentEntryPatientId ist nicht identisch mit dem Wert der Variable trc_accesscode oder trc_accesscode ist leer.</p>		<p>"Access denied. The patient's access code is missing or malformed. Please ask the patient for access authorization and the proper access code."</p>		<p>Keine Angaben</p>
<p>Die Variable tls_country aus dem TLS-Zertifikat des NCPeH Land-B DARF NICHT leer sein (siehe [4.1.3.1 Sicherer Kanal: TESTA-ng und TLS]) und MUSS in der WHITELIST_NCPeH_COUNTRY-B nach [4.1.2 "Datenaustausch mit zugelassenen EU-Ländern"] enthalten sein.</p>		<p>"The german patient summary service is not agreed with the requesting country. Please contact your service provider or administrator."</p>		<p>"The DN structure in the subject of the received TLS certificate does not contain a valid EU country code or the addressed service is not agreed between the requesting country and germany. Received country code= " + Wert der Variable tls_country</p>
<p>Die Variable</p>		<p>"Access</p>		<p>"Received</p>

<p>ida_permissions, falls sie nicht leer ist, enthält nicht alle Permission Codes gemäß Vorgaben aus [4.1.8- Festlegungen zur Prüfung der Zugriffsberechtigung auf Fachdienste der TI] für den eHDSI Use Case "Request for Patient Summary".</p>		<p>denied. Please contact your service provider or administrator and check the access rights for your health professional role in your country."</p>	<p>permission codes=" + Wert der Variable ida_permissions</p>
<p>Die Variable ida_permissions ist leer und die Bedingungen zur Erlangung einer Zugriffsberechtigung auf ePA-Aktensysteme nach [4.1.8- Festlegungen zur Prüfung der Zugriffsberechtigung auf Fachdienste der TI] sind nicht erfüllt.</p>		<p>"Access denied. The information provided about the role of the health professional does not comply with German regulations."</p>	<p>"No permission codes received and the access cannot be granted for the received practitioner role code in accordance with national regulations. Received practitioner role code=" + Wert der Variable ida_practitioner_role_code</p>
<p>Die Variable ida_name-id ist leer.</p>	<p>ERROR_HPI_INSUFFICIENT_INFORMATION</p>	<p>"Access denied. The identifier of the health professional is missing in the</p>	<p>Keine Angaben</p>

		provide d identit y informa tion."		
Die Variable ida_practitioner_r ole ist leer.		"Access denied. The informa tion about the role of EU health profess ional is missing in the provide d identit y informa tion."		Keine Angaben
Die Variable ida_practitioner_n ame ist leer.		"Access denied. The name of the EU health profess ional is missing in the provide d identit y informa tion."		Keine Angaben
Der Wert der Variable ida_practitioner_r ole_code ist leer oder dieser ist nicht identisch mit einem der möglichen Werte für das Element urn:oasis:names:tc :xacml:2.0:subject		"Access denied. Missing or unknown role of the EU health profess		"Received role code from the identity assertion of health professional; see element urn:oasis:n ames:tc:xacml:2.0: subject:role= " + Wert der

<p>:role aus [eHDSI_SAML_Profile #2.3].</p>		<p>ional in the provided identity information."</p>	<p>Variable ida_practitioner_role_code</p>
<p>Die Variable ida_point_of_care ist leer.</p>	<p>ERROR_HPI_POC_NO_INFORMATION</p>	<p>"Access denied. Missing name of the point of care in the provided identity information."</p>	<p>Keine Angaben</p>
<p>Der Wert der Variable ida_healthcare_facility_type_code ist leer oder nicht identisch mit einem der vorgegebenen Werte aus [eHDSI_SAML_Profile #2.3] für das Identitätsattribut urn:ehdsi:names:subject:healthcare-facility-type.</p>		<p>"Access denied. Missing or unknown type of Healthcare Provider Organization in the provided identity information."</p>	<p>"Received healthcare facility type=" + Wert der Variable ida_healthcare_facility_type_code</p>

<p>Das Element XSDDocumentEntryStatus enthält einen Wert der mit dem vorgeschriebenen Wert gemäß [eHDSI_XCA_Profile#2.1] nicht identisch ist.</p>	<p>ERROR_INCORRECT_FORMATTING</p>	<p>"The requested document status for patient summary is not supported."</p>	<p>"The value ofXSDDocumentEntryStatus does not correspond to the required value from [eHDSI_XCA_Profile#2.1]. Received value of XSDDocumentEntryStatus=" + der Wert aus dem Element XSDDocumentEntryStatus</p>
<p>Wenn das Element XSDDocumentEntryFormatCode angegeben ist und der Wert des Elementes entspricht keinem der Werten urn:epsos:ps:ps:2010 oder urn:ihe:iti:xds-sd:pdf:2008.</p>		<p>"The requested format for patient summary is not supported."</p>	<p>"Received XSDDocumentEntryFormatCode= " + der Wert aus dem Element XSDDocumentEntryFormatCode</p>
<p>Der classCode des XSDDocumentEntryClassCode ist nicht identisch mit dem Wert 57833-5.</p>	<p>ERROR_GENERIC_SERVICE_SIGNIFIER_UNKNOWN</p>	<p>"Unknown service . Please contact your service provider or administrator."</p>	<p>"Received XSDDocumentEntryClassCode= " + der Wert aus dem Element XSDDocumentEntryClassCode</p>
<p>Das Format des XSDDocumentEntryClassCode entspricht nicht den oben genannten Anforderungen an die inhaltliche Struktur.</p>			

Hinweis: Die Initiierung der Variablen ida_healthcare_facility_type_code, ida_name-id, ida_practitioner_role und ida_point_of_care erfolgt im [4.1.5- Validierung der Identity Assertion des LE-EU] und die Variablen trc_kvnr und trc_accesscode im [4.1.6- Validierung der TRC Assertion].

Das folgende Beispiel zeigt die Struktur der Cross Gateway Query Anfrage:

```

<?xml version="1.0" encoding="UTF8" standalone="yes"?>
<Envelope>
  <Header> ... </Header>
  <Body>
    <AdhocQueryRequest>
      <ResponseOption returnComposedObjects="true" returnType="LeafClass"/>
      <AdhocQuery id="urn:uuid:14d4debf-8f97-4251-9a74-a90016b0af0d">
        <Slot name="$XDSDocumentEntryPatientId">
          <ValueList>
            <Value>'B123456789|
A2C4E6^^^&amp;1.2.276.0.76.3.1.580.147&amp;ISO'</Value>
          </ValueList>
        </Slot>
        <Slot name="$XDSDocumentEntryStatus">
          <ValueList>
<Value>('urn:oasis:names:tc:ebxml-regrep:StatusType:Approved')</Value>
          </ValueList>
        </Slot>
        <Slot name="$XDSDocumentEntryClassCode">
          <ValueList>
            <Value>('60591-5^^2.16.840.1.113883.6.1')</Value>
          </ValueList>
        </Slot>
      </AdhocQuery>
    </AdhocQueryRequest>
  </Body>
</Envelope>

```

Ausgabeparameter des TUC

Nach erfolgreicher Durchführung dieses TUC stehen folgende Ausgabeparameter zur Verfügung und können im entsprechenden Anwendungsfall verwendet werden:

- KVNR
- Zugriffscode

6.1.2.2 TUC_NCPeH_004: Cross Gateway Query Response für PS-A versenden

Für diesen TUC gelten folgende übergreifende Festlegungen

- [4.1.3- eHDSI Basisleistungen]
- [[4.1.7.1 Non-Repudiation of Origin erstellen](#)]
- [4.1.7.3- Patient Privacy Audit Trail Eintrag erstellen]

Ablauf des TUC

Der NCPeH-FD MUSS die Inhalte und Struktur der XCA.Query-Antwort nach Vorgaben aus [eHDSI_XCA_Profile#2.2] umsetzen. Zusätzlich müssen Vorgaben gemäß

[ebRIM_Representation_DocumentEntry#4.2.3.2] zur Erstellung von DocumentEntry-Elementen und -Attributen beachtet werden.

Der NCPeH-FD MUSS für das ePKA MIO des Versicherten zwei ExtrinsicObject-Elemente erstellen. Das eine ExtrinsicObject-Element MUSS das Name-Subelement mit dem Wert "Patient Summary PDF/A document" enthalten. Das zweite ExtrinsicObject-Element MUSS das Name-Subelement mit dem Wert "Patient Summary coded document" enthalten. Darüber hinaus MÜSSEN in beiden ExtrinsicObject-Elementen für Subelemente die Nutzungskonventionen gemäß der Tabelle Nutzungskonvention_Erstellung_XCA.Query-Response_PS beachtet werden.

Tabelle 46: TAB_NCPeH_Nutzungskonvention_Erstellung_XCA.Query_Response_PS-A

Element in der Query Response	Nutzungskonvention
status	siehe Vorgaben für das Element in [eHDSI_NCPeH_Components#3.1.4.2.3]
contentType	siehe Vorgaben für das Element in [eHDSI_NCPeH_Components#3.1.4.2.3]
VersionInfo	siehe Vorgaben für das Element in [eHDSI_NCPeH_Components#3.1.4.2.3]
sourcePatientId	MUSS den Wert der Variable METADATA_ePKA_MIO_patientId (siehe [6.2.1- TUC_NCPeH_013: Metadatenattribute des ePKA MIO abrufen]) enthalten + " " + Wert des Zugriffscode aus der TRC Assertion (siehe Variable trc_accesscode im [4.1.6- Validierung der TRC Assertion]) + "^^^&" + der OID-Wert aus dem Parameter XSDocumentEntryPatientId des XCA.Query Request (siehe [6.1.2.1- TUC_NCPeH_003: Cross Gateway Query Request für PS-A verarbeiten]) + "& ISO" Beispiel: B123456789 A2C4E6^^^&;1.2.276.0.76.3.1.580.147&; ISO
creationTime	MUSS den Wert der Variable METADATA_ePKA_MIO_creationTime aus [6.2.1- TUC_NCPeH_013: Metadatenattribute des ePKA MIO abrufen] enthalten
repositoryUniqueId	MUSS den Wert der Variable METADATA_ePKA_MIO_repositoryUniqueId aus [6.2.1- TUC_NCPeH_013: Metadatenattribute des ePKA MIO abrufen] enthalten
Description	Für die Dokumentenreferenz "Patient Summary PDF/A document" (eHDSI CDA L1), dann: "The Patient Summary document (CDA L1 / PDF) for patient" + Wert der Variable METADATA_ePKA_MIO_patientId

	<p>Beispiel: The Patient Summary document (CDA L1 / PDF) for patient B123456789</p> <p>Für die Dokumentenreferenz "Patient Summary coded document" (eHDSI CDA L3), dann: "The Patient Summary document (CDA L3 / Structured body) for patient" + Wert der Variable METADATA_ePKA_MIO_patientId</p> <p>Beispiel: The Patient Summary document (CDA L3 / Structured body) for patient B123456789</p>
classCode	Es ist eine Klassifikation und MUSS den Wert 60591-5 enthalten. Der Wert 60591-5 ist ein Code aus dem Codesystem LOINC und hat den Display Name "Patient summary Document" (siehe [LOINC_Patient_Summary]).
confidentialityCode	siehe Vorgaben für das Element in [eHDSI_NCPeH_Components#3.1.4.2.3]
typeCode	Es ist eine Klassifikation und MUSS den Wert 60591-5 enthalten. Der Wert 60591-5 ist ein Code aus dem Codesystem LOINC und hat den Display Name "Patient Summary Document" (siehe [LOINC_Patient_Summary]).
formatCode	<p>Für die Dokumentenreferenz "Patient Summary PDF/A document" (eHDSI CDA L1) MUSS urn:epsos:ps:ps:2010 übernommen werden.</p> <p>Für die Dokumentenreferenz "Patient Summary coded document" (eHDSI CDA L3) MUSS urn:ihe:iti:xds-sd:pdf:2008 übernommen werden.</p>
patientId	Siehe die Nutzungskonvention für das Element sourcePatientId
healthcareFacilityType Code	<p>MUSS für das nodeRepresentation-Attribut den Code DE aus dem Kodiersystem "ISO 3166-1" mit der OID 1.0.3166.1 verwenden. Dem LocalizedString-Element MUSS der Wert Germany hinzugefügt werden.</p> <p>Beispiel für LocalizedString-Element: <Name> <LocalizedString value="Germany"/> </Name></p>
practiceSettingCode	Es MUSS der Wert "Not used" gesetzt werden.
uniqueId	Das Element DARF nur einen Wert enthalten, der davon abhängig ist, ob das ePKA MIO des Versicherten dem NCPeH Land-B im PDF/A-Format oder als strukturiertes Dokument im

	<p>XML-Format bereitgestellt werden soll. Der Wert des Elementes MUSS inhaltlich folgender Struktur entsprechen:</p> <p>Für die Repräsentation des ePKA MIO im PDF-Format (CDA Level 1 / PDF Body):</p> <ol style="list-style-type: none">1. Wert der Variable METADATA_ePKA_MIO_uniqueld2. "^"3. "PS.PDF" <p>Beispiel: 1.2.84.116.1.800.254.370.349.563.1605.469.534.1338^PS.PDF</p> <p>Für die Repräsentation des ePKA MIO im XML-Format (CDA Level 3 / Structured Body):</p> <ol style="list-style-type: none">1. Wert der Variable METADATA_ePKA_MIO_uniqueld2. "^"3. "PS.XML" <p>Beispiel: 1.2.84.116.1.800.254.370.349.563.1605.469.534.1338^PS.XML</p>
--	---

Der NCPeH-FD MUSS Vorgaben aus [eHDSI_XCA_Profile#2.2.1] zur Erstellung von ebRIM-Assoziations-Elementen in der Query-Response erfüllen. Der Wert des sourceObject-Attributs MUSS den Wert des id-Attributs des jeweiligen ExtrinsicObject-Elementes enthalten.

Nach Versand der Query-Response MUSS der NCPeH-FD einen Non-Repudiation of Origin Eintrag gemäß [4.1.7.1 - Non-Repudiation of Origin erstellen] in die Komponente Audit Repository speichern.

Das folgende Beispiel stellt die Struktur und Inhalte einer Query-Response dar:

```

<?xml version="1.0" encoding="UTF8" standalone="yes"?>
<Envelope>
  <Header> ... </Header>
  <Body>
    <AdhocQueryResponse status="urn:oasis:names:tc:ebxml-
  regrep:ResponseStatusType:Success">
      <RegistryObjectList>
        <ExtrinsicObject home="urn:oid:2.16.17.710.860.1000.990.1"
          id="urn:uuid:7bea8a52-9fdc-4b81-b47f-736e79df164b"
          lid="urn:uuid:7bea8a52-9fdc-4b81-b47f-736e79df164b"
          mimeType="text/xml"
          objectType="urn:uuid:7edca82f-054d-47f2-a032-9b2a5b5186c1"
          status="urn:oasis:names:tc:ebxml-
  regrep:StatusType:Approved">
          <Slot name="creationTime">
            <ValueList>
              <Value>20170914133309</Value>
            </ValueList>
          </Slot>
          <Slot name="repositoryUniqueId">
            <ValueList>
              <Value>2.16.620.1.101.10.3.29.54290</Value>
            </ValueList>
          </Slot>
          <Slot name="sourcePatientId">
            <ValueList>
              <Value>B123456789|
  A2C4E6^^^&amp;1.2.276.0.76.3.1.580.147&amp;ISO</Value>
            </ValueList>
          </Slot>
          <Name>
            <LocalizedString value="Patient Summary"/>
          </Name>
          <Description>
            <LocalizedString
  value="The Patient Summary document (CDA L3 / Structured body)
  for patient B123456789|A2C4E6"/>
          </Description>
          <VersionInfo versionName="1.1"/>
          <Classification classificationScheme="urn:uuid:41a5887f-8865-4c09-adf7-
  e362475b143a"
          classifiedObject="urn:uuid:7bea8a52-9fdc-4b81-b47f-
  736e79df164b"
          id="urn:uuid:5bfe8833-44b7-417f-9fb7-ca20f311edd8"
          nodeRepresentation="60591-5">
            <Slot name="codingScheme">
              <ValueList>
                <Value>2.16.840.1.113883.6.1</Value>
              </ValueList>
            </Slot>
            <Name>
              <LocalizedString value="Patient Summary"/>
            </Name>
          </Classification>
          <Classification classificationScheme="urn:uuid:f0306f51-975f-434e-a61c-
  c59651d33983"
          classifiedObject="urn:uuid:7bea8a52-9fdc-4b81-b47f-
  736e79df164b"
          id="urn:uuid:acf94398-f397-427b-b87e-f83065191005"
          nodeRepresentation="60591-5">
            <Slot name="codingScheme">
              <ValueList>
                <Value>2.16.840.1.113883.6.1</Value>
              </ValueList>
            </Slot>
            <Name>
              <LocalizedString value="Patient Summary"/>
            </Name>
          </Classification>
          <Classification classificationScheme="urn:uuid:f4f85eac-e6cb-4883-b524-
  f2705394840f"
          classifiedObject="urn:uuid:7bea8a52-9fdc-4b81-b47f-

```

```

736e79df164b"
nodeRepresentation="N">
    id="urn:uuid:92e3eef3-9b07-488d-a679-b029fe829e40"
    <Slot name="codingScheme">
        <ValueList>
            <Value>2.16.840.1.113883.5.25</Value>
        </ValueList>
    </Slot>
    <Name>
        <LocalizedString value="Normal"/>
    </Name>
</Classification>
<Classification classificationScheme="urn:uuid:a09d5840-386c-46f2-b5ad-
9c3699a4309d"
    classifiedObject="urn:uuid:7bea8a52-9fdc-4b81-b47f-
736e79df164b"
    id="urn:uuid:da087097-7d5a-45bd-8506-27037af88833"
    nodeRepresentation="urn:epSOS:ps:ps:2010">
    <Slot name="codingScheme">
        <ValueList>
            <Value>epSOS formatCodes</Value>
        </ValueList>
    </Slot>
    <Name>
        <LocalizedString value="epSOS coded Patient Summary"/>
    </Name>
</Classification>
<Classification classificationScheme="urn:uuid:f33fb8ac-18af-42cc-ae0e-
ed0b0bdb91e1"
    classifiedObject="urn:uuid:7bea8a52-9fdc-4b81-b47f-
736e79df164b"
    id="urn:uuid:545fbf53-9cf8-477c-829d-98b492730e8c"
nodeRepresentation="CY">
    <Slot name="codingScheme">
        <ValueList>
            <Value>1.0.3166.1</Value>
        </ValueList>
    </Slot>
    <Name>
        <LocalizedString value="CYPRUS"/>
    </Name>
</Classification>
<Classification classificationScheme="urn:uuid:ccc5598-8b07-4b77-a05e-
ae952c785ead"
    classifiedObject="urn:uuid:7bea8a52-9fdc-4b81-b47f-
736e79df164b"
    id="urn:uuid:0979226c-4fbe-4ff4-8120-f13d79189ca9"
    nodeRepresentation="Not Used">
    <Slot name="codingScheme">
        <ValueList>
            <Value>epSOS Practice Setting Codes-Not Used</Value>
        </ValueList>
    </Slot>
    <Name>
        <LocalizedString value="Not Used"/>
    </Name>
</Classification>
<ExternalIdentifier id="urn:uuid:f0eeb7ce-7b37-4e33-954f-2ca7b8072551"
    identificationScheme="urn:uuid:58a6f841-87b3-4a3e-
92fd-a8ffeff98427"
    objectType="urn:oasis:names:tc:ebxml-
regrep:ObjectType:RegistryObject:ExternalIdentifier"
    registryObject="urn:uuid:7bea8a52-9fdc-4b81-b47f-
736e79df164b"
value="123456^^^&2.16.17.710.860.1000.990.1&ISO">
    <Name>
        <LocalizedString value="XDSDocumentEntry.patientId"/>
    </Name>
</ExternalIdentifier>
<ExternalIdentifier id="urn:uuid:9b7f4301-9991-4fc7-a7b1-9a3ae59dff11"

```

```

9da3-8640a32e42ab"                identificationScheme="urn:uuid:2e82c1f6-a085-4c72-
                                     objectType="urn:oasis:names:tc:ebxml-
regrep:ObjectType:RegistryObject:ExternalIdentifier"
736e79df164b"                registryObject="urn:uuid:7bea8a52-9fdc-4b81-b47f-
value="1.2.84.116.1.800.254.370.349.563.1605.469.534.1338^PS.XML">
    <Name>
      <LocalizedString value="XSDDocumentEntry.uniqueId"/>
    </Name>
  </ExternalIdentifier>
</ExtrinsicObject>
<ExtrinsicObject home="urn:oid:2.16.17.710.860.1000.990.1"
  id="urn:uuid:5e099a45-ff39-41bb-857a-506c0b9a5ca7"
  lid="urn:uuid:5e099a45-ff39-41bb-857a-506c0b9a5ca7"
mimeType="text/xml"
                                     objectType="urn:uuid:7edca82f-054d-47f2-a032-9b2a5b5186c1"
                                     status="urn:oasis:names:tc:ebxml-
regrep:StatusType:Approved">
  <Slot name="creationTime">
    <ValueList>
      <Value>20170914133309</Value>
    </ValueList>
  </Slot>
  <Slot name="repositoryUniqueId">
    <ValueList>
      <Value>2.16.620.1.101.10.3.29.54290</Value>
    </ValueList>
  </Slot>
  <Slot name="sourcePatientId">
    <ValueList>
      <Value>B123456789|
A2C4E6^^^&1.2.276.0.76.3.1.580.147&ISO</Value>
    </ValueList>
  </Slot>
  <Name>
    <LocalizedString value="Patient Summary"/>
  </Name>
  <Description>
    <LocalizedString value="The Patient Summary document (CDA L1 / PDF
body) for patient
                                     B123456789|A2C4E6"/>
  </Description>
  <VersionInfo versionName="1.1"/>
  <Classification classificationScheme="urn:uuid:41a5887f-8865-4c09-adf7-
e362475b143a"
                                     classifiedObject="urn:uuid:5e099a45-ff39-41bb-857a-
506c0b9a5ca7"
                                     id="urn:uuid:b0b22491-e7bf-43b8-8f9a-370424da045b"
                                     nodeRepresentation="60591-5">
    <Slot name="codingScheme">
      <ValueList>
        <Value>2.16.840.1.113883.6.1</Value>
      </ValueList>
    </Slot>
    <Name>
      <LocalizedString value="Patient Summary"/>
    </Name>
  </Classification>
  <Classification classificationScheme="urn:uuid:f0306f51-975f-434e-a61c-
c59651d33983"
                                     classifiedObject="urn:uuid:5e099a45-ff39-41bb-857a-
506c0b9a5ca7"
                                     id="urn:uuid:87b7eec0-b638-450d-850c-b2a88ee31de3"
                                     nodeRepresentation="60591-5">
    <Slot name="codingScheme">
      <ValueList>
        <Value>2.16.840.1.113883.6.1</Value>
      </ValueList>
    </Slot>

```

```

        <Name>
          <LocalizedString value="Patient Summary"/>
        </Name>
      </Classification>
      <Classification classificationScheme="urn:uuid:f4f85eac-e6cb-4883-b524-
f2705394840f"
        classifiedObject="urn:uuid:5e099a45-ff39-41bb-857a-
506c0b9a5ca7"
        id="urn:uuid:a1667eaf-e293-4e3c-bcd5-e43b37f2b5e7"
nodeRepresentation="N">
        <Slot name="codingScheme">
          <ValueList>
            <Value>2.16.840.1.113883.5.25</Value>
          </ValueList>
        </Slot>
        <Name>
          <LocalizedString value="Normal"/>
        </Name>
      </Classification>
      <Classification classificationScheme="urn:uuid:a09d5840-386c-46f2-b5ad-
9c3699a4309d"
        classifiedObject="urn:uuid:5e099a45-ff39-41bb-857a-
506c0b9a5ca7"
        id="urn:uuid:ff108db4-4867-4f3b-a067-3865182001ee"
nodeRepresentation="urn:ihe:iti:xds-sd:pdf:2008">
        <Slot name="codingScheme">
          <ValueList>
            <Value>IHE PCC</Value>
          </ValueList>
        </Slot>
        <Name>
          <LocalizedString value="PDF/A coded document"/>
        </Name>
      </Classification>
      <Classification classificationScheme="urn:uuid:f33fb8ac-18af-42cc-ae0e-
ed0b0bdb91e1"
        classifiedObject="urn:uuid:5e099a45-ff39-41bb-857a-
506c0b9a5ca7"
        id="urn:uuid:c0a8b915-e23e-4140-af9a-8ee16cd3f473"
nodeRepresentation="CY">
        <Slot name="codingScheme">
          <ValueList>
            <Value>1.0.3166.1</Value>
          </ValueList>
        </Slot>
        <Name>
          <LocalizedString value="CYPRUS"/>
        </Name>
      </Classification>
      <Classification classificationScheme="urn:uuid:ccc5598-8b07-4b77-a05e-
ae952c785ead"
        classifiedObject="urn:uuid:5e099a45-ff39-41bb-857a-
506c0b9a5ca7"
        id="urn:uuid:fc5ce656-87f7-4655-9ba4-327c05fc3846"
nodeRepresentation="Not Used">
        <Slot name="codingScheme">
          <ValueList>
            <Value>epSOS Practice Setting Codes-Not Used</Value>
          </ValueList>
        </Slot>
        <Name>
          <LocalizedString value="Not Used"/>
        </Name>
      </Classification>
      <ExternalIdentifier id="urn:uuid:f7383a55-7aa9-4dec-9b6e-73e72461ee51"
92fd-a8ffeff98427"
        identificationScheme="urn:uuid:58a6f841-87b3-4a3e-
        objectType="urn:oasis:names:tc:ebxml-
regrep:ObjectType:RegistryObject:ExternalIdentifier"
        registryObject="urn:uuid:5e099a45-ff39-41bb-857a-
506c0b9a5ca7"

```

```

value="123456^^^&2.16.17.710.860.1000.990.1&ISO">
  <Name>
    <LocalizedString value="XSDDocumentEntry.patientId"/>
  </Name>
</ExternalIdentifier>
<ExternalIdentifier id="urn:uuid:199425df-d4f8-41a1-85a7-e49307c8abe3"
  identificationScheme="urn:uuid:2e82c1f6-a085-4c72-
9da3-8640a32e42ab"
  objectType="urn:oasis:names:tc:ebxml-

regrep:ObjectType:RegistryObject:ExternalIdentifier"
  registryObject="urn:uuid:5e099a45-ff39-41bb-857a-
506c0b9a5ca7"

value="1.2.84.116.1.800.254.370.349.563.1605.469.534.1338^PS.PDF">
  <Name>
    <LocalizedString value="XSDDocumentEntry.uniqueId"/>
  </Name>
</ExternalIdentifier>
</ExtrinsicObject>
<Association associationType="urn:ihe:iti:2007:AssociationType:XFRM"
  id="urn:uuid:a0a2a0a8-4c91-46dd-9aa7-e43b5b9bb645"
  sourceObject="urn:uuid:5e099a45-ff39-41bb-857a-506c0b9a5ca7"
  targetObject="urn:uuid:7bea8a52-9fdc-4b81-b47f-736e79df164b"/>
</RegistryObjectList>
</AdhocQueryResponse>
</Body>
</Envelope>

```

Ausgabeparameter des TUC

- Dieser TUC hat keine Ausgabeparameter.

6.1.2.3 TUC_NCPeH_025: Cross Gateway Query Request für ePeD-A verarbeiten

Für diesen TUC gelten folgende übergreifende Festlegungen

- [[4.1.2 - Datenaustausch mit zugelassenen EU-Ländern](#)]
- [[4.1.3 - eHDSI Basisleistungen](#)]
- [[4.1.5 - Validierung der Identity Assertion des LE-EU](#)]
- [[4.1.6 - Validierung der TRC-Assertion](#)]
- [[4.1.7 - Non-Repudiation und Audit Trail Schemas](#)]
- [[4.1.8 - Festlegungen zur Prüfung der Zugriffsberechtigung auf Fachdienste der TI](#)]
- [[4.1.9- Format und Validierung der KVNR](#)]

Ablauf des TUC

Der NCPeH-FD MUSS die Umsetzung der Operation Cross_Gateway_Query::FindDocuments gemäß den Vorgaben, Einschränkungen und der definierten Ablauflogik aus [eHDSI_XCA_Profile] implementieren.

Nach Eingang der Anfrage MUSS der NCPeH-FD einen Non-Repudiation of Receipt Eintrag gemäß [4.1.7.2 - Non-Repudiation of Receipt erstellen] und einen Audit Trail Eintrag gemäß [4.1.7.3 - Patient Privacy Audit Trail Eintrag erstellen] in der Komponente Audit Repository speichern. Bei der Erstellung des Audit Trail Eintrages müssen Vorgaben aus [eHDSI_XCA_Profile#4.3] umgesetzt werden. Wenn zum Zeitpunkt der Erstellung des Audit Trail Eintrags nicht alle erforderlichen Daten im NCPeH-FD verfügbar sind, MÜSSEN

die Daten in den Audit Trail Eintrag aufgenommen werden, sobald sie im NCPeH-FD verfügbar sind, spätestens nach dem Versand der Antwort an NCPeH Land-B.

Der NCPeH-FD MUSS Inhalte des Parameters XSDDocumentEntryPatientId aus der Anfrage auf folgende Kriterien prüfen:

- Der Wert des Parameters XSDDocumentEntryPatientId ist inhaltlich nach der folgenden Vorschrift strukturiert:
 1. "",
 2. der unveränderbare Teil der KVNR des Versicherten (10 Stellen),
Der Wert MUSS gemäß den Vorgaben im [\[4.1.9- Format und Validierung der KVNR\]](#) geprüft und valide sein.
 3. der senkrechte Strich ohne Anführungszeichen: "|",
 4. 6-stelliger Zugriffscode,
 5. "^^^&",
 6. Wert des Konfigurationsparameters OID_KVNR_ASSIGNING_AUTHORITY aus [\[4.1.1 - Konfigurationsparameter\]](#),
 7. "&ISO'".

Beispiel des Wertes: 'B123456789|
A2C4E6^^^&;1.2.276.0.76.3.1.580.147&ISO'

- Der Wert des Parameters muss mit Hochkomma beginnen und enden.
- Die in dem Parameter enthaltene Versichertenkennung muss identisch mit dem Wert der Variable trc_kvnr sein (siehe [\[4.1.6 - Validierung der TRC-Assertion\]](#)).
- Der in dem Parameter enthaltene Zugriffscode muss identisch mit dem Wert der Variable trc_accesscode sein (siehe [\[4.1.6 - Validierung der TRC-Assertion\]](#)).
- Die im Parameter enthaltene OID muss identisch mit dem Wert des Konfigurationsparameters OID_KVNR_ASSIGNING_AUTHORITY sein (siehe [\[4.1.1 - Konfigurationsparameter\]](#)).

Der NCPeH-FD MUSS bei der Prüfung des Parameters XSDDocumentEntryClassCode auf folgende Prüfkriterien achten:

- Der classCode MUSS den Wert 57833-6 enthalten.
Der Wert 57833-6 ist ein Code aus dem Codesystem LOINC und hat den Display Name "Prescription for medication" (siehe [\[LOINC_ePrescription\]](#)). classCode DARF andere Codes NICHT enthalten.
- Das Klassifikationsschema MUSS die OID 2.16.840.1.113883.6.1 enthalten. Die OID referenziert auf das Kodiersystem LOINC.
- Der Parameter MUSS mit dem folgendem Wert identisch sein:
('57833-6^^2.16.840.1.113883.6.1').

Falls es bei der Prüfung der oben angegebenen Kriterien zu Fehlern bzw. Abweichungen kommt, MUSS der NCPeH-FD eine weitere Verarbeitung der Anfrage abbrechen und dem NCPeH Land-B mit einer Fehlernachricht antworten. Neben Vorgaben zur Fehlerbehandlung aus [\[eHDSI_XCA_Profile#2.2.3\]](#) und [\[eHDSI_NCPeH_Components#6.4\]](#) MUSS der NCPeH-FD beim Auftreten von Fehlerbedingungen folgende Zuordnung von Fehlernachrichten umsetzen:

Tabelle 47: TAB_NCPeH_XCA_QUERY_ePeD-A Fehlerbedingungen_Fehlercodes

Fehlerbedingung	errorCode	codeCo	severity	location
-----------------	-----------	--------	----------	----------

	gemäß [eHDSI_NCPeH_Components#6.4]	ntext		
Die Variable <code>tls_country</code> aus dem TLS-Zertifikat des NCPeH Land-B DARF NICHT leer sein (siehe [4.1.3.1 Sicherer Kanal: TESTA-ng und TLS]) und MUSS in der WHITELIST_NCPeH_COUNTRY-B nach [4.1.2 "Datenaustausch mit zugelassenen EU-Ländern"] enthalten sein.	ERROR_EP_GENERIC	"The german ePrescription service is not agreed with the requesting country . Please contact your service provider or administrator ."	urn:oasis:names:tc:ebxml-regrep:ErrorSeverityType:Error	"The DN structure in the subject of the received TLS certificate does not contain a valid EU country code or the addressed service is not agreed between the requesting country and germany. Received country code= " + Wert der Variable <code>tls_country</code>
Die Variable <code>ida_permissions</code> , falls sie nicht leer ist, enthält nicht alle Permission Codes gemäß den Vorgaben aus [4.1.8 - Festlegungen zur Prüfung der Zugriffsberechtigung auf Fachdienste der TI] für den eHDSI Use Case "Request for ePrescriptions".		"Access denied. Please contact your service provider or administrator and check the access rights for your health care professional role in your country ."		"Received permission codes=" + Wert der Variable <code>ida_permissions</code>
Die Variable <code>ida_permissions</code> ist leer und die		"Access denied. The		"No permission codes received and the access cannot be

<p>Bedingungen zur Erlangung einer Zugriffsberechtigung auf das E-Rezept-FD nach [4.1.8 - Festlegungen zur Prüfung der Zugriffsberechtigung auf Fachdienste der TI] sind nicht erfüllt.</p>		<p>information provided about the role of the health professional does not comply with German regulations."</p>		<p>granted for the received practitioner role code in accordance with national regulations. Received practitioner role code=" + Wert der Variable ida_practitioner_role_code</p>
<p>Der Wert des XSDocumentEntry PatientId entspricht nicht den oben genannten Prüfkriterien und der inhaltlichen Struktur.</p>		<p>"Please make sure the health insurance identifier is correct."</p>		<p>"Received XSDocumentEntryPatientId=" + Wert aus dem XSDocumentEntryPatientId-Slot</p>
<p>Die Versichertenkennung aus dem Wert des XSDocumentEntry PatientId ist nicht identisch mit dem Wert der Variable trc_kvnr oder die Variable trc_kvnr ist leer.</p>				
<p>Die OID aus dem Slot XSDocumentEntry PatientId ist nicht identisch mit dem Wert des Konfigurationsparameters OID_KVNR_ASSIGNING_AUTHORITY (siehe [4.1.1 - Konfigurationsparameter]).</p>		<p>"Unknown type of health insurance identifier. Please contact your service provider or</p>		<p>"The service request is incorrectly configured for the health insurance identifier. Received OID of XSDocumentEntryPatientId-Slot=" + der Wert der OID aus dem Slot XSDocumentEntryPatientId</p>

		adminis trator. "		
Der Wert für den Zugriffscode aus dem Element XSDocumentEntry PatientId ist nicht identisch mit dem Wert der Variable trc_accesscode oder trc_accesscode ist leer.		"Access denied. The patient's access code is missing or malformed. Please ask the patient for access authorization and the proper access code."		Keine Angaben
Die Variable ida_name-id ist leer.	ERROR_HPI_INSUFFICIENT_INFORMATION	"Access denied. The identifier of the health professional is missing in the provided identity information."		Keine Angaben
Die Variable ida_practitioner_role ist leer.		"Access denied. The information about the role of EU health		Keine Angaben

		professional is missing in the provided identity information."	
Die Variable ida_practitioner_name ist leer.		"Access denied. The name of the EU health professional is missing in the provided identity information."	Keine Angaben
Der Wert der Variable ida_practitioner_role_code ist leer oder dieser ist nicht identisch mit einem der möglichen Werte für das Element urn:oasis:names:tc:xacml:2.0:subject:role aus [eHDSI_SAML_Profile#2.3].		"Access denied. Missing or unknown role of the EU health professional in the provided identity information."	"Received role code from the identity assertion of healthcare professional; see element urn:oasis:names:tc:xacml:2.0:subject:role= " + Wert der Variable ida_practitioner_role_code
Die Variable ida_point_of_care ist leer.	ERROR_HPI_POC_NO_INFORMATION	"Access denied. Missing name of the point of care in the	Keine Angaben

		provide d identit y informa tion."		
Die Variable ida_healthcare_facility_type_code ist entweder leer oder oder nicht identisch mit einem der vorgegebenen Werte aus [eHDSI_SAML_Profile#2.3] für das Identitätsattribut urn:ehdsi:names:subject:healthcare-facility-type		"Access denied. Missing or unknown type of Healthcare Provider Organization in the provided identity information."		"Received healthcare facility type=" + Wert der Variable ida_healthcare_facility_type_code
Das Element XDSDocumentEntry Status enthält einen Wert der mit dem vorgeschriebenen Wert gemäß [eHDSI_XCA_Profile#2.1] nicht identisch ist.	ERROR_INCORRECT_FORMATTING	"The requested document status for patient prescriptions is not supported."		"The value ofXDSDocumentEntry Status does not correspond to the required value from [eHDSI_XCA_Profile#2.1]. Received value of XDSDocumentEntryStatus=" + der Wert aus dem Element XDSDocumentEntryStatus
Wenn das Element XDSDocumentEntry FormatCode angegeben ist und der Wert des Elementes entspricht keinem der Werte urn:epsos:ep:pre:2010 oder urn:ihe:iti:xds-sd:pdf:2008		"The requested format for patient prescriptions is not supported."		"Received XDSDocumentEntryFormatCode= " + der Wert aus dem Element XDSDocumentEntryFormatCode

<p>Der classCode des XSDDocumentEntry ClassCode ist nicht identisch mit dem Wert 57833-6.</p>	<p>ERROR_GENERIC_SERVICE_SIGNIFIER_UNKNOWN</p>	<p>"Unknown service . Please contact your service provider or administrator."</p>		<p>"Received XSDDocumentEntryClassCode= " + der Wert aus dem Element XSDDocumentEntryClassCode</p>
<p>Das Format des XSDDocumentEntryClassCode entspricht nicht den oben genannten Anforderungen an die inhaltliche Struktur</p>				

Hinweis: Die Initiierung der Variablen `ida_healthcare_facility_type_code`, `ida_name-id`, `ida_practitioner_role` und `ida_point_of_care` erfolgt im [\[4.1.5 - Validierung der Identity Assertion des LE-EU\]](#) und die Variablen `trc_kvnr` und `trc_accesscode` im [\[4.1.6 - Validierung der TRC-Assertion\]](#).

Das folgende Beispiel zeigt die Struktur des XCA.FindDocuments Request für ePrescriptions:

```
<?xml version="1.0" encoding="UTF8" standalone="yes"?>
<Envelope>
  <Header> ... </Header>
  <Body>
    <AdhocQueryRequest>
      <ResponseOption returnComposedObjects="true" returnType="LeafClass"/>
      <AdhocQuery id="urn:uuid:14d4debf-8f97-4251-9a74-a90016b0af0d">
        <Slot name="$XDSDocumentEntryPatientId">
          <ValueList>
            <Value>'B123456789|
A2C4E6^^^&1.2.276.0.76.3.1.580.147&ISO'</Value>
          </ValueList>
        </Slot>
        <Slot name="$XDSDocumentEntryStatus">
          <ValueList>
            <Value>('urn:oasis:names:tc:ebxml-regrep:StatusType:Approved')</Value>
          </ValueList>
        </Slot>
        <Slot name="$XDSDocumentEntryClassCode">
          <ValueList>
            <Value>('57833-6^^2.16.840.1.113883.6.1')</Value>
          </ValueList>
        </Slot>
      </AdhocQuery>
    </AdhocQueryRequest>
  </Body>
</Envelope>
```

Ausgabeparameter des TUC

Nach erfolgreicher Durchführung dieses TUC stehen folgende Ausgabeparameter zur Verfügung und können im entsprechenden Anwendungsfall verwendet werden:

- Keine

6.1.2.4 TUC_NCPeH_026: Cross Gateway Query Response für ePeD-A versenden

Für diesen TUC gelten folgende übergreifende Festlegungen

- [[4.1.3 - eHDSI Basisleistungen](#)]
- [[4.1.7 - Non-Repudiation und Audit Trail Schemas](#)]
- fhir_erp_bundle_collection - Ein FHIR-Bundle vom Typ collection liegt im Klartext vor. Das FHIR-Bundle enthält mindestens ein inneres, schemakonformes Bundle vom Typ document mit der Profilierung KBV_PR_ERP_Bundle gemäß [KBV_PR_ERP_Bundle] mit Angaben zu jeweils einem E-Rezept.

Ablauf des TUC

Der NCPeH-FD MUSS die Inhalte und Struktur der XCA.Query-Antwort nach Vorgaben aus [eHDSI_XCA_Profile#2.2] erstellen. Zusätzlich müssen Vorgaben gemäß

[ebRIM_Representation_Document#4.2.3.2] zur Erstellung von DocumentEntry-Elementen und -Attributen beachtet werden.

In diesem TUC werden die Einträge des Eingangsparameters `fhir_erp_bundle_collection` (siehe Ausgabeparameter im [6.2.5- TUC_NCPeH_036: Liste der einlösbaren E-Rezepte des Versicherten aus dem E-Rezept-FD abrufen]) verarbeitet. Der Eingangsparameter `fhir_erp_bundle_collection` enthält mindestens einen "inneren Bundle" vom Typdocument. In jedem inneren Bundle stellt eine FHIR-Resource Composition vom Profil [KBV_PR_ERP_Composition] eine Referenzsammlung zu allen anderen entry-Elementen (FHIR-Resource) dar, in denen relevante Angaben zu MedicationRequest-, Medication- und Practitioner enthalten sind.

Der NCPeH-FD MUSS für jedes innere Bundle resource/entry-Elemente ermitteln, die zu folgende FHIR-Resources führen:

FHIR-Resource MedicationRequest

- Die Referenz (ein UUID-Wert), die zur FHIR-Resource MedicationRequest mit dem Profil [KBV_PR_ERP_Prescription] führt, ist im Element `Bundle/entry/resource/Composition/section/entry` enthalten. Dabei MUSS der Code des section-Elements mit dem Wert Prescription identisch sein. Die ermittelte die FHIR-Resource MedicationRequest enthält Informationen über die Verordnung.

FHIR-Resource Medication

- Die ermittelte MedicationRequest-Resource enthält im medicationReference-Element wiederum eine Referenz (ein UUID-Wert) auf die eigentliche FHIR-Resource Medication, in der weitere Angaben zur Verordnung enthalten sind.

FHIR-Resource Practitioner

- Die Referenz (ein UUID-Wert), die zur FHIR-Resource Practitioner mit dem Profil [KBV_PR_FOR_Practitioner] führt, ist im Element `Bundle/entry/resource/Composition/author` enthalten. Die ermittelte FHIR-Resource Practitioner enthält Informationen zum verordnenden LE-DE.

FHIR-Resource Organization

- Die Referenz (ein UUID-Wert), die zur FHIR-Resource Organization mit dem Profil [KBV_PR_FOR_Organization] führt, ist im Element `Bundle/entry/resource/custodian` enthalten. Die ermittelte FHIR-Resource Organization enthält Informationen zur Gesundheitseinrichtung des verordnenden LE-DE.

Der NCPeH-FD MUSS in der XCA.Query-Antwortnachricht für jedes innere Bundle zu der darin enthaltenen Verordnung (FHIR-Resource MedicationRequest) jeweils ein ExtrinsicObject-Element mit einem Name-Subelement `ePrescription source coded PDF/A document` und ein weiteres ExtrinsicObject-Element mit einem Name-Subelement `ePrescription coded document` erstellen.

Darüber hinaus MUSS der NCPeH-FD in den ExtrinsicObject-Elementen Informationen zum verordnenden LE-DE (FHIR-Resource Practitioner aus dem jeweiligen inneren Bundle) angeben und zusätzlich für folgende Elemente die Nutzungskonventionen einhalten:

Tabelle 48: TAB_NCPeH_Nutzungskonvention_Erstellung_XCA.Query_Response_ePeD-A

Element in der	Nutzungskonvention
----------------	--------------------

Query Response	
status	Siehe Vorgaben für das Element in [eHDSI_NCPeH_Components#3.1.4.2.3]
mimeType	Siehe Vorgaben für das Element in [eHDSI_NCPeH_Components#3.1.4.2.3]
Description	<p>Siehe Vorgaben für das Element in [eHDSI_NCPeH_Components#3.1.4.2.3]</p> <p>Der Inhalt des Elementes MUSS den Wert aus der FHIR-Resource Medication des jeweiligen inneren Bundle enthalten, nachdem die Mapping-Regeln gemäß den BfArM-Vorgaben angewendet wurden.</p>
VersionInfo	Siehe Vorgaben für das Element in [eHDSI_NCPeH_Components#3.1.4.2.3]
sourcePatientId	Das Element MUSS den Wert des XSDocumentEntryPatientId-Parameters aus der Anfrage enthalten (siehe [6.1.2.3-TUC_NCPeH_025: Cross Gateway Query Request für ePeD-A verarbeiten]).
repositoryUniqueId	Das Element MUSS den Wert des Konfigurationsparameters OID_AC_ePKA_ASSIGNING_AUTHORITY enthalten (siehe [4.1.1 - Konfigurationsparameter]).
classCode	<p>Es ist eine Klassifikation und MUSS den Wert 57833-6 enthalten. Der Wert 57833-6 ist ein Code aus dem Codesystem LOINC (siehe [LOINC_ePrescription]).</p> <p>Für weitere Informationen siehe [ebRIM_Representation_Document#4.2.3.2.3]</p>
formatCode	<p>Durch das Element wird festgelegt, in welcher Kodierung die Verordnung dem NCPeH Land-B bereitgestellt werden kann.</p> <p>Das Element MUSS den Wert urn:epsos:ep:pre:2010 für "ePrescription coded document" oder urn:ihe:iti:xds-sd:pdf:2008 für "ePrescription source coded PDF/A" enthalten.</p> <p>Für weitere Informationen siehe [ebRIM_Representation_Document#4.2.3.2.9]</p>

<p>healthcareFacility TypeCode</p>	<p>MUSS für das nodeRepresentation-Attribut den Code DE aus dem Kodiersystem "ISO 3166-1" mit der OID1.0.3166.1 verwenden. Dem LocalizedString-Element MUSS der Wert Germany hinzugefügt werden.</p> <p>Für weitere Informationen siehe [ebRIM_Representation_Document#4.2.3.2.11]</p>
<p>practiceSettingCo de</p>	<p>Siehe Vorgaben für das Element in [eHDSI_NCPeH_Components#3.1.4.2.3]</p> <p>Für weitere Informationen siehe [ebRIM_Representation_Document#4.2.3.2.11]</p>
<p>eventCodeList</p>	<p>Das nodeRepresentation-Attribut MUSS den Wert urn:ihe:iti:xdw:2011:eventCode:open gemäß XDS Format Codes Schema "1.3.6.1.4.1.19376.1.2.3" enthalten. Dem LocalizedString-Element MUSS der Wert Open hinzugefügt werden.</p> <p>(Dispensable - Für mehr Informationen siehe [eHDSI_XCA_Profile#2.2.2.1.2])</p>
<p>uniqueId</p>	<p>Das Element MUSS genau einen Wert enthalten, der davon abhängig ist, ob eine Verordnung dem NCPeH Land-B im PDF-Format oder als strukturiertes Dokument im XML-Format bereitgestellt werden soll.</p> <p>Für die Repräsentation der Verordnung im PDF/A-Format (CDA Level 1):</p> <ol style="list-style-type: none"> 1. Wert aus dem Element Bundle.identifier gemäß Profil [GEM_ERP_NS_PrescriptionId], 2. "^", 3. "eP.PDF". <p>Beispiel: 160.000.000.000.123.76^eP.PDF</p> <p>Für die Repräsentation der Verordnung im XML-Format (CDA Level 3):</p> <ol style="list-style-type: none"> 1. Wert aus dem Element Bundle.identifier gemäß Profil [GEM_ERP_NS_PrescriptionId], 2. "^", 3. "eP.XML". <p>Beispiel: 160.000.000.000.123.76^eP.XML</p>

<p>patientId</p>	<p>Das Element MUSS den Wert aus dem Element Assertion/AttributeStatement/Attribute[@Name="urn:oasis:names:tc:xacml:1.0:resource:resource-id] der TRC Assertion enthalten (siehe [4.1.6 - Validierung der TRC-Assertion]).</p> <p>Beispiel: B123456789 A2C4E6^^^&1.2.276.0.76.3.1.580.147&ISO</p>
<p>authorPerson</p>	<p>Das Element MUSS Angaben aus dem Element Practitioner.name der FHIR-Resource Practitioner gemäß Profil [KBV_PR_FOR_Organization] enthalten.</p> <p>Falls das Element Practitioner.name neben Vorname und Nachname weitere Namen und Bezeichnungen enthält, MUSS vor der Zuweisung der endgültige Wert in folgender Reihenfolge gebildet werden:</p> <p>Präfix Vorname Namenszusatz Vorsatzwort Nachname</p> <p>Einzelne Namen bzw. Bezeichnungen sind durch ein Leerzeichen getrennt. Beispiel: Dr. Johanna Gräfin von Oberberg</p>
<p>authorInstitution</p>	<p>Wenn Organization.name der FHIR-Resource Organization gemäß Profil [KBV_PR_FOR_Organization] nicht leer ist, MUSS das Element authorInstitution Informationen aus dem Element Organization.name enthalten. Ansonsten DARF das Element authorInstitution NICHT in der XCA.Query-Antwortnachricht angegeben werden.</p>
<p>confidentialityCode</p>	<p>Siehe Vorgaben für das Element in [eHDSI_NCPeH_Components#3.1.4.2.3]</p> <p>Das Attribut nodeRepresentation des Elementes MUSS den Code "R" (restricted) gemäß Kodsystem Confidentiality (2.16.840.1.113883.5.25) enthalten.</p> <p>Für weitere Informationen siehe [ebRIM_Representation_Document#4.2.3.2.5]</p>

Disclaimer: Die Vorgaben zur Verarbeitung von Informationen für jede Verordnungen aus jedem inneren Bundle der fhir_erp_bundle_collection nach verschiedenen relevanten FHIR-Profilen (z.B. [KBV_PR_ERP_Medication_PZN]), Transformation und Transkodierung von Inhalten (insbesondere Fachinformationen zu Arzneimitteln gemäß [eHDSI_XCA_Profile#2.2.2.1 eP List Metadata]) MÜSSEN durch das BfArM entwickelt und zur Nutzung im NCPeH-FD bereitgestellt werden.

Der NCPeH-FD MUSS Vorgaben aus [eHDSI_XCA_Profile#2.2.1] zur Erstellung von ebRIM-Assoziations-Elementen in der Query-Response erfüllen.

Der NCPeH-FD MUSS für AdhocQueryResponse@status in der Antwortnachricht einen entsprechenden Wert setzen, der anhand des Gesamtstatus aller RegistryResponse/RegistryErrorList/RegistryError@Severities-Attribute, erfolgreich verarbeiteter interner Bundles und unter Berücksichtigung der Kriterien aus der Tabelle "Registry Stored Query [ITI-18] and Cross Gateway Query [ITI-38] Responses" in [ebRIM_Representation_Document#4.2.4.2] zu bestimmen ist.

Nach Versand der Query-Response MUSS der NCPeH-FD einen Non-Repudiation of Origin Eintrag gemäß [4.1.7.1 - Non-Repudiation of Origin erstellen] in die Komponente Audit Repository speichern.

Das folgende Beispiel stellt die Struktur und Inhalte eines XCA FindDocuments-Response für ePrescriptions dar:

```

<?xml version="1.0" encoding="UTF8" standalone="yes"?>
<Envelope>
  <Header> ... </Header>
  <Body>
    <AdhocQueryResponse status="urn:oasis:names:tc:ebxml-
regrep:ResponseStatus:Success">
      <RegistryObjectList>
        <!-- ExtrinsicObject zur ePrescription 160.000.000.000.123.76^eP.XML (CDA
Level 3) -->
        <ExtrinsicObject home="urn:oid:1.2.246.556.12001.4.1000.990.1"
id="urn:uuid:cb804da7-407c-4590-b394-ad3d7617995d" lid="urn:uuid:cb804da7-407c-4590-b394-
ad3d7617995d" mimeType="text/xml" objectType="urn:uuid:7edca82f-054d-47f2-a032-9b2a5b5186c1"
status="urn:oasis:names:tc:ebxml-regrep:StatusType:Approved">
          <Slot name="sourcePatientId">
            <ValueList>
              <Value>B123456789|
A2C4E6^^^&amp;1.2.276.0.76.3.1.580.147&amp;ISO</Value>
            </ValueList>
          </Slot>
          <Slot name="size">
            <ValueList>
              <Value>0</Value>
            </ValueList>
          </Slot>
          <Slot name="creationTime">
            <ValueList>
              <Value>20230717</Value>
            </ValueList>
          </Slot>
          <Slot name="repositoryUniqueId">
            <ValueList>
              <Value>1.2.276.0.76.3.1.580.147</Value>
            </ValueList>
          </Slot>
          <Name>
            <LocalizedString value="ePrescription coded document"/>
          </Name>
          <Description>
            <LocalizedString value="Lercanidipin Omniapharm, 10 mg, tablet"/>
          </Description>
          <VersionInfo versionName="1.1"/>
          <Classification classificationScheme="urn:uuid:f4f85eac-e6cb-4883-b524-
f2705394840f" classifiedObject="urn:uuid:cb804da7-407c-4590-b394-ad3d7617995d"
id="urn:uuid:4240e4af-0a0c-48ae-88e0-8804e0736cc2" nodeRepresentation="R">
            <Slot name="codingScheme">
              <ValueList>
                <Value>2.16.840.1.113883.5.25</Value>
              </ValueList>
            </Slot>
            <Name>
              <LocalizedString value="restricted"/>
            </Name>
          </Classification>
          <Classification classificationScheme="urn:uuid:41a5887f-8865-4c09-adf7-
e362475b143a" classifiedObject="urn:uuid:cb804da7-407c-4590-b394-ad3d7617995d"
id="urn:uuid:32d2d7bc-dcf7-455f-a89d-bea6d8ba53f3" nodeRepresentation="57833-6">
            <Slot name="codingScheme">
              <ValueList>
                <Value>2.16.840.1.113883.6.1</Value>
              </ValueList>
            </Slot>
            <Name>
              <LocalizedString value="eHDSI - ePrescription"/>
            </Name>
          </Classification>
          <Classification classificationScheme="urn:uuid:f33fb8ac-18af-42cc-ae0e-
ed0b0bdb91e1" classifiedObject="urn:uuid:cb804da7-407c-4590-b394-ad3d7617995d"
id="urn:uuid:096d34cb-f5f8-41c0-94f9-f2ab0955c212" nodeRepresentation="DE">
            <Slot name="codingScheme">
              <ValueList>
                <Value>1.0.3166.1</Value>
              </ValueList>
            </Slot>
          </Classification>
        </ExtrinsicObject>
      </RegistryObjectList>
    </AdhocQueryResponse>
  </Body>
</Envelope>

```

```

        </Slot>
        <Name>
          <LocalizedString value="Germany"/>
        </Name>
      </Classification>
      <Classification classificationScheme="urn:uuid:cccf5598-8b07-4b77-a05e-ae952c785ead" classifiedObject="urn:uuid:cb804da7-407c-4590-b394-ad3d7617995d" id="urn:uuid:4d8f8407-c10b-4b32-b12f-33c37cf31fa0" nodeRepresentation="Not Used">
        <Slot name="codingScheme">
          <ValueList>
            <Value>eHDSI Practice Setting Codes-Not Used</Value>
          </ValueList>
        </Slot>
        <Name>
          <LocalizedString value="Not Used"/>
        </Name>
      </Classification>
      <Classification classificationScheme="urn:uuid:2c6b8cb7-8b2a-4051-b291-b1ae6a575ef4" classifiedObject="urn:uuid:cb804da7-407c-4590-b394-ad3d7617995d" id="urn:uuid:5dae84b8-aac3-426d-a7a4-2720636dead9" nodeRepresentation="urn:ihe:iti:xdw:2011:eventCode:open">
        <Slot name="codingScheme">
          <ValueList>
            <Value>1.3.6.1.4.1.19376.1.2.3</Value>
          </ValueList>
        </Slot>
        <Name>
          <LocalizedString value="Open"/>
        </Name>
      </Classification>
      <Classification classificationScheme="urn:uuid:2c6b8cb7-8b2a-4051-b291-b1ae6a575ef4" classifiedObject="urn:uuid:cb804da7-407c-4590-b394-ad3d7617995d" id="urn:uuid:9be3b429-862a-462b-8255-3897f81eb237" nodeRepresentation="C08CA13">
        <Slot name="codingScheme">
          <ValueList>
            <Value>2.16.840.1.113883.6.73</Value>
          </ValueList>
        </Slot>
        <Name>
          <LocalizedString value="Lercanidipin"/>
        </Name>
      </Classification>
      <Classification classificationScheme="urn:uuid:2c6b8cb7-8b2a-4051-b291-b1ae6a575ef4" classifiedObject="urn:uuid:cb804da7-407c-4590-b394-ad3d7617995d" id="urn:uuid:750199ba-bc51-43b8-a4b4-239f8bd9b164" nodeRepresentation="10 mg">
        <Slot name="codingScheme">
          <ValueList>
            <Value>eHDSI_Strength_CodeSystem</Value>
          </ValueList>
        </Slot>
        <Name>
          <LocalizedString value="Strength of medication"/>
        </Name>
      </Classification>
      <Classification classificationScheme="urn:uuid:a09d5840-386c-46f2-b5ad-9c3699a4309d" classifiedObject="urn:uuid:cb804da7-407c-4590-b394-ad3d7617995d" id="urn:uuid:5922a634-fd9b-444c-9c14-46434d81649b" nodeRepresentation="urn:epsos:ep:pre:2010">
        <Slot name="codingScheme">
          <ValueList>
            <Value>eHDSI formatCodes</Value>
          </ValueList>
        </Slot>
        <Name>
          <LocalizedString value="epSOS coded ePrescription"/>
        </Name>
      </Classification>
      <Classification classificationScheme="urn:uuid:93606bcf-9494-43ec-9b4e-a7748d1a838d" classifiedObject="urn:uuid:cb804da7-407c-4590-b394-ad3d7617995d" id="urn:uuid:ab25d055-e681-44c3-8092-fdec60f1c43b" nodeRepresentation="">
        <Slot name="authorPerson">
          <ValueList>

```

```

                <Value>Manfred Lapp</Value>
            </ValueList>
        </Slot>
        <Slot name="authorInstitution">
            <ValueList>
                <Value>Bundeswehrkrankenhaus
Berlin^^^^^^^^^^2.999.1.2.3.5.8.9.1789.45</Value>
            </ValueList>
        </Slot>
    </Classification>
    <ExternalIdentifier id="urn:uuid:4d433f10-09fb-4f38-b377-579550c393ba"
identificationScheme="urn:uuid:58a6f841-87b3-4a3e-92fd-a8ffeff98427"
objectType="urn:oasis:names:tc:ebxml-regrep:ObjectType:RegistryObject:ExternalIdentifier"
registryObject="urn:uuid:cb804da7-407c-4590-b394-ad3d7617995d" value="B123456789|
A2C4E6^^^&1.2.276.0.76.3.1.580.147&ISO">
        <Name>
            <LocalizedString value="XSDDocumentEntry.patientId"/>
        </Name>
    </ExternalIdentifier>
    <ExternalIdentifier id="urn:uuid:a4ced7f7-e7ff-4547-91f5-1d64a183b38a"
identificationScheme="urn:uuid:2e82c1f6-a085-4c72-9da3-8640a32e42ab"
objectType="urn:oasis:names:tc:ebxml-regrep:ObjectType:RegistryObject:ExternalIdentifier"
registryObject="urn:uuid:cb804da7-407c-4590-b394-ad3d7617995d"
value="160.000.000.000.123.76^eP.XML">
        <Name>
            <LocalizedString value="XSDDocumentEntry.uniqueId"/>
        </Name>
    </ExternalIdentifier>
</ExtrinsicObject>
<!-- ExtrinsicObject zur ePrescription 160.000.000.000.123.76^eP.PDF (CDA
Level 1) -->
    <ExtrinsicObject home="urn:oid:1.2.246.556.12001.4.1000.990.1"
id="urn:uuid:740c850d-67c3-4481-bb0b-8bf32a17e034" lid="urn:uuid:740c850d-67c3-4481-bb0b-
8bf32a17e034" mimeType="text/xml" objectType="urn:uuid:7edca82f-054d-47f2-a032-9b2a5b5186c1"
status="urn:oasis:names:tc:ebxml-regrep:StatusType:Approved">
        <Slot name="sourcePatientId">
            <ValueList>
                <Value>B123456789|
A2C4E6^^^&1.2.276.0.76.3.1.580.147&ISO</Value>
            </ValueList>
        </Slot>
        <Slot name="size">
            <ValueList>
                <Value>0</Value>
            </ValueList>
        </Slot>
        <Slot name="creationTime">
            <ValueList>
                <Value>20230717</Value>
            </ValueList>
        </Slot>
        <Slot name="repositoryUniqueId">
            <ValueList>
                <Value>1.2.276.0.76.3.1.580.147</Value>
            </ValueList>
        </Slot>
        <Name>
            <LocalizedString value="ePrescription source coded PDF/A"/>
        </Name>
        <Description>
            <LocalizedString value="Lercanidipin Omniapharm, 10 mg, tablet"/>
        </Description>
        <VersionInfo versionName="1.1"/>
        <Classification classificationScheme="urn:uuid:f4f85eac-e6cb-4883-b524-
f2705394840f" classifiedObject="urn:uuid:740c850d-67c3-4481-bb0b-8bf32a17e034"
id="urn:uuid:a46daadc-6ef9-45ae-943a-1e433fc60ca5" nodeRepresentation="N">
            <Slot name="codingScheme">
                <ValueList>
                    <Value>2.16.840.1.113883.5.25</Value>
                </ValueList>
            </Slot>
        <Name>

```

```

        <LocalizedString value="normal"/>
    </Name>
</Classification>
<Classification classificationScheme="urn:uuid:41a5887f-8865-4c09-adf7-
e362475b143a" classifiedObject="urn:uuid:740c850d-67c3-4481-bb0b-8bf32a17e034"
id="urn:uuid:445581e6-14e3-45d6-b745-8ab8f8996883" nodeRepresentation="57833-6">
    <Slot name="codingScheme">
        <ValueList>
            <Value>2.16.840.1.113883.6.1</Value>
        </ValueList>
    </Slot>
    <Name>
        <LocalizedString value="eHDSI - ePrescription"/>
    </Name>
</Classification>
<Classification classificationScheme="urn:uuid:f0306f51-975f-434e-a61c-
c59651d33983" classifiedObject="urn:uuid:740c850d-67c3-4481-bb0b-8bf32a17e034"
id="urn:uuid:1edf12fc-03eb-4419-8fb2-2aefbc3ecd75" nodeRepresentation="57833-6">
    <Slot name="codingScheme">
        <ValueList>
            <Value>2.16.840.1.113883.6.1</Value>
        </ValueList>
    </Slot>
    <Name>
        <LocalizedString value="eHDSI - ePrescription"/>
    </Name>
</Classification>
<Classification classificationScheme="urn:uuid:f33fb8ac-18af-42cc-ae0e-
ed0b0bdb91e1" classifiedObject="urn:uuid:740c850d-67c3-4481-bb0b-8bf32a17e034"
id="urn:uuid:c6bded8b-7ebc-44cf-8069-6883eb76003c" nodeRepresentation="DE">
    <Slot name="codingScheme">
        <ValueList>
            <Value>1.0.3166.1</Value>
        </ValueList>
    </Slot>
    <Name>
        <LocalizedString value="Germany"/>
    </Name>
</Classification>
<Classification classificationScheme="urn:uuid:ccc598-8b07-4b77-a05e-
ae952c785ead" classifiedObject="urn:uuid:740c850d-67c3-4481-bb0b-8bf32a17e034"
id="urn:uuid:cb94e806-c7a6-4afa-9726-94a4718f1123" nodeRepresentation="Not Used">
    <Slot name="codingScheme">
        <ValueList>
            <Value>eHDSI Practice Setting Codes-Not Used</Value>
        </ValueList>
    </Slot>
    <Name>
        <LocalizedString value="Not Used"/>
    </Name>
</Classification>
<Classification classificationScheme="urn:uuid:2c6b8cb7-8b2a-4051-b291-
b1ae6a575ef4" classifiedObject="urn:uuid:740c850d-67c3-4481-bb0b-8bf32a17e034"
id="urn:uuid:9108022e-620f-46d6-a2df-1196f3e03f7c"
nodeRepresentation="urn:ihe:iti:xdw:2011:eventCode:open">
    <Slot name="codingScheme">
        <ValueList>
            <Value>1.3.6.1.4.1.19376.1.2.3</Value>
        </ValueList>
    </Slot>
    <Name>
        <LocalizedString value="Open"/>
    </Name>
</Classification>
<Classification classificationScheme="urn:uuid:2c6b8cb7-8b2a-4051-b291-
b1ae6a575ef4" classifiedObject="urn:uuid:740c850d-67c3-4481-bb0b-8bf32a17e034"
id="urn:uuid:6ecba789-4372-410a-816b-2dab0fae53a1" nodeRepresentation="C08CA13">
    <Slot name="codingScheme">
        <ValueList>
            <Value>2.16.840.1.113883.6.73</Value>
        </ValueList>
    </Slot>

```

```

        <Name>
          <LocalizedString value="Lercanidipin"/>
        </Name>
      </Classification>
      <Classification classificationScheme="urn:uuid:2c6b8cb7-8b2a-4051-b291-
b1ae6a575ef4" classifiedObject="urn:uuid:740c850d-67c3-4481-bb0b-8bf32a17e034"
id="urn:uuid:2a6b8821-7e12-4edd-bbcc-dfe5b9fe976d" nodeRepresentation="10219000">
        <Slot name="codingScheme">
          <ValueList>
            <Value>0.4.0.127.0.16.1.1.2.1</Value>
          </ValueList>
        </Slot>
      </Name>
      <Name>
        <LocalizedString value="Tablet"/>
      </Name>
    </Classification>
    <Classification classificationScheme="urn:uuid:2c6b8cb7-8b2a-4051-b291-
b1ae6a575ef4" classifiedObject="urn:uuid:740c850d-67c3-4481-bb0b-8bf32a17e034"
id="urn:uuid:88f555f9-aaad-4f0b-8bb6-00f57c1f57cd" nodeRepresentation="10 mg">
      <Slot name="codingScheme">
        <ValueList>
          <Value>eHDSI_Strength_CodeSystem</Value>
        </ValueList>
      </Slot>
    </Name>
    <Name>
      <LocalizedString value="Strength of medication"/>
    </Name>
  </Classification>
  <Classification classificationScheme="urn:uuid:a09d5840-386c-46f2-b5ad-
9c3699a4309d" classifiedObject="urn:uuid:740c850d-67c3-4481-bb0b-8bf32a17e034"
id="urn:uuid:d581da40-cd28-4723-a655-27cd71f10ff1" nodeRepresentation="urn:ihe:iti:xds-
sd:pdf:2008">
    <Slot name="codingScheme">
      <ValueList>
        <Value>IHE PCC</Value>
      </ValueList>
    </Slot>
  </Name>
  <Name>
    <LocalizedString value="PDF/A coded document"/>
  </Name>
</Classification>
<Classification classificationScheme="urn:uuid:93606bcf-9494-43ec-9b4e-
a7748d1a838d" classifiedObject="urn:uuid:740c850d-67c3-4481-bb0b-8bf32a17e034"
id="urn:uuid:15d15a88-49a5-4d27-80bd-d633e39c709a" nodeRepresentation="">
  <Slot name="authorPerson">
    <ValueList>
      <Value>Manfred Lapp</Value>
    </ValueList>
  </Slot>
  <Slot name="authorInstitution">
    <ValueList>
      <Value>Bundeswehrkrankenhaus
Berlin^^^^^^^^^2.999.1.2.3.5.8.9.1789.45</Value>
    </ValueList>
  </Slot>
</Classification>
<ExternalIdentifier id="urn:uuid:b5618bd5-21bd-4d4c-ae7f-cd4bac8d87f1"
identificationScheme="urn:uuid:58a6f841-87b3-4a3e-92fd-a8ffeff98427"
objectType="urn:oasis:names:tc:ebxml-regrep:ObjectType:RegistryObject:ExternalIdentifier"
registryObject="urn:uuid:740c850d-67c3-4481-bb0b-8bf32a17e034" value="B123456789|
A2C4E6^^^&1.2.276.0.76.3.1.580.147&ISO">
  <Name>
    <LocalizedString value="XSDDocumentEntry.patientId"/>
  </Name>
</ExternalIdentifier>
<ExternalIdentifier id="urn:uuid:294f2a0b-a31e-463d-85ae-bd702e4a17ef"
identificationScheme="urn:uuid:2e82c1f6-a085-4c72-9da3-8640a32e42ab"
objectType="urn:oasis:names:tc:ebxml-regrep:ObjectType:RegistryObject:ExternalIdentifier"
registryObject="urn:uuid:740c850d-67c3-4481-bb0b-8bf32a17e034"
value="160.000.000.000.123.76^eP.PDF">
  <Name>
    <LocalizedString value="XSDDocumentEntry.uniqueId"/>
  </Name>

```

```

        </Name>
        </ExternalIdentifier>
    </ExtrinsicObject>
    <Association associationType="urn:ihe:iti:2007:AssociationType:XFRM"
id="urn:uuid:3bbf0de6-e186-4b18-b3ad-302790ef7c1c" sourceObject="urn:uuid:740c850d-67c3-
4481-bb0b-8bf32a17e034" targetObject="urn:uuid:cb804da7-407c-4590-b394-ad3d7617995d"/>
    </RegistryObjectList>
    </AdhocQueryResponse>
</Body>
</Envelope>
    
```

Ausgabeparameter des TUC

- Dieser TUC hat keine Ausgabeparameter.

6.1.3 Operation Cross_Gateway_Retrieve::RetrieveDocument

Tabelle 49: TAB_NCPeH_Definition_Operation_RetrieveDocument

Operation	Cross_Gateway_Retrieve::RetrieveDocument	
Beschreibung	Diese Operation wird aufgerufen, wenn das Initiating Gateway (NCPeH Land-B) eine Anfrage von einem behandelnden LE-EU empfängt und sie nachfolgend an diese Operation sendet. Durch die Anfrage MUSS der NCPeH-FD anhand konkreter Identifikatoren die Gesundheitsdaten des Versicherten aus dem jeweiligen Fachdienst in der TI ermitteln und diese dem NCPeH Land-B im angeforderten eHDSI CDA-Pivotformat bereitstellen. In Abhängigkeit vom angeforderten Dokumentenformat MUSS der NCPeH-FD die abgerufenen Gesundheitsdaten im strukturierten Dokumentenformat (CDA Level 3) und/oder im PDF/A-Format (CDA Level 1) bereitstellen.	
Eingangsparameter		
Name	Beschreibung	Typ
Cross Gateway Retrieve Request	Eingangsnachricht zur Abfrage eines ePKA MIO gemäß [eHDSI_XCA_Profile#2.4]	RetrieveDocumentSetRequest [ITI-39]
X-User Assertion	Authentication Assertion des anfragenden LE-EU	SAML 2.0 Assertion gemäß [eHDSI_SAML_Profile#2] inkl. X.509 öffentliches Signaturzertifikat des NCPeH Land-B [eHDSI_X.509_Certificates_Profile]
TRC Assertion	Bestätigung über das Bestehen einer Behandlungsbeziehung zwischen LE-EU und Versicherter	SAML 2.0 Assertion gemäß [eHDSI_SAML_Profile#4] inkl. X.509 öffentliches Signaturzertifikat des NCPeH Land-B [eHDSI_X.509_Certificates_Profile]
Ausgangsparameter		

Name	Beschreibung	Typ
Cross Gateway Retrieve Response	Ausgangsnachricht gemäß [eHDSI_XCA_Profile#2.4]	RetrieveDocumentSetResponse [ITI-39]

Der NCPeH-FD MUSS in der Lage sein, aus der IHE XCA.RetrieveDocument-Anfrage für jedes DocumentRequest-Element anhand der Kriterien aus der Tabelle TAB_NCPeH_Kriterien_Zuordnung_IHE-XCA.RetrieveDocument_Anfragen_zu_Anwendungsszenarien das passende Anwendungsszenario eindeutig zu bestimmen und die Anfrage dem entsprechenden TUC zuzuordnen, von dem aus die Anfrage weiterverarbeitet wird.

Tabelle 50: TAB_NCPeH_Kriterien_Zuordnung_IHE-XCA.RetrieveDocument_Anfragen_zu_Anwendungsszenarien

DocumentUniqueId	Technischer Use Case (TUC)
Endet mit "^PS.XML"	[6.1.3.1- TUC_NCPeH_005: Cross Gateway Retrieve Request zur Abfrage der Patient Summary CDA Level 3 verarbeiten] (Anwendungsszenario: Patient Summary Land-A; Abfrage eines kodierten ePKA MIO in CDA Level 3)
Endet mit "^PS.PDF"	[6.1.3.3- TUC_NCPeH_007: Cross Gateway Retrieve Request zur Abfrage der Patient Summary CDA Level 1 verarbeiten] (Anwendungsszenario: Patient Summary Land-A; Abfrage eines ePKA MIO im PDF/A-Format, CDA Level 1)
Endet mit "^eP.XML" oder mit "^eP.PDF"	[6.1.3.7- TUC_NCPeH_027: Cross Gateway Retrieve Request für ePeD-A auf Einhaltung von allgemeinen Kriterien prüfen] Anwendungsszenario: ePrescription/eDispensation Land-A
Eine Mischung aus DocumentUniqueId-Elementen mit unterschiedlichen Endungen für verschiedene Anwendungsszenarien (z.B. "^PS.XML" und "^eP.XML")	Das Abrufen von Dokumenten für verschiedene Anwendungsszenarien in derselben Anfrage wird derzeit nicht unterstützt. Nach Eingang der Anfrage MUSS der NCPeH-FD einen Non-Repudiation of Receipt Eintrag gemäß [4.1.7.2 - Non-Repudiation of Receipt erstellen] und einen Audit Trail Eintrag gemäß [4.1.7.3 Patient

	<p>Privacy Audit Trail Eintrag erstellen] in der Komponente Audit Repository speichern. Bei der Erstellung des Audit Trail Eintrages der NCPeH-FD MUSS Vorgaben aus [eHDSI_XCA_Profile#4.3] umsetzen.</p> <p>Der NCPeH-FD MUSS eine weitere Verarbeitung der Anfrage abbrechen und dem anfragenden NCPeH Land-B mit einer Cross GatewayRetrieveResponse-Nachricht gemäß Vorgaben aus [eHDSI_XCA_Profile#2.4] antworten und dabei folgende Informationen zum Fehler angeben:</p> <ul style="list-style-type: none"> • errorCode: ERROR_EP_GENERIC • codeContext: "" • severity: urn:oasis:names:tc:ebxml-regrep:ErrorSeverityType:Error • location: "" <p>Nach Versand der Fehlermeldung an den jeweiligen NCPeH Land-B MUSS der NCPeH-FD einen Non-Repudiation of Origin Eintrag gemäß [4.1.7.1 - Non-Repudiation of Origin erstellen] und einen Audit Trail Eintrag gemäß [4.1.7.3 Patient Privacy Audit Trail Eintrag erstellen] in der Komponente Audit Repository speichern. Bei der Erstellung des Audit Trail Eintrages der NCPeH-FD MUSS Vorgaben aus [eHDSI_XCA_Profile#4.3] umsetzen.</p>
<p>Ein anderer Wert</p>	<p>Das angeforderte Anwendungsszenario und das Dokumentenformat sind nicht bekannt oder werden derzeit nicht unterstützt.</p> <p>Nach Eingang der Anfrage MUSS der NCPeH-FD einen Non-Repudiation of Receipt Eintrag gemäß [4.1.7.2- Non-Repudiation of Receipt erstellen] und einen Audit Trail Eintrag gemäß [4.1.7.3- Patient Privacy Audit Trail Eintrag erstellen] in der Komponente Audit Repository speichern. Bei der Erstellung des Audit Trail Eintrages der NCPeH-FD MUSS Vorgaben aus [eHDSI_XCA_Profile#4.3] umsetzen.</p> <p>Der NCPeH-FD DARF die Anfrage zum DocumentRequest-Element NICHT weiter bearbeiten und MUSS auf das DocumentRequest-Element mit dem Fehlercode ERROR_GENERIC antworten.</p> <p>Nach Versand der Fehlermeldung an den jeweiligen NCPeH Land-B MUSS der NCPeH-FD einen Non-Repudiation of Origin Eintrag gemäß [4.1.7.1 Non-Repudiation of Origin erstellen] und einen Audit</p>

	Trail Eintrag gemäß [4.1.7.3- Patient Privacy Audit Trail Eintrag erstellen] in der Komponente Audit Repository speichern. Bei der Erstellung des Audit Trail Eintrages der NCPeH-FD MUSS Vorgaben aus [eHDSI_XCA_Profile#4.3] umsetzen.
--	--

6.1.3.1 TUC_NCPeH_005: Cross Gateway Retrieve Request zur Abfrage der Patient Summary CDA Level 3 verarbeiten

Für diesen TUC gelten folgende übergreifende Festlegungen

- [4.1.3- eHDSI Basisleistungen]
- [4.1.5- Validierung der Identity Assertion des LE-EU]
- [4.1.6- Validierung der TRC Assertion]
- [4.1.7.2- Non-Repudiation of Receipt erstellen]
- [4.1.7.3- Patient Privacy Audit Trail Eintrag erstellen]
- [4.1.8- Festlegungen zur Prüfung der Zugriffsberechtigung auf Fachdienste der TI]

Ablauf des TUC

Der NCPeH-FD MUSS einen Non-Repudiation of Receipt Eintrag gemäß [4.1.7.2 - Non-Repudiation of Receipt erstellen] und einen Audit Trail Eintrag gemäß [4.1.7.3 Patient Privacy Audit Trail Eintrag erstellen] in der Komponente Audit Repository speichern. Bei der Erstellung des Audit Trail Eintrages MUSS der NCPeH-FD die Vorgaben aus [eHDSI_XCA_Profile#4.3] umsetzen. Wenn zum Zeitpunkt der Erstellung des Audit Trail Eintrags nicht alle erforderlichen Daten im NCPeH-FD verfügbar sind, MÜSSEN die Daten in den Audit Trail Eintrag aufgenommen werden, sobald sie im NCPeH-FD verfügbar sind, spätestens aber nachdem die Antwort an NCPeH Land-B gesendet wurde.

Der NCPeH-FD MUSS bei der Verarbeitung der Anfrage neben den Vorgaben aus [eHDSI_XCA_Profile#2.4] auch die folgenden Vorgaben für das DocumentRequest-Element umsetzen:

Tabelle 51: TAB_NCPeH_Nutzungskonvention_XCA_Retrieve_Request_PSA_CDA3

Element aus der Anfrage	Nutzungskonvention
HomeCommunityId	Der Wert MUSS ohne das Präfix "urn:oid:" identisch mit dem Wert des Konfigurationsparameters HOME_COMMUNITY_ID_NCPeH-FD aus [4.1.1- Konfigurationsparameter] sein.
RepositoryUniqueld	Der Wert DARF NICHT leer sein und MUSS der Variable METADATA_ePKA_MIO_repositoryUniqueld zugewiesen werden.
DocumentUniqueld	Der Wert DARF NICHT leer sein und nur der erste Teil "DocumentIdentifier des ePKA MIO" MUSS zum Abruf des ePKA MIO des Versicherten im ePA-Aktensystem verwendet werden. Der Wert des Elementes muss nach folgender Vorschrift

	<p>strukturiert sein:</p> <ol style="list-style-type: none"> 1. DocumentIdentifier des ePKA MIO 2. "^" 3. "PS.XML" <p>Aus dem Wert des Elementes MUSS der Wert des ersten Teils "DocumentIdentifier des ePKA MIO" der Variable METADATA_ePKA_MIO_uniqueld für Zwecke der internen Verwendung zugewiesen werden. Anhand des letzten Teils PS.XML wird festgestellt, dass der LE-EU kodierte medizinische Daten angefordert hat.</p>
--	---

Bei folgenden Fehlerfällen MUSS der NCPeH-FD eine weitere Verarbeitung der Anfrage abbrechen und dem anfragenden NCPeH Land-B mit einer Fehlernachricht mittels der Response-Nachricht gemäß [6.1.3.2 TUC_NCPeH_006: Cross Gateway Retrieve Response mit Patient Summary CDA Level 3 senden] antworten:

Tabelle

52: TAB_NCPeH_Fehlerfälle_Verarbeitung_Cross_Gateway_Retrieve_Request_PSA_CDA3

Fehlerfall	errorCode (gemäß [eHDSI_NCPeH_Components#6.4])	codeContext	severity	location
Die Variable ida_name-id ist leer.	ERROR_HPI_INSUFFICIENT_INFORMATION	"Access denied. The identifier of the health professional is missing in the provided identity information."	urn:oasis:names:tc:ebxml-regrep:ErrorSeverityType:Error	Keine Angaben
Die Variable ida_practitioner_name ist leer.		"Access denied. The		Keine Angaben

		<p>name of the EU health professional is missing in the provided identity information."</p>	
<p>Die Variable ida_practitioner_role ist leer.</p>		<p>"Access denied. The information about the role of EU health professional is missing in the provided identity information."</p>	<p>Keine Angaben</p>
<p>Der Wert der Variable ida_practitioner_role_code ist leer oder dieser ist nicht identisch mit einem der möglichen Werte für das Element urn:oasis:names:tc:xacml:2.0:subject:role aus</p>		<p>"Access denied. Missing or unknown role</p>	<p>"Received role code of the health professional from the identity assertion; see element urn:oasis:names:tc:xacml:2.0:subject:role=" +</p>

[eHDSI_SAML_Profile#2.3].		of the EU health professional in the provided identity information."	Wert der Variable ida_practitioner_role_code
Der Wert der Variable ida_healthcare_facility_type_code ist leer oder nicht identisch mit einem der vorgegebenen Werte aus [eHDSI_SAML_Profile#2.3] für das Identitätsattribut urn:ehdsi:names:subject:healthcare-facility-type.	ERROR_HPI_POC_NO_INFORMATION	"Access denied. Missing or unknown type of Healthcare Provider Organization in the provided identity information."	"Received healthcare facility type code=" + Wert der Variable ida_healthcare_facility_type_code
Die Variable ida_point_of_care ist leer.		"Access denied. Missing name of the point of care in	Keine Angaben

		the provided identity information."	
Die Variable <code>tls_country</code> aus dem TLS-Zertifikat des NCPeH Land-B (siehe [4.1.3.1 Sicherer Kanal: TESTA-ng und TLS]) DARF NICHT leer sein und MUSS in der <code>WHITELIST_NCPeH_COUNT RY-B</code> nach [4.1.2 "Datenaustausch mit zugelassenen EU-Ländern"] enthalten sein.	ERROR_PS_GENERIC	"The patient summary service is not agreed with the requesting country. Please contact your service provider or administrator."	"The DN structure in the subject of the received TLS certificate does not contain a valid EU country code or the addressed service is not agreed between the requesting country and germany. Received country code from TLS certificate= " + Wert der Variable <code>tls_country</code>
Die Variable <code>ida_permissions</code> , falls sie nicht leer ist, enthält nicht alle Permission Codes gemäß den Vorgaben aus [4.1.8 - Festlegungen zur Prüfung der Zugriffsberechtigung auf Fachdienste der TI] für den eHDSI Use Case "Request for Patient Summary"		"Access denied. Please contact your service provider or administrator and check	"Received permission codes=" + Wert der Variable <code>ida_permissions</code>

		<p>the access rights for your health care professional role in your country."</p>		
<p>Die Variable ida_permissions ist leer und die Bedingungen zur Erlangung einer Zugriffsberechtigung auf ePA nach [4.1.8 - Festlegungen zur Prüfung der Zugriffsberechtigung auf Fachdienste der TI] sind nicht erfüllt.</p>		<p>"Access denied. The information provided about the role of the health professional does not comply with German regulations."</p>		<p>"No permission codes have been received and the access cannot be granted for the received practitioner role code in accordance with national regulations. Received practitioner role code=" + Wert der Variable ida_practitioner_role_code</p>
<p>Der Wert der Variable trc_kvnr ist leer oder verletzt die Vorgaben aus [4.1.9- Format und Validierung der KVNR].</p>		<p>"Please make sure that the health</p>		<p>"Health insurant number is missing or invalid."</p>

		<p>h insur ant ident ifier is given and corre ct"</p>	
<p>Der Wert der Variable trc_accesscode ist leer oder verletzt die Formatvorgaben aus [4.1.6 - Validierung der TRC-Assertion]</p>		<p>"Acce ss denie d. Th e patie nts acce s code is missi ng or malfo rmed. Pleas e ask the patie nt for acce s autho risat ion and the prope r acce s code. "</p>	<p>Keine Angaben</p>
<p>Das Element HomeCommunityId entspricht nicht der Nutzungskonvention gemäß Tabelle TAB_NCPeH_Nutzungskonvention_XCA_Retrieve_Request_PSA_CDA3.</p>		<p>"Wron g ident ifier for the germa n gatew ay</p>	<p>"The Home Community ID for the German NCPeH is wrong. Received HomeCommunityI d= " + Wert aus dem ElementHomeComm unityId (falls der</p>

		<p>service received. Please contact your service provider or administrator."</p>	<p>Wert nicht leer ist, ansonsten keine Angaben)</p>
<p>Das Element RepositoryUniqueId entspricht nicht der Nutzungskonvention gemäß Tabelle TAB_NCPeH_Nutzungskonvention_XCA_Retrieve_Request_PSA_CDA3.</p>		<p>"Wrong identifier for the german ehealth record service received. Please contact your service provider or administrator."</p>	<p>"The Repository Unique ID does not match with an ID of the German ehealth record services. Received RepositoryUniqueId= " + Wert aus dem ElementRepositoryUniqueId (falls der Wert nicht leer ist, ansonsten keine Angaben)</p>
<p>Die Prüfung des vorderen Teils (ohne Endung "^PS.XML") des Elementes DocumentUniqueid gemäß Nutzungskonvention aus Tabelle TAB_NCPeH_Nutzungskonvention_XCA_Retrieve_Request_PSA_CDA3 ist</p>	<p>ERROR_INCORRECT_FORMATTING</p>	<p>"The identifier of the requested document</p>	<p>"The identifier of the patient summary document is missing or not correct. Received DocumentUniqueid = " + Wert aus</p>

nicht erfolgreich.		is missing or not correct. Please contact your service provider or administrator."	dem ElementDocumentUniqueId
--------------------	--	--	-----------------------------

Hinweis: Die Initiierung der Variablen ida_permissions, ida_practitioner_role_code, ida_healthcare_facility_type_code, ida_name-id, ida_practitioner_role und ida_point_of_care erfolgt im [4.1.5 - Validierung der Identity Assertion des LE-EU] und der Variablen trc_kvnr und trc_accesscode im [4.1.6 - Validierung der TRC-Assertion].

Beispiel für eine XCA.Retrieve-Anfrage in der eHDSI zur Abfrage eines kodierten ePKA MIO:

```
<RetrieveDocumentSetRequest>
  <DocumentRequest>
    <HomeCommunityId>urn:oid:1.2.276.0.76.4.291</HomeCommunityId>
    <RepositoryUniqueId>2.16.620.1.101.10.3.29.54290</RepositoryUniqueId>
    <DocumentUniqueId>1.2.84.116.1.800.254.370.349.563.1605.469.534.1338^PS.XML</
DocumentUniqueId>
  </DocumentRequest>
</RetrieveDocumentSetRequest>
```

Ausgabeparameter des TUC

- METADATA_ePKA_MIO_repositoryUniqueId
- METADATA_ePKA_MIO_uniqueId

6.1.3.2 TUC_NCPeH_006: Cross Gateway Retrieve Response mit Patient Summary CDA Level 3 senden

Für diesen TUC gelten folgende übergreifende Festlegungen

- [4.1.3- eHDSI Basisleistungen]
- [4.1.7.1 Non-Repudiation of Origin erstellen]
- [4.1.7.3- Patient Privacy Audit Trail Eintrag erstellen]

Ablauf des TUC

Der NCPeH-FD MUSS die Antwort auf die Anfrage vom NCPeH Land-B gemäß Vorgaben aus [eHDSI_XCA_Profile#2.4] erstellen und dabei folgende Nutzungsvorgaben beachten:

Tabelle 53: TAB_NCPeH_Nutzungskonvention_XCA_Retrieve_Response_PSA_CDA3

Element in der Antwort	Nutzungskonvention
HomeCommunityId	Dieses Element MUSS einen Wert wie folgt enthalten: "urn:oid:" + Wert des Konfigurationsparameters HOME_COMMUNITY_ID_NCPeH-FD aus [4.1.1- Konfigurationsparameter] Beispiel: urn:oid:2.16.17.710.860.1000.990.1
RepositoryUniqueld	Dieses Element MUSS den Wert der Variable METADATA_ePKA_MIO_repositoryUniqueld aus [6.1.3.1-TUC_NCPeH_005: Cross Gateway Retrieve Request zur Abfrage der Patient Summary CDA Level 3 verarbeiten] enthalten.
DocumentUniqueld	Der Wert dieses Elementes MUSS nach folgender Vorschrift aufgebaut sein: 1. Wert der Variable METADATA_ePKA_MIO_uniqueld aus [6.1.3.1-TUC_NCPeH_005: Cross Gateway Retrieve Request zur Abfrage der Patient Summary CDA Level 3 verarbeiten] 2. "^" 3. "PS.XML" Z. B.: 1.2.84.116.1.800.254.370.349.563.1605.469.534.1338^PS.XML
contentType	text/xml
Document	Dieses Element MUSS ein Dokument (siehe Ausgabeparameter in [6.1.3.5- TUC_NCPeH_009: NFD des ePKA MIO transkodieren und transformieren]) im Format eHDSI Patient Summary CDA Pivotformat Level 3 in Base64-Kodierung enthalten

In der Response können [ebRIM_Representation_Document#4.2.4] Error Codes auftreten, die entsprechende ResponseStatus-Informationen aufweisen. Das Vorhandensein einer Error-List ist prinzipiell vereinbar mit einer teilweise erfolgreichen Verarbeitung. Wenn die ErrorList nur Warnings enthält (RegistryError elements mit warning severity, aber ohne error severity), dann MUSS die Verarbeitung als erfolgreich angesehen werden. Die Rückmeldungen zu Fehlern und Warnungen an NCPeH Land-B, die bei der Verarbeitung der Anfrage, dem Abruf des ePKA MIO des Versicherten oder der Transkodierung und Transformierung entstanden sind, MÜSSEN das in [ebRIM_Representation_Document#4.2.4] "Success and Error Reporting" beschriebene Format haben und MÜSSEN in die Response-Nachricht aufgenommen werden. Es wird im Fehlerfall ggf. eine Fehlerliste (RegistryErrorList) und darin ein Fehler (RegistryError) je fehlgeschlagenem DocumentRequest mit den Attributen errorCode, codeContext, severity und location zurückgegeben.

Darüber hinaus MUSS der NCPeH-FD die Vorgaben aus [ebRIM_Representation_Document#4.2.4.2] für die Verwendung des status-Attributs im RegistryResponse-Element und die Vorgaben für den Umgang mit dem RegistryErrorList-Element umsetzen.

Der NCPeH-FD MUSS beim Versenden der Response-Nachricht einen Non-Repudiation of Origin Eintrag gemäß [4.1.7.1 - Non-Repudiation of Origin erstellen] in der Komponente Audit Repository speichern.

Beispiel einer Retrieve-Response mit einem CDA-Dokument Level 3 in Base64-Kodierung.

```
<RetrieveDocumentSetResponse>
  <RegistryResponse status="urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Success"/>
  <DocumentResponse>
    <HomeCommunityId>urn:oid:2.16.17.710.860.1000.990.1</HomeCommunityId>
    <RepositoryUniqueId>2.16.620.1.101.10.3.29.54290</RepositoryUniqueId>
    <DocumentUniqueId>1.2.84.116.1.800.254.370.349.563.1605.469.534.1338^PS.XML</
DocumentUniqueId>
    <mimeType>text/xml</mimeType>
    <Document>... CDA LEVEL 3 BASE64 ENCODED...</Document>
  </DocumentResponse>
</RetrieveDocumentSetResponse>
```

Ausgabeparameter des TUC

- Keine

6.1.3.3 TUC_NCPeH_007: Cross Gateway Retrieve Request zur Abfrage der Patient Summary CDA Level 1 verarbeiten

Für diesen TUC gelten folgende übergreifende Festlegungen

- [4.1.3- eHDSI Basisleistungen]
- [4.1.5- Validierung der Identity Assertion des LE-EU]
- [4.1.6- Validierung der TRC Assertion]
- [4.1.7.2- Non-Repudiation of Receipt erstellen]
- [4.1.7.3- Patient Privacy Audit Trail Eintrag erstellen]
- [4.1.8- Festlegungen zur Prüfung der Zugriffsberechtigung auf Fachdienste der TI]

Ablauf des TUC

Nach Eingang der Anfrage MUSS der NCPeH-FD einen Non-Repudiation of Receipt Eintrag gemäß [4.1.7.2- Non-Repudiation of Receipt erstellen] und einen Audit Trail Eintrag gemäß [4.1.7.3- Patient Privacy Audit Trail Eintrag erstellen] in der Komponente Audit Repository speichern. Bei der Erstellung von Audit Trails MÜSSEN die Vorgaben aus [eHDSI_XCA_Profile#4.3] umgesetzt werden. Wenn zum Zeitpunkt der Erstellung des Audit Trail Eintrags nicht alle erforderlichen Daten im NCPeH-FD verfügbar sind, MÜSSEN die Daten in den Audit Trail Eintrag aufgenommen werden, sobald sie im NCPeH-FD verfügbar sind, spätestens aber nachdem die Antwort an NCPeH Land-B gesendet wurde.

Der NCPeH-FD MUSS bei der Verarbeitung der Anfrage neben den Vorgaben aus [eHDSI_XCA_Profile#2.4] auch die folgenden Vorgaben für das DocumentRequest-Element umsetzen:

Tabelle 54: TAB_NCPeH_Nutzungskonvention_XCA_Retrieve_Request_PSA_CDA1

Element aus der Anfrage	Nutzungskonvention
-------------------------	--------------------

HomeCommunityId	Dieser Wert MUSS ohne das Präfix "urn:oid:" identisch mit dem Wert des Konfigurationsparameters HOME_COMMUNITY_ID_NCPeH-FD aus [4.1.1- Konfigurationsparameter] sein.
RepositoryUniqueld	Dieser Wert MUSS der Variable METADATA_ePKA_MIO_repositoryUniqueld zugewiesen werden.
DocumentUniqueld	<p>Der Wert DARF NICHT leer sein. Der erste Teil "DocumentIdentifier des ePKA MIO" MUSS zum Abruf des ePKA MIO des Versicherten aus dem ePA-Aktensystem verwendet werden.</p> <p>Der Wert des Elementes MUSS nach folgender Vorschrift strukturiert sein:</p> <ol style="list-style-type: none"> 1. DocumentIdentifier des ePKA MIO 2. "^" 3. "PS.PDF" <p>Aus dem Wert des Elementes MUSS der Wert "DocumentIdentifier des ePKA MIO" der Variable METADATA_ePKA_MIO_uniqueld für Zwecke der internen Verwendung zugewiesen werden. Anhand des letzten Teils PS.PDF kann festgestellt werden, dass der LE-EU die medizinischen Daten aus dem ePKA MIO im Originalzustand (ohne Transkodierung von ePKA MIO und Inhalte des ePKA MIO im PDF/A-Format) anfordert.</p>

Bei folgenden Fehlerfällen MUSS der NCPeH-FD eine weitere Verarbeitung der Anfrage abbrechen und dem anfragenden NCPeH Land-B mit einer Fehlernachricht mittels der Response-Nachricht gemäß [6.1.3.4 TUC_NCPeH_008: Cross Gateway Retrieve Response mit dem Patient Summary CDA Level 1 senden] antworten:

Tabelle
55: TAB_NCPeH_Fehlerfälle_Verarbeitung_Cross_Gateway_Retrieve_Request_PSA_CDA1

Fehlerfall	errorCode (gemäß [eHDSI_NCPeH_Components#6.4])	codeContext	severity	location
Die Variable ida_name-id ist leer.	ERROR_HPI_INSUFFICIENT_INFORMATION	"Access denied . The identifier of the health professional is missin	urn:oasis:names:tc:ebxml-regrep:ErrorSeverity Type:Error	Keine Angaben

		g in the provided identity information."		
Die Variable ida_practitioner_name ist leer.		"Access denied . The name of the EU health professional is missing in the provided identity information."		Keine Angaben
Die Variable ida_practitioner_role ist leer.		"Access denied . The information about the role of EU health professional is missing in the provided identity information."		Keine Angaben

<p>Der Wert der Variable <code>ida_practitioner_role_code</code> ist leer oder dieser ist nicht identisch mit einem der möglichen Werte für das Element <code>urn:oasis:names:tc:xacml:2.0:subject:role</code> aus [eHDSI_SAML_Profile#2.3].</p>		<p>"Access denied · Missing or unknown role of the EU health professional in the provided identity information."</p>	<p>"Received role code of the health professional from the identity assertion; see element <code>urn:oasis:names:tc:xacml:2.0:subject:role</code> = " + Wert der Variable <code>ida_practitioner_role_code</code></p>
<p>Der Wert der Variable <code>ida_healthcare_facility_type_code</code> ist leer oder nicht identisch mit einem der vorgegebenen Werte aus [eHDSI_SAML_Profile#2.3] für das Identitätsattribut <code>urn:ehdsi:names:subject:healthcare-facility-type</code>.</p>	<p>ERROR_HPI_POC_NO_INFORMATION</p>	<p>"Access denied · Missing or unknown type of Health care Provider Organization in the provided identity information."</p>	<p>"Received healthcare facility type=" + Wert der Variable <code>ida_healthcare_facility_type_code</code></p>
<p>Die Variable <code>ida_point_of_care</code> ist leer.</p>		<p>"Access denied · Missing name of the point of care"</p>	<p>Keine Angaben</p>

		in the provided identity information."	
<p>Die Variable <code>tls_country</code> aus dem TLS-Zertifikat des NCPeH Land-B (siehe [4.1.3.1 Sicherer Kanal: TESTA-ng und TLS]) DARF NICHT leer sein und MUSS in der WHITELIST_NCPeH_COUNT RY-B nach [4.1.2 "Datenaustausch mit zugelassenen EU-Ländern"] enthalten sein.</p>	<p>ERROR_PS_GENERIC</p>	<p>"The patient summary service is not agreed with the requesting country. Please contact your service provider or administrator."</p>	<p>"The DN structure in the subject of the received TLS certificate does not contain a valid EU country code or the addressed service is not agreed between the requesting country and germany. Received country code from TLS certificate= " + Wert der Variable <code>tls_country</code></p>
<p>Die Variable <code>ida_permissions</code>, falls sie nicht leer ist, enthält nicht alle Permission Codes gemäß den Vorgaben aus [4.1.8 - Festlegungen zur Prüfung der Zugriffsberechtigung auf Fachdienste der TI] für den eHDSI Use Case "Request for Patient Summary"</p>		<p>"Access denied. Please contact your service provider or administrator and check the access rights for your health</p>	<p>"Received permission codes=" + Wert der Variable <code>ida_permissions</code></p>

		<p>professional role in your country."</p>		
<p>Die Variable ida_permissions ist leer und die Bedingungen zur Erlangung einer Zugriffsberechtigung auf ePA nach [4.1.8 - Festlegungen zur Prüfung der Zugriffsberechtigung auf Fachdienste der TI] sind nicht erfüllt.</p>		<p>"Access denied . The information provided about the role of the health professional does not comply with German regulations."</p>		<p>"No permission codes received and the access cannot be granted for the received practitioner role code in accordance with national regulations. Received practitioner role code=" + Wert der Variable ida_practitioner_role_code</p>
<p>Der Wert der Variable trc_kvnr ist leer oder verletzt die Vorgaben aus [4.1.9- Format und Validierung der KVNR].</p>		<p>"Please make sure that the health insurance identifier is given and correct"</p>		<p>"Health insurance number is missing or invalid."</p>
<p>Der Wert der Variable trc_accesscode ist leer oder verletzt die Formatvorgaben aus [4.1.6 - Validierung der TRC-Assertion]</p>		<p>"Access denied . The patient's access code</p>		<p>Keine Angaben</p>

		<p>is missing or malformed. Please ask the patient for access authorization and the proper access code."</p>	
<p>Das Element HomeCommunityId entspricht nicht der Nutzungskonvention gemäß Tabelle TAB_NCPeH_Nutzungskonvention_XCA_Retrieve_Request_PSA_CDA1.</p>		<p>"Wrong identifier for the german gateway service received. Please contact your service provider or administrator."</p>	<p>"The Home Community ID for the German NCPeH is wrong. Received HomeCommunityd= " + Wert aus dem ElementHomeCommunityId (falls der Wert nicht leer ist, ansonsten keine Angaben)</p>
<p>Das Element RepositoryUniqueId entspricht nicht der Nutzungskonvention gemäß Tabelle TAB_NCPeH_Nutzungskonvention_XCA_Retrieve_Request_PSA_CDA1.</p>		<p>"Wrong identifier for the german ehealth record service received. Please contact</p>	<p>"The Repository Unique ID does not match with an ID of the German ehealth record services. Received RepositoryUniqueid= " + Wert aus dem ElementRepositoryUniqueid (falls der Wert nicht leer ist, ansonsten keine Angaben)</p>

		t your service provider or administrator."	
Die Prüfung des vorderen Teils (ohne Endung "^PS.PDF") des Elementes DocumentUniqueId gemäß Nutzungskonvention aus Tabelle TAB_NCPeH_Nutzungskonvention_XCA_Retrieve_Request_PSA_CDA1 ist nicht erfolgreich.	ERROR_INCORRECT_FORMATTING	"The identifier of the requested document is missing or not correct. Please contact your service provider or administrator."	"The identifier of the patient summary document is missing or not correct. Received DocumentUniqueId= " + Wert aus dem ElementDocumentUniqueId

Hinweis: Die Initiierung der Variablen `ida_permissions`, `ida_practitioner_role_code`, `ida_healthcare_facility_type_code`, `ida_name-id`, `ida_practitioner_role` und `ida_point_of_care` erfolgt im [4.1.5 - Validierung der Identity Assertion des LE-EU] und der Variablen `trc_kvnr` und `trc_accesscode` im [4.1.6 - Validierung der TRC-Assertion].

Beispiel einer XCA.Retrieve Anfrage in der eHDSI zur Abfrage des ePKA MIO eines Versicherten im PDF/A-Format:

```
<RetrieveDocumentSetRequest>
  <DocumentRequest>
    <HomeCommunityId>urn:oid:2.16.17.710.860.1000.990.1</HomeCommunityId>
    <RepositoryUniqueId>2.16.620.1.101.10.3.29.54290</RepositoryUniqueId>
    <DocumentUniqueId>1.2.84.116.1.800.254.370.349.563.1605.469.534.1338^PS.PDF</
DocumentUniqueId>
  </DocumentRequest>
</RetrieveDocumentSetRequest>
```

Ausgabeparameter des TUC

- METADATA_ePKA_MIO_repositoryUniqueId
- METADATA_ePKA_MIO_uniqueId

6.1.3.4 TUC_NCPeH_008: Cross Gateway Retrieve Response mit dem Patient Summary CDA Level 1 senden

Für diesen TUC gelten folgende übergreifende Festlegungen

- [4.1.3- eHDSI Basisleistungen]
- [[4.1.7.1 Non-Repudiation of Origin erstellen](#)]
- [4.1.7.3- Patient Privacy Audit Trail Eintrag erstellen]

Ablauf des TUC

Der NCPeH-FD MUSS die Antwort auf die Anfrage vom NCPeH-Land-B gemäß Vorgaben aus [eHDSI_XCA_Profile#2.4] erstellen und folgende Nutzungsvorschriften beachten:

Tabelle 56: TAB_NCPeH_Nutzungskonvention_XCA_Retrieve_Response_PSA_CDA1

Element in der Antwort	Nutzungskonvention
HomeCommunityId	Dieses Element MUSS einen Wert wie folgt enthalten: "urn:oid:" + Wert des Konfigurationsparameters HOME_COMMUNITY_ID_NCPeH-FD aus [4.1.1- Konfigurationsparameter] Beispiel: urn:oid:2.16.17.710.860.1000.990.1
RepositoryUniqueld	Dieses Element MUSS den Wert der Variable METADATA_ePKA_MIO_repositoryUniqueld aus [6.1.3.3- TUC_NCPeH_007: Cross Gateway Retrieve Request zur Abfrage der Patient Summary CDA Level 1 verarbeiten] enthalten.
DocumentUniqueld	Der Wert dieses Elementes MUSS nach folgender Vorschrift aufgebaut sein: 1. Wert der Variable METADATA_ePKA_MIO_uniqueld aus [6.1.3.3- TUC_NCPeH_007: Cross Gateway Retrieve Request zur Abfrage der Patient Summary CDA Level 1 verarbeiten] 2. "^" 3. "PS.PDF" Z.B.: 1.2.84.116.1.800.254.370.349.563.1605.469.534.1338^PS.PDF
contentType	text/xml
Document	Dieses Element MUSS das transformierte ePKA MIO des Versicherten als Dokument im Format eHDSI Patient Summary CDA embedded PDF/A Pivotformat Level 1 in Base64-Kodierung enthalten (siehe Ausgabeparameter in [6.1.3.6- TUC_NCPeH_010: NFD des ePKA MIO ins PDF/A-Format transformieren])

In der Response können [ebRIM_Representation_Document#4.2.4] Error Codes auftreten, die entsprechende ResponseStatus-Informationen aufweisen. Das Vorhandensein einer Error-List ist prinzipiell vereinbar mit einer teilweise erfolgreichen Verarbeitung. Wenn die ErrorList nur Warnings enthält (RegistryError elements mit warning severity, aber ohne error severity), dann MUSS die Verarbeitung als erfolgreich angesehen werden. Die Rückmeldungen zu Fehlern und Warnungen an NCPeH Land-B, die bei der Verarbeitung der Anfrage, dem Abruf des ePKA MIO des Versicherten oder der

Transformierung entstanden sind, MÜSSEN das in [ebRIM_Representation_Document#4.2.4] "Success and Error Reporting" beschriebene Format haben und in die Response-Nachricht aufgenommen werden. Es wird im Fehlerfall ggf. eine Fehlerliste (RegistryErrorList) und darin ein Fehler (RegistryError) je fehlgeschlagenem DocumentRequest mit den Attributen errorCode, codeContext, severity und location zurückgegeben.

Darüber hinaus MUSS der NCPeH-FD die Vorgaben aus [ebRIM_Representation_Document#4.2.4.2] für die Verwendung des status-Attributs im RegistryResponse-Element und die Vorgaben für den Umgang mit dem RegistryErrorList-Element umsetzen.

Der NCPeH-FD MUSS beim Versenden der Response-Nachricht einen Non-Repudiation of Origin Eintrag gemäß [4.1.7.1 - Non-Repudiation of Origin erstellen] in der Komponente Audit Repository speichern.

Beispiel einer Retrieve-Response mit einem CDA-Dokument embedded PDF/A Level 1 in Base64-Kodierung.

```
<RetrieveDocumentSetResponse>
  <RegistryResponse status="urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Success"/>
  <DocumentResponse>
    <HomeCommunityId>urn:oid:2.16.17.710.860.1000.990.1</HomeCommunityId>
    <RepositoryUniqueId>2.16.620.1.101.10.3.29.54290</RepositoryUniqueId>
    <DocumentUniqueId>1.2.84.116.1.800.254.370.349.563.1605.469.534.1338^PS.PDF</
DocumentUniqueId>
    <mimeType>text/xml</mimeType>
    <Document>... CDA LEVEL 1 EMBEDDED PDF/A BASE64 ENCODED...</Document>
  </DocumentResponse>
</RetrieveDocumentSetResponse>
```

Ausgabeparameter des TUC

- Keine

6.1.3.5 TUC_NCPeH_009: NFD des ePKA MIO transkodieren und transformieren

Für diesen TUC gelten folgende übergreifende Festlegungen

- [4.1.7.4- Translation Audit Trail Eintrag erstellen]

Ablauf des TUC

Um die medizinischen Versichertendaten in das eHDSI CDA Pivotformat Level 3 umwandeln zu können, ist es bei diesem TUC erforderlich, dass der NFD des ePKA MIO des Versicherten im Klartext vorliegt. Der NCPeH-FD DARF die DPE-Daten aus dem ePKA MIO (siehe Komposition KBV_PR_MIO_DPE_Composition_DPE) NICHT verarbeiten oder daraus Versichertendaten beziehen.

Für eine erfolgreiche Transkodierung des NFD des ePKA MIO muss der NCPeH-FD den MTC inkl. Transkodierungs- bzw. Mappingdaten enthalten, die die Verbindungen zwischen Konzepten in verschiedenen Codesystemen definieren. Die Transkodierungsregeln definieren konkrete Assoziationen zwischen Konzepten, die in ePKA MIO verwendet

werden und Konzepten, die zu Value Sets im MVC gehören. Sie legen fest, wie ein Code in einem bestimmten Codesystem, welches im ePKA MIO verwendet werden darf, auf einen anderen Code in einem anderen Codesystem gemäß MVC (siehe [eHDSI_MVC]) abgebildet wird. Das Vorgehen zum Herunterladen der korrekten Version des MTC vom zentralen eHDSI Configuration Service ist im [5.3.3- NCPeH.UC_7 - MTC vom eHDSI Terminology Service herunterladen] beschrieben.

Der NCPeH-FD MUSS anhand der FHIR-Komposition KBV_PR_MIO_NFD_Composition_NFD aus ePKA MIO die Transformierung und Transkodierung durchführen. Alle anderen Inhalte des FHIR-Bundle ePKA MIO DÜRFEN NICHT für Zwecke der grenzübergreifenden Übertragung oder internen Verarbeitung verwendet werden.

Der NCPeH-FD MUSS zur Transformierung der FHIR-Komposition KBV_PR_MIO_NFD_Composition_NFD in das eHDSI Patient Summary CDA Pivotformat Level 3 die Vorgaben gemäß [eHDSI_CDA_Format] umsetzen und dabei das CDA Document Template "eHDSI Patient Summary" verwenden. Die Identifizierung von relevanten strukturierten Elementen aus der FHIR-Komposition KBV_PR_MIO_NFD_Composition_NFD und die Umwandlung dieser in das eHDSI Patient Summary CDA Pivotformat Level 3 unter Anwendung von Transkodierungsregeln MUSS der NCPeH-FD nach Vorgaben der BfArM umsetzen.

Hinweis: Die Transformierung und Transkodierung der FHIR-Komposition KBV_PR_MIO_NFD_Composition_NFD in das eHDSI Patient Summary CDA Pivotformat Level 3 erfolgt nach Vorgaben der BfArM.

Der NCPeH-FD MUSS bei der Verletzung der Schemakonformität eine weitere Verarbeitung der Anfrage abbrechen und dem NCPeH Land-B mit dem Fehlercode ERROR_PS_GENERIC gemäß [eHDSI_XCA_Profile#2] und [eHDSI_NCPeH_Components#6.4] antworten.

Ausgabeparameter des TUC

- Strukturierte Inhalte der FHIR-Komposition KBV_PR_MIO_NFD_Composition_NFD im eHDSI Patient Summary CDA Pivotformat Level 3

6.1.3.6 TUC_NCPeH_010: NFD des ePKA MIO ins PDF/A-Format transformieren

Für diesen TUC gelten folgende übergreifende Festlegungen

- [4.1.7.4- Translation Audit Trail Eintrag erstellen]

Ablauf des TUC

Der NCPeH-FD MUSS anhand der FHIR-Komposition KBV_PR_MIO_NFD_Composition_NFD aus dem ePKA MIO die Transformierung ins PDF/A-Format durchführen. Alle anderen Inhalte des FHIR-Bundle ePKA MIO DÜRFEN vom NCPeH-FD NICHT für Zwecke der grenzübergreifenden Übertragung oder internen Verarbeitung verwendet werden. Der NCPeH-FD DARF die DPE-Daten aus dem ePKA MIO (siehe Komposition KBV_PR_MIO_DPE_Composition_DPE) NICHT verarbeiten oder daraus relevante Versichertendaten beziehen.

Der NCPeH-FD MUSS zur Transformierung der FHIR-Komposition KBV_PR_MIO_NFD_Composition_NFD in das eHDSI CDA embedded PDF/A Pivotformat Level 1 nach Vorgaben gemäß [eHDSI_CDA_Format] umsetzen und dabei das CDA Document Template "eHDSI Patient Summary PDF embedded" verwenden. Die Transformierung von Daten aus der FHIR-

Komposition KBV_PR_MIO_NFD_Composition_NFD in das eHDSI CDA embedded PDF/A Pivotformat Level 1 MUSS der NCPeH-FD nach Vorgaben der BfArM umsetzen.

Hinweis: Die Transformierung der FHIR-Komposition KBV_PR_MIO_NFD_Composition_NFD in das eHDSI Patient Summary CDA Pivotformat Level 1 erfolgt nach Vorgaben der BfArM.

Der NCPeH-FD MUSS bei der Verletzung der Schemakonformität eine weitere Verarbeitung der Anfrage abbrechen und dem NCPeH Land-B mit dem Fehlercode ERROR_PS_GENERIC gemäß [eHDSI_XCA_Profile#2] und [eHDSI_NCPeH_Components#6.4] antworten.

Ausgabeparameter des TUC

- Inhalte der FHIR-Komposition KBV_PR_MIO_NFD_Composition_NFD im eHDSI CDA embedded PDF/A Pivotformat Patient Summary Level 1

6.1.3.7 TUC_NCPeH_027: Cross Gateway Retrieve Request für ePeD-A auf Einhaltung von allgemeinen Kriterien prüfen

Für diesen TUC gelten folgende übergreifende Festlegungen

- [[4.1.2 - Datenaustausch mit zugelassenen EU-Ländern](#)]
- [[4.1.3 - eHDSI Basisleistungen](#)]
- [[4.1.3.1 Sicherer Kanal: TESTA-ng und TLS](#)]
- [[4.1.5 - Validierung der Identity Assertion des LE-EU](#)]
- [[4.1.6 - Validierung der TRC-Assertion](#)]
- [[4.1.7 - Non-Repudiation und Audit Trail Schemas](#)]
- [[4.1.8 - Festlegungen zur Prüfung der Zugriffsberechtigung auf Fachdienste der TI](#)]
- [[4.1.9- Format und Validierung der KVNR](#)]

Der NCPeH-FD MUSS einen Non-Repudiation of Receipt Eintrag gemäß [[4.1.7.2 - Non-Repudiation of Receipt erstellen](#)] und einen Audit Trail Eintrag gemäß [[4.1.7.3 Patient Privacy Audit Trail Eintrag erstellen](#)] in der Komponente Audit Repository speichern. Bei der Erstellung des Audit Trail Eintrages MUSS der NCPeH-FD die Vorgaben aus [eHDSI_XCA_Profile#4.3] umsetzen. Wenn zum Zeitpunkt der Erstellung des Audit Trail Eintrags nicht alle erforderlichen Daten im NCPeH-FD verfügbar sind, MÜSSEN die Daten in den Audit Trail Eintrag aufgenommen werden, sobald sie im NCPeH-FD verfügbar sind, spätestens aber nachdem die Antwort an NCPeH Land-B gesendet wurde.

Beim Auftreten eines der folgenden Fehlerfälle MUSS der NCPeH-FD eine weitere Verarbeitung der Anfrage abbrechen und dem anfragenden NCPeH Land-B mit einer Fehlernachricht mittels der Antwortnachricht gemäß [[6.1.3.9- TUC_NCPeH_029: Cross Gateway Retrieve Response mit ePeD-A CDA senden](#)] antworten:

Tabelle

57: TAB_NCPeH_Fehlerfälle_Verarbeitung_Cross_Gateway_Retrieve_Request_ePeD-A

Fehlerfall	errorCode (gemäß [eHDSI_NCPeH_Components#6.4])	codeCont ext	severity	location
Die	ERROR_EP_GENER	"The	urn:oasis:	"The DN structure

<p>Variable <code>tls_country</code> aus dem TLS-Zertifikat des NCPeH Land-B (siehe [4.1.3.1 Sicherer Kanal: TESTA-ng und TLS]) DARF NICHT leer sein und MUSS in der <code>WHITELIST_NCPeH_COUNTRY-B</code> nach [4.1.2 "Datenaustausch mit zugelassenen EU-Ländern"] enthalten sein.</p>	<p>IC</p>	<p>german ePrescription service is not agreed with the requesting country. Please contact your service provider or administrator."</p>	<p><code>names:tc:ebxml-regrep:ErrorSeverityType:Error</code></p>	<p>in the subject of the received TLS certificate does not contain a valid EU country code or the addressed service is not agreed between the requesting country and germany. Received country code from TLS certificate= " + Wert der Variable <code>tls_country</code></p>
<p>Die Variable <code>ida_permissions</code>, falls sie nicht leer ist, enthält nicht alle Permission Codes gemäß den Vorgaben aus [4.1.8 - Festlegungen zur Prüfung der Zugriffsberechtigung auf Fachdienste der TI] für den eHDSI Use Case "Request for ePrescriptions"</p>		<p>"Access denied. Please contact your service provider or administrator and check the access rights for your health professional role in your country."</p>		<p>"Received permission codes=" + Wert der Variable <code>ida_permissions</code></p>
<p>Die Variable <code>ida_permissions</code> ist leer und die Bedingungen zur Erlangung einer Zugriffsberechtigung auf E-Rezept-FD nach [4.1.8 - Festlegungen zur Prüfung der Zugriffsberechtigung auf Fachdienste der TI] sind nicht erfüllt</p>		<p>"Access denied. The information provided about the role of the health professional does not comply with German regulatio</p>		<p>"No permission codes received and the access cannot be granted for the received practitioner role code in accordance with national regulations. Received practitioner role code=" + Wert der Variable <code>ida_practitioner_role_code</code></p>

		ns."	
Der Wert der Variable trc_kvnr ist leer oder verletzt die Vorgaben aus [4.1.9-Format und Validierung der KVNR] .		"Please make sure that the health insurant identifier is given and correct"	"Health insurant number is missing or invalid."
Der Wert der Variable trc_accesscode ist leer oder verletzt die Formatvorgaben aus [4.1.6 - Validierung der TRC-Assertion] .		"Access denied. The patients access code is missing or malformed . Please ask the patient for access authorisation and the proper access code."	Keine Angaben
Die Anfrage enthält keine DocumentUniqueid-Elemente	ERROR_MISSING_REQUIRED_FIELDS	"The request does not contain any ePrescription ID. Please contact your service provider or administrator."	"Missing any DocumentUniqueId-Element in the request."
Die Variable ida_name-id ist leer.	ERROR_HPI_INSUFFICIENT_INFORMATION	"Access denied. The identifier of the health	Keine Angaben

		professional is missing in the provided identity information."	
Die Variable ida_practitioner_role ist leer.		"Access denied. The information about the role of EU health professional is missing in the provided identity information."	Keine Angaben
Die Variable ida_practitioner_name ist leer.		"Access denied. The name of the EU health professional is missing in the provided identity information."	Keine Angaben
Der Wert der Variable ida_practitioner_role_code ist leer oder dieser ist nicht identisch mit einem der möglichen Werte für das Element urn:oasis:names:tc:xacml:2.0:subject:role aus [eHDSI_SAML_Profile #2.3].		"Access denied. Missing or unknown role of the EU professional in the provided identity information."	"Received role code of the health professional from the identity assertion; see element urn:oasis:names:tc:xacml:2.0:subject:role= " + Wert der Variable ida_practitioner_role_code

Die Variable <code>ida_point_of_care</code> ist leer.	ERROR_HPI_POC_NO_INFORMATION	"Access denied. Missing name of the point of care in the provided identity information."		Keine Angaben
Der Wert der Variable <code>ida_healthcare_facility_type_code</code> ist leer oder nicht identisch mit einem der vorgegebenen Werte aus [eHDSI_SAML_Profile #2.3] für das Identitätsattribut <code>urn:ehdsi:names:subject:healthcare-facility-type</code> .		"Access denied. Missing or unknown type of Healthcare Provider Organisation in the provided identity information."		"Received healthcare facility type=" + Wert der Variable <code>ida_healthcare_facility_type_code</code>

Hinweis: Die Initiierung der Variablen `ida_permissions`, `ida_practitioner_role_code`, `ida_healthcare_facility_type_code`, `ida_name-id`, `ida_practitioner_role` und `ida_point_of_care` erfolgt im [4.1.5 - Validierung der Identity Assertion des LE-EU] und die der Variablen `trc_kvnr` und `trc_accesscode` im [4.1.6 - Validierung der TRC-Assertion].

Ausgabeparameter des TUC

- Fehlernachricht an NCPeH Land-B (falls vorhanden)

6.1.3.8 TUC_NCPeH_028: Cross Gateway Retrieve Request für ePeD-A CDA verarbeiten

Für diesen TUC gelten folgende übergreifende Festlegungen

- [[4.1.1 - Konfigurationsparameter](#)]
- [[4.1.2 - Datenaustausch mit zugelassenen EU-Ländern](#)]
- [[4.1.3 - eHDSI Basisleistungen](#)]
- [[4.1.5 - Validierung der Identity Assertion des LE-EU](#)]
- [[4.1.6 - Validierung der TRC-Assertion](#)]
- [[4.1.7 - Non-Repudiation und Audit Trail Schemas](#)]
- [[4.1.8 - Festlegungen zur Prüfung der Zugriffsberechtigung auf Fachdienste der TI](#)]

Ablauf des TUC

Der NCPeH-FD MUSS zusätzlich zu den Vorgaben aus [eHDSI_XCA_Profile#2.4] für jedes DocumentRequest-Element die Vorgaben aus der Tabelle TAB_NCPeH_Nutzungskonvention_Cross_Gateway_Retrieve_Request_ePeD-A umsetzen.

Tabelle 58: TAB_NCPeH_Nutzungskonvention_Cross_Gateway_Retrieve_Request_ePeD-A

Element aus der Anfrage	Nutzungskonvention
HomeCommunityId	<p>Dieser Wert, ohne das Präfix "urn:oid:", MUSS identisch mit dem Wert des Konfigurationsparameters HOME_COMMUNITY_ID_NCPeH-FD aus [4.1.1 - Konfigurationsparameter] sein.</p> <p>Wenn der Wert des Elementes leer oder nicht identisch mit dem Wert des Konfigurationsparameters HOME_COMMUNITY_ID_NCPeH-FD ist, MUSS der NCPeH-FD für das angeforderte E-Rezept ein /RetrieveDocumentSetResponse/RegistryResponse/RegistryErrorList/RegistryError-Element in der Antwortnachricht (IHE XCA.Retrieve-Response) gemäß Vorgaben aus [ebRIM_Representation_Document#4.2.4] und [ITI-43#3.43.5] erstellen und mit folgenden Angaben zum Fehler befüllen:</p> <ul style="list-style-type: none"> • errorCode: ERROR_EP_GENERIC • codeContext: "Wrong identifier for the german gateway service received. Please contact your service provider or administrator." • severity: urn:oasis:names:tc:ebxml-regrep:ErrorSeverityType:Error • location: "The Home Community ID for the German NCPeH is wrong. Received HomeCommunityId= " + Wert aus dem Element HomeCommunityId (falls der Wert nicht leer ist, ansonsten keine Angaben)

RepositoryUniqueid	<p>Dieser Wert MUSS mit dem Wert des Konfigurationsparameters <code>OID_AC_eRp_ASSIGNING_AUTHORITY</code> aus [4.1.1 - Konfigurationsparameter] identisch sein.</p> <p>Wenn der Wert des Elementes leer oder nicht identisch mit dem Wert des Konfigurationsparameters <code>OID_AC_eRp_ASSIGNING_AUTHORITY</code> ist, MUSS der NCPeH-FD für das angeforderte E-Rezept ein <code>/RetrieveDocumentSetResponse/RegistryResponse/RegistryErrorList/RegistryError</code>-Element in der Antwortnachricht (IHE XCA.Retrieve-Response) gemäß Vorgaben aus [ebRIM_Representation_Document#4.2.4] und [ITI-43#3.43.5] erstellen und mit folgenden Angaben zum Fehler befüllen:</p> <ul style="list-style-type: none">• errorCode: ERROR_EP_GENERIC• <code>codeContext: "Wrong identifier for the german ePrescription service received. Please contact your service provider or administrator."</code>• <code>severity: urn:oasis:names:tc:ebxml-regrep:ErrorSeverityType:Error</code>• <code>location: "The Repository Unique ID is not identical to the ID of the German ePrescription Service. Received RepositoryUniqueid= " + Wert aus dem ElementRepositoryUniqueid (falls der Wert nicht leer ist, ansonsten keine Angaben)</code>
--------------------	---

<p>DocumentUniqueId</p>	<p>Der Wert DARF NICHT leer sein. Nur der vordere Teil (ohne Endung "^eP.XML" oder "^eP.PDF") des Wertes MUSS als E-Rezept-ID verwendet werden, um das passende E-Rezept des Versicherten im E-Rezept-FD eindeutig ermitteln zu können. Der NCPeH-FD MUSS die E-Rezept-ID (ohne Endung "^eP.XML" oder "^eP.PDF") aus der Anfrage gemäß den Vorgaben in [gemSpec_DM_eRp#2.2] prüfen. Wenn die Prüfung der E-Rezept-ID erfolgreich war, MUSS der NCPEH-FD die E-Rezept-ID für die weitere Datenverarbeitung in einer Variable list_ePrescription_uniqueIds zwischenspeichern.</p> <p>Wenn festgestellt wird, dass der Wert des Elementes leer ist oder die Prüfung der E-Rezept-ID auf Erfüllung von Vorgaben aus [gemSpec_DM_eRp#2.2] nicht erfolgreich war, MUSS der NCPeH-FD für das angeforderte E-Rezept ein /RetrieveDocumentSetResponse/RegistryResponse/RegistryErrorList/RegistryError-Element in der Antwortnachricht (IHE XCA.Retrieve-Response) gemäß Vorgaben aus [ebRIM_Representation_Document#4.2.4] und [ITI-43#3.43.5] erstellen und mit folgenden Angaben zum Fehler befüllen:</p> <ul style="list-style-type: none"> • errorCode: ERROR_INCORRECT_FORMATTING • codeContext: "The identifier of an ePrescription is missing or not correct. Please contact your service provider or administrator." • severity: urn:oasis:names:tc:ebxml-regrep:ErrorSeverityType:Error • location: "The identifier of an ePrescription is missing or not correct. Received DocumentUniqueId= " + Wert aus dem ElementDocumentUniqueId <p>Beim Feststellen eines Fehlers DARF der Wert des Elementes NICHT in der Variable list_ePrescription_uniqueIds zwischengespeichert werden. Die Variable DARF E-Rezept-IDs NICHT enthalten, die die Vorgaben aus [gemSpec_DM_eRp#2.2] verletzen.</p>
-------------------------	--

Beispiel eines RetrieveDocumentSetRequest zur Abfrage von strukturierten E-Rezepten:

```

<RetrieveDocumentSetRequest>
  <DocumentRequest>
    <HomeCommunityId>urn:oid:1.2.276.0.76.4.291</HomeCommunityId>
    <RepositoryUniqueId>1.2.276.0.76.4.299</RepositoryUniqueId>
    <DocumentUniqueId>160.000.000.000.123.76^eP.XML</DocumentUniqueId>
  </DocumentRequest>
  <DocumentRequest>
    ...
  </DocumentRequest>
</RetrieveDocumentSetRequest>
    
```

Ausgabeparameter des TUC

- list_ePrescription_uniqueIds

6.1.3.9 TUC_NCPeH_029: Cross Gateway Retrieve Response mit ePeD-A CDA senden

Für diesen TUC gelten folgende übergreifende Festlegungen

- [[4.1.3 - eHDSI Basisleistungen](#)]
- [[4.1.7 - Non-Repudiation und Audit Trail Schemas](#)]

Ablauf des TUC

Dieser TUC enthält die Vorgaben für die Erstellung von IHE XCA.Retrieve-Response Nachrichten.

Als Eingangsparameter für diesen TUC dienen die Listen list_transcoded_eprescriptions_cda und list_registry_error_transcoding_cda. Beide wurden im [6.1.3.10- TUC_NCPeH_030: Abgerufene E-Rezepte transkodieren und transformieren] erstellt. Als weiterer Eingangsparameter für diesen TUC gilt die Liste der RegistryError-Elemente, die ggf. im [6.2.6- TUC_NCPeH_037: Abzugebende E-Rezepte vom E-Rezept-FD abrufen] erstellt sind.

Der NCPeH-FD MUSS für jedes DocumentRequest-Element aus der XCA.Retrieve-Anfrage ein entsprechendes DocumentResponse-Element in der XCA.Retrieve-Antwort erstellen, jedoch nur unter der Bedingung, dass in der Liste list_transcoded_eprescriptions_cda ein CDA-Dokument existiert, dessen Document Identifier mit dem Wert des DocumentUniqueId-Elementes aus der XCA.Retrieve-Anfrage übereinstimmt.

Bei der Erstellung der XCA.Retrieve-Antwort MÜSSEN die Vorgaben aus [eHDSI_XCA_Profile#2.4] und [ITI-43#3.43.4.2] umgesetzt werden. Für die Befüllung des DocumentResponse-Elementes MÜSSEN die Nutzungsvorgaben aus der Tabelle AB_NCPeH_Nutzungskonvention_Cross_Gateway_Retrieve_Response_ePeD-A eingehalten werden.

Tabelle 59: TAB_NCPeH_Nutzungskonvention_Cross_Gateway_Retrieve_Response_ePeD-A

Element in der Antwort	Nutzungskonvention
HomeCommunityId	Dieses Element MUSS mit der HomeCommunityId aus der Anfrage identisch sein. Der Wert besteht aus "urn:oid:" (ohne Anführungszeichen) gefolgt vom Wert des Konfigurationsparameters HOME_COMMUNITY_ID_NCPeH-FD aus [4.1.1 - Konfigurationsparameter] . Beispiel: urn:oid:1.2.276.0.76.4.291
RepositoryUniqueId	Dieses Element MUSS mit der RepositoryUniqueId aus der Anfrage identisch sein. Das Element besteht aus dem Wert der Variable OID_AC_eRp_ASSIGNING_AUTHORITY aus [4.1.1 - Konfigurationsparameter] .
DocumentUniqueId	Der Wert dieses Elementes MUSS identisch mit dem Wert des DocumentUniqueId-Elementes aus der Anfrage sein. Beispiel: 160.000.000.000.123.76^eP.XML

contentType	text/xml
Document	Dieses Element enthält ein Base64-kodiertes CDA-Dokument aus der Liste <code>list_transcoded_eprescriptions_cda</code> . Der ePrescription-Identifizier des CDA-Dokumentes MUSS identisch mit dem Wert des <code>DocumentUniqueId</code> -Elementes aus der Anfrage sein.

Der NCPeH-FD MUSS für jedes `DocumentRequest/DocumentUniqueId`-Element (für die angeforderten E-Rezepte) aus der Anfrage, für das es

- kein passendes CDA-Dokument mit identischem ePrescription Identifier in der Liste `list_transcoded_eprescriptions_cda` vorhanden ist,
- kein `RegistryError`-Element in der Liste `list_registry_error_transcoding_cda` zu diesem ePrescription-Identifizier existiert,
- kein `RegistryError`-Element aus [\[6.2.6- TUC_NCPeH_037: Abzugebende E-Rezepte vom E-Rezept-FD abrufen\]](#) zu diesem ePrescription-Identifizier existiert und
- kein `RegistryError`-Element aus [\[6.1.3.8- TUC_NCPeH_028: Cross Gateway Retrieve Request für ePeD-A CDA verarbeiten\]](#) zu diesem ePrescription-Identifizier gibt,

ein

`/RetrieveDocumentSetResponse/RegistryResponse/RegistryErrorList/RegistryError`-Element in der Antwortnachricht (IHE XCA.Retrieve-Response) gemäß den Vorgaben aus [\[ebRIM_Representation_Document#4.2.4\]](#) und [\[ITI-43#3.43.5\]](#) erstellen und folgende Informationen im Fehlereintrag angeben:

- `errorCode: WARNING_EP_GENERIC`
- `codeContext: "The requested ePrescription could not be found."`
- `severity: urn:oasis:names:tc:ebxml-regrep:ErrorSeverityType:Warning`
- `location: "Received ePrescription identifier: %Wert des Elementes DocumentUniqueId aus der Anfrage%"`

Wenn die

Listen `list_registry_error_transcoding_cda`, `list_registry_error_xca_retrieve` aus [\[6.2.6- TUC_NCPeH_037: Abzugebende E-Rezepte vom E-Rezept-FD abrufen\]](#) und [\[6.1.3.8- TUC_NCPeH_028: Cross Gateway Retrieve Request für ePeD-A CDA verarbeiten\]](#) nicht leer sind, MUSS der NCPeH-FD die Einträge (`RegistryError`-Element) aus den Listen in die Antwortnachricht übertragen, bevor er die Antwortnachricht an den NCPeH Land-B sendet.

In der Antwortnachricht können [\[ebRIM_Representation_Document#4.2.4\]](#) Error Codes enthalten sein, die entsprechende `ResponseStatus`-Informationen aufweisen. Das Vorhandensein einer `ErrorList` ist prinzipiell vereinbar mit einer teilweise erfolgreichen Verarbeitung. Wenn die `ErrorList` nur Warnings enthält (`RegistryError` elements mit `warning severity`, aber ohne `error severity`), dann MUSS die Verarbeitung als erfolgreich angesehen werden.

Die Rückmeldungen zu Fehlern und Warnungen an den NCPeH Land-B, die bei der Verarbeitung der IHE XCA.Retrieve-Request Nachricht, dem Abruf von E-Rezepten aus dem E-Rezept-FD oder der Transkodierung und Transformierung von E-Rezepten entstanden sind, MÜSSEN das in [\[ebRIM_Representation_Document#4.2.4\]](#) beschriebene Format haben und in die Response-Nachricht aufgenommen werden.

Darüber hinaus MUSS der NCPeH-FD die Vorgaben aus [ebRIM_Representation_Document#4.2.4.2] für die Verwendung des status-Attributs im RegistryResponse-Element und für den Umgang mit dem RegistryErrorList-Element umsetzen.

Der NCPeH-FD MUSS beim Versenden der Antwortnachricht einen Non-Repudiation of Origin Eintrag gemäß [4.1.7.1 - Non-Repudiation of Origin erstellen] in der Komponente Audit Repository speichern.

Der NCPeH-FD MUSS unmittelbar nach dem Senden der Antwortnachricht die Listen list_transcoded_eprescriptions_cda, list_registry_error_transcoding und list_ePrescription_uniqueIds und ihre Verweise auf die TRC Assertion des entsprechenden IHE XCA.Retrieve-Requests löschen.

Beispiel einer Antwortnachricht mit einem ePrescription CDA-Dokument Pivotformat Level 3 in Base64-Kodierung. Aufgrund der Länge des CDA-Dokumentes enthält das Beispiel im Element <Document> einen Platzhalter "...":

```
<RetrieveDocumentSetResponse>
  <RegistryResponse status="urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Success"/>
  <DocumentResponse>
    <HomeCommunityId>urn:oid:1.2.276.0.76.4.291</HomeCommunityId>
    <RepositoryUniqueId>1.2.276.0.76.4.299</RepositoryUniqueId>
    <DocumentUniqueId>160.000.000.000.123.76^eP.XML</DocumentUniqueId>
    <mimeType>text/xml</mimeType>
    <Document>PENsaw5pY2FsRG9jdW1lbn...</Document>
  </DocumentResponse>
  <DocumentResponse>
    ...
  </DocumentResponse>
</RetrieveDocumentSetResponse>
```

Ausgabeparameter des TUC

- Keine

6.1.3.10 TUC_NCPeH_030: Abgerufene E-Rezepte transkodieren und transformieren

Für diesen TUC gelten folgende übergreifende Festlegungen

- [[4.1.7 - Non-Repudiation und Audit Trail Schemas](#)]

Ablauf des TUC

In diesem TUC führt der NCPeH-FD gemäß den Vorgaben des BfArM die Transformierung und Transkodierung von "inneren Bundles" aus der Liste fhir_erp_bundle_collection in das geforderte eHDSI ePrescription CDA Pivotformat durch. Neben jedem "inneren Bundle" besteht in der Variable fhir_erp_bundle_collection eine eindeutige Referenz zu einem E-Rezept-ID. Anhand der E-Rezept-ID kann in diesem TUC ermittelt werden, ob bei einem referenzierten inneren Bundle eine Transformierung oder sowohl eine Transformierung als auch eine Transkodierung erforderlich ist.

Die Erstellung und Befüllung der Variable `fhir_erp_bundle_collection` ist im [6.2.6-TUC_NCPeH_037: Abzugebende E-Rezepte vom E-Rezept-FD abrufen] beschrieben.

Wenn die E-Rezept-ID mit "`^eP.PDF`" endet, dann MUSS der NCPeH-FD das referenzierte innere Bundle aus der Liste `fhir_erp_bundle_collection` in das eHDSI ePrescription Pivotformat CDA Level 1 embedded PDF/A nach Vorgaben aus [eHDSI_CDA_Format] transformieren und dabei das aktuelle CDA Document Template "eHDSI ePrescription PDF embedded" verwenden. Der NCPeH-FD MUSS die Transformierung und Erstellung des PDF/A-Dokumentes nach Vorgaben des BfArM umsetzen.

Disclaimer: Die Vorgaben für die Transformierung der "inneren Bundles" in das eHDSI ePrescription CDA Pivotformat Level 1 embedded PDF/A werden vom BfArM erarbeitet.

Wenn die E-Rezept-ID mit "`^eP.XML`" endet, MUSS der NCPeH-FD das referenzierte innere Bundle aus der Liste `fhir_erp_bundle_collection` in das eHDSI ePrescription Pivotformat CDA Level 3 nach den Vorgaben aus [eHDSI_CDA_Format] transformieren und transkodieren. Dabei MUSS das Template "eHDSI ePrescription" verwendet werden.

Disclaimer: Die Vorgaben zur Transformierung und Transkodierung von "inneren Bundles" (FHIR-Profil [KBV_PR_ERP_Bundle]) in das eHDSI CDA Pivotformat ePrescription Level 3 und der Fehlerverwaltung werden vom BfArM erarbeitet.

Für eine erfolgreiche Transformierung und Transkodierung der E-Rezepte MUSS der NCPeH-FD sicherstellen, dass er die aktuellen, von der BfArM bereitgestellten Transformierungs- und Transkodierungsregeln und Daten bei sich integriert hat. Dabei sind die Vorgaben aus [4.2.10.7-Regelung zur Unterstützung von mehreren FHIR-Package Versionen] mit zu berücksichtigen.

Die Ergebnisse der erfolgreichen Transformierung und Transkodierung MÜSSEN in der Liste `list_transcoded_eprescriptions_cda` zwischengespeichert werden, um sie im [6.1.3.9-TUC_NCPeH_029: Cross Gateway Retrieve Response mit ePeD-A CDA senden] für die Aufnahme in die Antwortnachricht an den NCPeH Land-B vorzubereiten.

Wenn die Transformierung und Transkodierung zu Fehlern oder Warnungen führt, MUSS der NCPeH-FD diese nach Vorgaben aus [eBRIM_Representation_Document#4.2.4] und der BfArM in dem dort beschriebenen Format erfassen. Die Fehler und Warnungen (RegistryError-Elemente) MÜSSEN nach Vorgaben des BfArM für die Attribute `errorCode`, `codeContext`, `severity` und `location` erstellt werden. Die erfassten Fehler und Warnungen MÜSSEN in der Liste `list_registry_error_transcoding_cda` zwischengespeichert werden. Die Angaben zu `errorCode` MÜSSEN den eHDSI Error Codes gemäß den Vorgaben aus [eHDSI_NCPeH_Components#6.4] entsprechen. Der NCPeH-FD MUSS für `codeContext` mit menschlich verständlichen Meldungen in englischer Sprache erstellen. Für Angaben zum Attribut `location` SOLL der NCPeH-FD technische Hinweise auf die Fehlerursache geben. Technische Informationen DÜRFEN Inhalte NICHT angeben, die Rückschluss auf Implementierungsdetails, eingesetzte Frameworks oder Tools zulassen.

A_27256 - NCPeH - XCA eD-A - Eindeutige Zuordnung von Verarbeitungsergebnissen zur TRC Assertion

Der NCPeH-FD MUSS bei der Zwischenspeicherung von Einträgen die Listen `list_transcoded_eprescriptions_cda` und `list_registry_error_transcoding_cda` eindeutig mit der TRC Assertion aus dem zugehörigen IHE XCA.Retrieve-Request verknüpfen und DARF diese Listen NICHT mit anderen TRC Assertions in Verbindung bringen. [<=]

A_27257 - NCPeH - XCA eD-A - Speicherung eines Audit Trail Eintrages nach jeder Transformierung und Transkodierung

Der NCPeH-FD MUSS für jedes erfolgreich transformierte und transkodierte Dispensierdokument einen Audit-Trail-Eintrag gemäß den Vorgaben aus [4.1.7.4 Translation Audit Trail Eintrag erstellen] in der Komponente Audit Repository speichern. [<=]

Ausgabeparameter des TUC

- list_transcoded_eprescriptions_cda
- list_registry_error_transcoding_cda

6.1.4 Nutzung der Schnittstelle des zentralen eHDSI Configuration Service

6.1.4.1 TUC_NCPeH_011: Service Metadata erstellen

Für diesen TUC gelten folgende übergreifende Festlegungen

Keine

Ablauf des TUC

Durch diesen TUC ermöglicht der NCPeH-FD über eine Management-Schnittstelle, den angemeldeten Systemadministratoren Service Metadata der angebotenen eHDSI-Schnittstellen des NCPeH-FD zu erstellen, zu verwalten und zu signieren. Der NCPeH-FD MUSS sicherstellen, dass der Systemadministrator und die in diesem TUC beschriebenen Abläufe von den restlichen Daten und Prozessen in der VAU isoliert sind.

Der NCPeH-FD MUSS dem authentifizierten Systemadministrator ermöglichen, über eine Management-Schnittstelle für jeden der folgenden Dienste bzw. Interaction Pattern eine separate ServiceMetadata-Datei neu zu erstellen oder bereits im NCPeH-FD vorhandene ServiceMetadata-Dateien auszuwählen und verwalten zu können:

- Patient Identification and Authentication (XCPD)
- Request of Data (für Operationen XCA.Query und XCA.Retrieve)
- Provisioning of Data (XDR)
- International Search Mask (für Operation ehealth-107)

Dabei MUSS der NCPeH-FD Vorgaben zur Befüllung der Service Metadata für den jeweiligen eHDSI-Dienst des NCPeH-FD aus [eHDSI_Audit_Trail_Profile#2.3.5.8] berücksichtigen. In jeder zugehörigen ServiceMetadata-Datei MUSS das Element ServiceMetadata/ServiceInformation/ParticipantIdentifier den Wert urn:ehealth:de:ncp-idp enthalten.

Das Element ServiceMetadata/ServiceInformation/DocumentIdentifier MUSS in Abhängigkeit von dem jeweiligen Interaction Pattern folgende Angaben enthalten (für die inhaltliche Struktur des Schemas siehe [eHDSI_Service_Location_and_Capability_Lookup_Profile#3.1.4]):

Tabelle 60: TAB_NCPeH_Service_Metadata_DocumentIdentifier

Dienst / Interaction Pattern	Operation	Event Name	Transaction / Event
------------------------------	-----------	------------	---------------------

			ID
PatientIdentificationAndAuthentication	XCPD	CrossGatewayPatientDiscovery	ITI-55
RequestofData	XCA	CrossGatewayQuery	ITI-38
RequestofData	XCA	CrossGatewayRetrieve	ITI-39
ProvisioningOfData:Provide	XDR	ProvideandRegisterDocumentSet-b	ITI-41
ISM	InternationalSearchMask		ehealth-107

Bei der Befüllung der Service Metadata für die vom Systemadministrator ausgewählten Service Metadata müssen die Vorgaben aus [eHDSI_Service_Location_and_Capability_Lookup_Profile#3.1.4] umgesetzt werden.

Für jeden Dienst bzw. Interaction Pattern aus der oberen Tabelle MUSS in jeder Service Metadata ein ServiceMetadata/ServiceInformation/ProcessList/Process/ProcessIdentifier Element mit einem entsprechenden Wert aus der Tabelle TAB_NCPeH_SERVICE_METADATA_PROCESSIDENTIFIER erstellt werden:

Tabelle 61: TAB_NCPeH_Service_Metadata_ProcessIdentifier

Interaction Pattern gemäß DocumentIdentifier-Element	Wert des ProcessIdentifier Elementes
PatientIdentificationAndAuthentication	urn:XCPD::CrossGatewayPatientDiscovery
RequestofData	urn:XCA::CrossGatewayQuery
RequestofData	urn:XCA::CrossGatewayRetrieve
ProvisioningOfData:Provide	urn:XDR::ProvideandRegisterDocumentSet-b
ISM	urn:ehealth:ncp:de:ism

Für das Interaction Pattern ISM (International Search Mask) MUSS das Attribut ProcessList/Process/ServiceEndpointList/Endpoint@transportProfile den Wert urn:ehealth:transport:none enthalten. Für andere Interaction Pattern müssen Werte für das Attribut transportProfile aus [eHDSI_Service_Location_and_Capability_Lookup_Profile#3.1.4] genommen werden.

Jeder der oben genannten Interaction Pattern MUSS im Element ProcessList/Process/ServiceEndpointList/Endpoint/ServiceDescription entsprechend der folgenden Tabelle eine Bezeichnung des Dienstes enthalten:

Tabelle 62: TAB_NCPeH_Service_Metadata_ServiceDescription

Interaction Pattern im DocumentIdentifier-Element	Wert des ServiceDescription-Elements
---	--------------------------------------

PatientIdentificationAndAuthentication	XCPD Service
RequestofData	XCA Service (Query)
RequestofData	XCA Service (Retrieve)
ProvisioningOfData:Provide	XDR Service
ISM	International Search Mask for DE

Für jeden Dienst bzw. Interaction Pattern MUSS das Element ServiceActivationDate ein Datum enthalten, das den Beginn der Bereitstellung des Dienstes darstellt. Angaben zum Element ServiceExpirationDate KÖNNEN gemacht werden. Ferner SOLL für jeden Dienst bzw. Interaction Pattern entweder das Element TechnicalContactUrl mit Angaben zu einer Webseite, auf der weitere relevanten Informationen (z.B. Kontaktdaten des Anbieters des NCPeH-FD) enthalten sind, oder das Element TechnicalInformationUrl mit Angaben zu einer E-Mail-Adresse des Anbieters des NCPeH-FD befüllt werden.

Das folgende Beispiel enthält Service Metadata für den XCPD Service:

Tabelle 63: TAB_NCPeH_Service_Metadata_XCPD-Service

```

<ServiceMetadata>
  <ServiceInformation>
    <ParticipantIdentifier
scheme="ehealth-participantid-qns">urn:ehealth:de:ncp-idp</ParticipantIdentifier>
    <DocumentIdentifier scheme="ehealth-resid-qns">
urn:ehealth:PatientIdentificationAndAuthentication::XCPD::CrossGatewayPatientDiscovery##ITI-
55
    </DocumentIdentifier>
    <ProcessList>
      <Process>
        <ProcessIdentifier scheme="ehealth-procid-qns">
urn:XCPD::CrossGatewayPatientDiscovery
        </ProcessIdentifier>
        <ServiceEndpointList>
          <Endpoint transportProfile="urn:ihe:iti:2013:xcpd">
            <EndpointURI>
https://ncp-ppt.de.ehealth.testa.eu:9443/openncp-ws-server/services/XCPD_Service
            </EndpointURI>
            <RequireBusinessLevelSignature>>false</RequireBusinessLevelSignature>
          </Endpoint>
        </ServiceEndpointList>
        <MinimumAuthenticationLevel>urn:epsOS:loa:1</MinimumAuthenticationLevel>
        <ServiceActivationDate>2022-03-01T07:44:00Z</ServiceActivationDate>
        <ServiceExpirationDate>2024-03-31T16:44:00Z</ServiceExpirationDate>
        <Certificate>... CERTIFICATE BASE64 ENCODED ...</Certificate>
        <ServiceDescription>XCPD Service</ServiceDescription>
      </Process>
    </ProcessList>
    <TechnicalContactUrl>https://www.dvka.de/en/ncpeh</TechnicalContactUrl>
    <TechnicalInformationUrl>ncpeh@dvka.de</TechnicalInformationUrl>
    </Endpoint>
  </ServiceEndpointList>
</Process>
</ProcessList>
<Extension>
  <Signature
xmlns="http://www.w3.org/2000/09/xmldsig#">
    <SignedInfo>
      <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-
c14n-20010315"/>
      <SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-
sha256"/>
      <Reference URI="">
        <Transforms>
          <Transform
Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
        </Transforms>
        <DigestMethod Algorithm="http://www.w3.org/2001/04/xmllenc#sha256"/>
        <DigestValue>... DIGEST VALUE BASE64 ENCODED ...</DigestValue>
      </Reference>
    </SignedInfo>
    <SignatureValue>... SIGNATURE VALUE BASE64 ENCODED ...</SignatureValue>
    <KeyInfo>
      <X509Data>
        <X509SubjectName>...</X509SubjectName>
        <X509Certificate>... CERTIFICATE BASE64 ENCODED
...</X509Certificate>
      </X509Data>
    </KeyInfo>
  </Signature>
</Extension>
</ServiceInformation>
</ServiceMetadata>

```

Beim Interaction Pattern ISM MUSS das Element ServiceMetadata/ServiceInformation/ProcessList/Process/ServiceEndpointList/Endpoint/Extension/searchFields Angaben zur Durchführung der Versichertenidentifizierung im Ausland enthalten und damit Vorgaben zur Anwendung der International Search Mask enthalten. Der NCPeH-FD MUSS Vorgaben aus [eHDSI_Requirements_Catalogue#02.01.02] zur Erstellung der International Search Mask umsetzen. Zusätzlich MUSS der NCPeH-FD folgende Vorschrift beachten:

Tabelle 64: TAB_NCPeH_Service_Metadata_ISM

ISM-Element	Nutzungsvorschrift
searchFields/country@code	DE
searchFields/country@friendlyName	Germany
searchFields/country@label	label.ism.addressCountry
searchFields/country/patientSearch@friendlyName	International Search Mask for Germany
searchFields/country/patientSearch@scope	ALL
searchFields/country/patientSearch/identifier@type	CHOICE
searchFields/country/patientSearch/identifier/ids[0]@display	Patient identification for Patient Summary
searchFields/country/patientSearch/identifier/ids[0]/id[0]@contextualDescription	Health insurant ID number
searchFields/country/patientSearch/identifier/ids[0]/id[0]@domain	Der Wert des Konfigurationsparameters OID_KVNR_ASSIGNING_AUTORITY aus [4.1.1 - Konfigurationsparameter]
searchFields/country/patientSearch/identifier/ids[0]/id[0]@format	[A-Z][0-9]{9}
searchFields/country/patientSearch/identifier/ids[0]/id[0]@min	10
searchFields/country/patientSearch/identifier/ids[0]/id[0]@max	10
searchFields/country/patientSearch/identifier/ids[0]/id[0]@label	label.ism.nationalPersonIdentifier
searchFields/country/patientSearch/identifier/ids[0]/	Versichertennummer

id[0]@originalContextualDescription	
searchFields/country/patientSearch/identifier/ids[0]/id[0]@mandatory	true
searchFields/country/patientSearch/identifier/ids[0]/id[1]@contextualDescription	Access code for Patient Summary
searchFields/country/patientSearch/identifier/ids[0]/id[1]@domain	Der Wert des Konfigurationsparameters OID_AC_ePKA_ASSIGNING_AUTHORITY aus [4.1.1 - Konfigurationsparameter]
searchFields/country/patientSearch/identifier/ids[0]/id[1]@format	[A-Za-z0-9]{6}
searchFields/country/patientSearch/identifier/ids[0]/id[1]@min	6
searchFields/country/patientSearch/identifier/ids[0]/id[1]@max	6
searchFields/country/patientSearch/identifier/ids[0]/id[1]@label	label.ism.accessCode
searchFields/country/patientSearch/identifier/ids[0]/id[1]@originalContextualDescription	Zugriffscod für die Patientenkurzakte
searchFields/country/patientSearch/identifier/ids[0]/id[1]@mandatory	true
searchFields/country/patientSearch/identifier/ids[1]@display	Patient identification for ePrescription
searchFields/country/patientSearch/identifier/ids[1]/id[0]@contextualDescription	Health insurant ID number
searchFields/country/patientSearch/identifier/ids[1]/id[0]@domain	Der Wert des Konfigurationsparameters OID_KVNR_ASSIGNING_AUTHORITY aus [4.1.1 - Konfigurationsparameter]
searchFields/country/patientSearch/identifier/ids[1]/id[0]@format	[A-Z][0-9]{9}
searchFields/country/patientSearch/identifier/ids[1]/id[0]@min	10
searchFields/country/patientSearch/identifier/ids[1]/id[0]@max	10

searchFields/country/patientSearch/identifier/ids[1]/id[0]@label	label.ism.nationalPersonIdentifier
searchFields/country/patientSearch/identifier/ids[1]/id[0]@originalContextualDescription	Versichertennummer
searchFields/country/patientSearch/identifier/ids[1]/id[0]@mandatory	true
searchFields/country/patientSearch/identifier/ids[1]/id[1]@contextualDescription	Access code for ePrescription/eDispensation (limited to one hour)
searchFields/country/patientSearch/identifier/ids[1]/id[1]@domain	Der Wert des Konfigurationsparameters OID_AC_eRp_ASSIGNING_AUTHORITY aus [4.1.1 - Konfigurationsparameter]
searchFields/country/patientSearch/identifier/ids[1]/id[1]@format	[A-Za-z0-9]{6}
searchFields/country/patientSearch/identifier/ids[1]/id[1]@min	6
searchFields/country/patientSearch/identifier/ids[1]/id[1]@min	6
searchFields/country/patientSearch/identifier/ids[1]/id[1]@label	label.ism.accessCode
searchFields/country/patientSearch/identifier/ids[1]/id[1]@originalContextualDescription	Zugriffscod für eRezept/eDispensierung
searchFields/country/patientSearch/identifier/ids[1]/id[1]@mandatory	true
searchFields/country/patientSearch/media[0]@description	Picture of the front of the german electronic health card
searchFields/country/patientSearch/media[0]@fileExtension	JPG oder JPEG
searchFields/country/patientSearch/media[0]@mediaName	DE_Front_Patient_Health_Card
searchFields/country/patientSearch/media[0]@label	label.ism.media[0]
searchFields/country/patientSearch/media[0]/mediaContent	Siehe Abbildung 7 in [7 - Anhang - Europäische

	Krankenversicherungskarte]
searchFields/country/patientSearch/media[1]@description	Picture of European Health Insurance Card
searchFields/country/patientSearch/media[1]@fileExtension	JPG oder JPEG
searchFields/country/patientSearch/media[1]@mediaName	DE_Back_Patient_Health_Card
searchFields/country/patientSearch/media[1]@label	label.ism.media[1]
searchFields/country/patientSearch/media[1]/mediaContent	Siehe Abbildung 8 in [7 - Anhang - Europäische Krankenversicherungskarte]

Folgendes Beispiel stellt die inhaltliche Struktur der deutschen International Search Mask inkl. Bildmaterialien, die den LE-EU bei der Findung der Krankenversichertennummer und des Geburtsdatums auf der eGK des Versicherten unterstützen sollen:

Tabelle 65: TAB_NCPeH_International_Search_Mask

```

<ism:searchFields
  xmlns:ism="http://ec.europa.eu/sante/ehncp/ism">
  <ism:country code="DE" friendlyName="Germany" label="label.ism.addressCountry">
    <ism:patientSearch friendlyName="International Search Mask for Germany" scope="All">
      <ism:identifier type="CHOICE">
        <ism:ids display="Patient identification for Patient Summary">
          <ism:id contextualDescription="Health insurance number"
            domain="1.2.276.0.76.3.1.580.147" format="[A-Z][0-9]{9}"
            min="10" max="10" label="label.ism.nationalPersonIdentifier"
            mandatory="true" originalContextualDescription="Krankenversichertennummer"/>
          <ism:id contextualDescription="Access code for Patient Summary"
            domain="1.2.276.0.76.4.298" format="[A-Za-z0-9]{6}" min="6"
            max="6" label="label.ism.accessCode" mandatory="true"
            originalContextualDescription="Zugriffscode für die Patientenkurzakte"/>
        </ism:ids>
        <ism:ids display="Patient identification for ePrescription">
          <ism:id contextualDescription="Health insurance number"
            domain="1.2.276.0.76.3.1.580.147" format="[A-Z][0-9]{9}"
            min="10" max="10" label="label.ism.nationalPersonIdentifier"
            mandatory="true" originalContextualDescription="Krankenversichertennummer"/>
          <ism:id contextualDescription="Access code for
            ePrescription/eDispensation (limited to one hour)"
            domain="1.2.276.0.76.4.299" format="[A-Za-z0-9]{6}" min="6"
            max="6"
            label="label.ism.accessCode" mandatory="true"
            originalContextualDescription="Zugriffscode für
            eRezept/eDispensierung"/>
        </ism:ids>
      </ism:identifier>
      <ism:media description="Picture of the front of the german electronic health
        card" fileExtension="JPG" label="label.ism.media[0]"
        mediaName="DE_Front_Patient_Health_Card">
        <ism:mediaContent>... PICTURE BASE64 ENCODED ...</ism:mediaContent>
      </ism:media>
      <ism:media description="Picture of European Health Insurance Card"
        fileExtension="JPG" label="label.ism.media[1]"
        mediaName="DE_Back_Patient_Health_Card">
        <ism:mediaContent>... PICTURE BASE64 ENCODED ...</ism:mediaContent>
    </ism:patientSearch>
  </ism:country>
</ism:searchFields>
    
```

```
</ism:media>
  </ism:patientSearch>
</ism:country>
</ism:searchFields>
```

Jede Service Metadata MUSS nach Vorgaben aus [eHDSI_Service_Location_and_Capability_Lookup_Profile#3.1.4] elektronisch signiert werden. Die Signaturerstellung MUSS nach Vorgaben der eHDSI mittels des privaten Schlüsselmaterials (TLS- oder SEAL-Zertifikat) durchgeführt werden, welches durch die eHDSI-PKI ausgestellt wurde. Das private Schlüsselmaterial MUSS im HSM erzeugt und dort zur Signaturerstellung angewendet werden (siehe [4.1.3.5- Umgang mit Zertifikaten der eHDSI]). Nur auf explizite Anforderung des Systemadministrators MUSS der NCPeH-FD die ausgewählten Service Metadata mit dem privaten Schlüsselmaterial (TLS- oder SEAL-Zertifikat) gemäß Vorgaben aus [BDX-smp-v1.0#3.6.2] signieren. Der NCPeH-FD DARF NICHT ohne Zustimmung durch einen Systemadministrator die ausgewählte Service Metadata automatisch signieren. Der Wert der Signatur MUSS im Element ServiceMetadata/ServiceInformation/Extension/Signature zusammen mit dem öffentlichen Zertifikat (TLS- oder SEAL-Zertifikat) enthalten sein.

Ausgabeparameter des TUC

- Eine oder mehrere signierte ServiceMetadata-Dateien

6.1.4.2 TUC_NCPeH_012: Signed Service Metadata auf eHDSI Configuration Service hochladen

Für diesen TUC gelten folgende übergreifende Festlegungen

- Öffentliche Zertifikate des Configuration Service der eHDSI sind im lokalen Truststore des NCPeH-FD (siehe [4.1.3.5- Umgang mit Zertifikaten der eHDSI])
- [4.1.3- eHDSI Basisleistungen]

Ablauf des TUC

In diesem TUC kann ein authentifizierter Systemadministrator die ausgewählten Service Metadata auf den Configuration Service der eHDSI hochladen.

Der NCPeH-FD MUSS sicherstellen, dass das Hochladen der ausgewählten und signierten Service Metadata auf dem Configuration Service der eHDSI erst dann erfolgen kann, nachdem eine präventive Kontrolle der Inhalte der Service Metadata nach dem Vier-Augen-Prinzip erfolgt ist. Die offizielle Entscheidung zum Hochladen der Service Metadata auf dem Configuration Service der eHDSI MUSS durch einen anderen authentifizierten Systemadministrator erfolgen, dessen Identität nicht mit der Identität des Systemadministrators gleichzusetzen ist, der die Service Metadata zuletzt geändert hat. Das Ziel des Vier-Augen-Prinzips ist es, das Risiko von Fehlern und Missbrauch zu reduzieren.

Falls es im Rahmen der präventiven Kontrolle (Vier-Augen-Prinzip) zu einer Änderungen an der Service Metadata durch einen zweiten Systemadministrator kommt, wird die in der Service Metadata enthaltene Signatur unbrauchbar und die Service Metadata muss erneut signiert werden (siehe [6.1.4.1- TUC_NCPeH_011: Service Metadata erstellen]).

Das Hochladen der Service Metadata erfolgt mittels SMP/SML-Protokolls. Um auf eine Patient Summary in der eHDSI erfolgreich zugreifen zu können, muss ein NCPeH Land-B in der Lage sein, wichtige Metadaten über die Dienstendpunkte des eHDSI Service

Providers (NCPeH Land-A) zu ermitteln. Daher MUSS der NCPeH-FD die Kommunikation zum eHDSI Configurations Service nach Vorgaben aus [eHDSI_Service_Location_and_Capability_Lookup_Profile] und [SMP_SML_eDelivery_BB#5] umsetzen. Nach erfolgreichem Hochladen bzw. Aktualisieren der Service Metadata auf dem eHDSI Configuration Service MUSS der NCPeH-FD dem Systemadministrator über die Management-Schnittstelle eine Erfolgsmeldung anzeigen.

Disclaimer: Der eHDSI Solution Provider hat keine Spezifikation der Schnittstelle des eHDSI Configuration Service oder zum Vorgang des Hochladens bzw. Registrierens der Service Metadata auf dem eHDSI Configuration Service durch einen NCPeH Land-A erstellt. Um den technischen Prozess des Hochladens der Service Metadata auf dem eHDSI Configuration Service im NCPeH-FD zu implementieren, empfiehlt der eHDSI Solution Provider den Einsatz entsprechender Komponenten der OpenNCP-Referenzimplementierung oder bei einer Neuentwicklung die Umsetzung der Vorgaben aus [SMP_SML_eDelivery_BB#5].

Falls die Service Metadata aufgrund eines Kommunikationsfehlers mit dem eHDSI Configuration Service nicht veröffentlicht bzw. aktualisiert werden können, MUSS der NCPeH-FD über die Management-Schnittstelle dem Systemadministrator die Fehlerdetails, Fehlercode und -beschreibung gemäß vorgegebenen Standards in [eHDSI_Service_Location_and_Capability_Lookup_Profile#3.1.1] anzeigen.

Der NCPeH-FD MUSS nach Veröffentlichung bzw. Aktualisierung einer Service Metadata auf dem eHDSI Configuration Service einen Audit Trail Eintrag nach Vorgaben aus [4.1.7.5- Security Audit Trail Eintrag erstellen] erstellen und in das lokalen Audit Repository speichern.

Ausgabeparameter des TUC

- Keine

6.1.5 Operation Cross-Enterprise

Document_Reliable_Interchange::ProvideAndRegisterDocumentSet-b

Diese Operation wird aufgerufen, wenn NCPeH Land-B in der Rolle als Document Source ein Ereignis vom LE-EU (z.B. Apotheker) empfängt und die Anfrage an die Operation sendet. Dabei möchte der LE-EU behandlungsrelevante Dokumente des Versicherten (z.B. Dispensierungsinformationen) an Deutschland übermitteln. Eine XDR-Anfrage kann mehrere eHDSI pivot-kodierte Dokumente enthalten.

A_26649 - NCPeH - XDR - Umsetzung der Operation

Enterprise_Document_Reliable_Interchange::ProvideAndRegisterDocumentSet-b

Der NCPeH-FD MUSS die Operation

Enterprise_Document_Reliable_Interchange::ProvideAndRegisterDocumentSet-b gemäß Vorgaben aus

Tabelle TAB_NCPeH_Enterprise_Document_Reliable_Interchange_ProvideAndRegisterDocumentSet-b umsetzen.

Tabelle 66:

TAB_NCPeH_Enterprise_Document_Reliable_Interchange_ProvideAndRegisterDocumentSet-b

Operation	Enterprise_Document_Reliable_Interchange::ProvideAndRegisterDocumentSet-b
-----------	---

Beschreibung	<p>Die Operation MUSS vom NCPeH-FD in der Rolle als Document Recipient gemäß Vorgaben aus [eHDSI_XDR_Profile] implementiert und den NCPeH Land-B zur Nutzung in der eHDSI bereitgestellt werden.</p> <p>Der NCPeH-FD MUSS die XDR-Anfrage bearbeiten, um Dokumente (z.B. für die Dispensierung von E-Rezepten) aus der XDR-Anfrage zu entnehmen und sie einzeln an den entsprechenden fachanwendungsspezifischen TI-Fachdienst zu übermitteln.</p> <p>Der NCPeH-FD MUSS auf die XDR-Anfrage antworten und dabei eine Statusrückmeldung an den NCPeH Land-B über den Erfolg des Workflows der Dokumente senden. Die Antwort kann weitere Informationen (Warnungen und Fehlermeldungen) über die Verarbeitung der übermittelten Dokumente enthalten.</p>	
Eingangsparameter		
Name	Beschreibung	Typ
provideDataRequest	Eingangsnachricht zur Übermittlung von Dokumenten für den Versicherten gemäß [eHDSI_XDR_Profile#2.1]	ProvideAndRegisterDocumentSetRequest [ITI-41]
X-User Assertion	Authentication Assertion des anfragenden LE-EU	SAML 2.0 Assertion gemäß [eHDSI_SAML_Profile#2] inkl. X.509 öffentliches Signaturzertifikat des NCPeH Land-B [eHDSI_X.509_Certificates_Profile]
TRC Assertion	Bestätigung über das Bestehen einer Behandlungsbeziehung zwischen LE-EU und Versichertem	SAML 2.0 Assertion gemäß [eHDSI_SAML_Profile#4] inkl. X.509 öffentliches Signaturzertifikat des NCPeH Land-B [eHDSI_X.509_Certificates_Profile]
Ausgangsparameter		
Name	Beschreibung	Typ
provideDataResponse	Ausgangsnachricht gemäß [eHDSI_XDR_Profile#2.2.1]	RegistryResponse [ITI-41]

[<=]

In der XDR-Anfrage werden die Dokumentenklassen auf der Grundlage von so genannten semantischen eHDSI-Signifiers klassifiziert.

A_26648 - NCPeH - Unterscheidung von XDR-Anfragen anhand von semantischen eHDSI-Signifier

Der NCPeH-FD MUSS den Wert aus dem XSDocumentEntryClassCode-Element mit dem Klassifikationsschema urn:uuid:41a5887f-8865-4c09-adf7-

e362475b143a entnehmen und den Wert verwenden, um die Verarbeitung der XDR-Anfragen einem entsprechenden Technischen Use Case (TUC) gemäß der Tabelle TAB_NCPeH_Kriterien_Zuordnung_IHE-XDR-Anfragen_zu_Anwendungsszenarien zuordnen.

Tabelle 67: TAB_NCPeH_Kriterien_Zuordnung_IHE-XDR-Anfragen_zu_Anwendungsszenarien

XSDDocumentEntryClass Code	Technischer Use Case (TUC)
60593-1	<p>[6.1.5.1- TUC_NCPeH_031: Überprüfung des Cross-Enterprise Document Reliable Interchange Request für eD-A auf allgemeine Vorgaben]</p> <p>Anwendungsszenario: eDispensation Land-A</p>
<p>Ein anderer Code oder das angegebene Kodiersystem zum XSDDocumentEntryClassCode entspricht nicht dem aus [eHDSI_XDR_Profile#2.1.1] bzw. ist noch nicht zur Verarbeitung durch NCPeH-FD vorgesehen.</p>	<p>ERROR_GENERIC_SERVICE_SIGNIFIER_UNKNOWN Anwendungsszenario: nicht bekannt</p> <p>Nach Eingang der XDR-Anfrage MUSS der NCPeH-FD einen Non-Repudiation of Receipt Eintrag gemäß [4.1.7.2 - Non-Repudiation of Receipt erstellen] und einen Audit Trail Eintrag gemäß [4.1.7.3 Patient Privacy Audit Trail Eintrag erstellen] in der Komponente Audit Repository speichern. Bei der Erstellung des Audit Trail Eintrages MUSS der NCPeH-FD die Vorgaben aus [eHDSI_XDR_Profile#4.3] umsetzen. Wenn zum Zeitpunkt der Erstellung des Audit Trail Eintrags nicht alle erforderlichen Daten im NCPeH-FD verfügbar sind, MÜSSEN die Daten in den Audit Trail Eintrag aufgenommen werden, sobald sie im NCPeH-FD verfügbar sind, spätestens aber nachdem die Antwort an NCPeH Land-B gesendet wurde.</p> <p>Der NCPeH-FD DARF die XDR-Anfrage NICHT weiterverarbeiten und MUSS dem NCPeH Land-B mit den folgenden Angaben zum Fehler antworten:</p> <ul style="list-style-type: none"> • errorCode: ERROR_GENERIC_SERVICE_SIGNIFIER_UNKNOWN, • codeContext: Unknown service. Please contact your service provider or administrator., • severity: urn:oasis:names:tc:ebxml-regrep:ErrorSeverityType:Error, • location: Received XSDDocumentEntryClassCode= + Wert des XSDDocumentEntryClassCode-Elementes. <p>Der NCPeH-FD MUSS für das Attribut RegistryResponse@status in der XDR-Antwortnachricht einen entsprechenden Wert setzen, der unter Berücksichtigung der Kriterien aus der Tabelle "Provide and Register Document Set-b [ITI-41] Responses" in [ebRIM_Representation_Document#"Error responses"] zu ermittelt ist.</p> <p>Nach Versand der Fehlernachricht MUSS der NCPeH-FD einen Non-Repudiation of Origin Eintrag gemäß [4.1.7.1-</p>

	<p><u>Non-Repudiation of Origin erstellen</u>] in die Komponente Audit Repository speichern. Bei der Vervollständigung des Patient Privacy Audit Trail Eintrages MÜSSEN Vorgaben aus [eHDSI_XCA_Profile#4.3] umgesetzt werden.</p>
--	--

[<=]

6.1.5.1 TUC_NCPeH_031: Überprüfung des Cross-Enterprise Document Reliable Interchange Request für eD-A auf allgemeine Vorgaben

Für diesen TUC gelten folgende übergreifende Festlegungen

- [[4.1.2 - Datenaustausch mit zugelassenen EU-Ländern](#)]
- [[4.1.3 - eHDSI Basisleistungen](#)]
- [[4.1.5 - Validierung der Identity Assertion des LE-EU](#)]
- [[4.1.6 Validierung der TRC-Assertion](#)]
- [[4.1.7.2 Non-Repudiation of Receipt erstellen](#)]
- [[4.1.7.3 Patient Privacy Audit Trail Eintrag erstellen](#)]
- [[4.1.8 - Festlegungen zur Prüfung der Zugriffsberechtigung auf Fachdienste der TI](#)]

Ablauf des TUC

A_26651 - NCPeH - XDR eD-A - Erfassung von Evidence und Audit Trail für die XDR-Anfrage

Der NCPeH-FD MUSS einen Non-Repudiation of Receipt Eintrag gemäß [[4.1.7.2 Non-Repudiation of Receipt erstellen](#)] und einen Audit Trail Eintrag gemäß [[4.1.7.3 Patient Privacy Audit Trail Eintrag erstellen](#)] in der Komponente Audit Repository speichern. Bei der Erstellung des Audit Trail Eintrages MUSS der NCPeH-FD die Vorgaben aus [eHDSI_XDR_Profile#3.2] umsetzen. Wenn zum Zeitpunkt der Erstellung des Audit Trail Eintrags nicht alle erforderlichen Daten im NCPeH-FD verfügbar sind, MÜSSEN die Daten in den Audit Trail Eintrag aufgenommen werden, sobald sie im NCPeH-FD verfügbar sind, spätestens aber nachdem die Antwort an NCPeH Land-B gesendet wurde. [<=]

A_27203 - NCPeH - XDR eD-A - Prüfung des Ländercodes aus TLS-Zertifikat des NCPeH Land-B

Der NCPeH-FD MUSS das vom NCPeH Land-B verwendete TLS-Zertifikat überprüfen. Dabei MUSS er sicherstellen, dass der Wert der Variable `tls_country` nicht leer (siehe [[4.1.3.1 Sicherer Kanal: TESTA-ng und TLS](#)]) und in der `WHITELIST_NCPeH_COUNTRY-B` nach [[4.1.2 "Datenaustausch mit zugelassenen EU-Ländern"](#)] enthalten ist. Wenn die Überprüfung fehlschlägt, dann MUSS der NCPeH-FD jede weitere Bearbeitung der XDR-Anfrage abbrechen, in der Antwortnachricht an den NCPeH Land-B ein `RegistryResponse/RegistryErrorList/RegistryError-Element` erstellen und folgende Angaben zum Fehler in das erstellte Element aufnehmen:

- `errorCode= ERROR_ED_GENERIC`
- `codeContext= "The german eDispensation service is not agreed with the requesting country. Please contact your service provider or administrator."`
- `severity= "urn:oasis:names:tc:ebxml-regrep:ErrorSeverityType:Error"`
- `location= "The DN structure in the subject of the received TLS certificate does not contain a valid EU country code or the addressed service is not"`

agreed between the requesting country and germany. Received country code= " + Wert der Variable `tls_country`.

[<=]

A_26652 - NCPeH - XDR eD-A - Prüfung auf relevante PermissionCodes zur Erlangung einer Zugriffsberechtigung auf E-Rezept-FD

Wenn die Variable `ida_permissions` (siehe [[4.1.5 Validierung der Identity Assertion des LE-EU](#)]) nicht leer ist, MUSS der NCPeH-FD prüfen, ob der Wert der Variable alle erforderlichen Permission Codes gemäß Vorgaben aus [[4.1.8 Festlegungen zur Prüfung der Zugriffsberechtigung auf Fachdienste der TI](#)] für den eHDSI Use Case "Notification on Dispensation" enthält. Wenn die relevanten Permission Codes nicht in der Variable `ida_permissions` enthalten sind, MUSS der NCPeH-FD jede weitere Bearbeitung der XDR-Anfrage abbrechen, in der Antwortnachricht an den NCPeH Land-B ein `RegistryResponse/RegistryErrorList/RegistryError-Element` erstellen und folgende Angaben zum Fehler in das erstellte Element aufnehmen:

- `errorCode= "ERROR_ED_GENERIC"`
- `codeContext= "Access denied. Please contact your service provider or administrator and check the access rights for your health professional role in your country."`
- `severity= "urn:oasis:names:tc:ebxml-regrep:ErrorSeverityType:Error."`
- `location= "Received permission codes=" + Wert der Variable ida_permissions`

[<=]

A_26699 - NCPeH - XDR eD-A - Prüfung der Bedingungen zur Erlangung einer Zugriffsberechtigung auf E-Rezept-FD anhand der Rolle des LE-EU

Wenn die Variable `ida_permissions` (siehe [[4.1.5 Validierung der Identity Assertion des LE-EU](#)]) leer ist, dann MUSS der NCPeH-FD anhand der Rolle des LE-EU prüfen, ob die Vorgaben aus [[4.1.8 - Festlegungen zur Prüfung der Zugriffsberechtigung auf Fachdienste der TI](#)] zur Erlangung einer Zugriffsberechtigung auf den E-Rezept-FD erfüllt sind. Wenn die Vorgaben für die Zugriffsberechtigung nicht erfüllt sind, dann MUSS der NCPeH-FD die weitere Bearbeitung der XDR-Anfrage abbrechen, in der Antwortnachricht an den NCPeH Land-B ein `RegistryResponse/RegistryErrorList/RegistryError-Element` erstellen und folgende Angaben zum Fehler in das erstellte Element aufnehmen:

- `errorCode= ERROR_ED_GENERIC`
- `codeContext= "Access denied. The information provided about the role of the health professional does not comply with German regulations."`
- `severity= urn:oasis:names:tc:ebxml-regrep:ErrorSeverityType:Error.`
- `location= "No permission codes received and the access cannot be granted for the received practitioner role code in accordance with national regulations. Received practitioner role code=" + Wert der Variable ida_practitioner_role_code.`

[<=]

A_27204 - NCPeH - XDR eD-A - Validierung der `trc_kvnr`

Der NCPeH-FD MUSS prüfen, ob der Wert der Variable `trc_kvnr` nicht leer ist und der Wert die Vorgaben aus [[4.1.9 Format und Validierung der KVNR](#)] erfüllt sind. Wenn die Kriterien nicht erfüllt sind, MUSS der NCPeH-FD jede weitere Bearbeitung der XDR-Anfrage abbrechen, in der Antwortnachricht an den NCPeH Land-B ein `RegistryResponse/RegistryErrorList/RegistryError-Element` erstellen und folgende Angaben zum Fehler in das erstellte Element aufnehmen:

- `errorCode= ERROR_ED_GENERIC`

- codeContext= "Please make sure that the health insurance identifier is given and correct"
- severity= urn:oasis:names:tc:ebxml-regrep:ErrorSeverityType:Error
- location= "Health insurant number is missing or invalid."

[<=]

A_27206 - NCPeH - XDR eD-A - Prüfung des trc_accesscode auf Formatvorgaben

Der NCPeH-FD MUSS prüfen, ob der Wert der Variable trc_accesscode nicht leer ist und der Wert die Formatvorgaben aus [\[4.1.6 - Validierung der TRC-Assertion\]](#) erfüllt. Wenn die Kriterien nicht erfüllt sind, MUSS der NCPeH-FD jede weitere Bearbeitung der XDR-Anfrage abbrechen, in der Antwortnachricht an den NCPeH Land-B ein RegistryResponse/RegistryErrorList/RegistryError-Element erstellen und folgende Angaben zum Fehler in das erstellte Element aufnehmen:

- errorCode= ERROR_ED_GENERIC
- codeContext= "Access denied. The patients access code is missing or malformed. Please ask the patient for access authorisation and the proper access code."
- severity= urn:oasis:names:tc:ebxml-regrep:ErrorSeverityType:Error
- location= Keine Angaben.

[<=]

A_27208 - NCPeH - eD-A - Überprüfung der Angabe eines Identifier des LE-EU

Der NCPeH-FD MUSS prüfen, ob der Wert der Variable ida_name-id (siehe [\[4.1.5 - Validierung der Identity Assertion des LE-EU\]](#)) nicht leer ist . Wenn die Variable leer ist, MUSS der NCPeH-FD jede weitere Bearbeitung der XDR-Anfrage abbrechen, in der Antwortnachricht an den NCPeH Land-B ein RegistryResponse/RegistryErrorList/RegistryError-Element erstellen und folgende Angaben zum Fehler in das erstellte Element aufnehmen:

- errorCode= ERROR_HPI_INSUFFICIENT_INFORMATION
- codeContext= "Access denied. The identifier of the health professional is missing in the provided identity information."
- severity= urn:oasis:names:tc:ebxml-regrep:ErrorSeverityType:Error
- location= Keine Angaben.

[<=]

A_27210 - NCPeH - eD-A - Überprüfung der Angabe der Rolle des LE-EU

Der NCPeH-FD MUSS prüfen, ob der Wert der Variable ida_practitioner_role (siehe [\[4.1.5 - Validierung der Identity Assertion des LE-EU\]](#)) nicht leer ist . Wenn die Variable leer ist, MUSS der NCPeH-FD jede weitere Bearbeitung der XDR-Anfrage abbrechen, in der Antwortnachricht an den NCPeH Land-B ein RegistryResponse/RegistryErrorList/RegistryError-Element erstellen und folgende Angaben zum Fehler in das erstellte Element aufnehmen:

- errorCode= ERROR_HPI_INSUFFICIENT_INFORMATION
- codeContext= "Access denied. The information about the role of EU health professional is missing in the provided identity information."
- severity= urn:oasis:names:tc:ebxml-regrep:ErrorSeverityType:Error
- location= Keine Angaben.

[<=]

A_27211 - NCPeH - XDR eD-A - Überprüfung der Angaben zum Namen des LE-EU

Der NCPeH-FD MUSS überprüfen, ob der Wert der Variable `ida_practitioner_name` (siehe [4.1.5 - Validierung der Identity Assertion des LE-EU]) nicht leer ist. Wenn die Variable leer ist, MUSS der NCPeH-FD jede weitere Bearbeitung der XDR-Anfrage abbrechen, in der Antwortnachricht an den NCPeH Land-B ein `RegistryResponse/RegistryErrorList/RegistryError-Element` erstellen und folgende Angaben zum Fehler in das erstellte Element aufnehmen:

- `errorCode= ERROR_HPI_INSUFFICIENT_INFORMATION`
- `codeContext= "Access denied. The name of the EU health professional is missing in the provided identity information."`
- `severity= urn:oasis:names:tc:ebxml-regrep:ErrorSeverityType:Error`
- `location= Keine Angaben.`

[<=]

A_27213 - NCPeH - XDR eD-A - Überprüfung des Rollencodes des LE-EU

Der NCPeH-FD MUSS überprüfen, ob der Wert der Variable `ida_practitioner_role_code` (siehe [4.1.5 - Validierung der Identity Assertion des LE-EU]) nicht leer ist und ob dieser identisch mit einem der zulässigen Werte für das Element `urn:oasis:names:tc:xacml:2.0:subject:role` aus [eHDSI_SAML_Profile#2.3] ist. Wenn die Überprüfung nicht erfolgreich war, MUSS der NCPeH-FD jede weitere Bearbeitung der XDR-Anfrage abbrechen, in der Antwortnachricht an den NCPeH Land-B ein `RegistryResponse/RegistryErrorList/RegistryError-Element` erstellen und folgende Angaben zum Fehler in das erstellte Element aufnehmen:

- `errorCode= ERROR_HPI_INSUFFICIENT_INFORMATION`
- `codeContext= "Access denied. Missing or unknown role of the EU health professional in the provided identity information."`
- `severity= urn:oasis:names:tc:ebxml-regrep:ErrorSeverityType:Error`
- `location= "Received role code of the health professional from the identity assertion; see element urn:oasis:names:tc:xacml:2.0:subject:role=" + Wert der Variable ida_practitioner_role_code.`

[<=]

A_27214 - NCPeH - XDR eD-A - Überprüfung der Angabe zum Behandlungsort

Der NCPeH-FD MUSS überprüfen, ob der Wert der Variable `ida_point_of_care` (siehe [4.1.5 - Validierung der Identity Assertion des LE-EU]) nicht leer ist. Wenn die Variable leer ist, dann MUSS der NCPeH-FD jede weitere Bearbeitung der XDR-Anfrage abbrechen, in der Antwortnachricht an den NCPeH Land-B ein `RegistryResponse/RegistryErrorList/RegistryError-Element` erstellen und folgende Angaben zum Fehler in das erstellte Element aufnehmen:

- `errorCode= ERROR_HPI_POC_NO_INFORMATION`
- `codeContext= "Access denied. Missing name of the point of care in the provided identity information."`
- `severity= urn:oasis:names:tc:ebxml-regrep:ErrorSeverityType:Error`
- `location= Keine Angaben.`

[<=]

A_27217 - NCPeH - XDR eD-A - Überprüfen der Angabe zum Typ der LEI-EU

Der NCPeH-FD MUSS überprüfen, ob der Wert der Variable `ida_healthcare_facility_type_code` (siehe [4.1.5 - Validierung der Identity Assertion

des LE-EU]) nicht leer ist und das dieser identisch mit einem der zulässigen Werte für das Identitätsattribut urn:ehdsi:names:subject:healthcare-facility-type aus [eHDSI_SAML_Profile#2.3] ist. Wenn die Überprüfung nicht erfolgreich war, MUSS der NCPeH-FD jede weitere Bearbeitung der XDR-Anfrage abbrechen, in der Antwortnachricht an den NCPeH Land-B ein RegistryResponse/RegistryErrorList/RegistryError-Element erstellen und folgende Angaben zum Fehler in das erstellte Element aufnehmen:

- errorCode= ERROR_HPI_POC_NO_INFORMATION
- codeContext= "Access denied. Missing or unknown type of Healthcare Provider Organisation in the provided identity information."
- severity= urn:oasis:names:tc:ebxml-regrep:ErrorSeverityType:Error
- location= "Received healthcare facility type= " + Wert der Variable ida_healthcare_facility_type_code.

[<=]

Hinweis: Die Strukturvorgaben für das SubmitObjectsRequest-Element sind in [Abstract_Metadata_for_Document_Sharing_profiles#4.1.4] beschrieben. Die Vorgaben für das RegistryObjectList-Element sind enthalten in [ebRIM_Representation_Document#4.2.1.4].

A_26650 - NCPeH - XDR eD-A - Prüfung des Formats der XDR-Anfrage auf eHDSI-Vorgaben

Der NCPeH-FD MUSS prüfen, dass die XDR-Anfrage vom Nachrichtentyp ProvideAndRegisterDocumentSetRequest ist und die Vorgaben aus [eHDSI_XDR_Profile#2.1] erfüllt. Wenn die Prüfung nicht erfolgreich war, MUSS der NCPeH-FD jede weitere Bearbeitung der XDR-Anfrage abbrechen und dem NCPeH Land-B mit einem RegistryError antworten:

- errorCode= ERROR_ED_GENERIC
- codeContext= "The type of the received request is invalid."
- severity= urn:oasis:names:tc:ebxml-regrep:ErrorSeverityType:Error
- location= "The request is not of the ProvideAndRegisterDocumentSetRequest message type or does not conform to the requirements of the eHDSI."

[<=]

A_27229 - NCPeH - XDR eD-A - Statusbestimmung für RegistryResponse in der XDR-Antwortnachricht

Wenn bei der Überprüfung der XDR-Anfrage auf Erfüllung von allgemeinen Vorgaben Fehler festgestellt werden, dann MUSS der NCPeH-FD für das Attribut RegistryResponse@status in der XDR-Antwortnachricht einen entsprechenden Wert setzen, der auf Basis des Gesamtstatus aller RegistryResponse/RegistryErrorList/RegistryError@Severities-Attribute und unter Berücksichtigung der Kriterien aus der Tabelle "Provide and Register Document Set-b [ITI-41] Responses" in [ebRIM_Representation_Document#"Error responses"] zu ermittelt ist.

[<=]

Ausgabeparameter des TUC

- Keine Ausgabeparameter

6.1.5.2 TUC_NCPeH_032: Cross-Enterprise Document Reliable Interchange Request für eD-A verarbeiten

Für diesen TUC gelten folgende übergreifende Festlegungen

- [[4.1.3 - eHDSI Basisleistungen](#)]
- [[4.1.6 Validierung der TRC-Assertion](#)]

Ablauf des TUC

A_26659 - XDR-Anfrage - Dekodierung und Validierung von Dispensierdokumenten

Der NCPeH-FD MUSS für jedes ProvideAndRegisterDocumentSetRequest/Document-Element in der XDR-Anfrage überprüfen, ob es einen base64-kodierten Wert enthält, diesen dekodieren und prüfen, ob das Ergebnis die Strukturvorgaben gemäß dem CDA-Template "eHDSI eDispensation" aus [<https://art-decor.ehdsi.eu/publication/>] erfüllt. Wenn die Dekodierung des Wertes aus einem Document-Element nicht möglich ist oder das Ergebnis der Dekodierung nicht die Strukturvorgaben erfüllt, MUSS der NCPeH-FD ein RegistryResponse/RegistryErrorList/RegistryError-Element erstellen und darin folgende Angaben zum Fehler setzen:

- `errorCode= InvalidDocumentContent`
- `codeContext= "The format of the dispensation document is invalid. Affected dispensation document with ID= " + Wert des XDSSubmissionSet.uniqueId-Elements aus dem entsprechenden ExtrinsicObject-Element, das in Verbindung mit dem vom Fehler betroffenen Document-Element steht`
- `severity= urn:oasis:names:tc:ebxml-regrep:ErrorSeverityType:Error`
- `location= "The decoding or format of the dispensation document is incorrect. Affected dispensation document with ID=" + Wert des XDSSubmissionSet.uniqueId-Elements aus dem entsprechenden ExtrinsicObject-Element, das in Verbindung mit dem vom Fehler betroffenen Document-Element steht + ". " + "Affected ePrescription with ID=" + E-Rezept-ID aus dem dekodierten vom Fehler betroffenen Document-Element (siehe /ClinicalDocument/inFulfillmentOf/order/id/), sofern die E-Rezept-Id im Dokument ermittelbar ist.`

Der NCPeH-FD MUSS das RegistryError-Element in einer Variable `list_registry_error_xdr_request` für die weitere Datenverarbeitung zwischenspeichern.

[<=]

A_27226 - NCPeH - XDR eD-A - Ermitteln des passenden ExtrinsicObject-Elements zum Document-Element

Der NCPeH-FD MUSS für jedes in der XDR-Anfrage enthaltene ProvideAndRegisterDocumentSetRequest/Document-Element überprüfen, ob ein entsprechendes ExtrinsicObject-Element existiert. Wenn die Prüfung nicht erfolgreich ist, dann MUSS der NCPeH-FD für das vom Fehler betroffene Document-Element ein RegistryResponse/RegistryErrorList/RegistryError-Element erstellen und darin folgende Angaben zum Fehler setzen:

- `errorCode= XDSSMissingDocumentMetadata`
- `codeContext= "There is no matching metadata information for the dispensation document with the ePrescription ID=" + Angabe zum E-Rezept-ID aus dem dekodierten Wert des vom Fehler betroffenen Document-Element`
- `severity= urn:oasis:names:tc:ebxml-regrep:ErrorSeverityType:Error`

- location= "Received dispensation document with ID= " + id-Wert aus dem dekodierten vom Fehler betroffenen Document-Element + ". " + "Affected ePrescription with ID= " + Wert der E-Rezept-ID aus dem dekodierten vom Fehler betroffenen Document-Element.

Der NCPeH-FD MUSS das RegistryError-Element in einer Variable list_registry_error_xdr_request für die weitere Datenverarbeitung zwischenspeichern.

[<=]

A_27227 - NCPeH - XDR eD-A - Überprüfen auf nicht eindeutige Document-Elemente

Der NCPeH-FD MUSS für jedes in der XDR-Anfrage enthaltene ProvideAndRegisterDocumentSetRequest/SubmitObjectsRequest/RegistryObjectList/ExtrinsicObject-Element überprüfen, ob ein eindeutiges Document-Element existiert. Wenn die Prüfung gezeigt hat, dass es der XDR-Anfrage ExtrinsicObject-Elemente gibt zu denen keine eindeutige Document-Elemente zu ermitteln sind, dann MUSS der NCPeH-FD ein RegistryResponse/RegistryErrorList/RegistryError-Element erstellen und darin folgende Angaben zum Fehler setzen:

- errorCode= XDSMissingDocument
- codeContext= "Missing dispensation document with the ID= " + Wert der uniqueId aus dem vom Fehler betroffenen ExtrinsicObject-Element
- severity= urn:oasis:names:tc:ebxml-regrep:ErrorSeverityType:Error
- location= "Missing dispensation document with the ID= " + Wert der uniqueId aus dem vom Fehler betroffenen ExtrinsicObject-Element.

Der NCPeH-FD MUSS das RegistryError-Element in einer Variable list_registry_error_xdr_request für die weitere Datenverarbeitung zwischenspeichern.

[<=]

A_26654 - NCPeH - XDR eD-A - Überprüfung des ExtrinsicObject-Elements auf die Erfüllung von eHDSI-Vorgaben

Der NCPeH-FD MUSS zu jedem ProvideAndRegisterDocumentSetRequest/Document-Element ein passendes ExtrinsicObject-Element ermitteln, dessen id-Wert identisch mit dem id-Wert des Document-Elementes ist. Der NCPeH-FD MUSS bei dem ermittelten ExtrinsicObject-Element und dazu passendem Document-Element folgende Überprüfungen durchführen:

- Die Attribute, Slots, Classifications und External identifiers MÜSSEN die Vorgaben aus [eHDSI_XDR_Profile#2.1] und [eHDSI_NCPeH_Components#3.1.5.2] erfüllen.
- Die Metadaten creationTime, languageCode, practiceSettingCode und confidentialityCode aus dem ExtrinsicObject-Element MÜSSEN ignoriert werden.
- Der Wert des XSDDocumentEntryPatientId aus dem ExtrinsicObject-Element MUSS identisch mit dem Wert der Variable trc_patient_identifizier aus [[4.1.6 Validierung der TRC-Assertion](#)] sein.
- Der Wert des Slots sourcePatientId aus dem ExtrinsicObject-Element MUSS identisch mit dem Wert der Variable trc_patient_identifizier aus [[4.1.6 Validierung der TRC-Assertion](#)] sein.
- Die KVNR des Versicherten aus dem dekodierten Document-Element MUSS identisch mit der trc_kvnr aus [[4.1.6 Validierung der TRC-Assertion](#)] sein. Wenn der Wert der

KVNR im dekodierten Document-Element die Angaben zum "|" -Zeichen und Zugriffscode enthält, dann MÜSSEN beim Abgleich der Werte diese Anteile ignoriert werden.

Wenn die Prüfungen nicht erfolgreich sind, dann MUSS der NCPeH-FD aus der XDR-Anfrage für das vom Fehler betroffene Document-Element ein RegistryResponse/RegistryErrorList/RegistryError-Element erstellen und darin folgende Angaben zum Fehler setzen:

- errorCode= InvalidDocumentContent
- codeContext= Der englische Text MUSS vom Anbieter des NCPeH-FD als konkrete Beschreibung des Fehlers für die betroffene MetaData gesetzt werden. Der Text MUSS für einen LE-EU einfach und verständlich sein.
- severity= urn:oasis:names:tc:ebxml-regrep:ErrorSeverityType:Error,
- location= Der englische Text MUSS vom Anbieter des NCPeH-FD als konkrete Beschreibung des Fehlers für die betroffene MetaData gesetzt werden. Die Fehlerbeschreibung MUSS den Wert des id-Attributs aus dem vom Fehler betroffenen Document-Element enthalten. Der Text MUSS für einen prüfenden Techniker verständlich sein.

Der NCPeH-FD MUSS das RegistryError-Element in einer Variable list_registry_error_xdr_request für die weitere Datenverarbeitung zwischenspeichern.

[<=]

A_27228 - NCPeH - XDR eD-A - Bereinigung und Zwischenspeicherung von dekodierten Inhalten aus Document-Element

Der NCPeH-FD MUSS bei der Verarbeitung des dekodierten Inhalts eines Document-Elements aus der XDR-Anfrage für Angaben zur KVNR des Versicherten das "|" -Zeichen und den Zugriffscode entfernen, bei Angaben zur E-Rezept-ID die Endungen "^eP.XML" und "^eP.PDF" entfernen, und anschließend den bereinigten dekodierten Inhalt des Document-Elements in einer Liste xdr_request_cda_dispensation_documents zwischenspeichern.

[<=]

Beispiel einer XDR-Anfrage in der eHDSI zur Übermittlung eines Dispensierdokumentes im base64-kodierten eHDSI CDA Pivotformat. Aufgrund der Länge des CDA-Dokumentes enthält das Beispiel im Element <Document> einen Platzhalter "...":

```
<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Body xmlns:soapenv="http://www.w3.org/2003/05/soap-envelope">
  <xdr:ProvideAndRegisterDocumentSetRequest xmlns:xdr="urn:ihe:iti:xds-b:2007">
    <ns3:SubmitObjectsRequest xmlns="urn:oasis:names:tc:ebxml-regrep:xsd:rim:3.0"
      xmlns:ns2="urn:oasis:names:tc:ebxml-regrep:xsd:rs:3.0"
      xmlns:ns3="urn:oasis:names:tc:ebxml-regrep:xsd:lcm:3.0"
      xmlns:ns4="urn:ihe:iti:xds-b:2007"
      xmlns:ns5="urn:oasis:names:tc:ebxml-regrep:xsd:query:3.0">
      <RegistryObjectList>
        <ExtrinsicObject id="urn:uuid:f8d6175f-3bb7-46e9-ac09-606383dcabab"
          mimeType="text/xml"
          objectType="urn:uuid:7edca82f-054d-47f2-a032-9b2a5b5186c1"
          status="urn:oasis:names:tc:ebxml-regrep:StatusType:Approved">
          <Slot name="creationTime">
            <ValueList>
              <Value>20230626122026</Value>
            </ValueList>
          </Slot>
          <Slot name="languageCode">
            <ValueList>
              <Value>lt-LT</Value>
            </ValueList>
          </ExtrinsicObject>
        </RegistryObjectList>
      </SubmitObjectsRequest>
    </xdr:ProvideAndRegisterDocumentSetRequest>
  </soapenv:Body>
</soapenv:Envelope>
```

```

        </Slot>
        <Slot name="sourcePatientId">
            <ValueList>
                <Value>B123456789|A2C4E6^^^&amp;1.2.276.0.76.3.1.580.147&amp;ISO</
Value>
            </ValueList>
        </Slot>
        <Slot name="sourcePatientInfo">
            <ValueList>
                <Value>PID-3|B123456789|
A2C4E6^^^&amp;1.2.276.0.76.3.1.580.147&amp;ISO</Value>
                <Value>PID-5|Johanna Gräfin von Oberberg</Value>
                <Value>PID-7|19800626152026.030+0300</Value>
            </ValueList>
        </Slot>
        <!-- healthCareFacilityTypeCode -->
        <Classification classificationScheme="urn:uuid:f33fb8ac-18af-42cc-ae0e-
ed0b0bdb91e1"
        606383dcabab"
            classifiedObject="urn:uuid:f8d6175f-3bb7-46e9-ac09-
            id="urn:uuid:b23dd8a1-e993-463d-b10b-abd75158626d"
            nodeRepresentation="LT">
                <Slot name="codingScheme">
                    <ValueList>
                        <Value>1.0.3166.1</Value>
                    </ValueList>
                </Slot>
                <Name>
                    <LocalizedString value="Lithuania"/>
                </Name>
            </Classification>
        <!-- practiceSettingCode -->
        <Classification classificationScheme="urn:uuid:cccf5598-8b07-4b77-a05e-
ae952c785ead"
        606383dcabab"
            classifiedObject="urn:uuid:f8d6175f-3bb7-46e9-ac09-
            id="urn:uuid:01bedd3e-bc25-48e0-b57e-27186868878f"
            nodeRepresentation="Not Used">
                <Slot name="codingScheme">
                    <ValueList>
                        <Value>eHDSI Practice Setting Codes-Not Used</Value>
                    </ValueList>
                </Slot>
                <Name>
                    <LocalizedString value="Not Used"/>
                </Name>
            </Classification>
        <!-- confidentialityCode -->
        <Classification classificationScheme="urn:uuid:f4f85eac-e6cb-4883-b524-
f2705394840f"
        606383dcabab"
            classifiedObject="urn:uuid:f8d6175f-3bb7-46e9-ac09-
            id="urn:uuid:0e5097bc-ef5d-42ec-8081-a1f62d63f3cd"
            nodeRepresentation="N">
                <Slot name="codingScheme">
                    <ValueList>
                        <Value>2.16.840.1.113883.5.25</Value>
                    </ValueList>
                </Slot>
                <Name>
                    <LocalizedString value="Normal"/>
                </Name>
            </Classification>
        <!-- classCode -->
        <Classification classificationScheme="urn:uuid:41a5887f-8865-4c09-adf7-
e362475b143a"
        606383dcabab"
            classifiedObject="urn:uuid:f8d6175f-3bb7-46e9-ac09-
            id="urn:uuid:c3a7f947-dcd4-4b2a-bd74-6f158158398d"
            nodeRepresentation="60593-1">
                <Slot name="codingScheme">
                    <ValueList>

```

```

        <Value>2.16.840.1.113883.6.1</Value>
      </ValueList>
    </Slot>
    <Name>
      <LocalizedString value="Medication dispensed"/>
    </Name>
  </Classification>
  <!-- formatCode -->
  <Classification classificationScheme="urn:uuid:a09d5840-386c-46f2-b5ad-
9c3699a4309d"
        classifiedObject="urn:uuid:f8d6175f-3bb7-46e9-ac09-
606383dcabab"
        id="urn:uuid:97bb44ff-5b0d-455f-afef-b4a1bd8f579a"
        nodeRepresentation="urn:epSOS:ep:dis:2010">
    <Slot name="codingScheme">
      <ValueList>
        <Value>eHDSI formatCodes</Value>
      </ValueList>
    </Slot>
    <Name>
      <LocalizedString value="eHDSI coded eDispensation"/>
    </Name>
  </Classification>
  <!-- typeCode -->
  <Classification classificationScheme="urn:uuid:f0306f51-975f-434e-a61c-
c59651d33983"
        classifiedObject="urn:uuid:f8d6175f-3bb7-46e9-ac09-
606383dcabab"
        id="urn:uuid:70324b06-6de5-4664-a860-e67b545591ec"
        nodeRepresentation="60593-1">
    <Slot name="codingScheme">
      <ValueList>
        <Value>2.16.840.1.113883.6.1</Value>
      </ValueList>
    </Slot>
    <Name>
      <LocalizedString value="eDispensation"/>
    </Name>
  </Classification>
  <ExternalIdentifier id="urn:uuid:52a2eb98-72c3-491a-8c58-80693f30934f"
        identificationScheme="urn:uuid:58a6f841-87b3-4a3e-92fd-
a8ffeff98427"
        objectType="urn:oasis:names:tc:ebxml-
regrep:ObjectType:RegistryObject:ExternalIdentifier"
        registryObject="urn:uuid:f8d6175f-3bb7-46e9-ac09-
606383dcabab"
        value="B123456789|
A2C4E6^^^&amp;1.2.276.0.76.3.1.580.147&amp;ISO">
    <Name>
      <LocalizedString value="XSDDocumentEntry.patientId"/>
    </Name>
  </ExternalIdentifier>
  <ExternalIdentifier id="urn:uuid:bef1f945-9eed-4cac-89fb-99eb9b0ab246"
        identificationScheme="urn:uuid:2e82c1f6-a085-4c72-9da3-
8640a32e42ab"
        objectType="urn:oasis:names:tc:ebxml-
regrep:ObjectType:RegistryObject:ExternalIdentifier"
        registryObject="urn:uuid:f8d6175f-3bb7-46e9-ac09-
606383dcabab"
        value="1.3.6.1.4.1.28284.6.2.4.4^3y5C0ceLhApariKC">
    <Name>
      <LocalizedString value="XSDDocumentEntry.uniqueId"/>
    </Name>
  </ExternalIdentifier>
</ExtrinsicObject>
<RegistryPackage id="urn:uuid:15cd166f-5d2b-4e18-b9b2-71f41eaeabaf6"
        objectType="urn:uuid:a54d6aa5-d40d-43f9-88c5-b4633d873bdd">
  <Slot name="submissionTime">
    <ValueList>
      <Value>20230626032026</Value>
    </ValueList>
  </Slot>

```

```

        <Name>
          <LocalizedString value="eDispensation"/>
        </Name>
        <Description>
          <LocalizedString value="Description of eDispensation"/>
        </Description>
        <Classification classificationScheme="urn:uuid:a7058bb9-b4e4-4307-ba5b-
e3f0ab85e12d"
                          classifiedObject="urn:uuid:15cd166f-5d2b-4e18-b9b2-
71f41eaeabaf6"
                          id="urn:uuid:036fd6db-b262-499a-940c-75f0586bc345"
                          nodeRepresentation="">
          <Slot name="authorInstitution">
            <ValueList>
              <Value>General
Hospital^^^^^&2.16.840.1.113883.2.11.4.6&ISO^^^^1000139817</Value>
              </ValueList>
            </Slot>
            <Slot name="authorPerson">
              <ValueList>
                <Value>Rasa
Keraité^^^&2.16.840.1.113883.2.11.4.6:1000139817&ISO</Value>
                </ValueList>
              </Slot>
            </Classification>
          <Classification classificationScheme="urn:uuid:aa543740-bdda-424e-8c96-
df4873be8500"
                          classifiedObject="urn:uuid:15cd166f-5d2b-4e18-b9b2-
71f41eaeabaf6"
                          id="urn:uuid:dd8c32b9-4e15-484d-a459-8683de77bb26"
                          nodeRepresentation="60593-1">
            <Slot name="codingScheme">
              <ValueList>
                <Value>2.16.840.1.113883.6.1</Value>
              </ValueList>
            </Slot>
            <Name>
              <LocalizedString value="eDispensation"/>
            </Name>
          </Classification>
        <ExternalIdentifier id="urn:uuid:0abc413c-75f4-4a60-ba62-22873e150173"
                          identificationScheme="urn:uuid:96fdda7c-d067-4183-912e-
bf5ee74998a8"
                          objectType="urn:oasis:names:tc:ebxml-
regrep:ObjectType:RegistryObject:ExternalIdentifier"
                          registryObject="urn:uuid:15cd166f-5d2b-4e18-b9b2-
71f41eaeabaf6"
                          value="2.16.840.1.113883.2.11.300.451">
          <Name>
            <LocalizedString value="XDSSubmissionSet.uniqueId"/>
          </Name>
        </ExternalIdentifier>
        <ExternalIdentifier id="urn:uuid:b3a7d356-c363-493a-b176-75e8b8f7051c"
                          identificationScheme="urn:uuid:6b5aea1a-874d-4603-a4bc-
96a0a7b38446"
                          objectType="urn:oasis:names:tc:ebxml-
regrep:ObjectType:RegistryObject:ExternalIdentifier"
                          registryObject="urn:uuid:15cd166f-5d2b-4e18-b9b2-
71f41eaeabaf6"
                          value="B123456789|
A2C4E6^^^&1.2.276.0.76.3.1.580.147&ISO">
          <Name>
            <LocalizedString value="XDSSubmissionSet.patientId"/>
          </Name>
        </ExternalIdentifier>
        <ExternalIdentifier id="urn:uuid:f3aac6fb-312a-46c0-9c55-39d748f062e5"
                          identificationScheme="urn:uuid:554ac39e-e3fe-47fe-b233-
965d2a147832"
                          objectType="urn:oasis:names:tc:ebxml-
regrep:ObjectType:RegistryObject:ExternalIdentifier"
                          registryObject="urn:uuid:15cd166f-5d2b-4e18-b9b2-
71f41eaeabaf6"

```

```

                                value="1.3.6.1.4.1.21367.2009.1.2.1">
      <Name>
        <LocalizedString value="XDSSubmissionSet.sourceId"/>
      </Name>
    </ExternalIdentifier>
  </RegistryPackage>
  <Classification classificationNode="urn:uuid:a54d6aa5-d40d-43f9-88c5-
b4633d873bdd"
                                classifiedObject="urn:uuid:15cd166f-5d2b-4e18-b9b2-71f41eabaf6"
                                id="urn:uuid:592d32ab-d3e3-4911-a6d3-8fd5de784e5a"/>
  <Association associationType="urn:oasis:names:tc:ebxml-
regrep:AssociationType:HasMember"
                                id="urn:uuid:eaea52a2-46bb-405a-85cd-742f755dd066"
                                sourceObject="urn:uuid:15cd166f-5d2b-4e18-b9b2-71f41eabaf6"
                                targetObject="urn:uuid:f8d6175f-3bb7-46e9-ac09-606383dcabab">
    <Slot name="SubmissionSetStatus">
      <ValueList>
        <Value>Original</Value>
      </ValueList>
    </Slot>
  </Association>
</RegistryObjectList>
</ns3:SubmitObjectsRequest>
<xdr:Document id="urn:uuid:f8d6175f-3bb7-46e9-ac09-606383dcabab">...</xdr:Document>
</xdr:ProvideAndRegisterDocumentSetRequest>
</soapenv:Body>

```

Ausgabeparameter des TUC

- xdr_request_cda_dispensation_documents,
(mit dekodierten Dispensierdokumenten im eHDSI eDispensation CDA-Pivotformat)
- list_registry_error_xdr_request.

6.1.5.3 TUC_NCPeH_033: Cross-Enterprise Document Reliable Interchange Response für eD-A senden

Für diesen TUC gelten folgende übergreifende Festlegungen

- [[4.1.3 - eHDSI Basisleistungen](#)]
- [[4.1.7 - Non-Repudiation und Audit Trail Schemas](#)]

Ablauf des TUC

Als Eingangsparameter für diesen TUC dient die Variable `list_registry_error_xdr_request`. Die Variable wurde im [6.1.5.2- TUC_NCPeH_032: Cross-Enterprise Document Reliable Interchange Request für eD-A verarbeiten] und [6.2.7- TUC_NCPeH_038: Dispensierdokumente an E-Rezept-FD übermitteln] mit entsprechenden RegistryError-Elementen befüllt.

A_27242 - NCPeH - XDR eD-A - Erstellung der XDR-Antwort für NCPeH Land-B

Der NCPeH-FD MUSS die Inhalte und Struktur der XDR-Antwort nach Vorgaben aus [eHDSI_XDR_Profile#2.2], [ITI-41#"Provide and Register Document Set-b Response"] und aus [ebRIM_Representation_Document#"Success and Error Reporting"] erstellen. [≤=]

A_27243 - NCPeH - XDR eD-A - Aufnahme von Warnung - und Fehlermeldungen in die XDR-Antwort

Der NCPeH-FD MUSS sämtliche in der Variable `list_registry_error_xdr_request` enthaltenen RegistryError-Elemente in die XDR-Antwort aufnehmen und dabei die Strukturvorgaben aus [ITI-41#"Provide and Register Document Set-b Response"] beachten. [≤=]

Hinweis: In der XDR-Antwort können nach [ebRIM_Representation_Document#4.2.4] Error Codes auftreten, die entsprechende ResponseStatus-Informationen aufweisen. Das

Vorhandensein eines RegistryErrorList-Elementes ist prinzipiell vereinbar mit einer teilweise erfolgreichen Verarbeitung. Falls die ErrorList nur Warnings enthält (RegistryError-Elemente mit warning severity, aber ohne error severity), dann muss die Verarbeitung der XDR-Anfrage als erfolgreich angesehen werden. Die Rückmeldungen zu Fehlern und Warnungen an NCPeH Land-B, die bei der Verarbeitung der XDR-Anfrage, der Transkodierung und Transformierung und Übermittlung des Dispensierdokumentes an E-Rezept-FD entstanden sind, haben das in [ebRIM_Representation_Document#4.2.4] "Success and Error Reporting" beschriebene Format und müssen explizit in die XDR-Antwort aufgenommen werden. Es wird im Fehlerfall eine Fehlerliste (RegistryErrorList) und darin für jeden festgestellten Fehler ein RegistryError-Element mit den Attributen errorCode, errorContext, severity und location zurückgegeben.

A_27244 - NCPeH - XDR eD-A - Bestimmung des Gesamtstatus der XDR-Antwort

Der NCPeH-FD MUSS für das Attribut RegistryResponse@status in der XDR-Antwort einen Wert setzen, der auf Basis des Gesamtstatus aller RegistryResponse/RegistryErrorList/RegistryError@severity-Attribute, der Anzahl erfolgreich verarbeiteter Document-Elemente und unter Berücksichtigung der Kriterien aus der Tabelle "Provide and Register Document Set-b [ITI-41] Responses" in [ebRIM_Representation_Document#4.2.4.2] ermittelt wird. [<=]

A_27245 - NCPeH - XDR eD-A - Erstellung und Speicherung des Non-Repudiation of Origin Eintrags beim Versand der XDR-Antwort

Der NCPeH-FD MUSS beim Versenden der XDR-Antwort an den NCPeH Land-B einen Non-Repudiation of Origin Eintrag gemäß den Vorgaben aus [4.1.7.1 - Non-Repudiation of Origin erstellen] in der Komponente Audit Repository speichern. [<=]

A_27246 - NCPeH - XDR eD-A - Bereinigung von Daten nach Versand der XDR-Antwort

Der NCPeH-FD MUSS unmittelbar nach dem Senden der XDR-Antwort an den NCPeH Land-B die

Listen list_registry_error_xdr_request, xdr_request_cda_dispensation_documents, list_transcoded_fhir_medication_dispensations und ihre Verweise auf die TRC Assertion des entsprechenden IHE XDR-Request löschen. [<=]

Beispiel einer XDR-Antwort als Bestätigung über die erfolgreiche Speicherung eines Dispensierdokumentes:

```
<?xml version="1.0" encoding="UTF-8"?>
<ns2:RegistryResponse status="urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Success"
  xmlns="urn:oasis:names:tc:ebxml-regrep:xsd:rim:3.0"
  xmlns:ns2="urn:oasis:names:tc:ebxml-regrep:xsd:rs:3.0"
  xmlns:ns4="urn:oasis:names:tc:ebxml-regrep:xsd:query:3.0"
  xmlns:ns3="urn:ihe:iti:xds-b:2007">
  <ns2:RegistryErrorList>
    <ns2:RegistryError
      codeContext="The dispensing information was successfully saved. The dispensed
e-prescription has the following ID= 12345678."
      errorCode="WARNING_ED_GENERIC"
      severity="urn:oasis:names:tc:ebxml-regrep:ErrorSeverityType:Warning" />
    </ns2:RegistryErrorList>
  </ns2:RegistryResponse>
```

Ausgabeparameter des TUC

- Keine

6.1.5.4 TUC_NCPeH_034: Dispensierdokumente transkodieren und transformieren

Für diesen TUC gelten folgende übergreifende Festlegungen

- [[4.1.7 - Non-Repudiation und Audit Trail Schemas](#)]
- [[4.2.10.6 Regelung zur Unterstützung von mehreren FHIR-Package Versionen](#)]

Ablauf des TUC

In diesem TUC führt der NCPeH-FD gemäß Vorgaben des BfArM die Transformierung und Transkodierung von Dispensierdokumenten aus der Liste

`xdr_request_cda_dispensation_documents` in das FHIR-Profil gemäß Vorgaben aus [GEM_ERPEU_PR_PAR_CloseOperation_Input] durch. Die Erstellung und Befüllung der Liste

`xdr_request_cda_dispensation_documents` ist im [6.1.5.2- TUC_NCPeH_032: Cross-Enterprise Document Reliable Interchange Request für eD-A verarbeiten] beschrieben.

A_27230 - NCPeH - XDR eD-A - Transformierung und Transkodierung von Dispensierdokumenten

Der NCPeH-FD MUSS alle Dispensierdokumente aus der Liste

`xdr_request_cda_dispensation_documents` (siehe [6.1.5.4- TUC_NCPeH_034: Dispensierdokumente transkodieren und transformieren]) nach Vorgaben des BfArM vom eHDSI eDispensation CDA-Pivotformat in das FHIR-Profil gemäß Vorgaben aus [GEM_ERPEU_PR_PAR_CloseOperation_Input] transformieren und transkodieren. [≤]

Disclaimer: Die Vorgaben zur Transformierung und Transkodierung von Dispensierdokumenten (eHDSI eDispensation CDA-Pivotformat) in das FHIR-Profil [GEM_ERPEU_PR_PAR_CloseOperation_Input] und der Fehlerverwaltung werden vom BfArM erarbeitet.

A_27231 - NCPeH - XDR eD-A - Integration von Transformierungs- und Transkodierungsregeln und Einhaltung der Regelung zur Unterstützung von mehreren FHIR-Package Versionen

Für eine erfolgreiche Transformierung und Transkodierung von Dispensierdokumenten MUSS der NCPeH-FD sicherstellen, dass er die aktuellen, vom BfArM bereitgestellten Transformierungs- und Transkodierungsregeln und Daten bei sich integriert hat und die Regelungen aus [4.2.10.7- Regelung zur Unterstützung von mehreren FHIR-Package Versionen] einhält. [≤]

A_27232 - NCPeH - XDR eD-A - Zwischenspeicherung transformierter und transkodierter Dispensierdokumente

Der NCPeH-FD MUSS die erfolgreich transformierten und transkodierten Dispensierdokumente, die dem FHIR-Profil nach [GEM_ERPEU_PR_PAR_CloseOperation_Input] entsprechen, in einer Variable `list_transcoded_fhir_medication_dispensations` zwischenspeichern. [≤]

A_27233 - NCPeH - XDR eD-A - Fehler- und Warnungsbehandlung bei Transformierung und Transkodierung von Dispensierdokumenten

Der NCPeH-FD MUSS bei Fehlern und Warnungen während der Transformierung und Transkodierung diese nach Vorgaben aus [ebRIM_Representation_Document#4.2.4] im dort beschriebenen Format erfassen. Die Fehler und Warnungen MÜSSEN gemäß den Vorgaben des BfArM für die Attribute `errorCode`, `codeContext`, `severity` und `location` erstellt und in der Liste `list_registry_error_xdr_request` (siehe [6.1.5.2- TUC_NCPeH_032: Cross-Enterprise Document Reliable Interchange Request für eD-A verarbeiten]) zwischengespeichert werden. Dabei MÜSSEN die Angaben zu `errorCode` den eHDSI Error Codes gemäß Vorgaben aus [eHDSI_NCPeH_Components#6.4] entsprechen, der `codeContext` MUSS mit menschlich verständlichen Meldungen in

englischer Sprache erstellt werden, und für das Attribut `location` SOLL der NCPeH-FD technische Hinweise auf die Fehlerursache geben, wobei technische Informationen KEINE Inhalte angeben DÜRFEN, die Rückschlüsse auf Implementierungsdetails, eingesetzte Frameworks oder Tools zulassen. [≤]

A_27234 - NCPeH - XDR eD-A - Verknüpfung von Dispensierdokumenten mit TRC Assertion

Der NCPeH-FD MUSS bei der Zwischenspeicherung von Einträgen sicherstellen, dass die Liste `list_registry_error_xdr_request` im Rahmen der weiteren Datenverarbeitung eindeutig mit der TRC Assertion aus dem entsprechenden IHE XDR-Request verknüpft wird, und er DARF diese Liste NICHT mit einer anderen TRC Assertion in Verbindung bringen. [≤]

A_27235 - NCPeH - XDR eD-A - Erstellung und Speicherung des Audit Trail Eintrags nach Transformierung und Transkodierung von Dispensierdokumenten

Der NCPeH-FD MUSS nach erfolgreicher Transformierung und Transkodierung jedes Dispensierdokumentes einen Audit Trail Eintrag gemäß den Vorgaben aus [\[4.1.7.4- Translation Audit Trail Eintrag erstellen\]](#) erstellen und diesen in der Komponente Audit Repository speichern. [≤]

Ausgabeparameter des TUC

- `list_transcoded_fhir_medication_dispensations,`
- `list_registry_error_xdr_request.`

6.2 Telematikinfrastruktur

6.2.1 TUC_NCPeH_013: Metadatenattribute des ePKA MIO abrufen

Für diesen TUC gelten folgende übergreifende Festlegungen

- [\[4.2.1- Schnittstellen zu Diensten der zentralen TI\]](#)
- [\[4.2.7.1- TLS-Verbindungsaufbau zum ePA-Aktensystem\]](#)
- [\[4.2.7.2- Interne Aktenkontosession für einen Versicherten\]](#)
- [\[4.2.7.3- Lokalisierung der Akte eines Versicherten\]](#)
- [\[4.2.7.4- Aufbau eines VAU-Kanals zum ePA-Aktensystem\]](#)
- [\[4.2.7.5- Nutzung eines etablierten VAU-Kanals zum ePA-Aktensystem\]](#)
- [\[4.2.7.7- Authentifizierung mit dem ePA Authorization Service\]](#)
- [\[4.2.7.8- Adressierung des Aktenkontos\]](#)
- [\[4.2.8- Befüllung von SOAP Header Elementen für Zugriff auf ePA XDS Document Service\]](#)
- [\[4.2.9- Elektronische Identitäten des NCPeH-FD\]](#)

Ablauf des TUC

Zur Ermittlung von demographischen Versichertendaten oder medizinischen Daten des Versicherten ist es notwendig, zuerst die UniqueID des FHIR-Bundles des ePKA MIOs vom XDS Document Service des in der Aktenkontosession zugeordneten ePA Aktensystems zu ermitteln (Metadaten).

Wenn der NCPeH-FD in einer existierenden Aktenkontosession für den Versicherten die Metadaten zu dem ePKA MIO zwischengespeichert hat, dann KANN der NCPeH-FD die

benötigten Metadaten aus dieser Session als Ausgabeparameter dieses TUCs wiederverwenden (Caching der Metadaten).

Wenn der NCPeH-FD keine Metadaten des ePKA MIO aus einer Aktenkontosession nutzen kann, dann MUSS der NCPeH-FD eine Suchanfrage an den XDS Document Service senden. Der NCPeH-FD MUSS dafür die Operation `I_Document_Management_Ncpeh::RegistryStoredQuery` gemäß [ITI-18] "Registry Stored Query", Query "FindDocument" nutzen. Zu weiterführenden Informationen siehe zusätzlich auch [gemSpec_Aktensystem_ePAfuerAlle#Registry Stored Query [ITI-18]].

Der NCPeH-FD agiert als "Document Consumer", während den XDS Document Service des ePA-Aktensystems eine "Document Registry" umsetzt (siehe Operation `I_Document_Management_Ncpeh::RegistryStoredQuery` gemäß [gemSpec_Aktensystem_ePAfueralle]).

Der NCPeH-FD MUSS im `RegistryStoredQuery-Request` die Parameter wie folgt befüllen:

- `returnType = LeafClass`
- `AdhocQuery id = (Stored Query Id für FindDocuments gemäß [ITI-18])`
- `$XDSDocumentEntryPatientId = (MUSS den Identifier des Versicherten gemäß der Bildungsregel in [gemSpec_Aktensystem_ePAfueralle#A_14974-*] enthalten)`
- `$XDSDocumentEntryFormatCode = (MUSS den Wert des Konfigurationsparameters ePKA_MIO_FORMATCODE gemäß [4.1.1- Konfigurationsparameter] enthalten)`
- `$XDSDocumentEntryStatus = urn:oasis:names:tc:ebxml-regrep:StatusType:Approved`

Der NCPeH-FD DARF in dem `RegistryStoredQuery-Request` NICHT das Attribut `home` benutzen (keine Angabe einer `homeCommunityId` für das ePA Aktensystem).

Beim Einstellen des ePKA MIO in dem XDS Document Service durch einen LE kann die bestehende Version durch eine neue Version des ePKA MIO ersetzt werden. Der XDS Document Service setzt intern den Status `availabilityStatus` (Metadatenattribut) für ältere Dokumente auf `Deprecated` und für das aktuelle Dokument auf den Wert `Approved`.

Durch Setzen des Parameters `returnType` auf `LeafClass` in der Anfrage soll die Liste der Suchergebnisse auf Dokumente beschränkt werden. Die Metaattribute von z.B. Verzeichnissen sollten nicht in die Liste der Suchergebnisse aufgenommen werden.

Der NCPeH-FD MUSS in die Operation `RegistryStoredQuery` den SOAP-Header nach [4.2.8- Befüllung von SOAP Header Elementen für Zugriff auf ePA XDS Document Service] mit aufnehmen.

Nach Versand der Anfrage an das ePA-Aktensystem MUSS der NCPeH-FD einen Non-Repudiation of Origin Eintrag gemäß [[4.1.7.1 Non-Repudiation of Origin erstellen](#)] in der Komponente Audit Repository speichern.

Nach Erhalt der Antwort von dem ePA-Aktensystem MUSS der NCPeH-FD einen Non-Repudiation of Receipt Eintrag gemäß [[4.1.7.2- Non-Repudiation of Receipt erstellen](#)] in der Komponente Audit Repository speichern.

Auf die gestellte Anfrage antwortet der ePA XDS Document Service mit passenden Suchergebnissen (Metadatenattribute).

Der Wert des Parameters `DocumentEntry.formatCode` aus der Antwort MUSS identisch mit dem Wert des Konfigurationsparameter `ePKA_MIO_FORMATCODE` (siehe [[4.1.1- Konfigurationsparameter](#)]) sein.

Der NCPeH-FD MUSS aus der Antwort folgende `DocumentEntry` Metadatenattribute gemäß [IHE_ITI_TF_Vol3#4.2.3.2] extrahieren, die im Zusammenhang mit dem ePKA MIO stehen und für Zwecke der internen Datenverarbeitung verwenden:

Tabelle 68: TAB_NCPeH_Relevante_Metadatenattribute_ePKA MIO

Variable für Zwecke der internen Datenverarbeitung	Metadatenattribut aus der erhaltenen Antwort gemäß [IHE_ITI_TF_Vol3#4.2.3.2]
METADATA_ePKA_MIO_creationTime	DocumentEntry.creationTime DARF NICHT leer sein.
METADATA_ePKA_MIO_repositoryUniqueId	DocumentEntry.repositoryUniqueId DARF NICHT leer sein.
METADATA_ePKA_MIO_uniqueId	DocumentEntry.uniqueId DARF NICHT leer sein.
METADATA_ePKA_MIO_patientId	MUSS den Wert der zehnstelligen KVNR enthalten, der aus DocumentEntry.patientId extrahiert werden MUSS. Der Wert MUSS identisch mit der KVNR der für die Operation genutzten internen Aktenkontosession sein.

Falls dieser TUC im Kontext des Anwendungsfalls [[NCPeH.UC_1 - Versicherten im Behandlungsland für PS-A identifizieren](#)] aufgerufen wird, MUSS der NCPeH-FD folgende Prüfschritte durchführen. Bei nicht erfolgreicher Ausführung der Prüfschritte MUSS der NCPeH-FD eine weitere Verarbeitung der Anfrage abbrechen und dem NCPeH Land-B mit der Fehlernachricht bzw. Reason Encoding inkl. acknowledgementDetail antworten:

Tabelle 69: TAB_NCPeH_Abruf_ePKA_Metadaten_Fehlerbehandlung_Zusammenhang_XCPD

Prüfschritte	Reason Encoding gemäß [eHDSI_XCPD_Profile#2.3.3]	acknowledgementDetail
Die Antwort des ePA XDS Document Service enthält einen der folgenden Fehlercodes: StatusMismatch oder NoHealthRecord (siehe IgemSpec_Aktensystem_ePAfueralle#A_26324-01) und IgemSpec_Aktensystem_ePAfueralle#A_26325-01).	<pre><mitigatedBy typeCode="MITGT"> <detectedIssueManagement classCode="ACT" moodCode="ENV"> <code code="AnswerNotAvailable" codeSystem="1.3.6.1.4.1.1937 6.1.2.27.3"/> </detectedIssueManagement> </mitigatedBy></pre>	<pre>acknowledgement.typeCode= AA queryAck.queryResponseCode= AE acknowledgementDetail.Code= ERROR_PI_NO_MATCH acknowledgementDetail.Text = Patient Identification Error acknowledgementDetail.Location = It was not possible to localise the patient's health record in the national health record</pre>

<p>Die Antwort des ePA XDS Document Service enthält keine Metadatenattribute des geforderten ePKA MIO.</p>		<p>system. acknowledgement.typeCode= AA queryAck.queryResponseCode= AE acknowledgementDetail.Code= ERROR_PI_NO_MATCH acknowledgementDetail.Text = Patient Identification Error acknowledgementDetail.Location = No match with an existing patient.</p>
<p>Die Prüfkriterien aus der Tabelle TAB_NCPeH_Relevante_Metadatenattribute_ePKA MIO sind nicht erfüllt.</p>		
<p>Die Kommunikation mit dem ePA XDS Document Service ergibt einen HTTP Statuscode 400 (siehe IgemSpec_Aktensystem_ePAfueralle#3.13.1.2).</p>	<pre><mitigatedBy typeCode="MITGT"> <detectedIssueManagement classCode="ACT" moodCode="ENV"> <code code="InternalError" codeSystem="1.3.6.1.4.1.19 376.1.2.27.3"/> </detectedIssueManagement> </mitigatedBy></pre>	<p>acknowledgement.typeCode= AA queryAck.queryResponseCode= AE acknowledgementDetail.Code= ERROR_PI_GENERIC acknowledgementDetail.Text = Patient Identification Error acknowledgementDetail.Location = Patient data could not be found due to an internal error.</p>
<p>Die Antwort enthält Metadatenattribute über andere Datensätze, die nicht ePKA MIO sind.</p>		
<p>Die Antwort des ePA XDS Document Service enthält den Fehlercode InvalAuth (siehe IgemSpec_Aktensystem_ePAfueralle#A_26459).</p>		
<p>Die Antwort des ePA XDS Document Service enthält den Fehlercode NotEntitled (siehe IgemSpec_Aktensystem_ePAfueralle#A_25683-01).</p>	<pre><mitigatedBy typeCode="MITGT"> <detectedIssueManagement classCode="ACT" moodCode="ENV"> <code code="InsufficientRights" codeSystem="1.3.6.1.4.1.12 559.11.10.1.3.2.2.1"/> </detectedIssueManagement> </mitigatedBy></pre>	<p>acknowledgement.typeCode= AA queryAck.queryResponseCode= AE acknowledgementDetail.Code= ERROR_PI_GENERIC acknowledgementDetail.Text = Patient Identification Error acknowledgementDetail.Location = The requestor has insufficient rights to query for patient's identity data. Please ask the patient for access rights.</p>

Hinweis: Weitere Fehlerbehandlungen werden in den für diesen TUC relevanten übergreifenden Festlegungen beschrieben.

Folgende Anforderung gilt bei der Nutzung dieses TUC durch die Anwendungsfälle wie [[NCPeH_UC_2 - Metadaten über ePKA MIO auflisten](#)]:

Der NCPeH-FD MUSS beim Auftreten eines Fehlerfalls gemäß Tabelle TAB_NCPeH_ePA_XDS_Fehlerfälle_eHDSI_XCA-Retrieve eine weitere Verarbeitung der Anfrage abbrechen und dem NCPeH Land-B mit einem Fehlercode gemäß Tabelle TAB_NCPeH_Abruf_ePKA_Metadaten_Fehlerbehandlung_Zusammenhang_XCA antworten.

Tabelle 70: TAB_NCPeH_Abruf_ePKA_Metadaten_Fehlerbehandlung_Zusammenhang_XCA

Fehlerfall	Fehlercode gemäß [eHDSI_NCPeH_Components# 6.4]
Die Antwort des ePA XDS Document Service enthält einen der folgenden Fehlercodes: StatusMismatch oder NoHealthRecord. (siehe IgemSpec_Aktensystem_ePAfueralle#A_263_24-01] und IgemSpec_Aktensystem_ePAfueralle#A_263_25-01).	ERROR_PS_GENERIC
Die Antwort des ePA XDS Document Service enthält keine Metadatenattribute des geforderten ePKA MIO.	ERROR_GENERIC_DOCUMENT_MISSING
Die Prüfkriterien aus der Tabelle TAB_NCPeH_Relevante_Metadatenattribute_ePKA MIO sind nicht erfüllt.	
Die Kommunikation mit dem ePA XDS Document Service ergibt einen HTTP Statuscode 400 (siehe IgemSpec_Aktensystem_ePAfueralle#3.13.1_2).	ERROR_INTERNAL_ERROR
Die Antwort enthält Metadatenattribute über andere Datensätze, die nicht ePKA MIO sind.	ERROR_GENERIC_DOCUMENT_MISSING
Die Antwort des ePA XDS Document Service enthält den Fehlercode InvalAuth. (siehe IgemSpec_Aktensystem_ePAfueralle#A_264_59).	ERROR_INTERNAL_ERROR
Die Antwort des ePA XDS Document Service enthält den Fehlercode NotEntitled (siehe IgemSpec_Aktensystem_ePAfueralle#A_256_83-01).	ERROR_NO_CONSENT

Wenn der NCPeH-FD gültige Metadaten zum ePKA MIO des Versicherten gefunden hat, dann KANN er diese Daten in der internen Aktenkontosession des Versicherten und LE-EU zwischenspeichern.

Ausgabeparameter des TUC

Nach erfolgreicher Ausführung dieses TUC stehen im NCPeH-FD folgende Ausgabeparameter für die weitere Datenverarbeitung zur Verfügung:

- METADATA_ePKA_MIO_creationTime
- METADATA_ePKA_MIO_repositoryUniqueId
- METADATA_ePKA_MIO_uniquelId
- METADATA_ePKA_MIO_patientId

6.2.2 TUC_NCPeH_014: FHIR-Bundle ePKA MIO abrufen

Für diesen TUC gelten folgende übergreifende Festlegungen

- [4.1.7- Non-Repudiation und Audit Trail Schemas]
- [4.2.1- Schnittstellen zu Diensten der zentralen TI]
- [4.2.7.1- TLS-Verbindungsaufbau zum ePA-Aktensystem]
- [4.2.7.2- Interne Aktenkontosession für einen Versicherten]
- [4.2.7.3- Lokalisierung der Akte eines Versicherten]
- [4.2.7.4- Aufbau eines VAU-Kanals zum ePA-Aktensystem]
- [4.2.7.5- Nutzung eines etablierten VAU-Kanals zum ePA-Aktensystem]
- [4.2.7.7- Authentifizierung mit dem ePA Authorization Service]
- [4.2.7.8- Adressierung des Aktenkontos]
- [4.2.8- Befüllung von SOAP Header Elementen für Zugriff auf ePA XDS Document Service]
- [4.2.9- Elektronische Identitäten des NCPeH-FD]

Ablauf des TUC

Um die relevanten Daten (demographische oder medizinische Versichertendaten - abhängig vom jeweiligen Anwendungsfall) aus dem ePKA MIO des Versicherten abrufen zu können, MUSS der NCPeH-FD eine Anfrage an den ePA XDS Document Service über die Operation `I_Document_Management_Ncpeh::RetrieveDocumentSet` (siehe [gemSpec_Aktensystem_ePAfuerAlle#RetrieveDocumentSet [ITI-43]]) gemäß [ITI-43] "Retrieve Document Set" senden. Dabei agiert der NCPeH-FD als IHE-XCA-Akteur „Document Consumer“, während den ePA XDS Document Service eine "Document Repository" umsetzt.

Der NCPeH-FD MUSS mit der Anfrage folgende Parameter senden:

- `DocumentEntry.uniqueId` muss den Wert aus der Variable `METADATA_ePKA_MIO_uniquelId` (siehe [6.2.1- TUC_NCPeH_013: Metadatenattribute des ePKA MIO abrufen]) enthalten
- `DocumentEntry.repositoryUniqueId` muss den Wert aus der Variable `METADATA_ePKA_MIO_repositoryUniqueId` (siehe [6.2.1- TUC_NCPeH_013: Metadatenattribute des ePKA MIO abrufen]) enthalten.

Der NCPeH-FD MUSS in die Anfrage zur Operation RetrieveDocumentSet den SOAP-Header nach [4.2.8- Befüllung von SOAP Header Elementen für Zugriff auf ePA XDS Document Service] mit aufnehmen.

Nach Versand der Anfrage an den ePA XDS Document Service MUSS der NCPeH-FD einen Non-Repudiation of Origin Eintrag gemäß [4.1.7.1 Non-Repudiation of Origin erstellen] in die Komponente Audit Repository speichern.

Nach Erhalt der Antwort von dem ePA XDS Document Service MUSS der NCPeH-FD einen Non-Repudiation of Receipt Eintrag gemäß [4.1.7.2- Non-Repudiation of Receipt erstellen] in die Komponente Audit Repository speichern.

Falls die Antwort mittels MTOM/XOP [MTOM] kodiert ist (siehe [gemSpec_Aktensystem_ePAfuerAlle#A_17832]), MUSS der NCPeH-FD die Nachricht gemäß Vorgaben aus [MTOM] mit Verweis auf [IHE-ITI-TF2x#v3.6] dekodieren können, so dass die weitere interne Verarbeitung der Nachricht möglich ist.

Die vom ePA XDS Document Service erhaltene Antwort auf die gestellte Anfrage MUSS genau ein FHIR-Bundle ePKA MIO des Versicherten im Klartext enthalten. Das zu verwendete Format des FHIR-Bundle ePKA MIO ist durch [KBV_ePKA_MIO_Format] vorgegeben. Die Spezifikation des ePKA MIO v1.0.0 ist von der mio42 GmbH auf den Webseiten der KBV unter [Simplifier_ePKA_MIO] veröffentlicht. Die Version v1.0.0 des ePKA MIO ist für die interne Datenverarbeitung im NCPeH-FD normativ.

Der NCPeH-FD MUSS die innerhalb des FHIR-Bundles ePKA MIO mindestens die enthaltene Komposition

KBV_PR_MIO_NFD_Composition_NFD einer FHIR-Validierung gegen die ePKA MIO Schema-Definition der KBV [Simplifier_ePKA_MIO] unterziehen, damit der nachfolgende Workflow ausschließlich auf Basis von schemakonformer Daten erfolgt. Die KBV stellt zum ePKA MIO in [Simplifier_ePKA_MIO_Validierungspakete] relevante Dateien bzw. Validierungspakete zur Verfügung, die zur Implementierung des ePKA MIO und der FHIR-Validierung benötigt werden. Die FHIR-Validierung des ePKA MIO MUSS lokal innerhalb der VAU-Umgebung im NCPeH-FD erfolgen. Der NCPeH-FD DARF NICHT das ePKA MIO an externe Dienste zur FHIR-Validierung senden. Bei Invalidität MUSS der NCPeH-FD die weitere Verarbeitung und Nutzung von Daten aus dem ePKA MIO abbrechen und dem NCPeH-FD mit einer entsprechenden Fehlernachricht gemäß Tabelle TAB_NCPeH_Abruf_ePKA MIO_Fehlerbehandlung_Zusammenhang_PI oder TAB_NCPeH_Abruf_ePKA MIO_Fehlerbehandlung_Zusammenhang_PS antworten.

Wenn dieser TUC im Kontext des Anwendungsfalls [NCPeH.UC_1 - Versicherten im Behandlungsland für PS-A identifizieren] aufgerufen wird, MUSS der NCPeH-FD, in Abhängigkeiten von der aufgetretenen Fehlerbedingung aus Tabelle "TAB_NCPeH_Abruf_ePKA MIO_Fehlerbehandlung_Zusammenhang_XCPD", eine weitere Verarbeitung der Anfrage abbrechen und mit der entsprechenden Fehlernachricht bzw. Reason Encoding inkl. acknowledgementDetail dem NCPeH Land-B gemäß [eHDSI_XCPD_Profile#2.3.3] antworten.

Tabelle 71: TAB_NCPeH_Abruf_ePKA MIO_Fehlerbehandlung_Zusammenhang_XCPD

Fehlerbedingung	Reason Encoding gemäß [eHDSI_XCPD_Profile#2.3.3]	acknowledgementDetail
Die Antwort des ePA XDS Document Service enthält einen der folgenden Fehlercodes:	<pre><mitigatedBy typeCode="MITGT"> <detectedIssueManagement classCode="ACT" moodCode="ENV"> <code</pre>	acknowledgement.typeCode= AA queryAck.queryResponseC

<p><i>StatusMismatch</i> oder <i>NoHealthRecord</i> (siehe IgemSpec_Aktensystem_ePAfueralle#A_26324-01) und IgemSpec_Aktensystem_ePAfueralle#A_26325-01).</p>	<pre>code="AnswerNotAvailable" codeSystem="1.3.6.1.4.1.19376.1 .2.27.3"/> </detectedIssueManagement> </mitigatedBy></pre>	<pre>ode= AE acknowledgementDetail.Co de= ERROR_PI_NO_MATCH acknowledgementDetail.Te xt = Patient Identification Error acknowledgementDetail.Lo cation = It was not possible to localise the patient's health record in the national health record system.</pre>
<p>Die Antwort vom ePA XDS Document Service enthält kein FHIR-Bundle ePKA MIO gemäß [KBV_ePKA_MIO_Format]</p>		<pre>acknowledgementDetail.Co de= ERROR_PI_GENERIC acknowledgementDetail.Te xt = Patient Identification Error acknowledgementDetail.Lo cation = Patient identity information is not available or accessible for European Member States. Please ask the patient for access authorisation.</pre>
<p>Das FHIR-Bundle ePKA MIO entspricht nicht der Version 1.0.0.</p>		<pre>acknowledgementDetail.Co de= ERROR_PI_GENERIC acknowledgementDetail.Te xt = Patient Identification Error acknowledgementDetail.Lo cation = The patient identity information in Germany has unknown version.</pre>
<p>Die FHIR-Validierung des ePKA MIO ist nicht erfolgreich</p>		<pre>acknowledgementDetail.Co de= ERROR_PI_GENERIC acknowledgementDetail.Te xt = Patient Identification Error acknowledgementDetail.Lo cation = The patient identity information in Germany is defective or missing and cannot be provided.</pre>
<p>Die Antwort des ePA XDS Document Service enthält den</p>	<pre><mitigatedBy typeCode="MITGT"></pre>	<pre>acknowledgement.typeCod e= AA</pre>

Fehlercode InvalAuth (siehe [gemSpec_Aktensystem_ePAfueralle#A_26459]).	<pre><detectedIssueManagement classCode="ACT" moodCode="ENV"> <code code="InternalError" codeSystem="1.3.6.1.4.1.19 376.1.2.27.3"/> </detectedIssueManagement> </mitigatedBy></pre>	queryAck.queryResponseCode= AE acknowledgementDetail.Code= ERROR_PI_GENERIC acknowledgementDetail.Text = Patient Identification Error acknowledgementDetail.Location = Patient data could not be found due to an internal error.
Die Antwort des ePA XDS Document Service enthält den Fehlercode NotEntitled (siehe [gemSpec_Aktensystem_ePAfueralle#A_25683-01]).	<pre><mitigatedBy typeCode="MITGT"> <detectedIssueManagement classCode="ACT" moodCode="ENV"> <code code="InsufficientRights" codeSystem="1.3.6.1.4.1.12 559.11.10.1.3.2.2.1"/> </detectedIssueManagement> </mitigatedBy></pre>	acknowledgement.typeCode= AA queryAck.queryResponseCode= AE acknowledgementDetail.Code= ERROR_PI_GENERIC acknowledgementDetail.Text = Patient Identification Error acknowledgementDetail.Location = The requestor has insufficient rights to query for patient's identity data. Please ask the patient for access rights.

Hinweis: Weitere Fehlerbehandlungen werden in den für diesen TUC relevanten übergreifenden Festlegungen beschrieben.

Folgende Anforderung gilt bei der Nutzung dieses TUC durch die Anwendungsfälle wie [\[5.1.3- NCPeH.UC_3 - ePKA MIO des Versicherten abrufen\]](#) oder [\[5.1.4- NCPeH.UC_4 - ePKA MIO des Versicherten als PDF/A abrufen\]](#):

Bei folgenden Fehlerbedingungen MUSS der NCPeH-FD eine weitere Verarbeitung der Anfrage abbrechen und dem NCPeH Land-B mit einer Fehlernachricht gemäß [\[eHDSI_XCA_Profile#2.4\]](#) und Tabelle "TAB_NCPeH_Abruf_ePKA_MIO_Fehlerbehandlung_Zusammenhang_PS" antworten:

Tabelle 72: TAB_NCPeH_Abruf_ePKA MIO_Fehlerbehandlung_Zusammenhang_PS

Fehlerbedingung	Fehlercode gemäß [eHDSI_NCPeH_Components#6.4]
Die Antwort des ePA XDS Document Service enthält einen der folgenden Fehlercodes: StatusMismatch oder NoHealthRecord (siehe [gemSpec_Aktensystem_ePAfueralle#A_26324-01] und [gemSpec_Aktensystem_ePAfueralle#A_26325-01]).	RROR_PS_GENERIC

Die Antwort des ePA XDS Document Service enthält den Fehlercode InvalAuth (siehe [gemSpec_Aktensystem_ePAfueralle#A_26459])	ERROR_INTERNAL_ERROR
Die Antwort des ePA XDS Document Service enthält den Fehlercode NotEntitled (siehe [gemSpec_Aktensystem_ePAfueralle#A_25683-01]).	ERROR_NO_CONSENT
Die Antwort vom ePA XDS Document Service enthält kein FHIR-Bundle ePKA MIO	ERROR_GENERIC_DOCUMENT_MISSING
Das FHIR-Bundle ePKA MIO entspricht nicht der Version 1.0.0.	
Die FHIR-Validierung des ePKA MIO ist nicht erfolgreich	
Dem FHIR-Bundle ePKA MIO fehlen wesentliche Teile	ERROR_PS_MISSING_BASIC_SECTIONS

Ausgabeparameter des TUC

- Bei Erfolg: FHIR-Bundle ePKA MIO

6.2.3 TUC_NCPeH_017: Demographische Versichertendaten aus NFD des ePKA MIO übernehmen

Für diesen TUC gelten folgende übergreifende Festlegungen

- keine

Ablauf des TUC

Die Struktur der demographischen Versichertendaten im FHIR-Bundle ePKA MIO ist in der Komposition KBV_PR_MIO_NFD_Composition_NFD durch das Profil [Simplifier_ePKA_MIO_NFD_Patient] definiert. Der NCPeH-FD DARF NICHT die DPE-Daten aus ePKA MIO (siehe Komposition KBV_PR_MIO_DPE_Composition_DPE) verarbeiten und daraus die demographischen Versichertendaten beziehen. Der NCPeH-FD MUSS folgende demographische Versichertendaten aus dem genannten Profil extrahieren und in die entsprechende Variablen abspeichern:

Variable für Zwecke der internen Datenverarbeitung	Element aus KBV_PR_MIO_NFD_Composition_NFD des ePKA MIO (gemäß [Simplifier_ePKA_MIO_NFD_Patient])
patient_kvnr	Patient.identifizier
patient_vorname	Patient.name:name.given
patient_nachname	Patient.name:name.family.extension:nachname

patient_vorsatzwort	Patient.name:name.family.extension:vorsatzwort
patient_namenszusatz	Patient.name:name.family.extension:namenszusatz
patient_geburtsdatum	Patient.birthDate

Das FHIR-Profil Patient im ePKA MIO [Simplifier_ePKA_MIO_NFD_Patient] lässt ein Fehlen des Geburtsdatums zu, wenn stattdessen die Extension "data-absent-reason" angegeben ist.

In diesem Fall MUSS der NCPeH-FD eine Fehlernachricht gemäß Tabelle TAB_NCPeH_Fehlen_Geburtstag_Fehler_XCPD_Response erstellen und an den NCPeH Land-B versenden.

Tabelle 73: TAB_NCPeH_Fehlen_Geburtstag_Fehler_XCPD_Response

Reason Encoding gemäß [eHDSI_XCPD_Profile#2.3.3]	acknowledgementDetail
<pre><mitigatedBy typeCode="MITGT"> <detectedIssueManagement classCode="ACT" moodCode="ENV"> <code code="AnswerNotAvailable" codeSystem="1.3.6.1.4.1.19376.1.2.27.3"/ > </detectedIssueManagement> </mitigatedBy></pre>	<pre>acknowledgement.typeCode= AA queryAck.queryResponseCode= AE acknowledgementDetail.Code= ERROR_PI_GENERIC acknowledgementDetail.Text = Patient Identification Error acknowledgementDetail.Location = The patient's health record data is not complete, the date of birth is missing.</pre>

Ausgabeparameter des TUC

- patient_kvnr
- patient_vorname
- patient_nachname
- patient_vorsatzwort
- patient_namenszusatz
- patient_geburtsdatum

6.2.4 TUC_NCPeH_035: Demographische Versichertendaten aus E-Rezept extrahieren

Für diesen TUC gelten folgende übergreifende Festlegungen

- [[4.2.1 - Schnittstellen zu Diensten der zentralen TI](#)]
- [4.2.10- Übergreifende Vorgaben an die Kommunikation mit E-Rezept-FD]
- [[4.2.9 Elektronische Identitäten des NCPeH-FD](#)]
- [4.2.10.4- Authentifizierung des NCPeH-FD am E-Rezept-FD]

Ablauf des TUC

Mit diesem TUC ruft der NCPeH-FD ein FHIR-Bundle vom E-Rezept-FD ab, um daraus demographische Versichertendaten zum Zwecke der Patientenidentifikation im Land-B zu extrahieren.

Der NCPeH-FD MUSS im inneren Request die HTTP-Operation des E-Rezept-FD mit dem Ausdruck

POST/get-eu-prescriptions?_count=1 aufrufen und zusammen mit dem Request den HTTP-Header "Authorization" und die FHIR-Parameter gemäß Vorgaben aus [4.2.10.6- Erstellung des Payload für die Kommunikation mit dem E-Rezept-FD] an die HTTP-Operation übermitteln. Der Aufruf dient dazu, das zuletzt erstellte und einlösbare E-Rezept abzurufen, damit der NCPeH-FD relevante demographische Versichertendaten extrahieren kann. Für weitere Informationen über die Definition der Schnittstellenoperation /get-eu-prescriptions siehe [gemSpec_FD_eRp#Http-Operation POST get-eu-prescriptions] und [API_EU_E-Rezepte "Abfragen von E-Rezepten des E-Rezept-Fachdienst"].

Nach Versand der Anfrage an den E-Rezept-FD MUSS der NCPeH-FD einen Non-Repudiation of Origin Eintrag gemäß [4.1.7.1 - Non-Repudiation of Origin erstellen] in die Komponente Audit Repository speichern.

Nach Erhalt der Antwort vom E-Rezept-FD MUSS der NCPeH-FD einen Non-Repudiation of Receipt Eintrag gemäß [4.1.7.2 - Non-Repudiation of Receipt erstellen] in die Komponente Audit Repository speichern.

Bei einer Antwort des E-Rezept-FD mit dem HTTP-Statuscode 401 MUSS der NCPeH-FD für das NCPeH Land-B ein neues ACCESS_TOKEN unter Verwendung der TI-Identität gemäß den Vorgaben in [4.2.10.4- Authentifizierung des NCPeH-FD am E-Rezept-FD] anfordern. Der NCPeH-FD MUSS die oben erwähnten Vorgaben zum Operationsaufruf erneut mit dem neuen ACCESS_TOKEN und den Vorgaben aus [4.2.10.6- Erstellung des Payload für die Kommunikation mit dem E-Rezept-FD] umsetzen.

Wenn der E-Rezept-FD mit dem HTTP Status Code 200 antwortet, ist in der Antwortnachricht ein FHIR-Bundle enthalten. Der NCPeH-FD MUSS validieren, ob das in der Antwortnachricht enthaltene FHIR-Bundle vom Typ collection ist und die Vorgaben aus [FHIR_Resource_Bundle] erfüllt.

Der NCPeH-FD MUSS aus dem FHIR-Bundle folgende FHIR-Ressource Bundle/entry/resource/Bundle/entry/resource/Patient ermitteln und prüfen, ob die ermittelte Patient-FHIR-Ressource die Vorgaben aus [KBV_PR_FOR_Patient] erfüllt.

Der NCPeH-FD MUSS demographische Versichertendaten aus der ermittelten Patient-FHIR-Ressource gemäß der Tabelle "TAB_NCPeH_Extrahierung_demographische_Versichertendaten_ePeD-A" extrahieren und diese in die entsprechenden Variablen für die spätere Datenverarbeitung abspeichern.

Tabelle 74 : TAB_NCPeH_Extrahierung_demographische_Versichertendaten_ePeD-A

Variable für Zwecke der internen Datenverarbeitung	Element gemäß [KBV_PR_FOR_Patient]
patient_kvnr	Patient.identifizier
patient_prefix	Patient.name:name.prefix
patient_vorname	Patient.name:name.given

patient_nachname	Patient.name:name.family.extension:nachname
patient_vorsatzwort	Patient.name:name.family.extension:vorsatzwort
patient_namenszusatz	Patient.name:name.family.extension:namenszusatz
patient_geburtsdatum	Patient.birthDate

Tritt einer der folgenden Fehlerfälle auf, MUSS der NCPeH-FD die weitere Verarbeitung der Anfrage abbrechen und dem NCPeH Land-B mit einer entsprechenden Fehlernachricht gemäß Tabelle "TAB_NCPeH_Fehlerfälle_Abruf_von_demographischen_Versichertendaten" antworten.

Tabelle 75 : TAB_NCPeH_Fehlerfälle_Abruf_von_demographischen_Versichertendaten

Fehlerfall	Reason Encoding (reasonOf-Element) gemäß [eHDSI_XCPD_Profile#2.3.3]	Acknowledgement
patient_kvnr, patient_vorname, patient_nachname oder patient_geburtsdatum sind im Ergebnis des TUC leer.	<pre><mitigatedBy typeCode="MITGT"> <detectedIssueManagement classCode="ACT" moodCode="ENV"> <code code="AnswerNotAvailable" codeSystem="1.3.6.1.4.1.1937 6.1.2.27.3"/> </detectedIssueManagement> </mitigatedBy></pre>	<pre>acknowledgement.typeCode= AA queryAck.queryResponseCode= NF acknowledgementDetail.Code= ER ROR_PI_NO_MATCH acknowledgementDetail.Text = Patient Identification Error acknowledgementDetail.Location = "No match with an existing patient."</pre>
Der E-Rezept-FD antwortet mit dem HTTP Status Code 404.	<pre></detectedIssueManagement> </mitigatedBy></pre>	
Der E-Rezept-FD antwortet mit dem HTTP Status Code 403.	<pre><mitigatedBy typeCode="MITGT"> <detectedIssueManagement classCode="ACT" moodCode="ENV"> <code code="InsufficientRights" codeSystem="1.3.6.1.4.1.1255 9.11.10.1.3.2.2.1"/> </detectedIssueManagement> </mitigatedBy></pre>	<pre>acknowledgement.typeCode= AA queryAck.queryResponseCode= AE acknowledgementDetail.Code= ER ROR_PI_GENERIC acknowledgementDetail.Text = Patient Identification Error acknowledgementDetail.Location = "The requestor has insufficient rights to query for patient's identity data. Please ask the patient for access authorisation."</pre>

<p>Der E-Rezept-FD antwortet mit dem HTTP Status Code 400.</p>	<pre><mitigatedBy typeCode="MITGT"> <detectedIssueManagement classCode="ACT" moodCode="ENV"> <code code="InternalError" codeSystem="1.3.6.1.4.1.1937 6.1.2.27.3"/> </detectedIssueManagement> </mitigatedBy></pre>	<pre>acknowledgement.typeCode= AE queryAck.queryResponseCode= AE acknowledgementDetail.Code= ER ROR_PI_INTERNAL_ERROR acknowledgementDetail.Text = Patient Identification Error acknowledgementDetail.Location = "No patient data available due to an internal error."</pre>
<p>Der E-Rezept-FD antwortet nach einem zweiten Operationsaufruf mit dem HTTP Status Code 401.</p>	<pre></detectedIssueManagement> </mitigatedBy></pre>	<pre>acknowledgement.typeCode= AE queryAck.queryResponseCode= AE acknowledgementDetail.Code= ER ROR_PI_INTERNAL_ERROR acknowledgementDetail.Text = Patient Identification Error acknowledgementDetail.Location = "No patient data available due to an internal error."</pre>
<p>Der E-Rezept-FD antwortet mit dem HTTP Status Code 408.</p>		<pre>acknowledgement.typeCode= AE queryAck.queryResponseCode= AE acknowledgementDetail.Code= ER ROR_PI_INTERNAL_ERROR acknowledgementDetail.Text = Patient Identification Error acknowledgementDetail.Location = "Internal error due to timeout. Please submit the request again."</pre>
<p>Der E-Rezept-FD antwortet mit dem HTTP Status Code 200, in der Antwortnachricht ist kein FHIR-Bundle vom Typ collection enthalten oder in der Antwort ist ein FHIR-Bundle enthalten, erfüllt aber nicht die Vorgaben aus [FHIR_Resource_Bundle].</p>		<pre>acknowledgement.typeCode= AE queryAck.queryResponseCode= AE acknowledgementDetail.Code= ER ROR_PI_INTERNAL_ERROR acknowledgementDetail.Text = Patient Identification Error acknowledgementDetail.Location = "No patient data available due to an internal error."</pre>
<p>Die ermittelte FHIR-Ressource Patient aus dem FHIR-Bundle entspricht nicht den Vorgaben</p>		

aus [KBV_PR_FOR_Patient].		
Der E-Rezept-FD antwortet mit dem HTTP Status Code 500.		acknowledgement.typeCode= AE queryAck.queryResponseCode= AE acknowledgementDetail.Code= ERROR_PI_INTERNAL_ERROR acknowledgementDetail.Text = Patient Identification Error acknowledgementDetail.Location = "Internal error when querying the patient demographic data."
Der E-Rezept-FD antwortet nicht und der hinterlegte Wert im Konfigurationsparameter eRp_RESPONSE_TIMEOUT (siehe [4.1.1 Konfigurationsparameter]) ist überschritten		

Ausgabeparameter des TUC

- patient_kvnr
- patient_prefix
- patient_vorname
- patient_nachname
- patient_vorsatzwort
- patient_namenszusatz
- patient_geburtsdatum

6.2.5 TUC_NCPeH_036: Liste der einlösbaren E-Rezepte des Versicherten aus dem E-Rezept-FD abrufen

Für diesen TUC gelten folgende übergreifende Festlegungen

- [[4.2.1 - Schnittstellen zu Diensten der zentralen TI](#)]
- [4.2.10- Übergreifende Vorgaben an die Kommunikation mit E-Rezept-FD]
- [4.2.10.4- Authentifizierung des NCPeH-FD am E-Rezept-FD]
- [4.2.10.7- Regelung zur Unterstützung von mehreren FHIR-Package Versionen]
- [[4.2.9 - Elektronische Identitäten des NCPeH-FD](#)]

Ablauf des TUC

Mit diesem TUC ruft der NCPeH-FD alle im EU-Ausland einlösbaren E-Rezepte des Versicherten vom E-Rezept-FD ab und erhält ein FHIR-Bundle.

Der NCPeH-FD MUSS im inneren Request die HTTP-Operation des E-Rezept-FD mit dem Ausdruck POST/get-eu-prescriptions aufrufen und zusammen mit dem Request den

HTTP-Header "Authorization" und die FHIR-Parameter gemäß Vorgaben aus [4.2.10.6- Erstellung des Payload für die Kommunikation mit dem E-Rezept-FD] an die HTTP-Operation übermitteln. Der HTTP Parameter_count DARF NICHT im Operationsaufruf angegeben werden.

Für weitere Informationen über die Definition der Schnittstellenoperation /get-eu-prescriptions siehe [gemSpec_FD_eRp#Http-Operation POST get-eu-prescriptions] und [API_EU_E-Rezepte#"Abfragen von E-Rezepten des E-Rezept-Fachdienst"].

Nach Versand der Anfrage an den E-Rezept-FD MUSS der NCPeH-FD einen Non-Repudiation of Origin Eintrag gemäß [4.1.7.1 - Non-Repudiation of Origin erstellen] in der Komponente Audit Repository speichern.

Nach Erhalt der Antwort vom E-Rezept-FD MUSS der NCPeH-FD einen Non-Repudiation of Receipt Eintrag gemäß [4.1.7.2 - Non-Repudiation of Receipt erstellen] in der Komponente Audit Repository speichern.

Bei einer Antwort des E-Rezept-FD mit dem HTTP Status Code 401 MUSS der NCPeH-FD für das NCPeH Land-B ein neues ACCESS_TOKEN unter Verwendung der TI-Identität gemäß den Vorgaben in [4.2.10.4- Authentifizierung des NCPeH-FD am E-Rezept-FD] anfordern. Der NCPeH-FD MUSS die oben erwähnte Vorgaben zum Operationsaufruf erneut mit dem neuen ACCESS_TOKEN und den Vorgaben aus [4.2.10.6- Erstellung des Payload für die Kommunikation mit dem E-Rezept-FD] umsetzen.

Wenn der E-Rezept-FD mit dem HTTP Status Code 200 antwortet, ist in der Antwortnachricht ein FHIR-Bundle enthalten. Der NCPeH-FD MUSS validieren, ob das in der Antwortnachricht enthaltene FHIR-Bundle vom Typ collection ist und die Vorgaben aus [FHIR_Resource_Bundle] erfüllt.

Das FHIR-Bundle (im weiteren Verlauf des Dokuments als "äußeres Bundle" bezeichnet) enthält mindestens ein entry-Element. Jedes entry-Element enthält wiederum ein FHIR-Bundle resource/Bundle (im weiteren Verlauf des Dokuments als "inneres Bundle" bezeichnet). Der NCPeH-FD MUSS das innere Bundle in allen entry-Elementen auf Schemakonformität gemäß Vorgaben aus [KBV_PR_ERP_Bundle] prüfen. Jedes innere Bundle kapselt Angaben zu genau einem E-Rezept.

Der NCPeH-FD MUSS für die nicht schemakonformen inneren Bundles in der Antwortnachricht an den NCPeH Land-B jeweils ein AdhocQueryResponse/RegistryErrorList/RegistryError-Element mit Angaben zum Fehler gemäß Tabelle "TAB_NCPeH_Fehler_nicht_schemakonform_UC_Auflistung_von_einlösbaren_E-Rezepten" erstellen.

Tabelle 76: TAB_NCPeH_Fehler_nicht_schemakonform_UC_Auflistung_von_einlösbaren_E-Rezepten

errorCode gemäß [eHDSI_XCA_Profile#2.2.3] und [eHDSI_NCPeH_Components #6.4]	codeContext	severity	location
ERROR_INTERNAL_ERROR	"Could not process a patients prescription."	urn:oasis:names:tc:ebxml-regrep:ErrorSeverityType:Error	Keine Angaben

Der NCPeH-FD MUSS für die weitere Datenverarbeitung ausschließlich schemakonformen innere Bundles in einer Variable `fhir_erp_bundle_collection` zwischenspeichern. Die inneren Bundles, die nicht schemakonform sind, DÜRFEN NICHT in die Variable `fhir_erp_bundle_collection` zwischengespeichert werden. Bei der Zwischenspeicherung MUSS der NCPeH-FD sicherstellen, dass das `fhir_erp_bundle_collection` im Rahmen der weiteren Datenverarbeitung mit der TRC Assertion aus dem entsprechenden IHE XCA.Query-Request verknüpft ist. Der NCPeH-FD DARF das FHIR-Bundle NICHT mit einer anderen TRC Assertion in Verbindung bringen.

Tritt einer der folgenden Fehlerfälle auf, MUSS der NCPeH-FD die weitere Verarbeitung der Anfrage abbrechen, in der Antwortnachricht an den NCPeH Land-B ein `AdhocQueryResponse/RegistryErrorList/RegistryError-Element` erstellen und mit entsprechenden Angaben zum Fehler gemäß Tabelle "TAB_NCPeH_Allgemeine_Fehlerfälle_Auflistung_von_einlösbaeren_E-Rezepten" an den NCPeH Land-B antworten. Die Antwortnachricht MUSS nach Vorgaben aus [6.1.2.4- TUC_NCPeH_026: Cross Gateway Query Response für ePeD-A versenden] erstellt werden.

Tabelle 77: TAB_NCPeH_Allgemeine_Fehlerfälle_Auflistung_von_einlösbaeren_E-Rezepten

Fehlerfall	errorCode gemäß [eHDSI_XCA_Profile #2.2.3] und [eHDSI_NCPeH_Components#6.4]	codeCont ext	severity	location
E-Rezept-FD antwortet mit dem HTTP Status Code 200, aber die Antwortnachricht enthält kein FHIR-Bundle vom Typ "collection"	ERROR_INTERNAL_ERROR	"Internal error when querying the patient's ePrescriptions."	urn:oasis:names:tc:ebxml-regrep:ErrorSeverityType:Error	"The response from the ePrescription service does not contain a FHIR bundle of type collection."
E-Rezept-FD antwortet mit dem HTTP Status Code 400				"The ePrescription service did respond with HTTP status code 400."
E-Rezept-FD antwortet nach einem zweiten				"The ePrescription

Operationsaufruf mit dem HTTP Status Code 401				service did respond with HTTP status code 401."
E-Rezept-FD antwortet mit dem HTTP Status Code 403	ERROR_NO_CONSENT	"There is no valid access authorisation for the requesting country in the german ePrescription service. Please ask the patient for access authorisation."		"The ePrescription service did respond with HTTP status code 403."
E-Rezept-FD antwortet mit dem HTTP Status Code 404	WARNING_EP_GENERIC	"No ePrescription for the patient found, which is dispensable in EU-countries"	urn:oasis:names:tc:ebxml-regrep:ErrorSeverityType:Warning	"The ePrescription service did respond with HTTP status code 404."
E-Rezept-FD antwortet mit dem HTTP Status Code 408	ERROR_REGISTRY_NOT_AVAILABLE	"Timeout during communication with the german ePrescription service. Please submit the request again."	urn:oasis:names:tc:ebxml-regrep:ErrorSeverityType:Error	"The ePrescription service did respond with HTTP status code 408."

<p>E-Rezept-Fachdienst antwortet mit dem HTTP Status Code 500</p>	<p>ERROR_INTERNAL_ERROR</p>	<p>"The request could not be processed by the german ePrescription service."</p>	<p>"The ePrescription service did respond with HTTP status code 500."</p>
<p>Der E-Rezept-FD antwortet nicht und der hinterlegte Wert im Konfigurationsparameter eRp_RESPONSE_TIMEOUT (siehe [4.1.1 Konfigurationsparameter]) ist überschritten</p>			<p>"Timeout. ePrescription service is not responding."</p>

Der NCPeH-FD MUSS für AdhocQueryResponse@status in der Antwortnachricht einen entsprechenden Wert setzen, der anhand des Gesamtstatus aller RegistryResponse/RegistryErrorList/RegistryError@Severities-Attribute, erfolgreich verarbeiteter innerer Bundles und unter Berücksichtigung der Kriterien aus der Tabelle "Registry Stored Query [ITI-18] and Cross Gateway Query [ITI-38] Responses" in [ebRIM_Representation_Document#4.2.4.2] zu bestimmen ist.

Ausgabeparameter des TUC

- fhir_erp_bundle_collection (Liste mit Einträgen der inneren Bundles)
- Cross Gateway Query Response inkl. RegistryError-Elementen (falls vorhanden)

6.2.6 TUC_NCPeH_037: Abzugebende E-Rezepte vom E-Rezept-FD abrufen

Für diesen TUC gelten folgende übergreifende Festlegungen

- [[4.2.1 - Schnittstellen zu Diensten der zentralen TI](#)]
- [[4.2.10- Übergreifende Vorgaben an die Kommunikation mit E-Rezept-FD](#)]
- [[4.2.9 - Elektronische Identitäten des NCPeH-FD](#)]

Ablauf des TUC

Dieser TUC beschreibt den Ablauf des Abrufs der vom LE-EU angeforderten E-Rezepte des Versicherten aus dem E-Rezept-FD. Die angeforderten E-Rezept-IDs sind in der Variable list_ePrescription_uniqueIds zwischengespeichert. Die Vorgaben zur Befüllung der Variable sind im [[6.1.3.8- TUC_NCPeH_028: Cross Gateway Retrieve Request für ePeD-A CDA verarbeiten](#)] beschrieben.

Der NCPeH-FD MUSS sicherstellen, wenn die Liste `list_ePrescription_uniqueIds` mehrfach dieselbe E-Rezept-ID (ohne die Endungen "eP.XML" und "eP.PDF") enthält, dass die E-Rezept-ID einmal an den E-Rezept-FD übermittelt wird.

Der NCPeH-FD MUSS im inneren Request die HTTP-Operation des E-Rezept-FD mit dem Ausdruck `POST /get-eu-prescriptions` aufrufen und dabei gleichzeitig mit dem Request den HTTP-Header "Authorization" sowie die FHIR-Parameter gemäß den Vorgaben aus dem [4.2.10.6- Erstellung des Payload für die Kommunikation mit dem E-Rezept-FD] an die HTTP-Operation übermitteln. Der HTTP-Parameter `_count` DARF NICHT im Operationsaufruf angegeben werden.

Der NCPeH-FD MUSS im Payload innerhalb des `requestData`-Parameter für jeden Eintrag aus der Variable `list_ePrescription_uniqueIds` jeweils ein `part`-Element entsprechend den Vorgaben aus der Tabelle `TAB_NCPeH_Payload_PrescriptionIds_Aufruf_Operation_get-eu-prescriptions` erstellen und befüllen. Der NCPeH-FD MUSS sicherstellen, dass in der Payload keine E-Rezept-IDs mehrfach enthalten sind.

Tabelle 78: TAB_NCPeH_Payload_PrescriptionIds_Aufruf_Operation_get-eu-prescriptions

name-Element	valueIdentifizier/value-Element	valueIdentifizier/system-Element
<p>prescription-id</p> <p><i>Hinweis:</i> Der Parameter MUSS ausschließlich im Rahmen des Anwendungsfalls [5.2.3- NCPeH.UC_11 - Ausgewählte E-Rezepte aus ePeD-A abrufen] gesetzt werden. In anderen Anwendungsfällen DARF der Parameter NICHT gesetzt und an E-Rezept-FD übermittelt</p>	<p>Ausgehend vom Wert der Variable <code>list_ePrescription_uniqueIds</code> aus dem [6.1.3.8- TUC_NCPeH_028: Cross Gateway Retrieve Request für ePeD-A CDA verarbeiten] MUSS der NCPeH-FD den Wert einer E-Rezept-ID aus der Variable ohne Endungen "^eP.XML" und "^eP.PDF") in den Parameter aufnehmen. Die Endungen DÜRFEN NICHT an den E-Rezept-FD übermittelt werden.</p>	<p>Der folgende Wert MUSS gesetzt werden: "https://gematik.de/fhir/erp/NamingSystem/GEM_ERP_NS_PrescriptionId"</p>

<p>werden. <i>Hinweis:</i> Für weitere Informationen zur Struktur des Parameters siehe [API_EU_E-Rezepte"Abfragen von E-Rezepten des E-Rezept-Fachdienst"]</p>		
---	--	--

Für weitere Informationen über die Definition der Schnittstellenoperation /get-eu-prescriptions siehe [gemSpec_FD_eRp#"Http-Operation POST get-eu-prescriptions"] und [API_EU_E-Rezepte#"Abfragen von E-Rezepten des E-Rezept-Fachdienst"].

Nach Versand der Anfrage an den E-Rezept-FD MUSS der NCPeH-FD einen Non-Repudiation of Origin Eintrag gemäß [[4.1.7.1 - Non-Repudiation of Origin erstellen](#)] in die Komponente Audit Repository speichern.

Nach Erhalt der Antwort vom E-Rezept-FD MUSS der NCPeH-FD einen Non-Repudiation of Receipt Eintrag gemäß [[4.1.7.2 - Non-Repudiation of Receipt erstellen](#)] in die Komponente Audit Repository speichern.

Bei einer Antwort des E-Rezept-FD mit dem HTTP-Statuscode 401 MUSS der NCPeH-FD für das NCPeH Land-B ein neues ACCESS_TOKEN unter Verwendung der TI-Identität gemäß den Vorgaben in [4.2.10.4 Authentifizierung des NCPeH-FD am E-Rezept-FD] anfordern. Der NCPeH-FD MUSS die oben erwähnten Vorgaben zum Operationsaufruf erneut mit dem neuen ACCESS_TOKEN und den Vorgaben aus [4.2.10.6- Erstellung des Payload für die Kommunikation mit dem E-Rezept-FD] durchführen.

Wenn der E-Rezept-FD mit dem HTTP Status Code 200 antwortet, ist in der Antwortnachricht ein FHIR-Bundle enthalten. Der NCPeH-FD MUSS validieren, ob das in der Antwortnachricht enthaltene FHIR-Bundle vom Typ collection ist und die Vorgaben aus [FHIR_Resource_Bundle] erfüllt.

Das FHIR-Bundle (im weiteren Verlauf des Dokuments als "äußeres Bundle" bezeichnet) enthält mindestens ein entry-Element. Jedes entry-Element enthält eine FHIR-Resource resource/Bundle (im weiteren Verlauf des Dokuments als "inneres Bundle" bezeichnet). Der NCPeH-FD MUSS das innere Bundle in allenBundle/entry-Elementen auf Schemakonformität gemäß den Vorgaben aus [KBV_PR_ERP_Bundle] prüfen. Jedes innere Bundle kapselt Angaben zu genau einem E-Rezept.

Der NCPeH-FD MUSS für die nicht schemakonformen inneren Bundles in der Antwortnachricht an den NCPeH Land-B jeweils ein AdhocQueryResponse/RegistryErrorList/RegistryError-Element mit Angaben zum Fehler gemäß Tabelle TAB_NCPeH_Fehler_nicht_schemakonform_UC_ausgewählte_E-Rezepte abrufen erstellen und in der Liste list_registry_error_xca_retrieve für weitere Datenverarbeitung zwischenspeichern.

Tabelle 79: TAB_NCPeH_Fehler_nicht_schemakonform_UC_ausgewählte_E-Rezepte_abrufen

errorCode gemäß [eHDSI_XCA_Profile#2.2.3] und [eHDSI_NCPeH_Components#6.4]	codeContext	severity	location
ERROR_INTERNAL_ERROR	"Could not process a patients prescription."	urn:oasis:names:tc:ebxml-regrep:ErrorSeverityType:Error	"Received ePrescriptions ID=" + Wert der betroffenen E-Rezept-ID

Der NCPeH-FD MUSS für jede E-Rezept-ID aus der Variable list_ePrescription_uniqueIds) überprüfen, ob in der Antwortnachricht des E-Rezept-FD exakt ein inneres Bundle existiert und ob dieses Bundle im /Bundle/identifizier-Element (gemäß FHIR-Profil GEM_ERP_NS_PrescriptionId) einen Wert aufweisen, der mit der jeweiligen E-Rezept-ID identisch ist.

Der NCPeH-FD MUSS für jede E-Rezept-ID, zu der der E-Rezept-FD kein entsprechendes E-Rezept finden konnte, in der Antwortnachricht an den NCPeH Land-B ein AdhocQueryResponse/RegistryErrorList/RegistryError-Element mit Angaben zum Fehler gemäß Tabelle TAB_NCPeH_Error_Not_Found_E-Rezept-ID_UC_ausgewählte_E-Rezepte_abrufen erstellen und dieses in der Liste list_registry_error_xca_retrieve für die weitere Datenverarbeitung zwischenspeichern. Der NCPeH-FD MUSS bei doppelt vorkommenden E-Rezept-IDs aus der Variable list_ePrescription_uniqueIds für jeden einzelnen Eintrag dieser E-Rezept-ID die gleiche Fehlerbehandlung durchführen wie bei nicht doppelten E-Rezepten-IDs.

Tabelle 80: TAB_NCPeH_Error_Not_Found_E-Rezept-ID_UC_ausgewählte_E-Rezepte_abrufen

errorCode gemäß [eHDSI_XCA_Profile#2.2.3] und [eHDSI_NCPeH_Components#6.4]	codeContext	severity	location
ERROR_NOT_FOUND	"No prescription found for the ePrescription ID= " + Wert der betroffenen E-Rezept-ID	urn:oasis:names:tc:ebxml-regrep:ErrorSeverityType:Warning	"The german ePrescription service could not find a prescription for the ID= " + Wert der betroffenen

		E-Rezept-ID
--	--	-------------

Der NCPeH-FD MUSS für die weitere Datenverarbeitung ausschließlich schemakonforme innere Bundles zusammen mit der jeweils zugehörigen E-Rezept-ID (siehe Variable `list_ePrescription_uniqueIds`) in der Variable `fhir_erp_bundle_collection` zwischenspeichern. Bei Vorhandensein von mehrfachen Einträgen derselben E-Rezept-ID mit unterschiedlichen Endungen (wie `"^eP.XML"` und `"^eP.PDF"`) in der Variable `list_ePrescription_uniqueIds`, dann MUSS der NCPeH-FD das entsprechende innere Bundle in der Variable `fhir_erp_bundle_collection` mit jedem einzelnen dieser E-Rezept-ID Einträge verknüpfen.

Die inneren Bundles, die nicht schemakonform sind, DÜRFEN NICHT in der Variable `fhir_erp_bundle_collection` zwischengespeichert werden.

A_27255 - NCPeH - XCA eD-A - Verknüpfung von inneren Bundles mit TRC Assertion

Der NCPeH-FD MUSS bei der Zwischenspeicherung eine eindeutige Verknüpfung zwischen der Liste `fhir_erp_bundle_collection` und der TRC Assertion aus dem entsprechenden IHE XCA.Retrieve-Request für die weitere Datenverarbeitung sicherstellen und DARF diese Liste NICHT mit anderen TRC Assertions in Verbindung bringen. [**<=**]

Tritt einer der folgenden Fehlerfälle auf, MUSS der NCPeH-FD die weitere gesamte Verarbeitung der Anfrage abbrechen, in der Antwortnachricht an den NCPeH Land-B ein `/RetrieveDocumentSetResponse/RegistryResponse/RegistryErrorList/RegistryError-Element` gemäß den Vorgaben aus [eBRIM_Representation_Document#4.2.4] und [ITI-43#3.43.5] erstellen und mit entsprechenden Angaben zum Fehler gemäß Tabelle "TAB_NCPeH_Fehlerfälle_Abzugebende_E-Rezepte_vom_E-Rezept-FD_abrufen" an den NCPeH Land-B befüllen.

Tabelle 81: TAB_NCPeH_Fehlerfälle_Abzugebende_E-Rezepte_vom_E-Rezept-FD_abrufen

Fehlerfall	errorCode gemäß [eHDSI_XCA_Profile #2.2.3] und [eHDSI_NCPeH_Components#6.4]	codeContent	severity	location
E-Rezept-FD antwortet mit dem HTTP Status Code 200, aber die Antwortnachricht enthält kein FHIR-Bundle vom Typ <code>collection</code>	ERROR_INTERNAL_ERROR	"Internal error when retrieving the patient's ePrescriptions."	rn:oasis:names:tc:ebxml-regrep:ErrorSeverityType:Error	"The response from the german ePrescription service did not contain a FHIR bundle of type <code>collection</code> ."
E-Rezept-FD antwortet mit				"The german

dem HTTP Status Code 400				ePrescription service did respond with HTTP status code 400."
E-Rezept-FD antwortet nach einem zweiten Operationsaufruf mit dem HTTP Status Code 401				"The german ePrescription service did respond with HTTP status code 401 after a second operation request."
Die Variable fhir_erp_bundle_collection ist nach Prüfung der inneren Bundles leer.				"The format of the patient's ePrescriptions is incorrect."
E-Rezept-FD antwortet mit dem HTTP Status Code 403	ERROR_NO_CONSENT	"There is no valid access authorization for the requesting country in the german ePrescription service. Please ask the patient		"The german ePrescription service did respond with HTTP status code 403"

		for access authorisation."		
E-Rezept-FD antwortet mit dem HTTP Status Code 404	WARNING_EP_GENERIC	"No ePrescription for the patient found, which is dispensable in EU-countries"	urn:oasis:names:tc:ebxml-regrep:ErrorSeverityType:Warning	"The german ePrescription service did respond with HTTP status code 404."
E-Rezept-FD antwortet mit dem HTTP Status Code 408	ERROR_REGISTRY_NOT_AVAILABLE	"Timeout during communication with the german ePrescription service. Please submit the request again."	urn:oasis:names:tc:ebxml-regrep:ErrorSeverityType:Error	"The german ePrescription service did respond with HTTP status code 408."
E-Rezept-Fachdienst antwortet mit dem HTTP Status Code 500	ERROR_INTERNAL_ERROR	"Internal error when retrieving the patient's ePrescriptions."		"The german ePrescription service did respond with HTTP status code 500."
Der E-Rezept-FD antwortet nicht und der hinterlegte Wert im Konfigurationsparameter eRp_RESPONSE_TIMEOUT (siehe				"Time-out. The german ePrescription service is not responding."

4.1.1 Konfigurationsparameter) ist überschritten				
---	--	--	--	--

Der NCPeH-FD MUSS für AdhocQueryResponse@status in der Antwortnachricht einen entsprechenden Wert setzen, der anhand des Gesamtstatus aller RegistryResponse/RegistryErrorList/RegistryError@Severities-Attribute, erfolgreich verarbeiteter innerer Bundles und unter Berücksichtigung der Kriterien aus der Tabelle "Retrieve Document Set [ITI-43] and Cross Gateway Retrieve [ITI-39] Responses" in [ebRIM_Representation_Document#4.2.4.2] zu bestimmen ist.

Ausgabeparameter des TUC

- fhir_erp_bundle_collection (Liste mit Einträgen der "inneren Bundles")
- list_registry_error_xca_retrieve

6.2.7 TUC_NCPeH_038: Dispensierdokumente an E-Rezept-FD übermitteln

Für diesen TUC gelten folgende übergreifende Festlegungen

- [[4.2.1 - Schnittstellen zu Diensten der zentralen TI](#)]
- [[4.2.10- Übergreifende Vorgaben an die Kommunikation mit E-Rezept-FD](#)]
- [[4.2.10.4- Authentifizierung des NCPeH-FD am E-Rezept-FD](#)]
- [[4.2.10.7- Regelung zur Unterstützung von mehreren FHIR-Package Versionen](#)]
- [[4.2.9 - Elektronische Identitäten des NCPeH-FD](#)]

Ablauf des TUC

Dieser TUC enthält Vorgaben zur Übermittlung von Dispensierdokumenten des Versicherten an den E-Rezept-FD, mit der der E-Rezept-Workflow für den unter dem E-Rezept-Identifizier geführten Task abgeschlossen wird. Der NCPeH-FD initiiert dazu eine HTTP POST-Anfrage an den Endpunkt /Task/<id>/\$eu-close des E-Rezept-FD. Die von der europäischen Apotheke bereitgestellten Dispensierinformationen werden anschließend für den Versicherten im E-Rezept-FD gespeichert. Für diesen TUC gelten als Eingabeparameter die Variablen list_transcoded_fhir_medication_dispensations und list_registry_error_xdr_request (beide aus dem [6.1.5.4- TUC_NCPeH_034: Dispensierdokumente transkodieren und transformieren]).

A_27236 - NCPeH - XDR eD-A - Übermittlung von Dispensierinformationen an E-Rezept-FD

Der NCPeH-FD MUSS den Eintrag (Dispensierdokument) aus der Variable list_transcoded_fhir_medication_dispensations im inneren Request die HTTP-Operation des E-Rezept-FD mit dem Ausdruck POST /Task/{id}/\$eu-close aufrufen. Dabei MUSS der NCPeH-FD gleichzeitig mit dem Request den HTTP-Header "Authorization" sowie die FHIR-Parameter gemäß Vorgaben aus dem [4.2.10.6- Erstellung des Payload für die Kommunikation mit dem E-Rezept-FD] setzen. Der NCPeH-FD MUSS das entsprechende Dispensierdokument in den Payload als ein parameter-Element gemäß dem FHIR-Profil [GEM_ERPEU_PR_PAR_CloseOperation_Input] aufnehmen. [<=]

A_27270 - NCPeH - XDR eD-A - Setzen der E-Rezept-ID als Task.id im Operationsaufruf des E-Rezept-FD

Der NCPeH-FD MUSS den Wert der E-Rezept-ID aus dem zu übermittelnden Eintrag (Dispensierdokument) der Variable `list_transcoded_fhir_medication_dispensations` für den Parameter `{id}` im inneren Request der HTTP-Operation des E-Rezept-FD mit dem Ausdruck `POST/Task/{id}/$eu-close` setzen. Mehrere E-Rezept-IDs für den Parameter `{id}` DÜRFEN NICHT in dem Operationsaufruf angegeben werden. [`<=`]

Für weitere Informationen über die Definition der Schnittstellenoperation `/Task/{id}/$eu-close` siehe [`gemSpec_FD_eRp#"POST /Task/<id>/$eu-close"`] und [`API_EU_E-Rezepte#"Abgabeinformationen zu einem E-Rezept einstellen"`].

A_27237 - NCPeH - XDR eD-A - Erstellung und Speicherung des Non-Repudiation of Origin Eintrags

Nach Versand der Anfrage an den E-Rezept-FD MUSS der NCPeH-FD einen Non-Repudiation of Origin Eintrag gemäß [[4.1.7.1 - Non-Repudiation of Origin erstellen](#)] in die Komponente Audit Repository speichern. [`<=`]

A_27238 - NCPeH - XDR eD-A - Erstellung und Speicherung des Non-Repudiation of Receipt Eintrags

Nach Erhalt der Antwort vom E-Rezept-FD MUSS der NCPeH-FD einen Non-Repudiation of Receipt Eintrag gemäß [[4.1.7.2 - Non-Repudiation of Receipt erstellen](#)] in die Komponente Audit Repository speichern. [`<=`]

A_27239 - NCPeH - XDR eD-A - Behandlung der ersten HTTP-401-Antwort des E-Rezept-FD und erneuter Aufruf

Der NCPeH-FD MUSS bei einer Antwort des E-Rezept-FD mit dem HTTP-Statuscode 401 für den NCPeH Land-B einmalig einen neuen ACCESS_TOKEN gemäß den Vorgaben in [[4.2.10.5- Abruf von Token vom IDP-Dienst](#)] anfordern und anschließend den [[6.2.7-TUC_NCPeH_038: Dispensierdokumente an E-Rezept-FD übermitteln](#)] erneut durchlaufen. [`<=`]

A_27267 - NCPeH - XDR eD-A - Fehlerbehandlung bei HTTP-Status 401 nach zweitem Operationsaufruf des E-Rezept-FD

Der NCPeH-FD MUSS bei einer Antwort des E-Rezept-FD mit dem HTTP-Status-Code 401 nach dem zweiten Operationsaufruf die weitere Bearbeitung der XDR-Anfrage abbrechen, in der Antwortnachricht an den NCPeH Land-B ein `RegistryResponse/RegistryErrorList/RegistryError-Element` erstellen und folgende Angaben zum Fehler in das erstellte Element aufnehmen:

- `errorCode= ERROR_INTERNAL_ERROR`
- `codeContext= "Internal error when sending the patient's eDispensation."`
- `severity= urn:oasis:names:tc:ebxml-regrep:ErrorSeverityType:Error`
- `location= "The german eDispensation service did respond with HTTP status code 401 after a second operation request."`

Der NCPeH-FD MUSS in die Antwortnachricht sämtliche `RegistryError-Elemente` aufnehmen, die sowohl für die im E-Rezept-FD gespeicherten Dispensierdokumente als auch für die nicht dispensierten Dokumente erstellt wurden. [`<=`]

A_27268 - NCPeH - XDR eD-A - Fehlerbehandlung bei HTTP-Statuscode 403 vom E-Rezept-FD

Der NCPeH-FD MUSS bei einer Antwort des E-Rezept-FD mit dem HTTP-Status-Code 403 die weitere Bearbeitung der XDR-Anfrage abbrechen, in der Antwortnachricht an den NCPeH Land-B ein `RegistryResponse/RegistryErrorList/RegistryError-Element` erstellen und folgende Angaben zum Fehler in das erstellte Element aufnehmen:

- `errorCode= ERROR_NO_CONSENT`

- codeContext= "There is no valid access authorisation for the requesting country in the german eDispensation service. Please ask the patient for access authorisation."
- severity= urn:oasis:names:tc:ebxml-regrep:ErrorSeverityType:Error
- location= "The german eDispensation service did respond with HTTP status code 403."

Der NCPeH-FD MUSS in die Antwortnachricht sämtliche RegistryError-Elemente aufnehmen, die sowohl für die im E-Rezept-FD gespeicherten Dispensierdokumente als auch für die nicht dispensierten Dokumente erstellt wurden. [≤=]

A_27269 - NCPeH - XDR eD-A - Behandlung der ersten HTTP-408-Antwort des E-Rezept-FD und erneuter Aufruf

Der NCPeH-FD MUSS bei einer Antwort des E-Rezept-FD mit dem HTTP-Statuscode 408 den [6.2.7- TUC_NCPeH_038: Dispensierdokumente an E-Rezept-FD übermitteln] erneut durchlaufen. [≤=]

Hinweis: Bei wiederholtem Auftreten des HTTP-Statuscode 408 in der Antwort vom E-Rezept-FD greift die Fehlerbedingung in Tabelle

TAB_NCPeH_RegistryError_Dispensierdokumente_an_E-Rezept-FD_übermitteln zum HTTP-Statuscode 408.

A_27241 - NCPeH - XDR eD-A - Verarbeitung von Antworten des E-Rezept-FD

Der NCPeH-FD MUSS nach Erhalt einer Antwort vom E-Rezept-FD auf das übermittelte Dispensierdokument in der Antwortnachricht an den NCPeH Land-B ein RegistryResponse/RegistryErrorList/RegistryError-Element gemäß den Vorgaben aus [ebRIM_Representation_Document#4.2.4] und [ITI-43#3.43.5] erstellen und dieses mit den entsprechenden Angaben zur Warnung oder zum Fehler gemäß den Vorgaben aus der Tabelle TAB_NCPeH_RegistryError_Dispensierdokumente_an_E-Rezept-FD_übermitteln befüllen.

Tabelle 82: TAB_NCPeH_RegistryError_Dispensierdokumente_an_E-Rezept-FD_übermitteln

HTTP Status Code	errorCode gemäß [eHDSI_XDR_Profile#2.2.2] und [eHDSI_NCPeH_Components#6.4]	codeContext	severity	location
E-Rezept-FD antwortet mit dem HTTP Status Code 400	ERROR_INTERNAL_ERROR	"Internal error in the german eDispensation service when processing the dispensing information . Affected ePrescription ID= " + Angabe der E-Rezept-ID aus dem an den E-	urn:oasis:names:tc:ebxml-regrep:ErrorSeverityType:Error	"The german eDispensation service did respond with HTTP status code 400. ePrescription ID= " + Angabe der E-Rezept-ID aus dem jeweiligen

		Rezept-FD übersandten Dispensierdokument		Dispensierdokument, für das der NCPeH-FD eine Antwort vom E-Rezept-FD erhalten hat
E-Rezept-FD antwortet mit dem HTTP Status Code 404	ERROR_ED_EPRESRIPTION_NOT_IDENTIFIABLE	"An ePrescription is not available anymore for the patient. Affected ePrescription ID= " + Angabe der E-Rezept-ID aus dem an den E-Rezept-FD übersandten Dispensierdokument		"The german eDispensation service did respond with HTTP status code 404. Affected ePrescription ID= " + Angabe der E-Rezept-ID aus dem jeweiligen Dispensierdokument, für das der NCPeH-FD eine Antwort vom E-Rezept-FD erhalten hat
E-Rezept-FD antwortet nach einem erneuten Operationsaufruf mit dem HTTP Status Code 408	ERROR_REGISTRY_NOT_AVAILABLE	"Internal error due to timeout. Please submit the request again. Affected ePrescription ID= " + Angabe der E-Rezept-ID aus dem an den E-Rezept-FD		"The german eDispensation service did respond with HTTP status code 408. Affected ePrescription ID= " + Angabe

		übersandten Dispensierdokument		der E-Rezept-ID aus dem an den E-Rezept-FD übersandten Dispensierdokument
E-Rezept-Fachdienst antwortet mit dem HTTP Status Code 500	ERROR_INTERNAL_ERROR	"Internal error in the german eDispensation service when processing the dispensation information . Affected ePrescription ID=" + Angabe der E-Rezept-ID aus dem an den E-Rezept-FD übersandten Dispensierdokument		"The german eDispensation service did respond with HTTP status code 500."
Der E-Rezept-FD antwortet nicht und der hinterlegte Wert im Konfigurationsparameter eRp_RESPONSE_TIMEOUT ist überschritten (siehe [4.1.1 Konfigurationsparameter])	ERROR_INTERNAL_ERROR	"Time-out. The german eDispensation service is not responding."		

Der NCPeH-FD MUSS das RegistryError-Element in einer Variable `list_registry_error_xdr_request` für die weitere Datenverarbeitung zwischenspeichern. [≤]

Für weitere Informationen über die Definition der Schnittstellenoperation `/Task/{id}/$eu-close` und den möglichen Fehlercodes siehe `[gemSpec_FD_eRp#POST /Task/<id>/$eu-close]` und `[API_EU_E-Rezpte#Abgabeformaten zu einem E-Rezept einstellen]`.

Ausgabeparameter des TUC

- `list_registry_error_xdr_request`

6.3 Administration

6.3.1 TUC_NCPeH_018: Systemadministrator oder Prozessverantwortlicher anmelden

Für diesen TUC gelten folgende übergreifende Festlegungen

- Keine

Ablauf des TUC

Der NCPeH-FD MUSS dem Systemadministrator bzw. Prozessverantwortlichen (berechtigte Akteure) eine Management- oder technische Schnittstelle zur Verfügung stellen, über die sie IT-Aktivitäten am NCPeH-FD durchführen können. Zu den IT-Aktivitäten gehören in Abhängigkeit vom jeweiligen Anwendungsfall die Erstellung und Verwaltung von Service Metadata des NCPeH-FD auf dem Configuration Service des NCPeH-FD, die Aktualisierung von Konfigurationsparametern (siehe [\[4.1.1-Konfigurationsparameter\]](#)), der Abruf des aktuellen MTC vom Terminology Service der eHDSI und der Abruf von Evidence und Audit Trail Einträgen.

Die technische Ausgestaltung der Management- bzw. technischen Schnittstelle und der begleitenden Prozesse liegt in der Verantwortung des Anbieters des NCPeH-FD.

Der NCPeH-FD MUSS sicherstellen, dass sich der Akteur mindestens mit einem 2-Faktor authentisiert. Der NCPeH-FD MUSS den Kommunikationskanal mit gegenseitiger Authentifizierung zwischen der Management- bzw. technischen Schnittstelle und dem Client des Akteurs oder zu einem anderen vertrauenswürdigen System (z. B. Identity Provider) des Anbieters mittels TLS Version 1.2 oder Version 1.3 aufbauen.

Der NCPeH-FD MUSS erfolgreich authentifizierten und berechtigten Akteuren die Nutzung der administrativen Aktivitäten über die Management- bzw. technischen Schnittstelle ermöglichen.

Der Akteur DARF KEINEN Zugriff auf die personenbezogenen Daten in der VAU haben oder andere Prozesse in der VAU beeinträchtigen.

Für die Gewährleistung der ordnungsgemäßen IT-Administration und des geforderten Sicherheitsniveaus MUSS der NCPeH-FD relevante Vorgaben aus [\[4.3- Sicherheit und Datenschutz\]](#) umsetzen.

Ausgabeparameter des TUC

- Identitätsangaben des authentifizierten Akteurs
(Die Identitätsangaben dienen z. B. zur Unterscheidung von Systemadministratoren bei der Anwendung des Vier-Augen-Prinzips. Die Identitätsangaben sollen auch für Protokollierungszwecke verwendet werden.)

6.3.2 TUC_NCPeH_019: Änderungen an Konfigurationsparameter planen

Für diesen TUC gelten folgende übergreifende Festlegungen

- [\[4.1.1- Konfigurationsparameter\]](#)

Ablauf des TUC

Der NCPeH-FD MUSS den authentifizierten Systemadministratoren über die Management-Schnittstelle ermöglichen, einzelne Konfigurationsparameter des NCPeH-FD (siehe [\[4.1.1-Konfigurationsparameter\]](#)) auszuwählen und ihre Werte zu verändern. Der NCPeH-FD

DARF die veränderte Konfigurationsparameter NUR nach Durchführung des Vier-Augen-Prinzips persistieren (siehe [6.3.3- TUC_NCPeH_020: Änderungen an Konfigurationsparametern und im Truststore aktivieren]). Bis zur Durchführung der Persistierung MUSS der authentifizierte Systemadministrator die veränderten Werte der Konfigurationsparameter im NCPeH-FD aufrufen und sie verändern können. Der NCPeH-FD MUSS sicherstellen, dass die restlichen Daten und Datenverarbeitungsprozessen in der VAU isoliert von den in diesem TUC beschriebenen Abläufen bleiben.

Der NCPeH-FD MUSS es den authentifizierten Systemadministratoren ermöglichen, beim Konfigurationsparameter WHITELIST_NCPeH_COUNTRY-B folgende Aktivität durchzuführen:

- Der Systemadministrator erstellt einen neuen Eintrag für ein Land-B und den NCPeH Land-B. Die relevanten Informationen zum Land-B und NCPeH Land-B sind zum Zeitpunkt der Erstellung des Eintrages nicht in der Liste enthalten. Pro Land-B und NCPeH Land-B darf höchstens ein Eintrag in der Liste existieren.
- Der Systemadministrator wählt einen Eintrag für ein bestimmtes Land-B aus und ändert den Wert des Attributes HomeCommunityId des NCPeH Land-B. Dabei DARF der Systemadministrator das Attribut Ländercode NICHT verändern.
- Der Systemadministrator wählt einen Eintrag für ein bestimmtes Land-B aus und entfernt den kompletten Eintrag aus der Liste.

Außerdem MUSS der NCPeH-FD dem Systemadministrator über die Management-Schnittstelle ermöglichen, neue öffentliche Zertifikate des Herausgebers (Root und Intermediate), der zentralen Dienste eHDSI Configuration Service und eHDSI Terminology Service zur Installation in den lokalen Truststore einzubringen. Der Systemadministrator MUSS über die Management-Schnittstelle des NCPeH-FD bereits im Truststore enthaltene Zertifikate des Herausgebers (Root und Intermediate), der zentralen Dienste eHDSI Configuration Service und eHDSI Terminology Service anhand der Angaben aus den Zertifikatselementen subject und validity einzeln auswählen und zur Löschung aus dem Truststore vorschlagen zu können.

Ausgabeparameter des TUC

- Identitätsangaben des Systemadministrators, der die Änderungen geplant hat (Die Identitätsangaben dienen z.B. zur Unterscheidung von Systemadministratoren bei der Anwendung des Vier-Augen-Prinzips)
- Liste der geplanten Änderungen

6.3.3 TUC_NCPeH_020: Änderungen an Konfigurationsparametern und im Truststore aktivieren

Für diesen TUC gelten folgende übergreifende Festlegungen

- [4.1.1- Konfigurationsparameter]
- [4.1.3.5- Umgang mit Zertifikaten der eHDSI]
- [4.1.4- Service Metadata des NCPeH Land-B abrufen]

Ablauf des TUC

In diesem TUC MUSS ein authentifizierter Systemadministrator die Konfigurationsparameter aus [6.3.2- TUC_NCPeH_019: Änderungen an Konfigurationsparameter planen], die von einem anderen Systemadministrator geändert wurden, offiziell zur Aktivierung freigeben.

Der NCPeH-FD MUSS sicherstellen, dass die Aktivierung von Änderungen an den Konfigurationsparametern erst dann erfolgen kann, nachdem eine präventive Kontrolle

der vorgeschlagenen Änderungen nach dem Vier-Augen-Prinzip stattgefunden hat. Die offizielle Freigabe zur Aktivierung von vorgeschlagenen Änderungen an den Konfigurationsparametern MUSS durch explizite Anforderung eines authentifizierten Systemadministrators erfolgen, dessen Identität nicht mit der Identität des Systemadministrators gleichzusetzen ist, der die Änderungen an Konfigurationsparametern zuletzt erstellt hat. Das Ziel des Vier-Augen-Prinzips ist es, das Risiko von Fehlern und Missbrauch zu reduzieren.

Der NCPeH-FD MUSS sicherstellen, dass während der Durchführung des Vier-Augen-Prinzips keine Änderungen an den Konfigurationsparametern durch Systemadministratoren erfolgen können. Falls während der Anwendung des Vier-Augen-Prinzips vom prüfenden Systemadministrator festgestellt wird, dass die vorgeschlagenen Änderungen an den Konfigurationsparametern nicht korrekt sind, MUSS der prüfende Systemadministrator die Aktivierung von Änderungen ablehnen können und den Systemadministrator, der die Änderungen erstellt hat, auffordern die betroffenen Konfigurationsparameter zu korrigieren.

Falls der prüfende Systemadministrator die offizielle Aktivierung von Änderungen an den Konfigurationsparametern freigegeben hat, MÜSSEN vom NCPeH-FD folgende Vorgaben umgesetzt werden:

- Bei der Erstellung eines neuen Eintrages für ein Land-B im Konfigurationsparameter WHITELIST_NCPeH_COUNTRY-B MUSS der NCPeH-FD den Ländercode und die HomeCommunityId des NCPeH Land-B in den Eintrag persistieren und aktivieren. Ferner MÜSSEN die ServiceMetadata-Dateien des NCPeH Land-B vom eHDSI Configurations Service gemäß Vorgaben aus [\[4.1.4- Service Metadata des NCPeH Land-B abrufen\]](#) abgerufen werden. Falls die heruntergeladenen ServiceMetadata-Dateien erfolgreich auf Authentizität und Identität geprüft wurden, MÜSSEN die entsprechenden Zertifikate aus ServiceMetadata gemäß [\[4.1.4- Service Metadata des NCPeH Land-B abrufen\]](#) in den lokalen Truststore aufgenommen werden.
- Bei Änderungen von Einträgen in dem Konfigurationsparameter WHITELIST_NCPeH_COUNTRY-B DARF NUR die HomeCommunityId des NCPeH Land-B geändert werden. Der Ländercode aus dem Eintrag MUSS unberührt bleiben. Der NCPeH-FD SOLL an dieser Stelle die Abläufe aus dem [\[4.1.4- Service Metadata des NCPeH Land-B abrufen\]](#) NICHT durchführen.
- Beim Löschen eines Eintrages aus dem Konfigurationsparameter WHITELIST_NCPeH_COUNTRY-B MUSS der NCPeH-FD alle Zertifikate des betroffenen NCPeH Land-B aus dem lokalen Truststore entfernen. Zusätzlich MÜSSEN Referenzwerte gemäß [\[4.1.4- Service Metadata des NCPeH Land-B abrufen\]](#) aus dem NCPeH-FD gelöscht werden, die mit den Zertifikaten des NCPeH Land-B verknüpft sind.

Bei Installation und Aktivierung der öffentlichen Zertifikate des Herausgebers (Root und Intermediate), der zentralen Dienste eHDSI Configuration Service und eHDSI Terminology Service MUSS der NCPeH-FD dem prüfenden Systemadministrator Zertifikatsinhalte aus Elementen subject und validity (Gültigkeit des Zertifikats von - bis) anzeigen. Nach dem der prüfende Systemadministrator die Zertifikate zur Aktivierung freigegeben hat, MUSS der NCPeH-FD die neuen Zertifikate in den lokalen Truststore installieren und sofort aktivieren.

Bei Entfernung von ausgewählten Zertifikaten aus dem Truststore MUSS der NCPeH-FD dem prüfenden Systemadministrator Zertifikatsinhalte aus Elementen subject und validity (Gültigkeit des Zertifikats von - bis) anzeigen. Nachdem der prüfende Systemadministrator die Entfernung der Zertifikate freigegeben hat, MUSS der NCPeH-FD diese Zertifikate aus dem Truststore dauerhaft entfernen.

Nach erfolgreicher Aktivierung der geänderten Konfigurationsparameter und Zertifikaten MUSS der NCPeH-FD dem prüfenden Systemadministrator über die Management-

Schnittstelle eine Erfolgsmeldung anzeigen. Falls Fehler bei der Aktivierung von geplanten Änderungen auftreten, MUSS der NCPeH-FD dem prüfenden Systemadministrator eine verständliche Fehlermeldung inkl. Fehlergrund anzeigen.

Im Fehlerfall MÜSSEN, in den von geplanten Änderungen betroffenen Konfigurationsparametern die ursprünglichen Werte wiederhergestellt werden, die die Konfigurationsparameter vor Beginn der Aktivierung hatten. Bei Fehlern zur Installation und Aktivierung von Zertifikaten MUSS der ursprüngliche Zustand des Truststore vor der Aktivierung wiederhergestellt werden.

Ausgabeparameter des TUC

Keine

6.3.4 TUC_NCPeH_021: Ausgewählte Evidence und Audit Trail Einträge ermitteln

Für diesen TUC gelten folgende übergreifende Festlegungen

- [4.1.7- Non-Repudiation und Audit Trail Schemas]

Ablauf des TUC

Der NCPeH-FD MUSS den authentifizierten Prozessverantwortlichen Audit Trails (Prozessverantwortlicher) über eine technische Schnittstelle ermöglichen, im Audit Repository nach Evidence- (SAR- und ARbR-Objekte) und Audit Trail-Einträgen (Patient Privacy und Translation) zu suchen und sie auszulesen. Der Prozessverantwortliche DARF andere Daten NICHT auslesen oder Datenverarbeitungsprozesse in der VAU beeinträchtigen können.

Der NCPeH-FD MUSS die Suche nach Evidence und Audit Trail Einträgen durchführen, wenn eine der folgenden Gruppen von Parametern in der Suchanfrage des Prozessverantwortlichen enthalten ist:

- Gruppe 1: KVNR des Versicherten und Kalenderjahr oder
- Gruppe 2: KVNR des Versicherten, Identifier des LE (gemäß [ida_name-id](#) aus [4.1.5- Validierung der Identity Assertion des LE-EU]) und Kalenderjahr oder
- Gruppe 3: KVNR des Versicherten, Identifier der LEI (gemäß [ida_organization-id](#) aus [4.1.5- Validierung der Identity Assertion des LE-EU]) und Kalenderjahr.

Der NCPeH-FD MUSS vor dem Suchvorgang die Suchparameter auf folgende Formatvorgaben prüfen:

- Identifier der LEI MUSS Vorgaben aus gemäß [eHDSI_SAML_Profile#2.3],
- Kalenderjahr MUSS dem Format YYYY entsprechen.

Falls die Suche erfolgreich war, MUSS der NCPeH-FD die ermittelten Evidence im Format gemäß Vorgaben aus [eHDSI_Audit_Trail_Profile#1.2] dem anfragenden Prozessverantwortlichen bereitstellen. Dabei MUSS der NCPeH-FD die Authentizität und Integrität der Evidence sicherstellen. Die ermittelten Audit Trail Einträge aus den Suchergebnissen MÜSSEN im Dokumentenformat nach Vorgaben aus [eHDSI_Audit_Trail_Profile#2] in der Antwort an den Prozessverantwortlichen gesendet werden.

Der NCPeH-FD MUSS den authentifizierten Prozessverantwortlichen über die technische Schnittstelle ermöglichen, nach Security Audit Trail Einträgen (siehe [4.1.7.5- Security Audit Trail Eintrag erstellen]) in dem Audit Repository unabhängig von Evidence und anderen Audit Trail Einträgen zu suchen. Der NCPeH-FD MUSS dem

Prozessverantwortlichen ermöglichen, unabhängig vom Kalenderjahr nach Security Audit Trail Einträgen zu suchen, da in dem Security Audit Trail-Schema keine Erfassung von personenbezogene Daten vorgesehen ist und das Schema auf das Interaction Pattern Configuration Manager (siehe [eHDSI_Audit_Trail_Profile#2.3.5.7]) beschränkt ist. Der NCPeH-FD MUSS die Suchanfragen nach Security Audit Trail Einträgen akzeptieren und durchführen, wenn in den Suchparametern Angaben zu Events mit Bezug auf das Interaction Pattern Configuration Manager gemäß [eHDSI_Audit_Trail_Profile#2.3.5.7] enthalten sind. Der NCPeH-FD MUSS im Erfolgsfall die Suchergebnisse über die technische Schnittstelle dem Prozessverantwortlichen auf seine Anfrage antworten.

Wenn in den Anfragen obligatorische Suchparameter fehlen, oder die Suchparameter erfüllen die oben genannten Formatvorgaben nicht oder die Suche ergibt keine Suchtreffer, MUSS der NCPeH-FD dem anfragenden Prozessverantwortlichen mit einer Fehlermeldung inkl. Fehlergrund antworten.

Ausgabeparameter des TUC

- Suchergebnisse im Erfolgsfall: Evidence und Audit Trails oder Security Audit Trails

6.3.5 TUC_NCPeH_022: MTC in der VAU speichern

Für diesen TUC gelten folgende übergreifende Festlegungen

- [4.1.3- eHDSI Basisleistungen]
- [4.1.7.5- Security Audit Trail Eintrag erstellen]

Ablauf des TUC

Dieser TUC beschreibt, wie ein neuer MTC auf Anfrage des authentifizierten Systemadministrators durch den NCPeH-FD vom Central Terminology Service (CTS) abgerufen und lokal in der VAU installiert bzw. aktiviert wird. Die Bereitstellung des MTC erfolgt über RESTful-Schnittstellen des CTS. Der Betrieb des Central Terminology Service und Definition der RESTful-Schnittstellen liegt im Zuständigkeitsbereich des eHDSI Solution Providers.

Der NCPeH-FD MUSS sich gegenüber dem Central Terminology Service gemäß [eHDSI_CTS#4.3] authentisieren und seine Zugangsdaten TERMINOLOGY_SERVICE_USERNAME und TERMINOLOGY_SERVICE_PASSWORD (siehe [4.1.1- Konfigurationsparameter]) zusammen mit der HTTP POST Anfrage an folgende Schnittstelle des Terminology Service senden:

TERMINOLOGY_SERVICE_BASE_URL + "/ehealth-term-server/login"

Nach erfolgreicher Authentifizierung und Aufbau einer gültigen Session zum CTS MUSS der NCPeH-FD vom CTS relevante Entitäten des MTC mittels einzelner RESTful-Schnittstellen gemäß Vorgaben aus [eHDSI_CTS_API] abrufen.

Disclaimer: Die definierten Schnittstellen des eHDSI Central Terminology Service in [eHDSI_CTS_API] dienen zur Abfrage einzelner Entitäten des MTC. Allerdings sind in [eHDSI_CTS_API] fachliche Beschreibungen zur Nutzung von relevanten Entitäten des MTC nicht enthalten. Aus diesem Grund muss das BfArM in einem gesonderten Dokument erläutern, welche Entitäten des MTC für den Transkodierungsprozess notwendig sind und wie die einzelnen Entitäten miteinander in Beziehung stehen. Erst anhand dieser Erläuterungen können konkrete Schnittstellen des Terminologiedienstes genannt und eine eventuelle Reihenfolge der Abrufe der Entitäten definiert werden.

Falls der Central Terminology Service im Erfolgsfall mit einem Response Code 200 antwortet, muss im Body-Teil der Antwort die entsprechende Entität des MTC im Format application/json enthalten sein. Falls es sich doch um ein anderes Format handelt, MUSS der NCPeH-FD eine weitere Verarbeitung des MTC und seiner Entitäten abbrechen und dem Systemadministrator über die entsprechende Management-Schnittstelle (bei manueller Aktualisierung) oder als ein Protokolleintrag (bei automatisierter Aktualisierung) mit einer entsprechenden Fehlernachricht antworten. Der NCPeH-FD MUSS sicherstellen, dass die abgerufene Entität inklusive der Referenzen zu anderen Entitäten des MTC die Schemavorgaben gemäß [eHDSI_CTS_API#Models] erfüllt.

Vor der lokalen Installation der Entitäten des MTC in der VAU MUSS der NCPeH-FD sicherstellen, dass in einem Fehlerfall die aktuell in der VAU installierten und aktivierten Entitäten des MTC wiederhergestellt werden können (Backup des vorherigen MTC). Während der Installation und Aktivierung des neuen MTC MUSS der NCPeH-FD sicherstellen, dass zu dem Zeitpunkt laufende Prozess der Transformierung und Transkodierung von ePKA MIO der Versicherten ins eHDSI Pivotformat nicht beeinträchtigt werden.

Der NCPeH-FD MUSS bei der erfolgreichen Installation und Aktivierung des MTC in der VAU einen Audit Trail Eintrag nach Vorgaben aus [4.1.7.5- Security Audit Trail Eintrag erstellen] erstellen und dabei folgende Vorgaben berücksichtigen:

Tabelle 83: TAB_NCPeH_Audit_Trail_Synchronize_MTC

Interaction Pattern gemäß [eHDSI_Audit_Trail_Profile#2.3.5.7]	Event ID	Event Name
Configuration Manager	EHDSI-95	Synchronize MVC/MTC

Nach erfolgreicher Installation und Aktivierung des gesamten MTC in der VAU oder bei Fehlern bei der Authentisierung des NCPeH-FD gegenüber dem Central Terminology Service, gescheitertem Abruf einzelner Entitäten des MTC oder bei fehlgeschlagener Installation und Aktivierung des MTC in der VAU MUSS der NCPeH-FD dem Systemadministrator über die Management-Schnittstelle (bei manueller Aktualisierung) eine Meldung anzeigen und ein Protokolleintrag erstellen. Im Falle eines Fehlers MÜSSEN die Meldung und der Protokolleintrag Informationen über die Fehlerdetails enthalten.

Ausgabeparameter des TUC

keine

7 Anhang - Europäische Krankenversicherungskarte

Ein Abbild der Vorderseite der eGK soll zur besseren Verständlichkeit mit der International Searchmask mitgeliefert werden (siehe TAB_NCPeH_Service_Metadata_ISM in [6.1.4.1-TUC_NCPeH_011: Service Metadata erstellen]).



Abbildung 6: Vorderseite der eGK - Identifikationsdokument

Ein Abbild der Rückseite der eGK - die europäische Krankenversichertenkarte - soll zur besseren Verständlichkeit mit der International Searchmask mitgeliefert werden (siehe TAB_NCPeH_Service_Metadata_ISM in [6.1.4.1-TUC_NCPeH_011: Service Metadata erstellen]).



Abbildung 7: Rückseite der eGK - die europäische Krankenversichertenkarte

8 Anhang - Verzeichnisse

8.1 Abkürzungen

Kürzel	Erläuterung
ARbR	AcceptanceRejectionByRecipient
AD	associatedData
BfArM	Bundesinstitut für Arzneimittel und Medizinprodukte
CA	Certificate Authority
CEF	Connecting Europe Facility
CRL	Certificate Revocation List
CSR	Certificate Signing Request
CSRF	Cross-Site-Request-Forgery
ePrescription	electronic Prescription
E2E	Ende-zu-Ende
ECDH-ES	Elliptic Curve Diffie-Hellman Ephemeral Static key agreement
ECDSA	Elliptic Curve Digital Signature Algorithm
eHDSI	eHealth Digital Services Infrastructure - eHealth-Dienstinfrastruktur
eHMSEG	eHealth MemberState ExpertGroup
eD	eDispensation
eD-A	eDispensation Land-A
eHN	electronic Health Network
eP-A	ePrescription Land-A
ePeD-A	ePrescription/eDispensation Land-A
ePKA	elektronische Patientenkurzakte

FdV	Frontend des Versicherten
FD	Fachdienst
FDB	Fachdienstbetreiber
FHIR	Fast Healthcare Interoperability Resources
FQDN	Fully Qualified Domain Name
HBA	Heilberufsausweis
HSM	Hardware Security Module
IdA	Identity Assertion des LE-EU
IDP	Identity Provider
IOP	Interoperabilität
ISM	International Search Mask
JWS	JSON Web Signature
KBV	Kassenärztliche Bundesvereinigung
KPI	Key Performance Indicator
KSP	Konnektor Service Plattform
KVNR	Krankenversicherthenummer Gemeint ist hierbei in diesem Dokument immer der 10stellige, unveränderliche Anteil der KVNR.
Land-A	Das Land aus dem medizinische und demographische Daten der Versicherten bezogen werden sollen.
Land-B	Das Land in dem eine Behandlung und somit der Bezug der Daten von Land-A erfolgen soll.
LE	Leistungserbringer
LE-DE	Leistungserbringer in Deutschland
LE-EU	Leistungserbringer im EU-Ausland
LEI	Leistungserbringerinstitution
LOINC	Logical Observation Identifiers Names and Codes

MIO	Medizinisches Informationsobjekt
MS	Member State
MTC	Master Translation/Transcoding Catalogue
MVC	Master Value Sets Catalogue
NCF	National Configuration File
NCPeH	National Contact Point for eHealth
NdB	Netze des Bundes
NFD	Notfalldatensatz
NRR	Non-Repudiation of Receipt
NRO	Non-Repudiation of Origin
OID	Objekt-Identifizier
OrCD	Original Clinical Document
PET	eHDSI: Production Environment Test
PPT	eHDSI: Formal/Upgrade Pre-Production Testing
Pre-PPT	eHDSI: Preparatory Pre-Production Testing
PS	Patient Summary
PS-A	Patient Summary Land-A
PU	Produktivumgebung der TI
RU	Referenzumgebung der TI
SAR	SubmissionAcceptanceRejection
SGD	Schlüsselgenerierungsdienst
SLM	Service Level Management
SM-B	Security Module Typ B
SMP/SML	Service Metadata Publisher / Service Metadata Locator
TI	Telematikinfrastruktur

TIP	TI-Plattform
TRC	Treatment Relationship Confirmation
TU	Testumgebung der TI
TUC	Technischer Use Case
UHD	User Help Desk gemäß [gemKPT_Betr]
URN	Uniform Resource Name
VAU	vertrauenswürdige Ausführungsumgebung
VHD	Versicherten Help Desk gemäß [gemKPT_Betr]
VZD	Verzeichnisdienst
WSDL	Web Service Description Language

8.2 Begriffe

Begriff	Erläuterung
Behandlungsland / Land-B	Das Behandlungsland, in dem die grenzüberschreitende Gesundheitsversorgung erbracht wird, wenn der Versicherte eine Behandlung im Ausland in Anspruch nimmt. Dies kann ein Krankenhaus, eine niedergelassene Praxis oder eine andere Einrichtung des Gesundheitssystems von Land-B sein.
Demographische Daten	Diese Nomenklatur stammt aus dem eHDSI Sprachgebrauch und wird daher zur Wahrung der Einheitlichkeit auch von der gematik so geführt, gemäß [eHDSI Requirements Catalogue#02.01] (Uniquely identify the Patient). Gemeint sind die nicht-medizinischen persönlichen Daten, die vor allem im Prozess der Identifikation des Versicherten genutzt werden.
Funktionsmerkmal	Der Begriff beschreibt eine Funktion oder auch einzelne, eine logische Einheit bildende Teilfunktionen der TI im Rahmen der funktionalen Zerlegung des Systems.
eHDSI Service Consumer	NCPeH eines anderen EU-Mitgliedsstaaten (Nicht Deutschland), welches Anfragen an einen eHDSI Service Provider sendet und Daten als Antwort auf die Anfrage empfängt und sie an die eigene nationale eHealth-Infrastruktur weiterleitet.
eHDSI Service Provider	Eine Komponente des NCPeH zur Bereitstellung von elektronischen Diensten gemäß eHDSI-Vorgaben, empfangene

	Anfragen aus Ausland werden an die nationale eHealth-Infrastruktur zur weiteren Datenverarbeitung weitergeleitet.
Anbieter, Betreiber, Hersteller	Im Allgemeinen erfolgt eine einfache Begriffsklärung in [gemGlossar]. Eine detailliertere Beschreibung zu diesen Begriffen ist in [gemKPT_Betr] zu finden.
ID_TOKEN	Ein auf JSON basiertes und nach [RFC7519] genormtes Identitäts-Token, mit dem der NCPeH-relevante Claims an den zuständigen Authorization Server übergeben und dadurch die Ausstellung eines ACCESS_TOKEN beantragen kann.
Löschung	Unter Löschung eines Schlüssels sollen pauschal alle Operationen verstanden werden, die einer Anwendung einen kryptographischen Schlüssel dauerhaft entziehen.
Token-Endpunkt	Ein Endpunkt des IDP-Dienstes, welcher für die Ausstellung von Token (ID_TOKEN und ACCESS_TOKEN) zuständig ist.

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

8.3 Abbildungsverzeichnis

Abbildung 1: Architektur des NCPeH-FD Patient Summary Land-A.....15

Abbildung 2: Architektur des NCPeH-FD ePrescription/eDispensation Land-A.....17

Abbildung 3: Nachrichtenfluss für die Authentifizierung gegenüber dem zentralen IDP-Dienst..... 76

Abbildung 4: Schematischer Testaufbau für den integrativen Test des NCPeH-FD mit der Telematikinfrastruktur..... 121

Abbildung 5: Schematischer Aufbau für den Produktivtest des NCPeH-FD mit der eHDSI 123

Abbildung 6: Vorderseite der eGK - Identifikationsdokument.....317

Abbildung 7: Rückseite der eGK - die europäische Krankenversichertenkarte.....318

8.4 Tabellenverzeichnis

Tabelle 1: TAB_NCPeH_Übersicht_NCPeH-FD_Akteure..... 19

Tabelle 2: TAB_NCPeH_Konfigurationsparameter.....23

Tabelle 3: TAB_NCPeH_XCPD_Fehlermeldung_nicht_zugelassenes_EU-Land.....27

Tabelle 4: TAB_NCPeH_Service_Metadata_IDP_Provider.....32

Tabelle 5: TAB_NCPeH_Identitätsattribute_LE-EU.....35

Tabelle 6: TAB_NCPeH_TRC Assertion.....42

Tabelle 7: TAB_NCPeH_Beiispiel_Translation_Audit_Trail.....58

Tabelle 8: TAB_NCPeH_Beispiel_Security_Audit_Trail.....	61
Tabelle 9: TAB_Zugriffsberechtigung_durch_Prüfung_PermissionCodes.....	63
Tabelle 10: TAB_Zugriffsberechtigung_durch_Prüfung_RollenCodes.....	65
Tabelle 11: TAB_NCPeH_Schnittstellen_TI-Dienste.....	67
Tabelle 12: TAB_nonQES_Zertifikatsübersicht.....	70
Tabelle 13: TAB_Prüfparameter_nonQES_Zertifikate_TI.....	71
Tabelle 14: TAB_NCPeH_OCSP_Übersicht_für_Zertifikate_TI.....	72
Tabelle 15: TAB_NCPeH_Authentifizierung_IDP-Dienst_Fehlerbehandlung_XCPD.....	79
Tabelle 16: TAB_NCPeH_Lokalisierung_Akte_Fehler_XCPD_Response.....	82
Tabelle 17: TAB_NCPeH_Aufbau_VAU-Kanal_ePA_Fehlerbehandlung_XCPD.....	83
Tabelle 18: TAB_NCPeH_Authentifizierung_ePA_Auth_Service_Fehlerbehandlung_XCPD. .	86
Tabelle 19: TAB_Befüllung_Elemente_SOAP_Header_XDS_Document_Service.....	87
Tabelle 20: Tab_NCPeH_Personalisierung_HSM.....	88
Tabelle 21: TAB_NCPeH_HTTP-Header_X-erp-resource.....	90
Tabelle 22: TAB_NCPeH_Payload_Aufruf_Operation_get-eu-prescriptions.....	94
Tabelle 23: TAB_NCPeH_Payload_Aufruf_Operation_Task_id_eu-close.....	99
Tabelle 24: TAB_NCPeH_VAU-Datenstruktur_zu_kritischer_KPI-1.12.....	113
Tabelle 25: TAB_NCPeH_Berichtsdatenstruktur_zu_kritischer_KPI-1.12.....	113
Tabelle 26: TAB_NCPeH_eHDSI-Kennzahlen.....	114
Tabelle 27: TAB_NCPeH_Versicherten_im_Behandlungsland_für_PS-A_identifizieren.....	124
Tabelle 28: TAB_NCPeH_Metadaten_des_ePKA_MIO_auflisten.....	126
Tabelle 29: TAB_NCPeH_ePKA_MIO_des_Versicherten_abrufen.....	127
Tabelle 30: TAB_NCPeH_ePKA_MIO_des_Versicherten_als_PDF/A_abrufen.....	129
Tabelle 31: TAB_NCPeH_Einlösbare_E-Rezepte_des_Versicherten_aus_ePeD-A_auflisten	133
Tabelle 32: TAB_NCPeH_UC_11_Ausgewählte_E-Rezepte_abrufen.....	134
Tabelle 33: TAB_NCPeH_Evidences_Audit_Trails_abrufen.....	138
Tabelle 34: TAB_NCPeH_Service_Metadata_verwalten.....	139
Tabelle 35: TAB_NCPeH_MTC_Terminology-Service_herunterladen.....	141
Tabelle 36: TAB_NCPeH_Konfigurationsparameter_verwalten.....	142
Tabelle 37: TAB_NCPeH_Cross_Gateway_Patient_Discovery.....	144
Tabelle 38: TAB_NCPeH_Kriterien_Zuordnung_IHE_XCPD- Anfragen_zu_Anwendungsszenarien.....	145
Tabelle 39: TAB_NCPeH_XCPD_Prüfkriterien_PSA.....	147
Tabelle 40: TAB_NCPeH_XCPD_Prüfschritte_Fehlermeldungen_PSA.....	148
Tabelle 41: TAB_NCPeH_XCPD_Prüfkriterien_ePeD-A.....	159
Tabelle 42: TAB_NCPeH_XCPD_Prüfschritte_Fehlermeldungen_ePeD-A.....	161
Tabelle 43: TAB_NCPeH_Cross_Gateway_Queries.....	173

Tabelle 44: TAB_NCPeH_Kriterien_Zuordnung_IHE- XCA.Query_Anfragen_zu_Anwendungsszenarien.....	174
Tabelle 45: TAB_NCPeH_XCA_QUERY_Fehlerbedingungen_Fehlercodes_PS-A.....	176
Tabelle 46: TAB_NCPeH_Nutzungskonvention_Erstellung_XCA.Query_Response_PS-A... ..	184
Tabelle 47: TAB_NCPeH_XCA_QUERY_ePeD-A_Fehlerbedingungen_Fehlercodes.....	193
Tabelle 48: TAB_NCPeH_Nutzungskonvention_Erstellung_XCA.Query_Response_ePeD-A	202
Tabelle 49: TAB_NCPeH_Definition_Operation_RetrieveDocument.....	212
Tabelle 50: TAB_NCPeH_Kriterien_Zuordnung_IHE- XCA.RetrieveDocument_Anfragen_zu_Anwendungsszenarien.....	213
Tabelle 51: TAB_NCPeH_Nutzungskonvention_XCA_Retrieve_Request_PSA_CDA3.....	215
Tabelle 52: TAB_NCPeH_Fehlerfälle_Verarbeitung_Cross_Gateway_Retrieve_Request_PSA_CD A3.....	216
Tabelle 53: TAB_NCPeH_Nutzungskonvention_XCA_Retrieve_Response_PSA_CDA3.....	225
Tabelle 54: TAB_NCPeH_Nutzungskonvention_XCA_Retrieve_Request_PSA_CDA1.....	227
Tabelle 55: TAB_NCPeH_Fehlerfälle_Verarbeitung_Cross_Gateway_Retrieve_Request_PSA_CD A1.....	227
Tabelle 56: TAB_NCPeH_Nutzungskonvention_XCA_Retrieve_Response_PSA_CDA1.....	235
Tabelle 57: TAB_NCPeH_Fehlerfälle_Verarbeitung_Cross_Gateway_Retrieve_Request_ePeD-A	238
Tabelle 58: TAB_NCPeH_Nutzungskonvention_Cross_Gateway_Retrieve_Request_ePeD-A	243
Tabelle 59: TAB_NCPeH_Nutzungskonvention_Cross_Gateway_Retrieve_Response_ePeD-A	246
Tabelle 60: TAB_NCPeH_Service_Metadata_DocumentIdentifier.....	251
Tabelle 61: TAB_NCPeH_Service_Metadata_ProcessIdentifier.....	251
Tabelle 62: TAB_NCPeH_Service_Metadata_ServiceDescription.....	252
Tabelle 63: TAB_NCPeH_Service_Metadata_XCPD-Service.....	253
Tabelle 64: TAB_NCPeH_Service_Metadata_ISM.....	255
Tabelle 65: TAB_NCPeH_International_Search_Mask.....	259
Tabelle 66: TAB_NCPeH_Enterprise_Document_Reliable_Interchange_ProvideAndRegisterDocume ntSet-b.....	261
Tabelle 67: TAB_NCPeH_Kriterien_Zuordnung_IHE-XDR- Anfragen_zu_Anwendungsszenarien.....	262
Tabelle 68: TAB_NCPeH_Relevante_Metadatenattribute_ePKA MIO.....	280
Tabelle 69: TAB_NCPeH_Abruf_ePKA_Metadaten_Fehlerbehandlung_Zusammenhang_XCPD.....	281
Tabelle 70: TAB_NCPeH_Abruf_ePKA_Metadaten_Fehlerbehandlung_Zusammenhang_XCA	282

Tabelle 71: TAB_NCPeH_Abruf_ePKA MIO_Fehlerbehandlung_Zusammenhang_XCPD....285

Tabelle 72: TAB_NCPeH_Abruf_ePKA MIO_Fehlerbehandlung_Zusammenhang_PS.....287

Tabelle 73: TAB_NCPeH_Fehlen_Geburtstag_Fehler_XCPD_Response.....289

Tabelle 74 : TAB_NCPeH_Extrahierung_demographische_Versichertendaten_ePeD-A....290

Tabelle 75 : TAB_NCPeH_Fehlerfälle_Abruf_von_demographischen_Versichertendaten..291

Tabelle 76: TAB_NCPeH_Fehler_nicht_schemakonform_UC_Auflistung_von_einlösbaren_E-Rezepten.....294

Tabelle 77: TAB_NCPeH_Allgemeine_Fehlerfälle_Auflistung_von_einlösbaren_E-Rezepten295

Tabelle 78: TAB_NCPeH_Payload_PrescriptionIds_Aufruf_Operation_get-eu-prescriptions298

Tabelle 79: TAB_NCPeH_Fehler_nicht_schemakonform_UC_ausgewählte_E-Rezepte_abrufen.....300

Tabelle 80: TAB_NCPeH_Error_Not_Found_E-Rezept-ID_UC_ausgewählte_E-Rezepte_abrufen.....301

Tabelle 81: TAB_NCPeH_Fehlerfälle_Abzugebende_E-Rezepte_vom_E-Rezept-FD_abrufen302

Tabelle 82: TAB_NCPeH_RegistryError_Dispensierdokumente_an_E-Rezept-FD_übermitteln307

Tabelle 83: TAB_NCPeH_Audit_Trail_Synchronize_MTC.....316

8.5 Referenzierte Dokumente

8.5.1 Dokumente der gematik

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

[Quelle]	Herausgeber: Titel
[api-ePA]	https://github.com/gematik/api-ePA
[api-erp]	E-Rezept API-Dokumentation: https://github.com/gematik/api-erp
[API_EU_E-Rezepte]	https://github.com/gematik/api-erp/blob/feature/eu-eprescription/docs/erp_eprescription.adoc
[E-Rezept_Nutzer_TI_authentisiert]	https://github.com/gematik/api-erp/blob/master/docs/authentisieren.adoc#als-nutzer-der-telematikinfrastruktur-authentifiziert-werden
[FHIR_Version_E-Rezept_EU]	E-Rezept API-Dokumentation:

	https://github.com/gematik/api-erp/blob/master/docs/erp_fhirversion.adoc#e-rezept-fhir-package-versionsmanagement
[GEM_ERPEU_PR_PAR_GET_Prescription_Input]	https://gematik.de/fhir/erp-eu/StructureDefinition/GEM_ERPEU_PR_PAR_GET_Prescription_Input
[GEM_ERPEU_PR_PAR_CloseOperation_Input]	https://gematik.de/fhir/erp-eu/StructureDefinition/GEM_ERPEU_PR_PAR_CloseOperation_Input
[gemGlossar]	gematik: Einführung der Gesundheitskarte - Glossar
[gematik_IDP-Dienst_Registrierung_Clientsysteme]	https://wiki.gematik.de/display/IDPKB/IDP-Dienst+und+Clientsysteme#IDPDienstundClientsysteme-Registrierung,%C3%84nderungundAbmeldungvonClientsystemen
[gemILF_PS_eRp]	gematik: Implementierungsleitfaden Primärsysteme - E-Rezept
[gemKPT_Betr]	gematik: Betriebskonzept Online-Produktivbetrieb
[gemKPT_ePAfuerAlle]	gematik: Grobkonzept ePA für alle
[gemKpt_Test]	gematik: Testkonzept der TI
[gemProdT_NCPeH_FD]	gematik: Produkttypsteckbrief - Fachdienst National Contact Point for eHealth
[gemRL_Betr_TI]	gematik: Übergreifende Richtlinien zum Betrieb der TI
[gemSpec_Aktensystem_ePAfuerAlle]	gematik: Spezifikation Aktensystem ePA für alle
[gemSpec_DM_eRp]	gematik: Spezifikation Datenmodell E-Rezept
[gemSpec_DS_Anbieter]	gematik: Spezifikation Datenschutz- und Sicherheitsanforderungen der TI an Anbieter
[gemSpec_FD_eRp]	gematik: Spezifikation E-Rezept-Fachdienst
[gemSpec_IDP_Dienst]	gematik: Spezifikation Identity Provider-Dienst
[gemSpec_Krypt]	gematik: Übergreifende Spezifikation Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur
[gemSpec_Net]	gematik: Übergreifende Spezifikation Netzwerk
[gemSpec_OID]	gematik: Spezifikation Festlegung von OIDs

[gemSpec_Perf]	gematik: Übergreifende Spezifikation Performance und Mengengerüst TI-Plattform
[gemSpec_PKI]	gematik: Übergreifende Spezifikation - Spezifikation PKI
[gemSpec_PK_eGK]	gematik: Spezifikation für Prüfkarten des Typs eGK
[gemSpec_Systemprozesse_dezTI]	gematik: Spezifikation der Systemprozesse der dezentralen TI
[gemTestTriggerNCPeH]	<p>gematik: Schnittstelle zum Triggern von eHDSI-Anwendungsfällen für den NCPeH-FD https://github.com/gematik/NCPeH-Simulation-API/tree/main und mit einem Release-Tag zum passenden Spezifikations-Release versehen. Die Datei YAML-Datei zur OpenAPI Spezifikation ist in einer ZIP-Datei zu finden im entsprechenden Release-Pfad unter https://repo1.maven.org/maven2/de/gematik/api/ncpeh-simulation-td-api/</p>
[gemTigerProxy]	gematik: https://github.com/gematik/app-Tiger
[gemWebShop]	https://fachportal.gematik.de/gematik-onlineshop/pruefkarte-egk-fuer-dvo?ai%5Baction%5D=detail&ai%5Bcontroller%5D=Catalog&ai%5Bd_name%5D=Pruefkarten-eGK&ai%5Bd_pos%5D=0
[github-Link-TLS]	https://github.com/gematik/epa4all-examples Path: /src/main/java/de/gematik/epa4all/tls/TLSExample.java
[github-Link-VAU]	https://github.com/gematik/epa4all-examples Path: /src/main/java/de/gematik/epa4all/tls/VAUExample.java
[I_Authorization_Service]	gematik: I_Authorization_Service REST-Schnittstelle zur Nutzerauthentifizierung GitHub: https://github.com/gematik/ePA-Basic Path: src/openapi/I_Authorization_Service.yaml
[I_Information_Service]	Schnittstellenspezifikation Information Service GitHub: https://github.com/gematik/ePA-Basic Path: src/openapi/I_Information_Service.yaml
[Schema_ePA_XDSDocument Service]	GitHub: https://github.com/gematik/ePA-XDS-Document.git Path: src/schema

8.5.2 Weitere Dokumente

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[Abstract_Metadata_for_Document_Sharing_profiles]	https://profiles.ihe.net/ITI/TF/Volume3/ch-4.1.html
[Anlage-1_Prüfziffernberechnung_KVNR]	Prüfziffernberechnung für die Krankenversichertennummer nach § 290 SGB V https://www.gkv-datenaustausch.de/media/dokumente/kvnr/Anlage_1_20230102_Pruefziffernberechnung-KVNR.pdf
[BDX-smp-v1.0]	http://docs.oasis-open.org/bdxr/bdx-smp/v1.0/cs01/bdx-smp-v1.0-cs01.html
[CAB Forum]	Certification Authority Browser Forum - https://cabforum.org/
[DIMDI_HCID_NCPeH]	https://portal.dimdi.de/websearch/servlet/Gate?accessid=showOidDoc&query=oid=1.2.276.0.76.4.291
[ebRIM_Representation_Document]	https://profiles.ihe.net/ITI/TF/Volume3/ch-4.2.html
[ebRIM_Representation_DocumentEntry]	https://profiles.ihe.net/ITI/TF/Volume3/ch-4.2.html#4.2.1.1
[eHDSI_Audit_Trail_Profile]	https://webgate.ec.europa.eu/fpfis/wikis/display/EHDSI/Audit+Trail+Profile
[eHDSI_Certificates_Procedure_Request]	https://webgate.ec.europa.eu/fpfis/wikis/display/EHDSI/Certificates+Procedure+Request
[eHDSI_CDA_Format]	https://art-decor.ehdsi.eu/html/publication/epSOS/
[eHDSI_CTS]	https://webgate.ec.europa.eu/fpfis/wikis/display/EHDSI/Central+Terminology+Services+Specification
[eHDSI_CTS_API]	https://webgate.training.ec.europa.eu/ehealth-term-server/swagger-ui.html
[eHDSI_CTS2.0_USER_GUIDE]	https://webgate.ec.europa.eu/fpfis/wikis/display/EHDSI/CTS+v2.0+-+User+Guide
[eHDSI_Interoperability_Specification]	https://webgate.ec.europa.eu/fpfis/wikis/display/EHDSI/Interoperability+Specifications
[eHDSI_Messaging_Profile]	https://webgate.ec.europa.eu/fpfis/wikis/display/EHDSI/Messaging+Profile

[eHDSI_MVC]	https://webgate.ec.europa.eu/fpfis/wikis/pages/viewpage.action?pagelId=912786418
[eHDSI_Operations_Framework]	https://webgate.ec.europa.eu/fpfis/wikis/display/EHDSI/6.+eHDSI+Operations+Framework
[eHDSI_NCPeH_Architecture_Specification]	https://webgate.ec.europa.eu/fpfis/wikis/display/EHDSI/NCPeH+Architecture+Specifications
[eHDSI_NCPeH_Components]	https://webgate.ec.europa.eu/fpfis/wikis/display/EHDSI/NCPeH+Components+Specifications
[eHDSI_NCPeH_Configuration_Production_Environment]	https://webgate.ec.europa.eu/fpfis/wikis/pages/viewpage.action?pagelId=888405252
[eHDSI_Requirements_Catalogue]	https://webgate.ec.europa.eu/fpfis/wikis/display/EHDSI/1.+MyHealth@EU+Requirements+Catalogue
[eHDSI_Service_Location_and_Capability_Lookup_Profile]	https://webgate.ec.europa.eu/fpfis/wikis/display/EHDSI/Service+Location+and+Capability+Lookup+Profile
[eHDSI_SAML_Profile]	https://webgate.ec.europa.eu/fpfis/wikis/display/EHDSI/SAML+Profile
[eHDSI_System_Architecture_Specifications]	https://webgate.ec.europa.eu/fpfis/wikis/display/EHDSI/System+Architecture+Specifications
[eHDSI_X.509_Certificates_Profile]	https://webgate.ec.europa.eu/fpfis/wikis/display/EHDSI/X.509+Certificates+Profile
[eHDSI_XCA_Profile]	https://webgate.ec.europa.eu/fpfis/wikis/display/EHDSI/XCA+Profile
[eHDSI_XCPD_Profile]	https://webgate.ec.europa.eu/fpfis/wikis/display/EHDSI/XCPD+Profile
[eHDSI_XDR_Profile]	https://webgate.ec.europa.eu/fpfis/wikis/display/EHDSI/XDR+Profile
[eHDSI_Monitoring_Framework]	https://webgate.ec.europa.eu/fpfis/wikis/pages/viewpage.action?pagelId=888405123
[eHDSI_Specifications]	https://webgate.ec.europa.eu/fpfis/wikis/display/EHDSI/2.+MyHealth@EU+Interoperability+Specifications%2C+Requirements+and+Frameworks
[eHDSI_Starting_Toolkit]	https://webgate.ec.europa.eu/fpfis/wikis/display/EHDSI/MyHealth@EU+STARTING+TOOLKIT

[eHDSI_Security_Services_Specification]	https://webgate.ec.europa.eu/fpfis/wikis/display/EHDSI/Security+Services+Specification
[eHDSI Test Services]	https://webgate.ec.europa.eu/fpfis/wikis/pages/viewpage.action?spaceKey=EHDSI&title=3.+eHDSI+TEST+SERVICES
[eHDSI Test Framework]	https://webgate.ec.europa.eu/fpfis/wikis/display/EHDSI/eHDSI+TEST+FRAMEWORK
[eHDSI Testing Platform]	https://gazelle.ehdsi.eu/
[eHDSI Test Dokumentation und Guidelines]	https://webgate.ec.europa.eu/fpfis/wikis/display/EHDSI/eHDSI+TEST+DOCUMENTATION+and+GUIDELINES
[eHDSI Testdaten]	https://webgate.ec.europa.eu/fpfis/wikis/display/EHDSI/eHDSI+Test+Data
[eHDSI Compliance Check Services]	https://webgate.ec.europa.eu/fpfis/wikis/display/EHDSI/4.+MyHealth@EU+Compliance+Checks+Services
[eHDSI Compliance Check Framework]	https://webgate.ec.europa.eu/fpfis/wikis/display/EHDSI/4.+MyHealth@EU+Compliance+Checks+Services
[Exception Handling in MyHealth@EU]	https://webgate.ec.europa.eu/fpfis/wikis/x/HlfdPw
[ETSI_REM]	https://www.etsi.org/deliver/etsi_ts/102600_102699/10264002/02.02.01_60/ts_10264002v020201p.pdf ETSI TS 102 640-2 v2.2.1, 2011 Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM); Part 2: Data requirements, Formats and Signatures for REM
[FHIR_Resource_Bundle]	https://build.fhir.org/bundle.html
[HL7_ValueSet_XDS]	https://wiki.hl7.de/index.php?title=IG:Value_Sets_f%C3%BCr_XDS
[IHE_ITI_TF]	IHE International (2018): IHE IT Infrastructure (ITI) Technical Framework, Revision 15.0
[IHE_ITI_TF_Vol3]	https://profiles.ihe.net/ITI/TF/Volume3/index.html
[IHE-ITI-TF2x]	https://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Rev15-1_Vol2x_FT_2018-10-18.pdf
[ITI-18]	https://profiles.ihe.net/ITI/TF/Volume2/ITI-18.html

[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-41]	https://profiles.ihe.net/ITI/TF/Volume2/ITI-41.html
[ITI-43]	https://profiles.ihe.net/ITI/TF/Volume2/ITI-43.html
[ITI-55]	https://profiles.ihe.net/ITI/TF/Volume2/ITI-55.html
[JWS_ECDSA]	https://openid.net/specs/draft-jones-json-web-signature-04.html#DefiningECDSA
[KBV_PR_ERP_Bundle]	https://simplifier.net/erezept/kbv_pr_erp_bundle
[KBV_PR_ERP_Medicatio n_Compounding]	https://simplifier.net/erezept/kbvprerppreparationcompounding
KBV_PR_ERP_Medicatio n_PZN	https://simplifier.net/erezept/kbvprerppreparationpzn
[KBV_PR_ERP_Prescriptio n]	https://simplifier.net/erezept/kbvprerpprescription
[KBV_PR_FOR_Organizati on]	https://fhir.kbv.de/StructureDefinition/KBV_PR_FOR_Organization
[KBV_PR_FOR_Patient]	https://fhir.kbv.de/StructureDefinition/KBV_PR_FOR_Patient
[KBV_PR_FOR_Practition er]	https://simplifier.net/packages/kbv.ita.for/1.1.0/files/720095
[LOINC_Patient_Summar y]	https://loinc.org/60591-5/
[LOINC_ePrescription]	https://loinc.org/57833-6/
[LVZ]	https://www.auswaertiges-amt.de/blob/215256/e13a148b838b0734f6fca63b15029c9f/laenderverzeichnis-data.pdf
[MyHealth@EU_Scope_a nd_Business_Goals]	https://webgate.ec.europa.eu/fpfis/wikis/display/EHDSI/MyHealth@EU+Scope+and+Business+Goals
[MTOM]	W3C (2005): SOAP Message Transmission Optimization Mechanism, https://www.w3.org/TR/soap12-mtom/
[OASIS_WS-Security]	http://docs.oasis-open.org/wss-m/wss/v1.1.1/os/wss-SOAPMessageSecurity-v1.1.1-os.html
[OIDC_CORE_IDToken]	https://openid.net/specs/openid-connect-core

	1_0.html#IDToken
[openid-connect-core]	OpenID Connect Core 1.0 incorporating errata set 2 https://openid.net/specs/openid-connect-core-1_0.html
[RFC5280]	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile https://datatracker.ietf.org/doc/html/rfc5280
[RFC6749]	The OAuth 2.0 Authorization Framework https://datatracker.ietf.org/doc/html/rfc6749
[RFC6960]	RFC 6960 (Juni 2013): X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP https://tools.ietf.org/html/rfc6960
[RFC7515]	JSON Web Signature (JWS) https://datatracker.ietf.org/doc/html/rfc7515
[RFC7517]	https://www.rfc-editor.org/rfc/rfc7517
[RFC7519]	https://datatracker.ietf.org/doc/html/rfc7519
[RFC7591#Section-2]	https://tools.ietf.org/html/rfc7519#section-2
[RFC7636]	Proof Key for Code Exchange by OAuth Public Clients https://datatracker.ietf.org/doc/html/rfc7636
[RFC8414]	OAuth 2.0 Authorization Server Metadata https://datatracker.ietf.org/doc/html/rfc8414
[RFC8693]	https://datatracker.ietf.org/doc/html/rfc8693
[Simplifier_ePKA_MIO]	https://simplifier.net/packages/kbv.mio.patientenkurzakte/1.0.0/
[Simplifier_ePKA_MIO_NFD_Patient]	https://simplifier.net/packages/kbv.mio.patientenkurzakte/1.0.0/files/611117
[Simplifier_ePKA_MIO_Validierungspakete]	https://github.com/mio42-GmbH/Validierungspaket-MIO-Patientenkurzakte
[SMP_SML_eDelivery_BB]	https://ec.europa.eu/digital-building-blocks/wikis/display/DIGITAL/SML+software?preview=/467118037/525042773/(eDelivery)(SML%2BSMP)(COD)(1.20).pdf
[SOGIS-IS-2020]	https://www.sogis.eu/documents/cc/crypto/SOGIS-Agreed-Cryptographic-Mechanisms-1.2.pdf
[KBV_ePKA_MIO_Format]	https://mio.kbv.de/display/PKA1X0X0/

	Patientenkurzakte+1.0.0
[KBV_ITA_VGEX_Technische_Anlage_ERP]	KBV: TECHNISCHE ANLAGE ZUR ELEKTRONISCHEN ARZNEIMITTELVORORDNUNG (E16A)
[TA7_Anhang2]	Anhang 2 - FHIR Versionen zur Technischen Anlage 7 zur Arzneimittelabrechnungsvereinbarung gemäß § 300 Absatz 3 SGB V
[WSS-SAML]	OASIS (2006): Web Services Security: SAML Token Profile 1.1, https://www.oasis-open.org/committees/download.php/16768/wss-v1.1-spec-os-SAMLSecurityProfile.pdf
[X.509]	ITU-T X.509 (10/2019): SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY, Directory, Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks http://www.itu.int/rec/T-REC-X.509/